

Technical safety

This NORSOK standard is developed with broad petroleum industry participation by interested parties in the Norwegian petroleum industry and is owned by the Norwegian petroleum industry represented by The Norwegian Oil Industry Association (OLF) and The Federation of Norwegian Industry. Please note that whilst every effort has been made to ensure the accuracy of this NORSOK standard, neither OLF nor The Federation of Norwegian Industry or any of their members will assume liability for any use thereof. Standards Norway is responsible for the administration and publication of this NORSOK standard.

Standards Norway
Strandveien 18, P.O. Box 242
N-1326 Lysaker
NORWAY

Copyrights reserved

Telephone: + 47 67 83 86 00
Fax: + 47 67 83 86 01
Email: petroleum@standard.no
Website: www.standard.no/petroleum



Documents
Document Sharing Hub

Foreword	6
Introduction	6
1 Scope	7
2 Normative and informative references	7
2.1 Normative references	7
2.2 Informative references	8
3 Terms, definitions and abbreviations	8
3.1 Terms and definitions	8
3.2 Abbreviations	10
4 Management of technical safety	11
4.1 General	11
4.2 Risk reduction principles – inherent safety design	12
4.3 Safety performance standards	12
4.4 Qualification of technology	12
4.5 Experience transfer	13
4.6 Integrity – availability and reliability	13
4.7 Dimensioning accidental load (DAL)	13
4.8 Documentation	14
5 Layout	14
5.1 Role	14
5.2 Interfaces	14
5.3 Required utilities	15
5.4 Functional requirements	15
5.5 Survivability requirements	17
6 Structural integrity	17
6.1 Role	17
6.2 Interfaces	17
6.3 Required utilities	17
6.4 Functional requirements	17
6.5 Survivability requirements	17
7 Containment	18
7.1 Role	18
7.2 Interfaces	18
7.3 Required utilities	18
7.4 Functional requirements	18
7.5 Survivability requirements	18
8 Open drain	18
8.1 Role	18
8.2 Interfaces	18
8.3 Required utilities	18
8.4 Functional requirements	19
8.5 Survivability requirements	19
9 Process safety	19
9.1 Role	19
9.2 Interfaces	19
9.3 Required utilities	19
9.4 Functional requirements	19
9.5 Survivability requirements	20
10 Emergency shut down (ESD)	20
10.1 Role	20
10.2 Interfaces	20
10.3 Required utilities	21
10.4 Functional requirements	21
10.5 Survivability requirements	24

11	Blow down (BD) and flare/vent system	25
11.1	Role	25
11.2	Interfaces	25
11.3	Required utilities	25
11.4	Functional requirements	25
11.5	Survivability requirements	26
12	Gas detection	26
12.1	Role	26
12.2	Interfaces	27
12.3	Required utilities	27
12.4	Functional requirements	27
12.5	Survivability requirements	33
13	Fire detection	33
13.1	Role	33
13.2	Interfaces	33
13.3	Required utilities	33
13.4	Functional requirements	34
13.5	Survivability requirements	40
14	Ignition source control (ISC)	40
14.1	Role	40
14.2	Interfaces	41
14.3	Required utilities	41
14.4	Functional requirements	41
14.5	Survivability requirements	43
15	Human – machine interface (HMI)	44
15.1	Role	44
15.2	Interfaces	44
15.3	Functional requirements	44
15.4	Survivability requirements	45
16	Natural ventilation and heating, ventilation and air conditioning (HVAC)	45
16.1	Role	45
16.2	Interfaces	46
16.3	Required utilities	46
16.4	Functional requirements	46
16.5	Survivability requirements	47
17	Public address (PA), alarm and emergency communication	48
17.1	Role	48
17.2	Interfaces	48
17.3	Required utilities	48
17.4	Functional requirements	48
17.5	Survivability requirements	50
18	Emergency power and lighting	50
18.1	Role	50
18.2	Interfaces	50
18.3	Required utilities	50
18.4	Functional requirements	50
18.5	Survivability requirements	52
19	Passive fire protection (PFP)	52
19.1	Role	52
19.2	Interfaces	52
19.3	Required utilities	52
19.4	Functional requirements	52
19.5	Survivability requirements	54
20	Fire fighting systems	54
20.1	Role	54
20.2	Interfaces	54
20.3	Required utilities	55

20.4	Functional requirements	55
20.5	Survivability requirements	61
21	Escape and evacuation	62
21.1	Role	62
21.2	Interfaces	62
21.3	Required utilities	62
21.4	Functional requirements	62
21.5	Survivability requirements	64
22	Rescue and safety equipment	65
22.1	Role	65
22.2	Interfaces	65
22.3	Required utilities	65
22.4	Functional requirements	65
22.5	Survivability requirements	67
23	Marine systems and position keeping	67
23.1	Role	67
23.2	Interfaces	67
23.3	Required utilities	67
23.4	Functional requirements	67
23.5	Survivability requirements	68
24	Ship collision barrier	68
24.1	Role	68
24.2	Interfaces	68
24.3	Required utilities	68
24.4	Functional requirements	68
24.5	Survivability requirements	69
Annex A (Informative) Fire protection data sheet		70

Foreword

The NORSOK standards are developed by the Norwegian petroleum industry to ensure adequate safety, value adding and cost effectiveness for petroleum industry developments and operations. Furthermore, NORSOK standards are, as far as possible, intended to replace oil company specifications and serve as references in the authorities' regulations.

The NORSOK standards are normally based on recognised international standards, adding the provisions deemed necessary to fill the broad needs of the Norwegian petroleum industry. Where relevant, NORSOK standards will be used to provide the Norwegian industry input to the international standardisation process. Subject to development and publication of international standards, the relevant NORSOK standard will be withdrawn.

The NORSOK standards are developed according to the consensus principle generally applicable for most standards work and according to established procedures defined in NORSOK A-001.

The NORSOK standards are prepared and published with support by The Norwegian Oil Industry Association (OLF), The Federation of Norwegian Industry, Norwegian Shipowners' Association and The Petroleum Safety Authority Norway.

NORSOK standards are administered and published by Standards Norway.

Annex A is informative.

Introduction

This NORSOK standard is organised according to principles given in clause 4. Each clause of this NORSOK standard describes requirements for the individual safety barriers/-systems, and represents a generic performance standard for the different safety barriers. The following elements have been addressed for each safety barrier/-system:

- role gives a short description of the safety aspects related to the specific safety systems and barriers;
- interfaces lists the interface with other safety systems and barriers;
- required utilities describes utilities required for the safety system and barriers to fulfil its role;
- functional requirements specifies the performance required for the safety system and barriers to fulfil its role;
- survivability requirements defines requirements for the safety systems and barriers to function in or after a dimensioning accidental event.

1 Scope

This NORSOK standard describes the principles and requirements for the development of the safety design of offshore installations for production of oil and gas. Where applicable, this NORSOK standard may also be used for mobile offshore drilling units.

This NORSOK standard, together with ISO 13702, defines the required standard for implementation of technologies and emergency preparedness to establish and maintain an adequate level of safety for personnel, environment and material assets.

2 Normative and informative references

The following standards include provisions and guidelines which, through reference in this text, constitute provisions and guidelines of this NORSOK standard. Latest issue of the references shall be used unless otherwise agreed. Other recognized standards may be used provided it can be shown that they meet the requirements of the referenced standards.

2.1 Normative references

API RP 14C,	Recommended Practice for Analysis, Design, Installation, and Testing of Basic Surface Safety Systems for Offshore Production Platforms
API RP 521,	Guide for Pressure-Relieving and Depressurizing Systems
Directive 94/9/EC,	Concerning equipment and protective systems intended for use in potentially explosive atmospheres (ATEX "Product")
CENELEC CLC/TR 50427,	Assessment of inadvertent ignition of flammable atmospheres by radio-frequency radiation
EN 1838,	Lighting applications – Emergency lighting
EN 13463 – (all parts),	Non-electrical equipment intended for use in potentially explosive atmospheres
IMO Res.A.653,	Flame spread, surface materials and floorings
ISO 5660 – (all parts),	Reaction-to-fire tests – Heat release, smoke production and mass loss rate
ISO 10418,	Petroleum and natural gas industries – Offshore production installations – Basic surface process safety systems
ISO 13702,	Petroleum and natural gas industries – Control and mitigation of fires and explosions on offshore production installations – Requirements and guidelines
IEC/TR 60079-13,	Electrical apparatus for explosive gas atmospheres – Part 13: Construction and use of rooms or buildings protected by pressurization
IEC 60331– (all parts),	Tests for electric cables under fire conditions – Circuit integrity
IEC 60332– (all parts),	Tests on electric and optical fibre cables under fire conditions
IEC 61508 – (all parts),	Functional safety of electrical/electronic/programmable electronic safety-related systems
IEC 61511– (all parts),	Functional safety – Safety instrumented systems for the process industry sector
IEC 61892-7,	Mobile and fixed offshore units – Electrical installations – Part 7: Hazardous areas
IP 15,	Area Classification code for installations handling flammable fluids
ISO 23251,	Petroleum, petrochemical and natural gas industries – Pressure-relieving and depressurizing systems
OLF Guideline No. 070,	Guidelines for the Application of IEC 61508 and IEC 61511 in the petroleum activities on the continental shelf
OLF Retningslinjer Nr. 075,	Anbefalte retningslinjer for vannbaserte brannbekjempelsessystemer
MODU Code,	Code for the construction and equipment of mobile offshore drilling units, 2003 Consolidated edition (2001 MODU Code)
NFPA 20,	Standard for the Installation of Stationary Fire Pumps for Fire Protection Spray Systems
NMD Regulation No.123,	Regulation for mobile offshore units with production plants and equipment
NMD Regulation No.492,	Regulation 11 April 2003 No.492 concerning lifesaving appliances and evacuation on mobile offshore units
NMD Regulation No.879,	Regulation concerning ballast systems on mobile offshore units
NORSOK C-001,	Living quarters area

NORSOK C-002,	Architectural components and equipment
NORSOK D-001,	Drilling facilities
NORSOK H-001,	HVAC (Heating, ventilation and air conditioning)
NORSOK L-001,	Piping and Valves
NORSOK L-002,	Piping design, layout and stress analysis
NORSOK M-501,	Surface preparation and protective coating
NORSOK N-001,	Structural design
NORSOK N-003,	Actions and action effects
NORSOK P-001,	Process Design
NORSOK P-100,	Process systems
NORSOK Z-013,	Risk and emergency preparedness analysis
SOLAS requirements	

2.2 Informative references

DNV-RP-A203,	Qualification Procedures for New Technology
Guidelines for protection of pressurised systems exposed to fire, Report 27.101.166/R1 Scandpower Risk Management AS	
ISO 17776,	Petroleum and natural gas industries – Offshore production installations – Guidelines on tools and techniques for hazard identification and risk assessment
NFPA 13,	Installation of Sprinkler Systems
NFPA 14,	Standard for the Installation of Standpipe and Hose Systems
NFPA 15,	Standard for Water Spray Fixed Systems for Fire Protection
NFPA 16,	Standard for the Installation of Foam-Water Sprinkler and Foam-Water Spray Systems
NFPA 750,	Standard on Water Mist Fire Protection Systems
NMD Regulations No.857,	Regulation concerning anchoring/positioning systems on mobile offshore units
NORSOK L-005,	Compact flanged connections
SINTEF NBL report A05103,	Branntekniske krav til materialer i boligkvarter offshore
YA 711,	Principles for alarm system design (Petroleum Safety Authority publication)

3 Terms, definitions and abbreviations

For the purposes of this NORSOK standard, the following terms, definitions and abbreviations apply.

3.1 Terms and definitions

3.1.1

area classification

division of an installation into hazardous areas and non-hazardous areas and the sub-division of hazardous zones

3.1.2

can

verbal form used for statements of possibility and capability, whether material, physical or casual

3.1.3

dimensioning accidental load (DAL)

most severe accidental load that the function or system shall be able to withstand during a required period of time, in order to meet the defined risk acceptance criteria

3.1.4

emergency lighting

lighting which will ensure adequate light conditions on the installation in the event of failure of the main power supply

3.1.5

explosion load

time dependent pressure or drag forces generated by violent combustion of a flammable atmosphere

3.1.6**fire area**

area separated from other areas either by physical barriers (fire/blast partition) or distance which will prevent dimensioning fire to spread

3.1.7**fire detection area**

area, or areas, of similar environmental conditions and hazards, and with similar detection and protection arrangements defined for the purpose of grouping areas or rooms into similar F&G logic

3.1.8**fire load**

heat load from a fire for a specified time period

3.1.9**firewater (FW) pump system**

total system, which supplies water for fire fighting system, i.e. water inlets with filters, FW pumps, risers, power sources, power transmissions, fuel pipes/tanks and control systems

3.1.10**hazardous area**

three-dimensional space in which a flammable atmosphere may be expected to be present at such frequencies as to require special precautions for the control of potential ignition sources

3.1.11**ignition source groups**

non-essential equipment, Group 1, is equipment not affecting production availability or safety integrity

NOTE Non-essential equipment may include equipment such as non-Ex lighting, heat tracing, welding socket outlets, electrical outlets for hand tools, air operated tools and other hot work activities.

essential equipment, Group 2, is equipment that shall be kept alive to maintain production or drilling operations

NOTE Affected equipment may include main power generator, main electrical distribution panels, all electrical consumers not required during ESD1, diesel engines, heaters, boilers, ventilation systems unless defined as a safety critical item.

safety critical equipment, Group 3, is equipment that shall be in operation to ensure escape, evacuation and/or to prevent escalation

3.1.12**intermittently manned**

work area or work place where inspection, maintenance or other work is planned to last at least 2 h, but less than 8 h a day for at least 50 % of the installation's operation time

3.1.13**may**

verbal form used to indicate a course of action permissible within the limits of this NORSOK standard

3.1.14**muster area**

area where mustering shall take place in the event of general and/or evacuation alarm

3.1.15**non-hazardous area**

area in which an explosive gas atmosphere is not expected to be present in quantities such as to require special precautions for the construction, installation and use of electrical apparatus and equipment in "normal operation"

NOTE Normal operation is a situation when the plant is operating within its design parameters. Minor releases of flammable material may be part of normal operation. For example, releases from seals that rely on wetting by the fluid being pumped are considered to be minor releases. Failures (such as breakdown of pump seals, flange gaskets or spillage caused by accidents) that involve repair or shut down are not considered to be part of normal operation, and may require special precautions of potential ignition sources.

3.1.16**normally not manned**

work area or work place that is not permanently or intermittently manned

3.1.17**safety function**

physical measures which reduce the probability of a situation of hazard and accident occurring, or which limit the consequences of an accident

3.1.18**shall**

verbal form used to indicate requirements strictly to be followed in order to conform to this NORSOK standard and from which no deviation is permitted, unless accepted by all involved parties

3.1.19**should**

verbal form used to indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred, but not necessarily required

3.1.20**temporary refuge**

place provided where personnel can take refuge for a pre-determined period whilst investigations, emergency response and evacuation pre-planning are undertaken

3.2**Abbreviations**

AC/h	air changes per hour
AFP	active fire protection
API	American Petroleum Institute
APS	abandon platform shut down
ATEX	EU Directive covering "Equipment Intended for Use in Potentially Explosive Atmosphere"
BD	blow down
BOP	blow out preventer
C&E	cause and effect
CAP	critical action panel
CCR	central control room
CENELEC	European Committee for Electrotechnical Standardization
DAL	dimensioning accidental load
DHSV	down hole safety valve
DIFFS	deck integrated fire fighting system
EERS	evacuation, escape and rescue strategy
EN	European Standard
ESD	emergency shut down
F&G	fire and gas
FES	fire and explosion strategy
FPDS	fire protection data sheet
FPSO	floating production, storage and offloading
FW	firewater
GA	general alarm
HC	hydro carbon
HMI	human-machine interface
HVAC	heating, ventilation and air conditioning
IEC	International Electrotechnical Commission
IMO	International Maritime Organisation
IP	Institute of Petroleum
ISC	ignition source control
ISO	International Organization for Standardization
IR	infrared
LAHH	level alarm high high (trip level)
LEL	lower explosion limit
LELm	lower explosion limit meters

LER	local equipment room
LIR	local instrument room
LQ	living quarter
MOB	man over board
MODU	mobile offshore drilling unit
NA	not applicable
NFPA	National Fire Protection Association
NMD	Norwegian Maritime Directorate
NNMI	normally not manned installations
OLF	Oljeindustriens Landsforening
PA	public address
PFP	passive fire protection
PSD	process shut down
PSV	pressure safety valve
RAL	Deutsches Institut für Gutesicherung und Kennzeichnung
SAS	safety and automation system
SINTEF NBL	Norwegian Fire Research Laboratory
SOLAS	International Convention for the Safety of Life at Sea
SSIV	subsea isolation valve
UHF	ultra high frequency
VDU	visual display unit
VHF	very high frequency
UPS	uninterruptible power supply

4 Management of technical safety

4.1 General

Technical safety management in project development and design processes comprises activities to identify risks, develop safety strategies and performance requirements for safety systems and barriers. Technical safety management shall also facilitate the design process to ensure that studies, analysis and reviews are performed in due time and properly documented with due consideration of the needs for timely input to design and procurement processes.

For modification projects (e.g. upgrading of existing installation/module, tie-in of satellite field), technical safety management activities adjusted to project scope and complexity shall be performed, including new analyses or updating of existing analyses for factors that are considered to be affected by the modification.

A follow-up system shall be established that enables proper documentation, handling, follow-up and closeout of agreed actions and recommendations from the various studies and analyses in the project.

The individual project or installation shall perform specific hazard identification and risk evaluation process, and supplement the requirements as necessary to manage the actual risk picture.

A flow diagram describing some of the main activities related to technical safety design is shown in Figure 1.

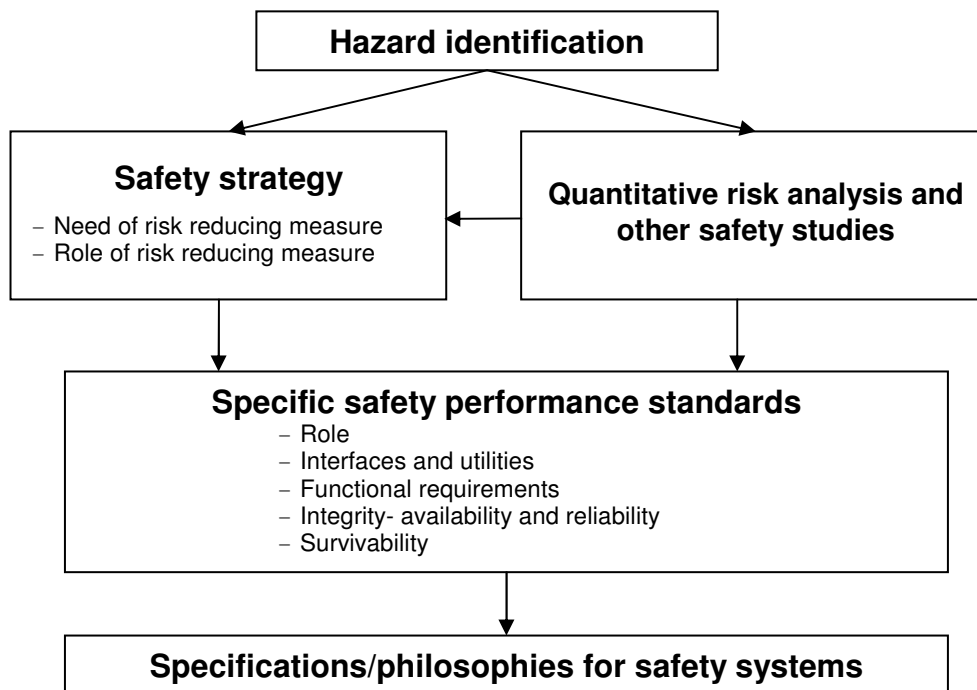


Figure 1 - Technical safety design

4.2 Risk reduction principles – inherent safety design

In concept optimisation and design development, priority shall always be given to use of preventive measures/exposure barriers and inherently safer design principles. The objectives with risk reduction principles and inherent safety design are to

- reduce potential hazards,
- reduce probability of unwanted events,
- reduce inventory and damage potential,
- strive for simplicity and reliability,
- prevent escalation, e.g. by safety barriers.

4.3 Safety performance standards

Safety performance standard shall be the verifiable standard to which safety system elements are to perform. The objective of the specific safety performance standards is to add any supplemental safety requirements other than those specified by authority requirements and standards.

The performance standards shall be based on the safety strategy document(s) and these should be read in conjunction with each other.

The specific safety performance standards shall ensure that barriers, safety systems or safety functions

- are suitable and fully effective for the type hazards identified,
- have sufficient capacity for the duration of the hazard or the required time to provide evacuation of the installation,
- have sufficient availability to match the frequency of the initiating event,
- have adequate response time to fulfil its role,
- are suitable for all operating conditions.

4.4 Qualification of technology

New technology is defined as systems or components for which an acceptable reliability is not demonstrated by a documented track record for the particular application. New technology shall be qualified following a systematic approach, such as laid down in DNV-RP-A203 or similar guideline, in order to demonstrate that it meets specified functional requirements and reliability targets.

4.5 Experience transfer

To ensure transfer of technical safety experience from relevant installations in operation, an experience transfer activity prior to start of detail engineering should be carried out. Sources of experience should include

- operational experience of relevant installations,
- project execution of relevant installations and modification to these,
- good technical solutions,
- solutions/equipment to be avoided.

4.6 Integrity – availability and reliability

The minimum requirements to availability and reliability for safety functions/systems shall be determined based on IEC 61508 or IEC 61511 or other specific safety analysis/risk assessments as relevant for the safety function in question.

All relevant safety function/systems shall be subject to testing at regular intervals. Test intervals should be determined based on relevant standards, criticality analysis and experience. For instrumented safety systems, see OLF Guideline No. 070.

The design of safety functions/systems shall, where practical, allow for required testing to be carried out without interrupting production or operations.

The applicable safety system or affected parts of it shall go to a predefined safe state in the event of detectable malfunction.

If not fail-safe, the same level of safety shall be achieved by redundancy, diagnostics and alarm to control room. Single faults/errors should not prohibit actions on demand.

4.7 Dimensioning accidental load (DAL)

DALs shall be established based on quantitative risk analysis and the comparison of estimated risk with risk acceptance and/or design criteria. Dimensioning loads shall be revised upon modifications, e.g. layout, equipment density and natural ventilation conditions.

Dimensioning load shall not cause loss of safety functions or escalation (locally). The following principles shall apply:

- dimensioning explosion loads shall be established using a recognised method (e.g. NORSOK Z-013) and a representative geometric explosion model. The loads shall be defined for relevant local horizontal and vertical area dividers (pressure and impulse from explosion) and equipment (pressure/drag forces);
- explosion loads shall also be defined for areas external to the initial explosion location (typical LQ, utility modules etc.);
- fire loads, (e.g. heat loads). Unless specific fire analysis is performed, Table 1 applies;
- ship collisions (e.g. impact loads to be absorbed by installation structure), see NORSOK Z-013 and NORSOK N-001;
- falling loads and dropped objects (e.g. impact loads to be absorbed by installation structure), see NORSOK Z-013.

Table 1 - Heat flux values

	Jet fire		Pool fire kW/m ²
	For leak rates m > 2 kg/s kW/m ²	For leak rates 0,1 kg/s < m < 2 kg/s kW/m ²	
Local peak heat load	350	250	150
Global average heat load	100	0	100

The effect of area deluge is not accounted for in Table 1. The effect of deluge may be taken into account for process piping/equipment (not for main structural elements and fire partitions) provided proper documentation is available on the effect of deluge as well as on the reliability of the FW supply system.

The global average heat load represents the average heat load that expose a significant part of the process segment or structure. The global average heat load provides the major part of the heat input to the process segment and, hence, affects the pressure in the segment.

The local peak heat load exposes a small (local) area of the process segment or of the structure to the peak heat flux. The local peak heat load, with the highest heat flux, determines the rupture temperature of different equipment and piping within the process segment. The local peak heat load has marginal influence on the pressure profile within the process segment.

An alternative approach to assessing the heat fluxes and the size of the fire is to base this on a probabilistic approach in combination with relevant acceptance criteria.

4.8 Documentation

The following technical safety documents should be developed during development of a new installation:

- hazard identification report, see ISO 17776;
- safety strategies and safety performance standards;
- specifications and philosophies for safety systems as required;
- FW report;
- dimensioning accidental load specification;
- safety analyses and evaluations, e.g.:
 - vulnerability analyses for safety systems;
 - sectionalisation of the process plant including categorization and location of safety critical valves;
 - reliability and availability;
 - fire load analyses;
 - explosion analyses;
 - dispersion analyses.
- FPDS/area safety charts/F&G C&E;
- safety arrangements drawings and diagrams as follows:
 - passive fire and blast protection;
 - area classification;
 - F&G detection layout;
 - escape routes, muster areas, evacuation means;
 - safety equipment plot plans;
 - fire fighting plot plans and process and instrument diagrams;
 - ESD C&E diagram (PSD C&E may be developed);
 - ESD hierarchy.

Safety interface documentation shall be produced where relevant in order to ensure that safety requirements are addressed and implemented in design development between different contractors and installations, e.g. subsea installation, storage units and fixed platforms.

5 Layout

5.1 Role

The layout of an installation shall reduce probability and the consequences of accidents through location, separation and orientation of areas, equipment and functions. The layout can amongst other contribute to

- minimize the possibility of hazardous accumulations and spread of both flammable liquids and gaseous hydrocarbon,
- minimize the probability of ignition,
- separate areas required to be non-hazardous from those designated as being hazardous,
- minimize the consequences of fire and explosions and thereby reduced escalation risk,
- facilitate effective emergency response,
- provide for adequate arrangements for escape and evacuation.

5.2 Interfaces

Layout has interfaces with all of the safety systems-/functions.

5.3 Required utilities

Layout is not dependent on any specific utility.

5.4 Functional requirements

5.4.1 Main design principles

The installation shall be oriented with respect to the dominant wind direction to minimize the likelihood of a gas release or smoke drifting towards the accommodation and primary evacuation means.

The installation shall be divided into main areas (accommodation, utility, drilling, wellhead, process and hydrocarbon storage). The main areas shall be located and designed to minimize the risk to people, environment and assets. Main areas shall normally be separated by use of physical barriers as fire and blast divisions to prevent the escalation of an accident from one main area to another.

The utility area should serve as a barrier between hazardous areas and LQ.

Temporary refuge, accommodation, evacuation means, escape routes and rescue facilities shall be located where they are least affected from fires and explosions.

Safety systems shall be located or protected to ensure operation during relevant emergency condition. Examples of relevant safety systems are FW pump units, emergency generator(s), UPS, ESD/PSD/F&G nodes, ballast system and position keeping system. As far as practical such systems shall be located in accommodation or utility area. CCR shall be located as safe as possible, normally in the accommodation area.

Doors from non-hazardous rooms facing directly towards hazardous areas should be avoided.

Non-hazardous rooms with doors or openings less than 3 m away from hazardous area should be avoided.

5.4.2 Riser flow line area

Hydrocarbon risers and conductors shall be designed and located or protected to minimize the likelihood of damage, including damage due to ship impact and dropped objects.

Pig launchers and receivers shall be located in open naturally ventilated areas at the periphery of the platform facing sea, and with hatches directed away from equipment and structures.

Topsides riser ESD valves should be located as low down the riser as practicable, so as to minimize the likelihood of damage below the ESD valves causing release of pipeline/riser inventories, see 10.5.

5.4.3 Process area

Fire and explosion evaluations shall be made along with the development of the layout to minimise the built in escalation potential. This shall be ensured through the following principles:

- equipment and piping containing high-pressure gas should be located in the upper decks above the module support frame or main hull;
- liquid vessels should be located lower than gas equipment;
- low-pressure equipment containing large amount of liquids should be located and arranged so that exposure to jet fires is minimised.

Process vessels, process piping, pig launchers and receivers and other hydrocarbon containing equipment shall be protected from external impact (e.g. from dropped objects or missiles due to disintegration of rotating machinery) or as found required through analysis.

5.4.4 Wellhead area

The wellheads should be located above the main support frame in order to reduce exposure of the main support frame from a wellhead fire.

The design of wellhead area shall be evaluated with respect to need for assistance from external fire fighting vessel.

5.4.5 Piping

Routing of piping containing hydrocarbon to or through the utility area shall be avoided except for fuel lines to utility systems. On FPSO crude lines to aft offloading systems are accepted provided they are located at the platform periphery and contain no leak sources.

Routing of hydrocarbon piping is not allowed in the LQ areas.

Routing of piping containing any liquid or hydrocarbon gas is not allowed through electrical room, instrument room and control room.

Routing of hydrocarbon piping within areas where emergency equipment is located shall be limited to diesel fuel supply lines for emergency equipment themselves.

5.4.6 Lifting and lay down

Crane coverage and lay down areas shall be arranged to promote safe crane operations with free visibility from crane cabin to minimise the risk of dropped objects. Considerations shall be given to sidewise movement of load.

Within defined lifting zones equipment, or piping, containing hydrocarbons, flammable or toxic gas/liquid shall be protected from dropped objects.

Lifting above high voltage equipment and cables shall be assessed, and protection shall be considered installed.

The lifting zones shall be defined and shown on the lifting map in crane cabin.

Crane software should give alarm in crane when lifting restriction boundaries are exceeded.

Allowable weight chart for laydown areas shall be established.

Laydown and storage area should not be located in hazardous area.

Storage of equipment shall be assessed regarding possible negative effects on technical barriers (e.g. F&G detection, FW system, natural ventilation), explosion risk and explosion relief (panels).

5.4.7 Storage and handling of explosives

Explosives shall be stored and handled such that the risk of fire or explosion is minimised.

All explosives shall be separated from other goods. Storage locations shall be clearly marked and located in areas without ignition sources. Incompatible explosives shall be separately stored.

The storage location for explosives shall allow for emergency dumping to sea.

5.4.8 Floating installations

5.4.8.1 General

For floating installations the following shall apply:

- systems with hydrocarbons with flashpoint below 60 °C shall not be installed in columns or pontoons for floating installations;
- vital control functions (e.g. maritime control/bridge, process control and special emergency preparedness functions) should be arranged in one common control centre for the entire installation;
- process area shall be separated from FPSO hydrocarbon storage tank top by air gap of minimum 3 m and plated deck;
- equipment that can represent an ignition source should be located upwind of potential leak sources on floating installation that will be turned up against the wind;
- the effects of "green sea" shall be carefully evaluated and means of protection arranged;
- location and type of crude oil pumps shall be based on a hazard evaluation for operation and maintenance of the pumps. Submerged pumps should be preferred. Crude oil transfer lines shall not be located in double bottom.

5.4.8.2 Turret

The turret arrangement design shall aim at achieving open naturally ventilated areas and minimising explosion pressure. Enclosed mechanically ventilated areas should be restricted to LER/LIR with control or special equipment that requires special protection or cannot be located in outdoor environment. Such enclosed premises shall have over pressure ventilation, with air taken from and exhausted to a non-hazardous area. Location of the premises themselves as well as their ventilation inlets shall take into account the prevailing wind directions.

Where anchor winches are arranged on the deck below riser termination and ESD valves, the deck separating the areas shall be solid and gas tight.

Turret areas and piping shall be designed to minimise the risk of jet fires towards tank tops.

5.4.9 Explosion design principles

The amount of explosion relief available, the degree of blockage and congestion in an area of an explosion shall be optimised to reduce explosion risk. Design principles in ISO 13702, B.10 to B.11, should be followed.

The use of explosion panels and weather protection shields shall be kept to a minimum. Natural ventilation and open modules shall be preferred. Where such arrangements are likely to cause an unacceptable working environment special solutions such as erection of temporary shields for maintenance operations should be considered.

The arrangement of equipment in an area, and particularly near ventilation openings, can have a major influence on the peak overpressures expected in an area. Cable trays, junction boxes, piping and equipment shall be located so that they will not significantly increase turbulence, block explosion ventilation openings and reduce the free vent area, and thus increase explosion loads.

5.5 Survivability requirements

Consideration shall be given to the protection of well and BOP equipment, such as control panels and hydraulic systems and their related signal paths.

6 Structural integrity

6.1 Role

Load bearing structure shall withstand all load conditions under normal operation and also ensure structural integrity during dimensioning accidental events.

6.2 Interfaces

Structural integrity has interfaces with the following safety systems/functions:

- passive fire protection;
- fire fighting systems;
- escape and evacuation;
- marine systems and position keeping;
- ship collision barrier.

6.3 Required utilities

Structural integrity is not dependent on any specific utility.

6.4 Functional requirements

Load bearing structures shall be designed so that single component failure cannot lead to loss of structural integrity.

6.5 Survivability requirements

The design shall ensure sufficient structural integrity during DALs. This applies to main structure as well as other structures such as derricks and flare towers which may lead to escalation in case of collapse. The main load carrying capacity shall be maintained until the facility has been evacuated.

The DALs shall be combined with other functional and environmental loads according to NORSOK N-003.

7 Containment

7.1 Role

The containment function shall prevent release of hydrocarbons, chemicals and/or toxic gases.

7.2 Interfaces

The containment function has interfaces with the following safety systems/functions:

- passive fire protection;
- fire fighting systems.

7.3 Required utilities

The containment function is not dependent on any specific utility.

7.4 Functional requirements

7.4.1 Piping

The use of flexible hose connections for well stream transfer, within the turret and between turret and ship, should be minimised.

7.4.2 Flanges and connections

The number of flanged connections in systems containing hydrocarbon fluids shall be kept to a minimum. Generally flanges shall be selected to reduce leakage probability.

Flanges on the pipeline side of the riser ESD valves shall not be used unless subsea isolation valve is installed and the shut in volume is sufficiently small. The flanges shall normally be of compact type, see NORSOK L-005. There shall not be instrument connections on the pipeline side of the riser ESD valve.

Relief/BD headers shall normally be designed without flanges.

Flanges in hydrocarbon piping to, or through, the utility area shall be avoided. One flanged connection is allowed on the fuel line to each combustion engine, turbines and fired units in the utility area.

Mechanical connections shall be designed to withstand vibrations, according to NORSOK L-001.

In modification projects a flanging philosophy shall be established prior to modifications taking into account the risk of ordinary flanges, compact flanges and welded solutions.

7.5 Survivability requirements

The equipment and piping components related to the containment function shall resist the DALs to which they may be exposed for the required period of time. Particular attention should be made to flanges exposed to fire.

8 Open drain

8.1 Role

Control of spills is fulfilled through the open drain system. The purpose of the open drain system is to provide measures for containment and proper disposal of liquids including handling of FW, e.g. through fire seals.

8.2 Interfaces

Open drain has interfaces with the fire fighting systems.

8.3 Required utilities

Open drain safety function is not dependent on any specific utility.

8.4 Functional requirements

8.4.1 Minimize fire/escalation risk arising from spills

The design of the open drain shall limit the spread of a spill and route the spill away to avoid escalation. The drainage systems shall be designed in accordance with NORSOK P-100 and ISO 13702.

Open drain systems on floating installations shall be designed to operate satisfactorily for all sea states in which the hydrocarbon inventory is present in the process system.

On floating installations with turret, decks above moon pool where liquid spills may occur shall have an adequate drain routed to a collection tank.

8.4.2 Separation of drain systems

Hazardous and non-hazardous open drains shall be physically separated to prevent back flow of hydrocarbons from a hazardous to a non-hazardous area. The design shall be in accordance with NORSOK P-100.

The hazardous drain collection tank shall be purged.

8.5 Survivability requirements

There are no specific survivability requirements.

9 Process safety

9.1 Role

Systems and equipment, typically PSD, PSV and local instrumented safety functions, shall control abnormal operating conditions to prevent possible hydrocarbon release. This includes typically

- stop hydrocarbon flow,
- shut down process and utility equipment,
- pressure relief.

9.2 Interfaces

The process safety system has interfaces with the following safety systems/functions:

- ESD;
- BD and flare/vent system.

9.3 Required utilities

Process safety system performance is dependent on:

- UPS;
- hydraulic power;
- instrument air.

9.4 Functional requirements

9.4.1 Process safety principles

Process and auxiliary systems shall be designed such that no single failure during operations can lead to unacceptable hazardous situations. Two independent levels of protection shall be provided. The design shall be in accordance with ISO 10418 (alternatively API RP 14C may be applied).

The PSD system shall be independent from the process control system.

9.4.2 Process shut down (PSD) valves

Shut down valves on the liquid phase outlet from pressure vessels shall be located as close to the pressure vessel as possible, and the number of leak sources between the pressure vessel and shut down valve shall be minimised.

9.4.3 Pressure safety valves (PSVs)

The PSV configuration on the pressure vessel shall be evaluated. Common mode failure shall be included in the evaluation. To ensure sufficient reliability "N-1 out of N configuration" (for $N \geq 4$) should be avoided.

9.4.4 Alarms, automatic actions

Alarms shall be initiated as quickly as possible upon abnormal process developments and when equipment protection exceeds the limit setting. The alarm shall warn personnel in CCR and initiate required automatic actions.

9.4.5 Response time

Maximum response time of the process safety function shall be defined in order to ensure that the total reaction time for each safety function can be fulfilled.

9.4.6 Logic solver

Logic solver compliance with the intended use and safety integrity requirements shall be demonstrated, i.e.:

- logic solver (firmware) compliance with IEC 61508 shall be documented, i.e. certified/type approved by an independent body;
NOTE This is also valid for system software revisions.
- use of non-certified equipment may be accepted subject to particular safety assessment and "proven in use" characteristics;
- the logic solver shall, by hardware and software means, permit adequate testing of the functions within specified limitations regarding degradation of safety and impact on production regularity. This shall also include trip signals between SAS units;
- logic solver software shall be protected against illegal access from external sources, i.e. external data communication interface security of common SAS network and units.

9.4.7 Instrument based systems for secondary pressure protection

In the event instrument based systems need to be installed for secondary pressure protection and rupture of the vessel may expose personnel, the solutions shall be designed such that the frequency of rupture due to over pressure is less than 10^{-5} per year and segment. Evaluations and implementation shall be performed in accordance with IEC 61508.

For guidance with respect to application of instrument based systems for secondary pressure protection, reference is made to NORSOK P-001.

9.5 Survivability requirements

The logic solver and essential utilities shall be located in a protected area that withstands the DALs.

10 Emergency shut down (ESD)

10.1 Role

The purpose of the ESD system is to prevent escalation of abnormal conditions into a major hazardous event and to limit the extent and duration of any such events that do occur.

10.2 Interfaces

ESD system has interfaces with the following safety systems/functions:

- process safety;
- BD and flare/vent system;
- gas detection;
- fire detection;
- ISC;

- PA, alarm and emergency communication.

In addition, ESD initiations will activate (direct or indirect) other safety systems/functions such as HVAC, emergency power and lighting, PA, subsea control, drilling and well intervention and marine systems.

10.3 Required utilities

ESD system performance is dependent on

- UPS,
- hydraulic power,
- instrument air.

10.4 Functional requirements

10.4.1 Manual release buttons

Manual activation buttons shall be located at strategic positions where accessibility and manning in a hazard situation is taken into account, such as:

- CCR (APS/ESD1/ESD2);
- helideck (APS);
- muster areas/lifeboat stations (APS);
- bridge connections (ESD2);
- drilling areas (driller shut down and ESD2);
- exits from process and wellhead areas (ESD2).

Manual activation buttons shall be protected against inadvertent activation, e.g. with protective covers. Each activation station shall be clearly marked, and a consistent colour coding shall be applied for the activation buttons, e.g. black with yellow stripes for APS and yellow for ESD2.

Isolation of emergency power supplies (e.g. UPS) upon APS shall be executed via a timer independent of the logic solver, normally 30 min. It shall be possible to initiate immediate shut down from CCR during timer countdown.

10.4.2 Emergency shut down (ESD) final elements

ESD valves shall isolate and sectionalise the installations process plant in a fast and reliable manner to reduce the total amount of released hydrocarbons in the event of a leakage.

A shut down valve shall be categorised as an ESD valve if the consequence of valve failure is that a possible fire will exceed the dimensioning fire load for the area in question. In addition the following shut down valves shall be categorised as ESD valves:

- valves located in, or are the nearest shut down valve to, a hydrocarbon riser;
- valves located on the liquid outlet of large liquid vessels, such as separators and coalescers, see 9.4.2 for location of valves;
- valves located in a utility system where the consequences of valve failure with respect to safety may be significant, shall be subject to special consideration;
- well stream isolation valves (DHSV, master valve, wing valve);
- BD valves, see 11.4.1.

An ESD valve may be used as a PSD valve, but combined ESD and PSD valves shall have physically separate ESD/PSD activation signals and solenoids.

ESD valves shall be equipped with both remote and local position indication.

ESD valves shall have either spring return or local accumulators to ensure fail-safe function. Spring return type of valves shall be used when required size is available. Local accumulators shall have capacity for at least three operations (close-open-close) and be placed as close as possible to the valve.

ESD valves shall have defined criteria for leakage rates based on safety criticality. There shall be facilities for testing of internal leakage rate.

ESD valves, except BD valves, shall only have local reset function. For NNMI reset of the ESD valves should be made at the valve itself, but shall also be possible from the remote CCR when the NNMI is unmanned.

Isolation valves in equalizing lines across ESD valves shall be secured in closed position during normal production. Such valves shall fulfil the specifications applicable for the ESD valve itself including acceptance criteria with respect to internal leakage.

Manual valves in safety control circuits (e.g. hydraulic return and accumulator supply, means for valve travel time adjustment) shall be secured in correct position.

10.4.3 Emergency shut down (ESD) actions

ESD system shall activate all actions in accordance with the FES. Consideration shall be given to interrelations between interconnected fields and installations, e.g. by pipelines or control systems.

The ESD functions shall be arranged in a tree-structured hierarchy, APS, ESD1 and ESD2. General principles are shown in Figure 2. A superior ESD level shall initiate lower levels including PSD. A signal on a certain level should never initiate shutdowns or actions on higher levels. The following automatic actions shall be executed:

- shut down of wells (installation and subsea) and import/export pipelines including stop of export from upstream installations;
- shut down and sectioning of the hydrocarbon process facilities;
- initiation of BD;
- ignition source isolation;
- shut down of main power generation;
- start/stop of emergency power generator;
- shut down of drilling, intervention and work-over equipment not required for well control.

It shall be possible to close DHSV and master valves during well intervention from a position outside the wellhead area, and locally from wellhead/drilling area.

Loss of ESD signals between an NNMI and remote control centre shall shut down the NNMI. A possible time delay in shut down due to a link failure should not exceed 10 min.

ESD of the remote control centre or plant should result in operational shut down of the NNMI.