Design reviews mentioned at 6.3.1 shall be performed on control systems. The acceptance procedures shall include confirmation of the safe operation of the process control system during malfunction and failure mode.

Remotely controlled equipment shall in case of an emergency or malfunction be capable of being stopped locally from plant.

7.5.1.2 Process Control System (PCS)

The PCS shall provide the operator with real time information to allow safe and efficient operation of the plant.

Some equipment can have an individual process shut down system (PSD).

Common process parameters can lead to a PSD of groups of equipment; this PSD may be activated by either PCS or the SIS.

The PCS shall indicate, store and/or print all information returned by the process control devices necessary for the safe and efficient operation of the plant. In order to analyse an incident, the system shall chronologically discriminate and store all information occurred during this time and all actions performing by the operator before and after the event.

The PCS shall inform the operator of essential electrical facility information necessary to operate the plant.

The PCS design shall present the operator with the optimum amount of data required for safe and efficient operation of the plant and shall minimize alarm overload in case of incident or a sudden state change.

7.5.1.3 Safety Instrumented System (SIS)

A SIS shall be provided to identify, inform and react appropriately to potential hazardous events. The SIS shall be independent of the PCS and identify the potential hazard and, were appropriate, automatically bring the plant to safe conditions.

All modifications of SIS shall be performed in compliance with the Safety Management System (Functional Safety Assessment - FSA).

The SIS shall be designed for detecting hazard situations and reducing their consequences. It shall have the following functions as a minimum:

— gas detection (LNG, refrigerant gas, natural gas);

— pressure detection;

— temperature detection;

— spillage detection;

— flame detection;

— ESD activation from a central system and/or local ESD station;

— monitoring, activation and control of safety devices;

— monitoring and control of essential parameters to keep the installation in safety situation.

The SIS shall be designed for:

— initiate automatically the appropriate ESD actions. ESD shall be reset manually and/or locally by an authorized person before re-energizing the system;

— shall handle Safety Instrumented Functions (SIF);

— where appropriate, activate automatically the necessary protection equipment;

— inform the PCS of ESD activation;

— control visual and sound emergency communication devices defined in emergency plans (i.e. siren);

— open gates to allow access of emergency crew and staff evacuation, where required by emergency plans.

Risk assessment conclusions shall be applied to the design of the safety control system. Type, redundancy, number and location of detectors or sensors shall be studied to ensure quick and reliable detection of a hazardous situation. The system specification is derived from the requirements of the risk assessment outlined in Clause 6. A cause and effect matrix shall be produced in compliance with risk assessment and HAZOP study requirements.

The SIS shall give the operator detailed information on areas involved in the hazardous event, type of hazard, concentration of gas, where in the area (if applicable), detector or loop involved, status of fire water pumps, status of protection systems, status of HVAC equipment involved (fans, dampers, etc.), wind force and direction, temperature and relative humidity, system faults, reduced safety in the fire zones.

The alarms received in the control rooms, details of automatic actions taken by the SIS together with detailed incident information and CCTV coverage, aid the operators in selecting appropriate operator controlled actions, such as:

— shut down or isolation of the process system involved;

— activation of appropriate remote operated fire protection systems;

— initiate emergency actions by operators with mobile/portable firefighting material.

The SIS shall be compliant with EN 61508 (all parts) and IEC 61511 series.

7.5.2 Emergency Shut Down (ESD)

All ESD actions shall be activated by the SIS central panel with supplementary activation from local ESD stations. ESD activation shall neither cause a new risk situation nor damage a machine or other equipment.

ESD activation shall cause equipment shut-down and ESD valves operation to their fail safe position in order to contain inventories.

The PCS shall put automatic sequences in such a position as to prevent unexpected equipment or valve operation which could occur at the time of ESD reset.

The principle of the ESD operation shall be to minimize the release of hydrocarbons and to minimize the escalation of any hazardous event into adjacent areas.

Plants are often divided into fire areas and subdivided into fire zones to enable the ESD actions limiting escalation to be defined.

Fire risks in a fire zone may be controlled by the operation of the ESD valves. The ESD shall isolate the fire zone to minimize the release of hydrocarbon from the fire zone, and to minimize the flow of flammable hydrocarbons into the fire zone to limit the fire event.

A fire zone may be depressurized after isolation by ESD valve operation to reduce hydrocarbon inventories and to minimize the potential for vessel failure or structural collapse due to the fire intensity and duration.

ESD valves are also used within fire zone to minimize the release of hazardous materials from vessels due to the failure of downstream equipment or piping.

ESD operation is usually provided as a structured response related to the hazardous event.

Typical ESD levels are:

— ESD 1: (un)loading shutdown;

— ESD 2: ship disconnection;

— ESD 3: process shutdown (liquefaction or vaporization). This ESD 3 could be organized to prevent total loss of operation, if applicable to the plant;

— ESD 4: Total Facility Shutdown: All equipment shut down.

The use of ESD systems for the protection of marine transfer operations is described in [52], [34] and [74].

7.5.3 Field instruments and valves

The amount of instrumentation required is determined by the hazard and operability risk assessment and reliability studies.

Sufficient instrumentation shall be installed to enable the plant to be commissioned, operated and decommissioned in a safe manner.

Typically instrumentation will include:

— liquid level indicators and/or switches;

— pressure indicators and/or switches;

— temperature indicators and/or switches;

— in-tank density indicator (except in pressurized tanks or if provisions as defined in EN ISO 16903 are taken to prevent roll-over).

In general, the reliability of such measurements is to be ensured by the following minimum arrangements:

— instrumentation should be able to be maintained in normal operation of the plant;

— instrumentation related to safety and operation for which maintenance requires dismantling shall have sufficient redundancy;

— threshold detectors which have a safety function (pressure, LNG level, etc.) are to be independent of the process measurements;

— measurements and alarms shall be transmitted to appropriate control system;

— in earthquake areas, critical alarms, e.g. pressure and level, shall be transmitted by duplicated, diverse routes to the control room.

7.5.4 Fire, spill and gas detection system

Systems shall be provided to detect possible accidental events, which could occur in the plant.

The arrangement of detectors shall provide adequate coverage. Selection and installation of detectors shall prevent false and spurious alarms. Voting technique arrangement may be used.

It is important to accept that not all leaks can be detected by instruments. Regular inspection by the operator is vital for the detection of minor leaks which shall be repaired to prevent these developing into larger leaks.

Detection systems are intended to rapidly and reliably detect any LNG spillage or flammable gas leakage and any fire condition in the plant and be connected to the ESD system.

Continuously operating detection systems shall be installed at every location, outdoors and indoors, where leaks are credible.

The following detection devices shall be provided:

— LNG spillage detection;

  LNG spills shall be detected by low temperature sensors, for example, resistance type device's or fibre optic systems. The sensors shall be, protected against accidental damage.

— Flammable gas detection;

— Flame detection;

— Smoke detection for buildings.

7.5.5 Earthquake detection

Where applicable seismic acceleration monitoring shall be provided, giving signals to automatically initiate the plant shutdown when the earthquake reaches a pre-defined level.

7.5.6 Human-Machine Interface (HMI)

The HMI shall be designed in accordance with an appropriate industry standard and should have the following features:

— process overview screen showing main equipment items and instrumentation;

— equipment or process operation detail screens;

— alarm summary screen;

— alarm log screen;

— valve status (manual, open, closed);

— colours that are in line with attention hierarchy;

— pre-programmed trend screens for relevant process parameters;

— pump status;

— show real-time data;

— show history data.

HMI functions at the LNG transfer locations shall be by means of one of the following:

— hardwired lamps and push buttons and instrument indications;

— touchscreen or computer based display.

Further information can be found in [70].

7.5.7 Alarm management

Alarm management shall be as per recognized guidelines (see [62] and [63] for more information).

7.5.8 Telecommunication and CCTV requirements

The requirement for telecommunication and CCTV shall be based on a risk assessment.

— Manual call points (e.g. telephone box, alarm push buttons).

  Manual call points shall be provided in the hazardous plant areas, typically those plant areas covered by flame and/or combustible gas detectors, and provided on likely escape routes from these areas. Manual call points can be replaced by ESD push buttons for immediate trip of an activity (typically LNG transfer from/to ship or truck to/from terminal) or immediate isolation of an area.

— CCTV monitoring.

  Remote operated cameras should be installed for viewing all events which could occur in hazardous and unmanned areas.

  Under abnormal conditions the operator should have the ability to use these CCTV systems to analyse the situation.

  The system shall be considered as a priority load and is connected to the UPS system. The system should automatically respond to alarms, and focus information presented on VDU’s (visual display unit) in the appropriate control room(s).

— Communication system.

  The control room operators shall be able to communicate with field operators via the terminal communication systems (specific mobile phones and radios).

  Special consideration shall be given to buildings with high noise levels where visual alarms shall also be installed.

  A combination of visual and sound alarms shall be installed in all plant locations.

  Direct communication links should be available with the port authority, the LNG carrier and the pipeline dispatching centre.

Internal transmission networks shall differentiate operation information (of process control system) from safety information (of safety control system). Internal transmission networks shall be made secure from external communication networks (no direct interfaces are recommended for manned plants).

7.5.9 Warning lights

Tanks and other elevated structures shall be fitted with warning lights which are expected to comply with air and safety navigation regulations.

The jetty shall have navigational lights which are expected to be in accordance with local marine regulations.

7.6 Process technical safety

7.6.1 Overfill protection

Storage tanks shall be fitted with instruments that enable the level of LNG to be monitored and that enable action to be taken. These instruments shall allow:

— continuous measurement of the fluid level;

— detection of critical level with initiation of cause and effect function for prevention of overfill.

The level of confidence for these instruments shall be defined by SIL allocation, refer 6.2.10.

NOTE A general description of the applicable risk assessment method can be found in 6.2.10. SIL analysis is expected to validate any design basis with a consequence in terms of overfill protection, typically number, accuracy and independence of the level gauges to be installed, normal range for continuous measurement and alarm indications till overfill condition could be attained.

7.6.2 Overpressure protection

7.6.2.1 Overpressure protection for storage tanks

To prevent overpressure of storage tanks the following shall be included as a minimum:

— relief devices shall be sized for all applicable upset scenarios (e.g. PBU runaway) and fire scenario, see 7.4.12;

— the LNG storage tank shall be protected from overpressure resulting from backflow from the downstream systems;

— detection of high pressure which trips ESD, by instrumentation which is independent of the continuous measurement.

In addition, the tank shall be fitted with instruments, permanently installed and properly located which enable the pressure to be monitored as follows:

— continuous pressure measurement;

— detection of too high pressure, by instrumentation which is independent of the continuous measurement;

— if the insulated space is not in communication with the internal container, differential pressure sensors between the insulation space and the internal container or separate pressure sensors in the insulation space shall be installed. For pressure storage this is not required.

For the low pressure storage tanks refer to EN ISO 28300.

7.6.2.2 Overpressure protection for other equipment

Overpressure Prevention shall be part of the risk analysis.

7.6.3 Vacuum protection for storage tanks

The tank shall be prevented from going into negative pressure beyond the permissible limit, by timely automatic shutdown of pumps and compressors, gas or nitrogen injection and for low pressure tanks by air vacuum breaker valves. As introduction of air can bring about a flammable mixture, the air vacuum breaker valves shall act only as a last resort in order to prevent permanent damage to the tank.

Gas may be injected under automatic control to minimize low pressure in tank.

The pressurized tank shall be designed for underpressure condition as per process and operating conditions.

As per risk assessment the tank may be fitted with detection of too low pressure (vacuum) by instrumentation, which is independent of the continuous measurement.

7.6.4 Leakage

Low pressure tanks as well as pressurized tanks are to be designed with the assumption that the liquid containing container could leak and gradual release of product could take place (ref. 7.8.5 and 7.8.6).

Measures of the adequate utilization of such upset condition shall be implemented into the design of the storage system as determined by the risk assessment. The possibility of sudden failure (zip failure) of the liquid containing is not a design consideration in present standard.

7.6.5 Roll-over

If roll-over is a credible scenario that could lead to overpressure of the tank, at least the following measures shall be taken:

— tank fitted with top and bottom filling connections;

— a recirculation system;

— monitor boil-off rate;

— temperature/density measurements throughout LNG depth.

Other operational preventive measures may be used, such as:

— avoiding storing significantly different qualities of LNG in the same tank;

— appropriate filling procedure considering the respective densities of the LNG;

— specific processing for LNG which contain a nitrogen molar fraction higher than 1 %;

— cycle tank usage to prevent stagnation of LNG inventories.

For the design of pressure safety device refer to 7.4.12 and for the flow rate refer to Annex B.

The design of the tank may be based on tank LNG behaviour simulation validated software which integrate filling and emptying phases. They may be used to predict stratification occurrences, to estimate consequences and to evaluate the means to avoid or to manage them.

In case of pressurized storage the risk of roll-over shall be considered. For more information refer to publications ([64],[65] and [66]).

7.6.6 Low temperature protection

At the vaporizer outlet, piping materials are to be chosen in terms of the lowest temperature that might occur. This depends on the following:

— the set point of the temperature switch which automatically closes the isolation valves;

— the time required to close the LNG valve;

— thermal transients before temperature stabilization;

— temperature drop due to expansion of the gas to a lower pressure.

Materials shall be:

— austenitic stainless steel up to isolation valves which close in the event of gas temperature below the specified threshold;

— suitable for the lowest temperature which can occur downstream of the isolation valve before it can be shut.

7.6.7 Liquid carryover

A temperature transmitter shall be installed in the vent stack/flare line downstream of the relief valves to detect LNG carryover.

7.6.8 Emergency depressurization

Emergency depressurization of plant parts may be recommended to prevent further escalation in emergency situations.

The intention of this measure is to:

— reduce the internal pressure;

— reduce the effect of leakage;

— avoid the risk of failure of LNG, hydrocarbon refrigerant or gas filled pressure vessels and piping from external radiation.

Devices for depressurizing high pressure equipment shall allow the pressure of one or more item of equipment to be reduced quickly (see [21]). These gases shall be sent to the boil-off gas or flare/vent system which shall be capable of handling the potentially high flow and the low temperatures generated during depressurizing.

Isolation valves, activated from a control room or other remote location or automatically, shall be provided so that the unit can be isolated into several sub-systems and where it is required to isolate sensitive equipment. This will make it possible to depressurize only one part of the plant, while limiting the entry of hydrocarbons into a fire containing zone.

7.7 Marine transfer systems

7.7.1 General

For conventional onshore LNG terminals, the jetty and marine facilities shall be designed in accordance with EN ISO 28460 and the requirements in this clause. For LNG bunkering installations, the jetty and marine facilities shall be designed in accordance with EN ISO 20519 and the requirements in this clause.

This clause deals with the siting, engineering design, pre-operational training and safety requirements of the jetty and marine facilities.

7.7.2 LNG marine transfer systems

Marine transfer systems shall be used for the transfer of LNG between ship and shore. These shall be in accordance with EN ISO 16904 or EN 1474-2.

Flexible hoses shall be designed in accordance with relevant codes and/or standards, such as EN ISO 21012, EN 1474-2, EN ISO 10380 and/or EN 13766.

Consideration shall be given to the transfer of gas from the tanks to the LNG carrier or reverse, to compensate the volume of liquid displaced during unloading or loading, and the collection of boil-off from the tanker while it stays at the jetty.

A blower or booster compressor can be used.

7.7.3 Jetty design

The positioning of a jetty at an LNG marine terminal is a prime factor in determining the overall risk of the ship/shore transfer operation and a detailed study to determine the most acceptable position shall be undertaken at the conceptual stage of the project. Determination of what is acceptable in specific circumstances shall follow from an assessment of the actual risks posed by the operation of adjacent sites and harbour traffic.

Provisions described in EN ISO 28460 shall be incorporated into jetty design and ship shore interface.

An appropriate standard for marine structures shall be used (see [38]) to determine the selection of relevant design parameters and methods of calculation to derive the resulting forces on the jetty structure. This shall allow for soil conditions, plus the loads imposed on an LNG terminal jetty due to natural phenomena, such as winds, tides, waves currents, temperature variation, ice and earthquakes and those imposed by operational activities, such as berthing and mooring, cargo handling and vehicles used during construction, operation and maintenance.

Consideration shall be given to the range of vessels that it is anticipated will berth at the terminal to ensure they can safely do so.

Consideration within the design shall be given to the possibility of LNG spills, particularly in the area adjacent to the transfer system. This may be by provisions for containment of LNG spill and brittleness protection of carbon steel structural members, or by other appropriate measures.

It shall contain controls for emergency shut down and release equipment for the LNG transfer system and jetty remote operated firefighting and vapour control equipment. A communication system between jetty and terminal operating control station shall be provided.

The need for quick release hooks shall be risk based. Quick release mooring hooks shall be provided and the design of the release system shall be such that the operation of one switch, or failure of a single component, cannot release all moorings simultaneously.

7.7.4 Jetty and marine monitoring and control

When following functions are available they shall be interfaced in the plant monitoring and control system:

— monitoring of weather conditions (wind, sea situation, etc.);

— berthing monitoring (speed, distance, etc.);

— mooring monitoring (mooring loads, etc.);

— status of quick release hooks;

— monitoring and control of marine transfer systems;

— marine transfer arm Emergency Release System.

For details, see EN ISO 28460, EN ISO 16904 and EN 1474 (all parts).

7.7.5 Jetty safety and security

7.7.5.1 Safety

Provision shall be made for rapid access and egress to the berth by emergency vehicles or vessels involved in firefighting, medical evacuation or pollution control if required by the emergency response plan.

On jetties relying on vehicular access it could be necessary to provide passing places.

Provision shall also be made for emergency escape routes from fire or liquid spill. From any point on the berth it shall be possible to escape to a place of safety. This is most easily achieved by providing two independent routes to safety from the berth. These may include:

— additional walkways;

— provision of a manned standby boat(s).

Escape route shall be protected by water spray if found necessary by the risk assessment.

Access to ship from jetty shall comply with requirements of EN ISO 28460.

7.7.5.2 Security

A security assessment shall be prepared for the marine and onshore facilities covering all expected security issues and their consequences. Further information is provided by IMO ISPS.

7.7.6 Unmanned transfer stations

In some cases, plants could be unmanned. In those cases, the following shall be included if required by risk assessment, but not limited:

— remote monitoring system and remote alarm management (24/7);

— CCTV (24/7);

— remote ESD-button.

When having unmanned facility, the risk assessment cannot take operator alarm intervention in account as mitigation in all cases. As such, additional mitigation barriers shall be considered compared to manned operated sites.

7.8 Storage unit

7.8.1 General

This Clause covers the minimum requirements for specifying, design, manufacturing and installation, construction, testing, operating and maintenance of storage units within an LNG plant.

NOTE In this document, low pressure tank is an equipment item in its entirety for the storage of LNG with a maximum allowable pressure PS < 50 kPa (0,5 bar). The different types of-low pressure storage tanks are described in EN 14620 (all parts). A pressurized tank is an equipment item in its entirety for the storage of LNG with a maximum allowable pressure PS > 50 kPa (0,5 bar.)

The storage unit shall be designed for normal and abnormal conditions, as given below.

7.8.2 Normal conditions

LNG storage systems shall be designed to:

— safely contain the liquid at cryogenic temperature;

— ensure gas tightness;

— permit the safe filling and removal of LNG;

— permit the boil-off gas to be safely removed;

— prevent the ingress of air and moisture;

— operate safely between the design maximum and minimum pressures and temperatures;

— limit the rate of heat in leak, consistent with operational requirements;

— prevent frost heave (i.e. ice build-up in the soil);

— withstand the number of filling and emptying cycles and the number of cool down and warming operations which are planned during its design life;

— OBE seismic;

— environmental loads at normal conditions (wind, ambient temperature fluctuation, etc.).

7.8.3 Abnormal conditions

Credible risk scenarios for abnormal condition of LNG storage systems could have their origin in:

— overfilling of the tank;

— over/under pressurization of the tank due to process upset;

— roll-over leading to over pressurization of the tank;

— leaks which result in the complete emptying of the inner tank;

— withstand the effect of low temperature fluid spills;

— fatigue and cyclic loading of key components;

— corrosion;

— failure of pipe work attached to the tank;