5. Design

This chapter outlines the design requirements that the manufacturer should address to ensure the equipment meets the terminal's requirements. Some aspects may require clarification or guidance by the terminal before it accepts the engineering solution.

Guidance in this section comes from safety advances, technological improvements, emerging applications and lessons learnt.

5.1 General Engineering

This section provides high-level considerations for human factors, equipment engineering and equipment reliability. The risks of ERS malfunction, misinstallation or misoperation should be addressed primarily by design. Any residual risks should be identified clearly along with mitigating measures, such as procedures, instructions for use or training.

5.1.1 Human factors

Human factors methods should be employed in the design of equipment to reduce the likelihood and impact of human error and to enable effective human performance. This includes analysing the intended operations during normal operation, maintenance and testing, to identify where errors are likely to occur so that systems can be redesigned to prevent those errors and to incorporate safeguards (eg interlocks and permissive logic).

5.1.2 Design and engineering

Manufacturers should regularly review their designs for improvement, considering feedback from terminals in operation and lessons learnt. New engineering practices, technologies and regulations may affect new and existing designs. Appropriate design factors should be applied to aspects such as the selection of components, actuators and springs, wiring materials, hydraulic and pneumatic tubing and safety pins.

Suitable methodologies should be followed during design activities, such as failure modes and effects analysis (FMEA),[18] fault tree analysis[19] or event tree analysis.[20] Loss of electric power should not lead directly to spurious activation of the ERS.

5.1.3 Material selection

Components should be suitable for the marine environment. Degradation of materials, for example through corrosion, may lead to equipment malfunction. Site-specific conditions, such as high levels of dust or ice in the sensing system or actuation system, should be considered as these may impair equipment functionality.

5.1.4 Equipment layout

ERS and ancillary equipment, such as panels or accumulators, should be accessible for inspection but protected from unintended personnel interaction. For example, installation of controls or valves in walkways should be avoided.

[18] IEC 60812 – *Failure modes and effects analysis (FMEA and FMECA)*

[19] IEC 61025 – *Fault tree analysis (FTA)*

[20] IEC 62502 – *Analysis techniques for dependability – Event tree analysis (ETA)*

5.2 Actuation System

The actuation system should follow the predetermined release sequence and operate within the prescribed time window. The most common actuation system is hydraulic, but pneumatic and electrical systems are also used.

5.2.1 Coupler and sequence of actuation

Coupler disconnection should not occur unless the isolation valves are closed and secured. This can be achieved by fitting safety interlocks according to ISO 16904 Section 6.4.3[21] or equivalent. Once the disconnection sequence starts, it should not be possible to stop. When the coupler is separated, the valves should remain closed, even in the event of power failure of the actuation system.

There should be reliable methods of verifying that the coupler is properly reassembled after disconnection or maintenance. For example, pins or sensors can be used to prevent the ERS being put back into operation unless correctly reassembled and verified.

5.2.2 Blowdown system

ERSs installed in high-pressure gas systems require the fitting of a BDS to reduce pressure in the trapped gas between the isolation valves to a safe level (see Figure 12). Coupler disconnection should not occur unless the isolation valves are closed and the pressure in the trapped section is below the pressure threshold specific to the equipment design.

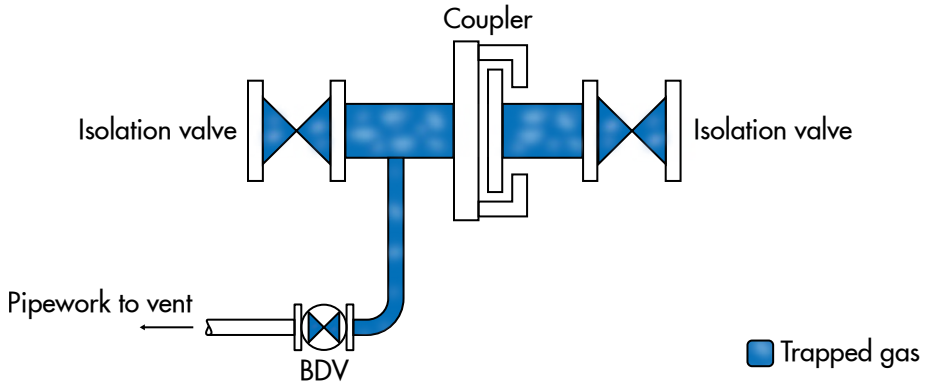


Figure 12: Trapped gas on an ERS with BDS

All pressure containment components should be able to withstand the pressure threshold. Computational fluid dynamics should be used to determine the time taken to reach the pressure limits, considering the back pressure imposed by the vent pipework. A finite element analysis should be used to demonstrate the strength of the pressure containment components. A conservative approach should be applied by, for example, the inclusion of safety factors in the analysis.

Pressure interlock logic should be implemented to disable disconnection unless the pressure of the gas in the trapped section is below the pressure threshold. Sufficient redundancy and reliability are necessary to prevent failure on demand. Redundant BDVs should be installed even when the SIL rating does not mandate it.

Local emergency venting at the manifold area should be avoided to prevent accidental gas release in the event of BDV failure in the open position.

[21] ISO 16904 – *Petroleum and natural gas industries – Design and testing of LNG marine transfer arms for conventional onshore terminals*

5.2.3 Actuation time

The end-to-end actuation time is terminal specific and the ERS should execute the disconnection sequence within the available actuation window. Depending on the type of ERS, the actuation time should consider the following:

- ERS without BDS: detection of position and the decision to activate and execute the disconnection sequence of all components should be executed within the actuation window
- ERS with BDS: in addition to the detection, decision and actuation sequence, the time required to depressurise the trapped gas to the pressure threshold should be included.

Some publications specify a fixed requirement of between 5 and 10 seconds for closure of the isolation valves and a maximum of 2 seconds for release of the coupler.[22, 23] However, following the proposed criteria provides manufacturers with the flexibility to develop the most suitable equipment for the specific terminal.

5.2.4 Control elements

DCVs are used in hydraulic systems to direct fluid flow to the actuators. They may be manually, solenoid, hydraulically or pneumatically operated. They should be designed to prevent internal leakage causing pressure build-up on the low-pressure side of the actuator. Any passing oil should be internally routed back to the hydraulic oil reservoir. All DCVs should be of the fully enclosed type (ie no bare metal pins exposed to ambient air) to minimise environmental corrosion.

The switching time of solenoid-operated DCVs should be monitored and an alarm or warning raised if it deviates from the design specification. This enables early detection of faulty conditions through, for example, self-diagnosis. Guidance on the deviation time can be obtained from the solenoid valve manufacturer.

5.2.5 Hydraulic fluid

The viscosity of hydraulic oil decreases as the temperature increases. High viscosity results in higher pressure losses, which leads to the need for larger hydraulic actuators and affects the actuation time.

Thermal expansion of the hydraulic oil caused by environmental temperature changes can generate excessive pressure build-up in locked-in sections. The hydraulic circuit design should be carefully evaluated to prevent local overpressure and to ensure that thermal expansion cannot lead to unwanted actuation of the coupler.

5.2.6 Energy accumulators

Hydraulic systems use pressure accumulators of the bladder or piston type. Pneumatic systems use compressed air bottles. Electrical actuation systems usually have a battery power storage system.

Energy accumulators should be sized for at least one full stroke of the actuation system. Pressure accumulators should be sized based on the minimum nitrogen pre-charge pressure and temperature and should feature a low-pressure alarm. Piston types should also have a low-level alarm.

5.2.7 Hydraulic oil reservoir

A hydraulic oil reservoir stores hydraulic fluid, ensuring a consistent supply for the system and aiding heat dissipation and contamination control. The hydraulic oil reservoir should have low-level and high-temperature detection features and a moisture removal filter.

---

[22] ISO 16904 Section 6.4.1: *"the ERS valves closure time should be set between 5 s to 10 s and PERC opening time shall be within 2 s."*

[23] OCIMF – *Design and Construction Specification for Marine Loading Arms (MLA4), Section 5.4.2 – "PERC release time should be within 2 seconds of ERS valve closure. […] The valve closure times should not cause unsafe surge pressures or column separation."*

5.3 Controls and Instrumentation

5.3.1 Controls and panel

The system should provide real-time information to the operator on the health of the system via, for example, an appropriately designed control panel, ideally with an indication of the faulty component (eg sensor). Loop monitoring of sensors and safety instrumentation should be implemented. The logic solver should be able to distinguish between power loss and a genuine ESD 2 signal.

The sensing system, actuation control elements and other safety-related instrumentation should be hard-wired, including communication with the ESD system. Typical communications are:

- The transfer system should send ESD 1 and ESD 2 signals to the terminal
- the terminal should send ESD 1 and ESD 2 signals to the transfer system
- the ESD 2 signal should trigger ESD 1.

The logic solver should communicate with the terminal's distributed control system (DCS) and ESD systems. In terminals with more than one transfer line, ESD 2 should disconnect all connected cargo transfer equipment. Position sensors should be capable of monitoring the condition of the loop. When proximity switches are used, the position switch configuration should have, for both apex and slew angles, one proximity switch at the ESD 1 position and two additional proximity switches at the ESD 2 position. Together, the set of switches should be configured as a 2oo3 (two-out-of-three) voting system for ESD 2. A similar configuration can be adopted for VSDSs.

Real-time position monitoring systems can be used if SIL capable.

5.3.2 Diagnostic coverage of system faults

Diagnostic coverage is a measure of the effectiveness of diagnostics in detecting faults within a system. High diagnostic coverage is desirable because it means that a larger number of faults can be identified and managed, reducing the likelihood of undetected failures that could lead to hazardous situations. Achieving high diagnostic coverage is essential in order for the equipment to meet the requirements of higher SILs and STRs. As far as reasonably practicable, self-diagnostic components should be selected with features to detect internal faults.

5.3.3 Manual activation

Push-buttons should be installed to allow operators to manually start the release. However, precautions should be taken to prevent unintentional starting of ESD 2. Push-buttons should have protective covers installed to prevent unintended operation. The number of push-buttons and their location should be considered carefully. For example, they should not be installed on the remote-control unit. A line-monitored push-button is recommended to prevent a trip on wire break or short circuit. When the ERS is disarmed, the push-button activation should be inhibited.

5.3.4 Safety overrides

To reduce errors and simplify the system, the number of safety overrides should be as low as possible. Overrides should only be enabled to perform testing or maintenance, and they should be designed to ensure that the safety function is reinstated before putting the ERS back in operation. These overrides may be physical (eg a pin or key) or software interlocks (see Section 7.4.3).

5.3.5 Permissive logic

Armed/disarmed safety functions with permissive logic should be implemented to prevent unintended release of the ERS coupler. The ERS should be armed only when the cargo transfer equipment is connected to the manifold. The system is disarmed by physically isolating the ERS from the power, hydraulic or pneumatic supply. The permissive logic allows release only when the system is armed and safety conditions are met. The armed/disarmed status should be indicated on the control panel, with an indication also visible from the manifold area.

5.4 Integrity Assessment

Suitable methodologies should be followed to demonstrate that the equipment meets the terminal's integrity requirements for safety, environmental protection and operations. Functional safety engineering can be useful and Annex 2 provides additional background information on SIL, STR and IEC standards.

5.4.1 Safety integrity level

IEC 61508[24] and IEC 61511[25] provide a structured and internationally recognised framework for functional safety. Devices intended for applications with SIL 1 or above should be supported by appropriate evidence of suitability, such as third-party certification or documented compliance assessments that demonstrate compliance with the agreed standards.

The assessment should address low-demand mode operation, hardware fault tolerance, diagnostic coverage and the agreed proof-test intervals.

Reliability data for critical components should be certified to recognised standards. Reliability data for non-certified components can be determined by:

- Dedicated testing or analytical methods complemented by suitable quality control and auditable systems to guarantee aspects such as traceability and consistency of data, or
- historical data from, for example, the Offshore and Onshore Reliability Data (OREDA) project or other recognised publications.

5.4.2 Spurious trip rate

In addition to the SIL, the STR should be calculated following suitable methodologies, such as FMEA,[26] fault tree analysis[27] or event tree analysis.[28] All components that can result in the ERS failing to perform should be included in the assessment, for example the sensors, logic solver, control elements, interlocks, overrides and final elements.

Section 5.5 lists the suggested failure modes that are used to define the dangerous and safe STRs for a typical design.

[24] IEC 61508 – *Functional safety of electrical/electronic/programmable electronic safety-related systems*

[25] IEC 61511 – *Functional safety – Safety instrumented systems for the process industry sector*

[26] IEC 60812 – *Failure modes and effects analysis (FMEA and FMECA)*

[27] IEC 61025 – *Fault tree analysis (FTA)*

[28] IEC 62502 – *Analysis techniques for dependability – Event tree analysis (ETA)*

5.4.3 Critical components and systematic failures

Critical components and activities are those that influence the achievement of the required SIL and STR. The instructions for use should clearly identify these elements and provide guidance on operation, end-to-end proof-test intervals, inspection requirements and maintenance activities. Human factor considerations, such as the risk of incorrect installation, configuration or operation, should be addressed to minimise systematic failures.

5.5 Suggested Spurious Failure Modes

Tables 2 to 5, and the accompanying legend in Annex 3, describe the suggested dangerous and safe spurious failure modes. The consequences provided are generic. Every terminal should provide guidance on its risk tolerability and apply the local regulation criteria.

5.5.1 Dangerous spurious failure modes

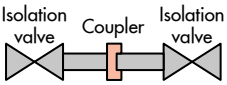
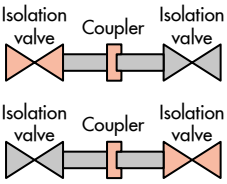
Scenario	ERS schematic	Failure description	Consequences
No. 1		Failure during cargo transfer operation leading to the release of the coupler. Both isolation valves remain open or not fully closed	Full-bore release is expected. Size of the release depends on multiple aspects, such as: – ESDVs closing and, if so, how fast they close, eg time to detect and act, etc – cargo transfer rate. Depending on the cargo, there is potential for a large fire, explosion or toxic cloud leading to multiple fatalities, environmental impact and damage to the assets and operations
No. 2		Failure during cargo transfer operation leading to the release of the coupler with one isolation valve still open or not fully closed	Similar to No. 1

Table 2: Suggested dangerous spurious failure modes (see legend in Annex 3)