



Exploration & Production

GENERAL SPECIFICATION

SAFETY

GS EP SAF 261

Emergency Shutdown and Emergency De-Pressurisation (ESD & EDP)

03	01/2011	General review
02	10/2005	Completely reviewed and moved PPR to GS EP SAF 262
01	10/2003	Change of group name and logo
00	04/2001	Old TotalFina SP SEC 261
Rev.	Date	Notes

Owner: EP/HSE	Managing entity: EP/SCR/ED/ECP
---------------	--------------------------------



Contents

1. Scope	3
1.1 Purpose of the specification.....	3
1.2 Application	3
2. Reference documents.....	4
3. Terminology and definitions	6
4. Emergency Shutdown (ESD).....	10
4.1 ESD purposes.....	10
4.2 Definition of the shutdown matrix.....	11
4.3 Integration of packages	24
4.4 Cascades and response time	24
5. Emergency De-Pressurisation (EDP).....	24
5.1 EDP application	24
5.2 EDP requirements	26
6. Architecture of the safety shutdown system.....	29
6.1 General.....	29
6.2 Principles of separation of Safety Instrumented Systems	31
6.3 Reliability requirements	33
6.4 Transmission of signals	35
6.5 Means of segregation	35
7. Shutdown devices, protection and other requirements	36
7.1 Shutdown devices.....	36
7.2 Physical position and protection	40
7.3 Isolations by ESDVs and SDVs	41
7.4 Additional functional requirements.....	43
7.5 EDP system - Protection and additional requirements	44
Appendix 1 Ultimate Safety System.....	45



1. Scope

1.1 Purpose of the specification

The purpose of this General Specification is to define the safety requirements for the design of the Emergency Shutdown (ESD) and Emergency De-Pressurisation (EDP) systems of hydrocarbon production, processing and storage installations. Transportation pipelines are excluded from this General Specification.

In accordance with the [API RP 14J](#) hazard tree for production installations, these systems contribute to the fulfilment of the following objectives:

- **Containment of hydrocarbon:** Limit the loss of containment by isolating incoming and outgoing hydrocarbon flows (ESD).
- **Prevention of ignition:** Isolate and de-energise potential sources of ignition (ESD).
- **Mitigation:** Depressurise equipment under fire (EDP); reduce or minimise hydrocarbon inventory by routing to the flare/vent (EDP); reduce the quantity released through a leak (EDP); initiate active fire-fighting.

1.2 Application

This General Specification is **not** retroactive. It shall apply to new installations and to major modifications or extensions of existing installations, both onshore and offshore, and including interfaces with wells and pipeline systems. It is also applicable to Vendor packages. It contains also the functional requirements of Fire & Gas systems.

This General Specification is limited to safety matters and does not cover in particular:

- Design of well-head control panels ([GS EP INS 147](#))
- Design of control and safety instrumented systems ([GS EP INS 134](#))
- Strict application to sub-sea control systems ([GS EP SPS 019](#))
- Design of High Integrity Protection Systems (HIPS) ([GS EP SAF 260](#))
- Design of pressure protection relief, such as PSVs, TSVs, etc. ([GS EP SAF 262](#))
- Design of hydrocarbon disposal systems, such as flares, vents, pits, etc. ([GS EP SAF 262](#))
- Design and sizing criteria of process ([GS EP ECP 103](#))
- Design of the Fire & Gas detection systems ([GS EP SAF 312](#))
- Hardware design and construction of Fire & Gas ([GS EP INS 134](#))
- Design of Burner Management Systems ([GS EP SAF 227](#))
- Emergency Release Systems (ERS) of (un-)loading arms
- Pipeline proprietary safety systems (SSIV, GOV, etc.).



2. Reference documents

The reference documents listed below form an integral part of this General Specification. Unless otherwise stipulated, the applicable version of these documents, including relevant appendices and supplements, is the latest revision published at the EFFECTIVE DATE of the CONTRACT.

Standards

Reference	Title
IEC 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems
IEC 61511	Functional safety Safety instrumented systems for the process industry sector
ISO 10417 / API RP 14B	Petroleum and natural gas industries - Subsurface safety valve systems - Design, installation, operation and redress
ISO 23251 / API STD 521	Petroleum and natural gas industries—Pressure-relieving and depressuring systems

Professional Documents

Reference	Title
API RP 14C	Recommended Practice for Analysis, Design, Installation, and Testing of Basic Surface Safety Systems for Offshore Production Platforms
API RP 14J	Recommended Practice for Design and Hazards Analysis for Offshore Production Facilities

Regulations

Reference	Title
Not applicable	

Codes

Reference	Title
Not applicable	



Other documents

Reference	Title
	Operating Philosophy Safety Concept Statement Of Requirements (SOR)

Total General Specifications

Reference	Title
GS EP ECP 103	Process sizing criteria
GS EP INS 120	Control Valves
GS EP INS 134	Design and supply of integrated control and safety system
GS EP INS 137	On/off valve control panels and actuators functional and construction requirements
GS EP INS 147	Design and supply of wellhead control panels
GS EP INS 150	Design method for system configuration - standard functions
GS EP INS 196	Input and Output Standard Functions
GS EP INS 198	Safety and Fire & Gas Standard Functions
GS EP PLR 100	Submarine pipeline systems
GS EP PLR 104	Onshore pipeline systems
GS EP PVV 112	Piping material classes
GS EP PVV 142	Valves
GS EP PVV 211	Design and fabrication of pressure vessels according to ASME VIII
GS EP SAF 021	Layout
GS EP SAF 226	Completed wells safety systems and safety rules
GS EP SAF 227	Safety rules for fired heaters
GS EP SAF 253	Impacted area, restricted area and fire zones
GS EP SAF 260	Design of High Integrity Protection Systems (HIPS)
GS EP SAF 262	Pressure protection relief and hydrocarbon disposal systems
GS EP SAF 312	Fire and gas detection systems
GS EP SAF 337	Passive fire protection: Basis of design
GS EP SAF 371	Emergency control facilities
GS EP SPS 019	Subsea production control system

3. Terminology and definitions

There are five types of statements in this specification, the “shall”, “should”, “may”, “can” and “must” statements. They are to be understood as follows:

Shall	Is to be understood as mandatory. Deviating from a “shall” statement requires derogation approved by Company.
Should	Is to be understood as strongly recommended to comply with the requirements of the specification. Alternatives shall provide a similar level of protection and this shall be documented.
May	Is to be understood as permission.
Can	Is to be understood as a physical possibility.
Must	Expresses a regulatory obligation

Note that “will” is not to be understood as a statement. Its use is to be avoided, unless it is necessary to describe a sequence of events.

For the purpose of this specification, the following **definitions** shall apply:

Abnormal operating condition	Condition which occurs in a process equipment or unit when an operating parameter ranges outside of its normal operating limits. (API)
Availability	Proportion of the total time during which a component, equipment, or system is performing in the desired manner. (UKOOA)
Blowdown (gas)	Used as a synonym for “emergency depressurisation” (see below).
Blowdown (liquid)	Control actions undertaken in response to a hazardous situation, to dispose of the liquid hydrocarbon inventory present in a capacity (Company).
Blowdown Valve (BDV)	Actuated fail-to-open valve, remotely operated by the ESD system to vent the pressure-containing unit or equipment to a safe location upon an emergency shutdown action (Company).
Boiling Liquid Expanding Vapour Explosion (BLEVE)	Sudden rupture due to fire impingement of a vessel and/or system containing liquefied flammable gas under pressure; the pressure burst and the flashing of the liquid to vapour creates a blast wave and potential missile damage, and immediate ignition of the expanding fuel-air mixture leads to intense combustion creating a fireball. (UKOOA) It is caused by the reduction of the vessel metal strength due to heat competing with the increasing pressure of the liquefied gases inside the vessel.
Cascade	In the context of ESD, a cascade is a series of actions; cascaded actions are not direct actions; they are either process-cascaded (e.g. high pressure propagates downstream from source) or instrument-cascaded (e.g. high shutdown level triggers lower shutdown levels).

Confirmed	In the context of Fire & Gas detection, means that at least two out of N sensors have detected Fire or Gas
Diversity (Diversification)	Different means of performing a required function. Diversity may be achieved by different physical methods or different design approaches (with the aim of minimising the common mode of failure) (IEC + Company).
Emergency De-Pressurisation (EDP)	Control actions undertaken to depressurise equipment or process down to a pre-defined threshold (generally 7 barg or 50% of design pressure) in a given period of time (generally 15 minutes) in response to a hazardous situation (ISO + Company).
Emergency Shutdown (ESD)	Control actions undertaken to shutdown equipment or process in response to a hazardous situation. (ISO)
Emergency shutdown system	Safety Instrumented System (SIS) consisting of manual release stations and automatic devices which, when activated, initiate installation shutdown (Company).
Emergency Shutdown Valve (ESDV)	Actuated fail-to-close valve, handling a hazardous fluid, remotely operated by the ESD system upon an emergency shutdown action, and being located either: a) at the limit of a fire zone b) within a fire zone to limit hydrocarbon inventory in isolatable sections c) at fuel distribution points to fired equipment.(Company).
Equipment	Any component or group of components specifically identified and itemised on the P&IDs (Company).
Failure	Termination of the ability of a device or equipment item to perform a required function. (IEC + API)
Fire and Gas (F&G) system	Safety Instrumented System (SIS) which monitors the temperature or the energy flux (fire), the concentration of flammable or toxic gases (gas), and initiates relevant actions (alarm, ESD, EDP active fire-fighting, electrical isolation, etc.) at pre-determined levels (Company).
Fire zone	Area within the installation where equipment is grouped by nature and/or homogeneous level of risk attached to them. The partition of an installation into fire zones results in a significant reduction of the level of risk. This implies that consequences of a fire, flammable gas leak or an explosion corresponding to the credible event likely to occur in the concerned fire zone, shall not impact other fire zones to an extent where their integrity could be put at risk (GS EP SAF 253).

High Integrity Protection System (HIPS)	Independent Safety Instrumented System (SIS) designed to protect a particular part of the installation against a possible particular operating condition (e.g. pressure, temperature, flow, level) exceeding the design parameters of that part of the installation. It does not duplicate the PSS or ESD system, but provides an independent additional layer of protection, with a sufficient reliability and response time faster than possible occurrence of the excessive operating condition, so as to make the probability of exceeding the design parameters lower than the target value. (refer to GS EP SAF 260)
Installation	Technical unit in which dangerous substances are produced, used, handled or stored, including all the equipment, structures, pipework, machinery, tools, private railway sidings, docks, unloading quays serving the installation, jetties, warehouses or similar structures, floating or otherwise, necessary for the operation of the installation (Company from European Directive 96/82/EC, dated December 9 th , 1996) (GS EP SAF 021).
Not permanently manned installation	Installation where personnel can be present, but less than 12 hours per day or less than 40 hours per week (Company).
Package	Prefabricated process or utility self-contained unit, generally able to operate on its own, supplied fully tested and ready for immediate installation, being supplied by a designated package Vendor (GS EP INS 120).
Permanently manned installation	Installation where personnel are routinely present for more than 12 hours per day (API + Company).
Pressure Safety Valve (PSV)	Valve releasing fluid contained inside process equipment in order to ensure that the prevailing pressure shall not exceed the design pressure (Company).
Process Safety System (PSS)	Safety Instrumented System (SIS) dedicated to shutdown to a safe state of particular units or equipment (e.g. SD3) (Company).
Redundancy	Existence of means, in addition to the means that would be sufficient for a functional unit to perform a required function or for data to represent information. (IEC)
Reliability	Probability that an item is able to perform a required function under stated conditions for a stated period of time or for a stated demand. (UKOOA)
Reset	Return of a system or component from its safety shutdown state to its normal shutdown state, to enable normal start-up procedure; reset can be local and/or remote, it can be manual or automatic (Company).

Safety Instrumented System (SIS)	A Safety Instrumented System (SIS) is a system comprising of dedicated sensors, logic solvers and final control elements for the purposes of taking a process automatically to a safe state when normal predetermined set points are exceeded, or when safe operating conditions are violated. (IEC, ISO, API) Multiple independent SIS normally exist at one installation (e.g. PSS, ESD, F&G, HIPS), forming together the “safety shutdown system”. Each SIS is entirely independent (logic and hardware) of the Process Control System (PCS) or from another SIS as to avoid any common cause failure, meaning separate sensors, logic solvers and final control elements (GS EP INS 134).
Safety Integrity	Average probability of a safety instrumented system satisfactorily performing the required safety instrumented functions under all the stated conditions within a stated period of time. (IEC)
Safety Integrity Level (SIL)	Discrete level (one of the four) for specifying the safety integrity requirement of the Safety Instrumented Functions (SIF) to be allocated to the Safety Instrumented System (SIS). Safety Integrity Level 4 has the highest level of safety integrity; Safety Integrity Level 1 has the lowest. (IEC) SIL is a measure of risk reduction provided by a Safety Instrumented Function (SIF), based on four levels. Each level represents an order of magnitude of risk reduction. Every Safety Instrumented Function (SIF) has a SIL assigned to it.
Shutdown (SD)	Control actions undertaken to stop operation of equipment or a process. The word “Shutdown” normally implies the “shut-in” of wells, the “tripping” of machines, the “closing” of valves and dampers, the “opening” of certain valves, the “electrical isolation” of consumers, and the “shut-off” of ignition sources. Shutdown can be automatically triggered or initiated by voluntary action.
Shutdown Valve (SDV)	Actuated fail to close valve, remotely operated by the Process Shutdown System (PSS) to isolate individual unit/equipment. <u>Note:</u> SDVs are sometimes referred to as Process Shutdown Valves (PSDV). The acronyms SDV and PSDV are considered equivalent but SDV is used in this specification because SDVs may be installed in non-process applications (Company).
Temperature Safety Valve (TSV)	Device releasing hydrocarbon trapped inside a capacity (usually a pipeline section) submitted to heat input in order to maintain pressure below design pressure (Company).
Ultimate Safety System (USS)	Optional Safety Instrumented System (SIS) designed to act in parallel with the ESD system (Company).



Uninterruptible Power Supply (UPS) System comprising battery chargers, stationary batteries and distribution panels, and supplying without interruption DC control power for switchgear, instrumentation and telecommunication systems, and/or emergency or essential services (Company).

Unit Division of the installation in a reasonable number of geographic and functional groups of equipment having the same type (hydrocarbon, pressure, inventory, ignition, etc.) and levels (high, medium, low) of risks (Company).

4. Emergency Shutdown (ESD)

4.1 ESD purposes

ESD system is here used as a generic term and consists in fact of process shutdown (SD) and emergency shutdown (ESD) functions.

4.1.1 General philosophy

A safety shutdown system consists of independent safety instrument systems at different levels: process (PSS), emergency (ESD), fire & gas (F&G) and optionally an ultimate safety system (USS), each of them consisting in a set of safety loops. In general safety loops themselves consist of field sensors (initiators), logic solvers and final elements (e.g. valves).

The ESD system is associated with other independent safety systems (e.g. PSVs, HIPS) and safeguard systems (fire fighting, escape evacuation and rescue, personnel protection systems, etc.) to reduce the industrial risk of the installation.

The main purposes of the safety shutdown system are:

- To limit the loss of containment, by isolating hydrocarbon production, processing and storage equipment,
- To protect personnel, environment and asset,
- To execute automatically a set of remedial actions, upon manual or automatic triggering,
- To prevent ignition by elimination of potential sources of ignition,
- To reduce flammable or toxic inventory by depressurisation through the EDP system, when appropriate.

4.1.2 Additional design considerations

The design of the ESD system shall take into account the needs resulting from normal operation and shall also fulfil the requirements that may arise during other possible (and likely to occur) abnormal or down-graded configurations. It is not the purpose of this General Specification to define the methodology that will be used to select relevant operating configurations. Nevertheless the following issues shall be adequately addressed when relevant:

- Tripping or stopping of an equipment or unit does **not** necessarily eliminate all sources of hazards.
- New hazards can appear as a consequence of the loss of essential utilities such as essential power, air, hydraulics, etc. These new hazards shall be identified, mitigated, and the associated risks shall be assessed.



- All operating configurations generated by the ESD system shall be safe, stable and reversible. All ESD related transitions from one operating configuration to another shall be safe.
- The ESD shall be compatible with the re-start philosophy. All operating configurations of the re-start sequence, from total black shutdown status to the full production status, shall be safe, stable and reversible. The inevitable inhibitions of the control and safety systems during the re-start sequence shall be identified, and shall be limited in number, time and duration.

4.1.3 Particular operations

Specific attention shall be paid to non-routine operating conditions and to the suitability of the ESD system, in combination with the EDP system, to deal with them. The main scenarios contemplated shall be:

- Abnormal or down-graded situations; well servicing, e.g. wireline job on a well, short-time deviation from product specification, maintenance of a safety system, etc.
- Simultaneous operations: drilling/work-over and production, construction and production, maintenance and production, etc.

Each operation shall be safe, but a specific attention shall be paid to the safety of the combination resulting from their simultaneity (example: simultaneous maintenance on two systems).

In some cases, particular operating conditions may require a different shutdown logic than that, or the combination of those, applicable under normal circumstances. For instance:

- A specific ESD logic can be activated when wireline job starts or when operators come to a not permanently manned wellhead platform.
- A temporary enhanced ESD logic can prove beneficial for simultaneous construction/major overhaul and production.
- An installation can operate under different conditions, e.g. high, medium or low pressure. Each condition may require a different ESD logic, but the differences shall be limited to process shutdowns. Emergency shutdowns shall result in the same actions independent of the condition. Before switching over between different ESD logics, the proper line-up of equipment and the status of valves need to be verified. This particular operation shall be addressed in the Safety Concept and the Operating Philosophy.

4.2 Definition of the shutdown matrix

4.2.1 Definition of shutdown levels

It is a common practice within Company to define a maximum of four typical shutdown levels with decreasing criticality, numbered 0 to 3 and affecting:

- all installations within a single restricted area (level-0) = ESD-0
- a given fire zone within the installation (level-1) = ESD-1
- a given unit within a given fire zone (level-2) = SD-2
- an individual equipment or package within a given unit (level-3) = SD-3

Level-0 and level-1 shall be called **ESD levels** because they involve either fire/gas detection in unconfined environment (hence a situation subject to possible escalation) or manual emergency action.

Level-2 and level-3 shall be called **SD levels** because they correspond either to a mere process upset or to confined fire/gas detection (sufficiently well contained) not threatening immediately the safety of the installation and of the personnel.

The safety shutdown system of an installation, consisting in a set of safety loops and devices, comprises different sub-systems organised as complementary barriers to the Process Control System, as represented in the following schematic in figure 1.

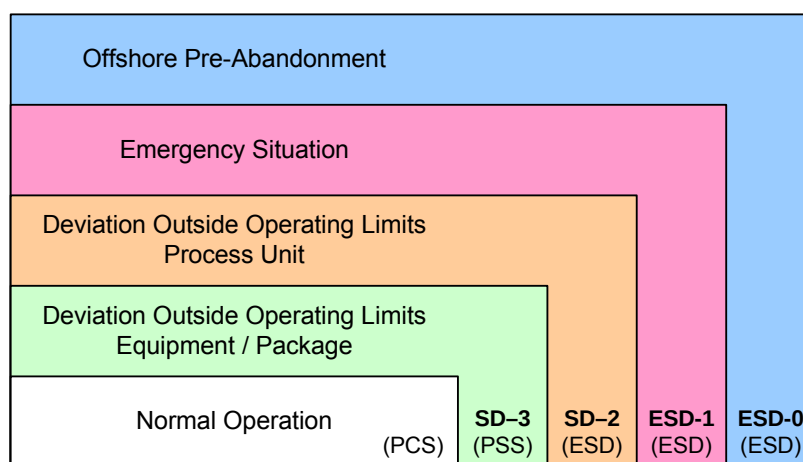


Figure 1 - Schematic of safety shutdown system operation

For each installation an ESD/SD logic shall be defined and represented in an ESD/SD logic diagram. This logic is based on the hierarchy of ESD and SD levels, the level N activating the level N+1. The ESD/SD logic diagram shows the hierarchy of ESD and SD levels, all their causes and actions in the form of a shutdown logic diagram (see also section 4.2.8).

The ESD/SD logic diagram shall cover all the installation. The causes and actions shall be described at a functional level (type and location of detection, closure/ opening of valve, tripping of equipment, etc.).

Each level is subdivided into several safety bars (up to one bar per equipment). The number of safety bars varies with the type of installation, the number of fire zones and their location, the number of independent units in each fire zone and other characteristics. Each case is specific and the following development is intended to provide guidelines and simplified examples. Reference is made to figure 2 and figure 3 with two typical shutdown logic diagrams respectively an offshore processing installation and a wellhead & riser platform with test separator.

At detailed engineering phase, each inhibit required to start-up the installation shall be clearly indicated on the safety bar diagrams for each item concerned.

Safety bars presentation can be either vertical bars or horizontal, but the presentation shall be consistent within a Company subsidiary.



4.2.2 Differences onshore/offshore

The fundamentals driving shutdown logic design are always the same, however the environment (onshore versus offshore) leads to three main differences:

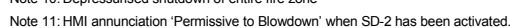
4.2.2.1 ESD-0

The ESD-0 level shall be applicable for permanently manned offshore installations, unless statutory requirements do not impose to do so and a risk assessment (size, lay-out and manning criteria) demonstrates the non-necessity of ESD-0.

In all other cases, not permanently manned offshore installations and all onshore plants (regardless of size), the number of shutdown levels may be limited to three, starting from ESD-1 level. The wordings “muster & evacuation of personnel” and “muster” denote voluntary procedures involving personnel but are not to be considered as ESD levels.

4.2.2.2 Emergency De-Pressurisation (EDP)

EDP is applicable to offshore and onshore installations if the criteria developed in section 5.1.3 are met. For all offshore installations (permanently and not permanently manned) EDP shall be (if installed) automatic upon activation of ESD-1 level. This requirement is not compulsory for onshore installations and EDP strategy shall be duly addressed in the Safety Concept.



Full document details: TOTAL GS EP SAF 261 2012