

GENERAL SPECIFICATION

Safety

GS EP SAF 261

Emergency Shutdown and Emergency Depressurisation (ESD & EDP)
--

07	07/2016	Review of §6.1.3 and §6.2.5
06	12/2015	General review
05	11/2012	Clarifications (standpipes, ESDV, EDP initial pressure, UPS)
04	01/2012	Update following the EP reorganization, March 2011
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	Purpose of the revision

Owning entity: HSEQ/SIRM	Managing entity: HSEQ/SIRM/SEM
Other Approving entity(ies):	

General Specification		GS EP SAF 261
Emergency Shutdown and Emergency Depressurisation (ESD & EDP)		
Rev.: 07	Effective date: 07/2016	Page: 2 of 45

Contents

1. Scope	4
1.1 Purpose	4
1.2 Application	4
2. Reference documents	4
3. Terminology, definitions and abbreviations	6
4. Differences onshore/offshore	11
4.1 ESD-0	11
4.2 EDP function	12
4.3 De-energising	12
5. Safety shutdown system (ESD, PSS, FGS)	12
5.1 General functional description	12
5.2 Additional design considerations	13
5.3 UPS power supply and emergency consumers	14
5.4 Definition of the shutdown matrix	14
5.5 Integration of packages	22
5.6 Cascades and response time	22
5.7 Safety valve reset philosophy	23
6. Emergency Depressurisation (EDP)	23
6.1 EDP application	23
6.2 EDP requirements	26
7. Architecture of the safety shutdown system	28
7.1 General	28
7.2 Reliability requirements	30
7.3 Transmission of signals	32
8. Shutdown devices, protection and other requirements	33
8.1 Shutdown devices	33
8.2 Physical position and protection	37
8.3 Isolations by ESDVs and SDVs	38

General Specification		GS EP SAF 261
Emergency Shutdown and Emergency Depressurisation (ESD & EDP)		
Rev.: 07	Effective date: 07/2016	Page: 3 of 45

8.4	Additional functional requirements	39
8.5	EDP system - Protection and additional requirements.....	41
Appendix 1	Typical shutdown logic diagram - Permanently manned offshore processing installation.....	42
Appendix 2	Typical shutdown logic diagram - Not Permanently manned wellhead & riser platform with test separator	43
Appendix 3	Typical shutdown logic diagram - Permanently manned onshore processing installation	44
Appendix 4	Typical safety shutdown system architecture.....	45

General Specification		GS EP SAF 261
Emergency Shutdown and Emergency Depressurisation (ESD & EDP)		
Rev.: 07	Effective date: 07/2016	Page: 4 of 45

1. Scope

1.1 Purpose

The purpose of this General Specification is to define the safety requirements for the design of the Emergency Shutdown (ESD) and Emergency Depressurisation (EDP) functions on hydrocarbon production, processing and storage installations.

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 the Fire & Gas systems (FGS) and its interfaces with the ESD system.

The Process Control System (PCS) is not part of this General Specification. It is linked to the Process Safety System (PSS), ESD and FGS systems for data acquisition, alarm handling and monitoring only.

This General Specification defines the general safety philosophy and should be read in conjunction with the following reference documents for design and implementation aspects.

2. Reference documents

The reference documents listed below form an integral part of this General Specification.

External Documents

Unless otherwise stipulated, the applicable version of these documents, including relevant appendices and supplements, is the latest revision published at the effective date of this document.

Reference	Title
API RP 14B	Design, Installation, Repair and Operation of Subsurface Safety Valve Systems
API RP 14C	Recommended Practice for Analysis, Design, Installation, and Testing of Basic Surface Safety Systems for Offshore Production Platforms

Reference	Title
API RP 14J	Recommended Practice for Design and Hazards Analysis for Offshore Production Facilities
API RP 2218	Fireproofing Practices in Petroleum and Petrochemical Processing Plants
API STD 521	Pressure-relieving and Depressuring Systems
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
ISO 13702	Petroleum and natural gas industries - Control and mitigation of fires and explosions on offshore production installations - Requirements and guidelines
NFPA 30	Flammable and Combustible Liquids Code

Total General Specifications

Unless otherwise stipulated, the applicable version of these documents, including relevant appendices and supplements, is the latest revision published.

Reference	Title
GS EP ECP 103	Process sizing criteria
GS EP ELE 001	Electrical design criteria
GS EP ELE 151	DC Uninterruptible Power Systems (UPS)
GS EP ELE 152	AC Uninterruptible Power Systems (UPS)
GS EP INS 101	Instrumentation Design
GS EP INS 106	Instrument Installation
GS EP INS 110	Instrumentation for package units
GS EP INS 134	Design and supply of integrated control and safety system
GS EP INS 137	On/Off Valve Control Panels and Actuators
GS EP INS 147	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 104	Onshore pipeline systems
GS EP PVV 142	Valves
GS EP PVV 211	Design and fabrication of pressure vessels according to ASME VIII

Reference	Title
GS EP PVV 212	Design and fabrication of pressure vessels according to BSI PD 5500
GS EP SAF 021	Layout
GS EP SAF 041	Technological risk assessment methodology
GS EP SAF 216	Area classification
GS EP SAF 222	Safety requirements for turbines, Diesel engines, gas engines and process units in sheltered or enclosed areas
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 361	SIL assignment
GS EP SAF 371	Emergency control facilities
GS EP SAF 380	Safety Engineering Requirements for an F(P)SO
GS EP SPS 002	Design of Subsea Stations
GS EP SPS 004	Subsea Valves
GS EP SPS 019	Subsea production control system
GS EP TEC 260	HIPS Design, Implementation and Life cycle
GS EP TEL 140	Public Address and General Alarm (PAGA)

3. Terminology, definitions and abbreviations

There are four types of statements in this specification: “shall”, “should”, and “may”. They shall 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 the same level of protection or performance and this shall be documented.

May Is used where alternatives are equally acceptable.

Can Is to be understood as a physical possibility.

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

Abnormal operating condition	Condition which occurs in a process equipment or unit when an operating parameter ranges outside of its normal expected operating limits.
Availability	Proportion of the total time during which a component, equipment, or system is performing in the desired manner.
Blowdown (gas)	Used as a synonym for “emergency depressurisation” (see below).
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 definition)
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. 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 from source to downstream process) or instrument-cascaded (e.g. high shutdown level triggers lower shutdown levels).
CCR	Central Control Room
Confirmed	In the context of Fire & Gas detection, means that at least two out of N sensors have detected Fire or Gas.
DHSV	Down Hole Safety Valve
Emergency Depressurisation (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. (Company definition)
Emergency Shutdown (ESD)	Control actions undertaken to shutdown equipment or processes in response to a hazardous situation. (ISO 13702)
Emergency shutdown system	Safety Instrumented System (SIS) which carries out the emergency shutdown and depressurisation functions, e.g. ESD-0 and ESD-1. (Company definition)

General Specification		GS EP SAF 261
Emergency Shutdown and Emergency Depressurisation (ESD & EDP)		
Rev.: 07	Effective date: 07/2016	Page: 8 of 45

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: (Company definition) • At the limit of a fire zone; • Within a fire zone to limit hydrocarbon inventory in isolatable sections; • At fuel distribution points to fired equipment.
Equipment	Any component or group of components specifically identified and itemized on the P&IDs.
Failure	Termination of the ability of a device or equipment item to perform a required function.
FEED	Front End Engineering and Design
Fire and Gas System (FGS)	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, active fire-fighting) at pre-determined levels. (Company definition)
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)
Flammable liquid	Is considered as flammable liquid, liquid handled above its flash point or liquid with a flash point lower than 60°C. (NFPA 30)
F(P)SO	Floating Production, Storage and Offloading unit
GOV	Gas Operated Valve
Hazardous area	A hazardous area is defined as a 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. All other areas are referred as non-hazardous areas in this context. In a hazardous area three types of zones (0,1 and 2) are recognized. (GS EP SAF 216)
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. (GS EP SAF 260)

General Specification		GS EP SAF 261
Emergency Shutdown and Emergency Depressurisation (ESD & EDP)		
Rev.: 07	Effective date: 07/2016	Page: 9 of 45

HMI	Human Machine Interface
HVAC	Heating, Ventilation and Air Conditioning
ICSS	Instrumented Control and Safety System which includes the ESD, PSS, FGS and PCS systems.
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. (GS EP SAF 021)
I/O	Inputs and Outputs
Liquid Emergency Blowdown (LEBD)	Control actions undertaken in response to a hazardous situation, to dispose of the liquid hydrocarbon inventory present in a capacity (i.e. emergency de-inventorying). (Company definition)
N.A.	Not Applicable
Not permanently manned installation	Stand-alone offshore or onshore installation on which personnel can be present, but less than 12 hours per day or less than 40 hours per week. (Company definition)
OWS	Operator Work Station
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 110)
PAGA	Public Address and General Alarm
Permanently manned installation	Installation on which people are routinely accommodated or which is continuously occupied during normal operation. (ISO 13702 and Company definition)
P&ID	Process and Instrument Diagram
PLC	Programmable Logic Controller
POB	People On Board
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.
Process Control System (PCS)	The PCS system forms part of the facility control systems. Its function is to control and monitor the process plant and utilities. It is linked to the PSS, ESD and FGS systems for data acquisition, alarm handling and monitoring only. (Company definition)
Process Safety System (PSS)	Safety Instrumented System (SIS) which carries out a process shutdown function (shutdown to a safe state of particular units or equipment, e.g. SD-2 or SD-3. (Company definition)

General Specification		GS EP SAF 261
Emergency Shutdown and Emergency Depressurisation (ESD & EDP)		
Rev.: 07	Effective date: 07/2016	Page: 10 of 45

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.
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.
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.
Restricted Area	Area within the boundaries of the installation and hence under the control of Company, affected permanently by normal operation of the facility or exceptionally by the consequences of an emergency situation caused by a major failure (GS EP SAF 253).
Risk Reduction Factor (RRF)	Reduction of failure probability provided by adding a new safety instrumented system to improve the safety of an installation (IEC 61508 and IEC 61511). This is used in order to define corresponding Safety Integrity Levels (SIL).
Safety Instrumented Function (SIF)	Safety function with a specified SIL which is necessary to achieve functional safety and which can be either a safety instrumented protection function or a safety instrumented control function. (IEC 61511)
Safety Instrumented System (SIS)	Instrumented system used to implement one or more safety instrumented functions. An SIS is composed of any combination of sensor, logic solver, and final elements. (IEC 61511) Implementation of one or more safety instrumented functions. Safety system comprising of dedicated sensors, logic solvers and final control elements for the purposes of taking a process automatically to a safe state when predetermined set points are exceeded, or when safe operating conditions are violated. The facility safety system typically includes the following SIS's: PSS, ESD, FGS, and HIPS. Each SIS is entirely independent (logic and hardware) from the PCS, and functionally independent from another SIS as to avoid any common cause failure. (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.
Safety Integrity Level (SIL)	Discrete level (one of the four) for specifying the safety integrity requirement of the SIF to be allocated to the SIS. SIL4 has the highest level of safety integrity; SIL1 has the lowest. SIL is a measure of risk reduction provided by a SIF, based on four levels. Each level represents an order of magnitude of risk reduction. Every SIF has a SIL assigned to it. (IEC 61511)
SCSSV	Surface Controlled Sub-surface Safety Valves

General Specification		GS EP SAF 261
Emergency Shutdown and Emergency Depressurisation (ESD & EDP)		
Rev.: 07	Effective date: 07/2016	Page: 11 of 45

SIMOPS

Simultaneous Operations

Shutdown (SD)

Control actions undertaken to stop operation of equipment or a process in response to deviation from normal operating conditions. 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 power consumers, and the "shut-off" of ignition sources. Shutdown can be automatically triggered or initiated by voluntary action. (Company definition)

Shutdown Valve (SDV)

Actuated fail to close valve, remotely operated by the PSS to isolate individual unit/equipment.

Note: 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 definition)

Thermal Safety Valve (TSV)

Overpressure protection device releasing liquid trapped inside a capacity and submitted to heat input (e.g. solar radiation; heat tracing, heater or heat exchanger) resulting in thermal expansion (typically a pipeline section in blocked-in conditions under solar radiation).

SSIV

Subsea Safety Isolation Valve

Uninterruptible Power Supply (UPS)

System comprising of battery chargers, stationary batteries and distribution panels, which supplies power without interruption to switchgear, instrumentation and telecommunication systems, and/or emergency or essential services. (Company definition)

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 definition)

WV

Wing Valve

4. Differences onshore/offshore

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

4.1 ESD-0

ESD-0 level shall be applicable for **permanently manned offshore installations**, unless statutory requirements do not impose to do so and a risk assessment (e.g. size criteria, lay-out criteria, 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.

4.2 EDP function

EDP function is applicable to **offshore** and **onshore** installations if the criteria developed in § 6.1.3 is met as summarized in table 1.

EDP function shall be installed for permanently manned installations and is optional when not permanently manned (e.g. asset protection criteria / to be addressed in the Safety Concept).

EDP automatic initiation (upon activation of ESD-1) is applicable to offshore installations and is optional for onshore installations.

EDP strategy shall be dully addressed in the Safety Concept.

Table 1: EDP function application summary

Manning	Offshore	Onshore
Permanently manned	• EDP function is applicable • Automatic EDP is applicable	• EDP function is applicable • Automatic EDP is optional
Not permanently manned	• EDP function is optional (e.g. asset protection criteria) • If EDP is installed, automatic EDP is applicable	

4.3 De-energising

De-energising including battery powered systems, but with the exception of emergency devices (emergency lighting, navigation aids, etc.) shall be achieved on permanently manned offshore installation through activation of ESD-0.

Onshore this functionality does not have to exist and shall then be compensated by the implementation of a specific push button for each fire zone that shall perform total de-energising, including UPS powered equipment.

Possible exception (onshore and offshore) is for emergency post-lube pumps, machinery helper, etc. and only if they are suitable for operation in Zone 1 hazardous area.

5. Safety shutdown system (ESD, PSS, FGS)

5.1 General functional description

The following SIS's shall be provided on all installations used for the development and the treatment and storage of hydrocarbons: process (**PSS**), emergency (**ESD**), fire & gas (**FGS**). Each of them consists of a set of SIF's.

In general, SIF's themselves comprise field sensors (initiators), logic solvers and final elements (e.g. valves, circuit breakers).

All SIF's shall be independent from PCS.

Emergency Shutdown System (ESD):

The ESD system forms part of the facility's safety systems. Its prime function is to shutdown the facilities to a safe state in case of an emergency situation, thus protecting personnel, the environment and the asset. It shall carry out the emergency shutdown and depressurisation functions of the facility (e.g. ESD-0; ESD-1) according to the defined safety philosophy.

General Specification		GS EP SAF 261
Emergency Shutdown and Emergency Depressurisation (ESD & EDP)		
Rev.: 07	Effective date: 07/2016	Page: 13 of 45

Once initiated, all actions required by the ESD system shall occur automatically.

The ESD system shall provide adequate information at the control room so that operators have all the information required to manage an emergency situation.

Push buttons for ESD actuation shall be located at strategic locations (See [GS EP SAF 371](#)) and upon installation specifics to be addressed in Operating philosophy and Safety Concept. They shall be readily accessible and protected against unintentional/accidental initiation.

Process Safety System (PSS):

The PSS system forms part of the facility's safety systems. Its prime function is to automatically carry out the safe shutdown of particular units or equipment (e.g. SD-2; SD-3).

Fire & Gas System (FGS):

The FGS system forms part of the facility's safety systems. Its prime function is to mitigate the consequences of a fire and/or gas releases to protect personnel, the environment and the asset. The FGS system continuously monitors the facilities and initiates the active fire fighting means or the PAGA system (see [GS EP TEL 140](#)).

Note: Refer to [GS EP SPS 019](#) for design requirements of Subsea Production Control System (SPCS) and associated interfaces with topside ICSS.

5.2 Additional design considerations

The design of the ESD and PSS systems 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 downgraded configurations. It is not the purpose of this General Specification to define the methodology 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.
- 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 and PSS systems shall be safe, stable and reversible. All ESD and PSS related transitions from one operating configuration to another shall be safe.
- The ESD and PSS systems 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.
- Specific attention shall be paid to non-routine operating conditions (e.g. SIMOPS, downgraded situations, well servicing, maintenance of a safety system, etc.) and to the suitability of the ESD and PSS systems design, in combination with the EDP system, to deal with them. These specific operating conditions shall be addressed in the Project Operating philosophy and the Safety Concept.

General Specification		GS EP SAF 261
Emergency Shutdown and Emergency Depressurisation (ESD & EDP)		
Rev.: 07	Effective date: 07/2016	Page: 14 of 45

5.3 UPS power supply and emergency consumers

ESD, PSS, FGS systems (as part of the ICSS system) shall have redundant and independent UPS power supplies.

Multiple UPS architecture shall be as such to minimise the risk of common mode of failure.

Reference is made to **GS EP ELE 001** for typical minimum UPS autonomy.

Required UPS autonomy is to be studied on the case by case basis upon installation specifics (e.g. installation manning criteria, installation size criteria, phased depressurisation constraints if any, etc.).

Reference is made to **GS EP ELE 151** and **GS EP ELE 152** for UPS design requirements.

The following typical emergency consumers on battery systems include, but not limited to (to be defined on the case by case basis upon installation specifics):

- Controls consumers: ESD, PSS, FGS systems.
- Emergency consumers: PAGA, emergency telecoms, post-lube pumps (where relevant), fire fighting.
- Vital consumers (on individual batteries suitable for Zone1): Emergency lighting and escape signs, navigation aids.

5.4 Definition of the shutdown matrix

5.4.1 Definition of shutdown levels

It is Company common practice 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 are called **ESD levels** because they involve either loss of containment in unconfined environment (hence a situation subject to possible escalation), fire & gas detection or manual emergency action.

Level-2 and level-3 are called **SD levels** because they correspond either to a significant process upset or to confined fire/gas detection (e.g. gas turbine package), not threatening immediately the safety of the installation/ personnel.

The safety shutdown system of an installation is organized in different sub-systems which complement the PCS, as represented in figure 1.