Chapter 11

Emergency Shutdown

Emergency shutdown capability is to be provided all petroleum facilities be it manual, remotely operated or automatic. Inherent safety practices rely on emergency shutdown capability as a prime facet in achieving a low risk facility. Without adequate shutdown capabilities a facility cannot be controlled during a major incident.

Definition and Objective

An Emergency Shutdown (ESD) system is a method to rapidly cease the operation of the process and isolate it from incoming or going connections or flows to reduce the likelihood of an unwanted event from occurring, continuing, or escalating. The aim of an ESD system is to protect personnel, afford protection to the facility, and prevention of an environmental impact from a process event.

Design Philosophy

The ESD system is distinguished from other facility safety systems in that it responds to a hazard situation which may affect the overall safety of the entire facility. It is therefore considered one of the prime safety systems that can be provided for any facility. Without an ESD system, an incident at a hydrocarbon facility may be provided with "unlimited" fuel supplies that can destroy the entire facility. Such situations are amply demonstrated by wellhead blowouts that can be fed from underground reservoirs and destruction of pipeline connections at offshore installations affecting the availability of further isolation means, e.g., "Piper Alpha".

Facilities that do not have the capability to immediately provide an emergency shutdown should be considered high risks. Similarly, if the reliability of an ESD system is very poor the facility might be considered without adequate protection and therefore also a high risk.

Activation Mechanisms

Most ESD systems are designed so that several mechanisms can initiate a facility shutdown. These mechanisms are provided by both manual and automatic means.
Typically they may include the following:

- Manual activation from a main facility control point.
- Manual activation from strategically located initiation stations within the facility.
- Automatic activation from fire or gas detection systems.
- Automatic activation from process instrumentation set points.

**Levels of Shutdown**

The activation logic for an ESD system should be kept as simple at possible. Typically most facilities specify plateaus or levels of ESD activation. These levels activate emergency measures for increasing amounts or areas of the facility as the emergency involves a larger and larger area or the degree of hazard from the initial event. Low hazards or small area involvement would only require a shutdown of individual equipment while major incidents would require a facility shutdown. The shutdown of one of a facility should not present a hazard to another portion of the facility otherwise both should be shut down. Typical levels utilized in the petroleum and related industries are identified in Table 12.

<table>
<thead>
<tr>
<th>ESD Level</th>
<th>Action</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Total Facility Shutdown</td>
<td>Catastrophic</td>
</tr>
<tr>
<td>2</td>
<td>Unit or Plant Shutdown</td>
<td>Severe</td>
</tr>
<tr>
<td>3</td>
<td>Equipment Shutdown</td>
<td>Major</td>
</tr>
<tr>
<td>4</td>
<td>Equipment Protective System Shutdown</td>
<td>Slight</td>
</tr>
<tr>
<td>5</td>
<td>Non-ESD Process and Control Alarms</td>
<td>Routine</td>
</tr>
</tbody>
</table>

**Table 12**

**Typical ESD Levels**

**Reliability and Fail Safe Logic**

The design of an ESD system has normally been based on independence and fail-safe component utilization. Independence is obtained by physical separation, using separate process locations, impulse lines, instruments, logic devices, and wiring than that of the BPCS. This avoids common failures in the system. Fail safe features are obtained by ensuring that selected components in an ESD system are such that during a failure of a component the process reverts to a condition considered "safe". Safe implies that the process or facility is not vulnerable to a catastrophic destructive event due to the release of hydrocarbons. For most facilities this implies that pipelines that could supply fuel to the incident (i.e., incoming and outgoing) are shut off and that high pressure, high volume gas supplies that are located in the incident are relieved to a remote disposal system.

ESD system performance is measured in terms of reliability and availability. Reliability is the probability a component or system will perform its logic function under stated operating conditions for a defined time period. Availability is the probability or mean fraction of total time that a protective component or system is able to function on demand. Increased reliability does not necessarily increase availability.

Reliability is a function the system failure rate or its reciprocal, mean time between failures (MTBF). The system failure rate in non-redundant systems is numerically equal to the sum of component failure rates.
Failures can either be fail-safe or fail dangerously. Fail safe incidents may be initiated by spurious trips that may result in accidental shutdown of equipment or processes. Fail dangerously incidents are initiated by undetected process design errors or operations, which disable the safety interlock. The fail dangerously activation may also result in accidental process liquid or gas releases, equipment damage, or fire and explosions.

ESD systems should be designed to be sufficiently reliable and fail safe that a (1) accidental initiation of the ESD is reduced to acceptable low levels or as low as reasonably practical, (2) availability is maximized as a function of the frequency of system testing and maintenance, and (3) the fractional MTBF of the system is sufficiently large to reduce the hazard rate to an acceptable level, consistent with the demand rate of the system.

Fail safe logic is normally referred to as de-energized to trip logic, since any impact to the inputs, outputs, wiring, utility supplies or component function should de-energize the final output allowing the safety device to revert to its fail safe mode. The specification of fail safe for valves can be accomplished by failing close (FC), failing open (FO) or failing steady (FS), i.e., in the last position depending on the service the valve is intended to perform. Valves that are specified to fail close on air or power failure should be provided with spring return actuators. The use of accumulators to meet control valve fail safe conditions should be avoided since these are less reliable fail safe mechanism and are more vulnerable to external impacts of an incident. Control mechanisms including power, air or hydraulic supplies to valves emergency valves (isolation, blowdown, depressuring, etc.) should be fireproofed if the valves are required to be operable during a fire situation.

For ESD isolation valves (i.e., EIVs) a fail safe mode is normally defined as fail closed in order to prevent the continued flow of fuel to the incident. Blowdown or depressurization valves would be specified as fail open to allow inventories to be disposed of during an incident. Special circumstances may require the use of a fail steady valve for operational or performance reasons. These applications are usually at isolation valves at components, i.e., individual vessels, pumps, etc., where a backup EIV is provided at the battery limits that is specified as fail closed. The fail safe mode can be defined by the action that is taken when the ESD system is activated. Since the function of the ESD system is to place the facility in its safest mode, by definition the ESD activation mode is the fail safe mode.

The utilization of a fail steady - fail safe mode may allow an undetected failure to occur unless additional instrumentation is provided on the ESD system components or unless the system is constantly fully function tested. The prime feature of a full fail close or fail open failure mode is that it will immediately indicate if the component is functioning properly.

The different safety integrity levels normally applied within the petroleum and related industries are usually the following:

<table>
<thead>
<tr>
<th>SIL</th>
<th>AVAILABILITY</th>
<th>RISK REDUCTION FACTOR (RRF)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>BPCS - Inherent</td>
<td>None</td>
</tr>
<tr>
<td>1</td>
<td>90 - 99%</td>
<td>10 - 100</td>
</tr>
<tr>
<td>2</td>
<td>99 - 99.9%</td>
<td>100 - 1,000</td>
</tr>
<tr>
<td>3</td>
<td>99.9 - 99.99%</td>
<td>1,000 - 10,000</td>
</tr>
<tr>
<td>4</td>
<td>99.99 - 99.999%</td>
<td>10,000 - 100,000</td>
</tr>
</tbody>
</table>

Table 13
Typical Safety Integrity Levels (SIL)
Generally by increasing the independent layers of protection (IPLs), which are applied to a potential hazardous event, the SIL number can be reduced. It should be noted that a SIL Level of 4 is seldom used in the petroleum or related industries but is common throughout the avionics, aerospace and nuclear industries.

Safety Integrity level one equates to a simple non redundant single path design, designed to fail safe with a typical availability of 0.99. Level two involves a partially redundant logic structure, with redundant independent paths for elements with lower availability. Overall availability is in the range of 0.999. Level three is composed of a totally redundant logic structure. Redundant, independent circuits are used for the total interlock system. Diversity is considered an important factor and used where appropriate. Fault tolerance is enhanced since a single fault of an ESD system component is unlikely to result in a loss of process protection.

ESD/DCS Interfaces

Where ESD and DCS systems are provided, they should be functionally segregated such that failure of the DCS does not prevent the ESD from shutting down and isolating the facilities. Alternatively, failure of the ESD system should not prevent an operator from using the DCS to shut down and isolate the facility. There should be no executable commands over the ESD-DCS communications links. Communication links should only be used for bypasses, status information and the transmission of reports. Confirmation of ESD reset actions can be incorporated into the DCS but actual reset capability should not.

Activation Points

The activation points for ESD systems should be systematically arranged to provide the optimum availability and afford adequate protection to the facility. The following guidelines provide some features that should be considered.

- The activation points should be located a minimum of 8 meters (25 ft.) away from a high process hazard location but not more than 5 minutes away from any location within the facility. 5 minutes is taken as the maximum allowable time since historical evidence indicates process vessel rupture may occur after this time period from flame impingement. If risk analysis calculations demonstrate longer vessel rupture periods are expected, longer time periods may be acceptable.

- The chosen locations should be preferably upwind from the protected hazard. Downwind sites may be affected by heat, smoke or toxic gases.

- They should be located in the path of normal and emergency evacuation routes from the immediate area. In an panic situation personnel may immediately evacuate and not activate emergency controls if they are located at inconvenient locations.

- Locating sites furthest from the sources of largest liquid holdups or highly probable leakage sources (i.e., the relatively higher hazards) is preferred.

- They should be located near other emergency devices that may need immediate activation in an emergency (i.e., fire water monitors, manual blowdown valves, etc.).

- The main access into the affected area should not be not impaired. Location of activation points
in normal vehicle or maintenance access routes will affect operations and cause the device to be eventually relocated or damaged.

- The activation point should be mounted at a height which is convenient to personnel. The ergonomics of personnel access to emergency controls should be accommodated.

- Manned control rooms should always be provided with hardwired ESD activation points located on the main control console easily accessible to the operators.

**Activation Hardware Features**

The hardwired ESD activation means is usually a push in knob or button. Confirmed action of the push button should be always be required to manually activate the ESD system in order to prevent accidental activations. Most commonly a protective cover is fitted over any of the push button or manual activation devices. All devices should only be manually resettable.

Each activation point should be labeled to area of coverage and provided with and identification as to which valves it operates or equipment it shutdowns. A specific identifier number should be assigned to each device. The location itself should be highly visible, preferably highlighted in contrasting colors to normal equipment housings.

In some instances it may be beneficial to maintain process inventories of certain process vessels until the incident is actually threatening the container. The inventory of the vessel may be crucial to the restart of a facility or the contents may be highly valuable. Loss of the inventory may be criticized if frequent false trips of the ESD blowdown system occur. In these cases an automatic fusible plug blowdown valve could be installed which would only activate from the heat of a real fire incident. In this way, a false disposal of the inventory can be avoided.

**Isolation Valve Requirements**

The failure mode of ESDVs for gas processing areas should always fail in the closed position, since this is the only mechanism to resolve gas fed fires or prevent explosive vapor buildups. The valves should be provided with an automatic fail close device such as an actuator with spring return specification.

ESD valves should lock in the fail safe mode once activated and be manually reset once it has been confirmed the emergency has passed or has been resolved.

The emergency isolation devices should be arranged so that they can be fully function tested without affecting the process operation. This entails that a full flow bypass should be installed at each emergency isolation valve. These bypass installations should be locked closed when not in service for functional testing the ESDV.

Where MOV or AOVs are selected as ESDVs they should as a minimum have a back up activation power sources and the utility service lines should be highly reliable and protected against an incident. It should be noted that full motor operated and air operated ESDV do not fully equate to a fail safe spring return valve, even if frequent functional testing is performed. The reliability of an internal spring return actuator is considered higher than a self contained MOV or AOV with its own local power source and protection of cabling. This is because that additional components of a MOV or AOV contribute to additional failure points and will also have a higher level of vulnerability from external events that the internal spring mechanism inherently contains.
Emergency Isolation Valves (EIV)

Emergency isolation valves (EIV) should be located based on two principals (1) the amount of isolatable inventory that is desired and (2) protection of the EIV from the affects of external events. EIV valves are normally required to have a fire-safe rating (i.e. minimal leakage and operability capability, Ref. Table 14). Valves and their actuating mechanisms should be afforded adequate protection when they are required to be located in an area that has potential to experience explosion and fire incidents.

Subsea Isolation Valves (SSIV)

Subsea pipeline emergency isolation valves for offshore facilities are provided where a risk analysis indicated topside isolation may be considered vulnerable. They should be protected from ship impacts, anchor dragging, flammable liquid spills and heavy objects that may be dropped from the offshore facility.

Protection Requirements

ESD system components that are located in areas that would be considered direct fire exposures, i.e. within or above fire hazardous risk areas should be provided fire protection measures to ensure integrity during ESD operation and the duration of the major efforts to control the emergency.

- Valve Actuating Mechanisms: 15-20 minutes H rating (H15 or H20, plus blast if applicable)
- Directly Exposed Valves: 60-120 minutes H rating (H60 or H120, plus blast if applicable)

Actuating mechanisms include control panels, air receivers, valve actuators, instrumentation controls or tubing, etc.
<table>
<thead>
<tr>
<th>Test Specification</th>
<th>API Std 607 3rd Edition</th>
<th>FM 6033 1981</th>
<th>OCMA FSV.1</th>
<th>Exxon Corp. BP3-14-1</th>
<th>Exxon Corp. BP3-14-1-2A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stem Position</td>
<td>Horizontal</td>
<td>Vertical</td>
<td>Vertical</td>
<td>Vertical</td>
<td>Vertical</td>
</tr>
<tr>
<td>Bore Position</td>
<td>Horizontal</td>
<td>Horizontal</td>
<td>Horizontal</td>
<td>Horizontal</td>
<td>Horizontal</td>
</tr>
<tr>
<td>Valve Setting</td>
<td>Closed</td>
<td>Closed</td>
<td>Open</td>
<td>Open</td>
<td>Open</td>
</tr>
<tr>
<td>Test Pressure During Fire</td>
<td>Approximately 75% ANSI rating</td>
<td>Rated Pressure</td>
<td>207 kPa (30 psi)</td>
<td>172 kPa (25 psi)</td>
<td>172 kPa (25 psi)</td>
</tr>
<tr>
<td>Test Medium</td>
<td>Water</td>
<td>Water</td>
<td>Diesel or Kerosene</td>
<td>Liquid Hydrocarbon</td>
<td>Liquid Hydrocarbon</td>
</tr>
<tr>
<td>Valve Body Temperature</td>
<td>705 °C (1300 °F) (Flame)</td>
<td>Not Mentioned</td>
<td>Able to destroy the soft seat</td>
<td>Minimum 650 °C (1200 °F)</td>
<td>Minimum 650 °C (1200 °F)</td>
</tr>
<tr>
<td>Fire Duration</td>
<td>30 Minutes (Flame)</td>
<td>15 Minutes</td>
<td>15 Minutes</td>
<td>15 Minutes at 1200 °F</td>
<td>15 Minutes at 1200 °F</td>
</tr>
<tr>
<td>When Valve Seat Leakage Measured</td>
<td>During and After Test</td>
<td>During Test</td>
<td>After Test</td>
<td>After Test</td>
<td>After Test</td>
</tr>
<tr>
<td>Maximum External Leakage</td>
<td>100 ml per NPS valve size/minute over total test period</td>
<td>Individual Drops</td>
<td>No Appreciable Leakage</td>
<td>Leakage Negligible</td>
<td>Leakage Negligible</td>
</tr>
<tr>
<td>Operation Requirements</td>
<td>1 Cycle Open to Closed</td>
<td>Must Operate</td>
<td>3 Cycles Open to Closed</td>
<td>3 Cycles Open to Closed</td>
<td>3 Cycles Open to Closed</td>
</tr>
<tr>
<td>Maximum Valve Seat Leakage Allowed</td>
<td>400 ml per NPS pipe size/min. over total fire test period</td>
<td>95 cc/min (1 qt./min.)</td>
<td>10 ml/min/in dia.</td>
<td>10 ml/min/in dia.</td>
<td>20 ml/min/in dia.</td>
</tr>
</tbody>
</table>

Table 14

Firesafe Valve Test Standards
System Interactions

Petroleum facilities exist where the operators are hesitant to activate the ESD system for fear of rupturing the incoming production pipelines due to their poor construction. This points out the fact that all mechanisms that introduce a change to the normal operating configuration of the system must be analyzed to determine what effect the proposed actions will produce. Whenever an ESD isolation valve is closed it will stop incoming or outgoing flows which may produce instantaneous pressure variations that can detrimentally affect the process system. An analysis of measures to prevent additional consequences should be undertaken where such effects are possible, such as slower valve closing times, increased integrity of piping systems, etc.
Bibliography


