Return to Session Directory

DYNAMIC POSITIONING CONFERENCE

October 13-14, 2009

Risk

ESD in a DP Vessel - For Safety, not for Blackout

Gilberto Beduhn Machado
Petrobras, Brazil

1- Abstract

The ESD - Emergency Shutdown or AVS - Abandon Vessel Shutdown system is installed on vessels with the aim to minimize the consequences of emergency situations. It is a Class Society requirement for any vessel regardless its application. However, for DP vessels there are no special rules and this can direct to a dangerous situation. Reliability of the DP system relies on avoidance of spurious operation of the ESD System, whereas reliability of the ESD System requires that it operates correctly when required to.

An ESD, after a fire emergency situation, for instance, will make the scenario even worse as the crew will face a critical situation with no power available. According to the specifications, the ESD levels begin from a single engine shutdown to a complete shutdown of the vessel. Because of that, an intentional activation, which can cause a blackout, must be highly restricted to authorized personnel and should be done only when no other solution can be taken. For other levels of minor importance, a mechanical protection that avoids an inadvertent actuation should be enough.

This paper intends to bring the subject ESD into view for specialist's discussion. Also, it wants to propose some alternatives to its application on DP vessels for they present characteristics that are considered critical and, for that reason and for that matter, should receive a different treatment from MODU and the Classification Societies.

2- ESD - Definition

A rig, DP or moored, is fitted with Emergency Shutdown and Fire & Gas (ESD/F & G) system. The reasons to use the ESD devices can be, for instance, a major gas emergency that forces the vessel to be abandoned. The consequence in a DP vessel is, for sure, an uncontrolled drifting after a total blackout.

The systems are interfaced to each other, the F & G system is used to detect gas leakage and fire, activating alarms and the ESD system activates the equipment shutdowns. The basic design intention is to have a system as simple and easy to understand and operate as possible.

The ESD system is primarily a manually operated system requiring an operator to activate the system. This activation will cause a procedure to commence or be progressed ultimately leading to automatic shutdown of operations or a group of equipment selected. The ESD system has, in general, three levels of shutdown, as follows:

- Level 0: Abandon Vessel Shutdown (total shutdown of the vessel with the exception of the emergency support systems)
- Level I: Topside Shutdown (main generators, main switchboard circuit incomers, sequential shutdown of all control systems excluding emergency support systems and safety systems)
- Level II: The lowest of the shutdowns levels, sub-divided into individual manual shutdowns of generator room and thruster room)

3- Related Rules and Standard

- IMO MODU Code

Item 4.12 below describes exactly what are the differences between a DP MODU and a Anchored MODU. By reading the text we find there are none. That is the main point Petrobras - DPPS wants to highlight on this paper: there are significant differences between the two units, not only regarding to the need of power to control the vessel and keep position because of the well control efforts but also after the ESD being activated the time spent to restore power – not

less than 45' – is too long for a DP MODU, especially in crowded areas where the risk of collision is present.

4.12 Dynamic positioning systems

Dynamic positioning systems used as a sole means of position keeping should provide a level of safety equivalent to that provided for anchoring arrangements. (emphasis added)

The Code on its Chapter 6, "*Machinery and electrical installations in hazardous areas* ***for all types of units***" (emphasis added), divides the hazardous areas into zones as follows:

- Zone 0: in which an explosive gas/air mixture is continuously present or present for long periods.
- Zone 1: in which an explosive gas/air mixture is likely to occur in normal operation.
- Zone 2: in which an explosive gas/air mixture is not likely to occur, or in which such a mixture, if it does occur, will only exist for a short time.

Defined these areas, the Code describes the arrangements for venting those areas and then, on its item 6.5 "Emergency conditions due to drilling operations" it specifies which equipments and systems should be disconnected or shut down (*see below*). Again, there is no specific reference to DP MODUs.

6.5 Emergency conditions due to drilling operations

6.5.1 In view of exceptional conditions in which the explosion hazard may extend outside the above-mentioned zones, special arrangements should be provided to facilitate the selective disconnection or shutdown of:

.1 ventilation systems, except fans necessary for supplying combustion air to prime movers for the production of electrical power;

.2 main generator prime movers, including the ventilation systems for these;

.3 emergency generator prime movers.

6.5.2 Disconnection or shutdown should be possible from at least two strategic locations, one of which should be outside hazardous areas.

6.5.3 Shutdown systems that are provided to comply with 6.5.1 should be so designed that the risk of unintentional stoppages caused by malfunction in a shutdown system and the risk of inadvertent operation of a shutdown are minimized.

6.5.4 Equipment which is located in spaces other than enclosed spaces and which is capable of operation after shutdown as given in 6.5.1 should be suitable for installation in zone 2 locations. Such equipment which is located in enclosed spaces should be suitable for its intended application to the satisfaction of the Administration. At least the following facilities should be operable after an emergency shutdown:

- emergency lighting required by 5.3.6.1.1 to 5.3.6.1.4 for half an hour;
- blow-out preventer control system;
- general alarm system;
- public address system; and
- battery-supplied radiocommunication installations.

- IMCA

The IMCA M 196 guideline refers to the ESD Requirements applicable to UPSs in mobile offshore units, which demands to shut down the UPSs for abandoning the vessel. It

mentions, however, that there are exceptions for mobile offshore drilling units to comply with IMO MODU-Code, section 6.5 in which the UPSs must remain operable and capable to supply sufficient power allowing the vessel to be 'black started' without the main power supply. The guideline reminds that there are UPSs which were not designed to do that. Also, the UPSs shall be supplied with a means to disconnect the UPS batteries remotely.

No specific tests as part of the annual trials program are mentioned on the guidelines.

- Classification Societies

A vessel either meets the relevant class society's rules or it does not. As a consequence it is either 'in' or 'out' of 'class'. Classification societies do issue statements or certifications that a vessel is in compliance with the required codes. This is in part related to legal liability of the classification society.

However, each of the classification societies has developed a series of notations that may be granted to a vessel to indicate that it is in compliance with some additional criteria that may be either specific to that vessel type or that are in excess of the standard classification requirements. As reference of those rules applicable to MODUs, three of those Classification societies are being quoted below:

DNV

Det Norske Veritas rules are very extensive and present separate sections on its OS-A101. Section 5 defines the ESD principles while Section 8 presents specific items for MODUs. Below, some highlights of these rules:

Section 5
Emergency Shutdown (ESD) Principles

A101 The provisions of this section aim to ensure that shutdown systems are provided as suitable and effective to safeguard personnel and plant against hazardous events on the unit or installation.

A201 These requirements shall be applied to all offshore units or installations having direct operational contact with hydrocarbons.

A301 An emergency shutdown system comprises:

— manual input devices (push buttons)

— interfaces towards other safety systems, as e.g.:

- — fire detection system
- — gas detection system
- — alarm and communication systems
- — process shutdown system
- — drilling and well control system
- — fire fighting systems
- — ventilation systems

A401 The ESD system shall be designed so that the risk of unintentional shutdown caused by malfunction or inadvertent operation is minimised.

B101 The philosophy shall comprise functional requirements for the safety systems upon detection of an abnormal condition.

The fail-safe functionality for the safety systems shall be included.

B102 The philosophy document shall indicate actions to:

— limit the duration and severity of the incident

— protect personnel exposed to the incident

— limit environmental impact

— facilitate escape, muster and evacuation, as necessary.

B103 Inter-relationships and requirements for the following systems shall be addressed:

— emergency shutdown system
— fire and gas detection system
— process shutdown system
— drilling and well control systems
— alarm and communication systems
— active fire fighting systems
— ventilation systems
— energy sources and associated utilities required to drive essential and emergency functions.

D101 Shutdown shall be executed in a pre-determined, logical manner to meet the objectives defined in Sec.5 B *(*items B101-B103 above)*. Definition of the logic and required response time shall include consideration of interactions between systems and dynamic effects, e.g. for process plant.

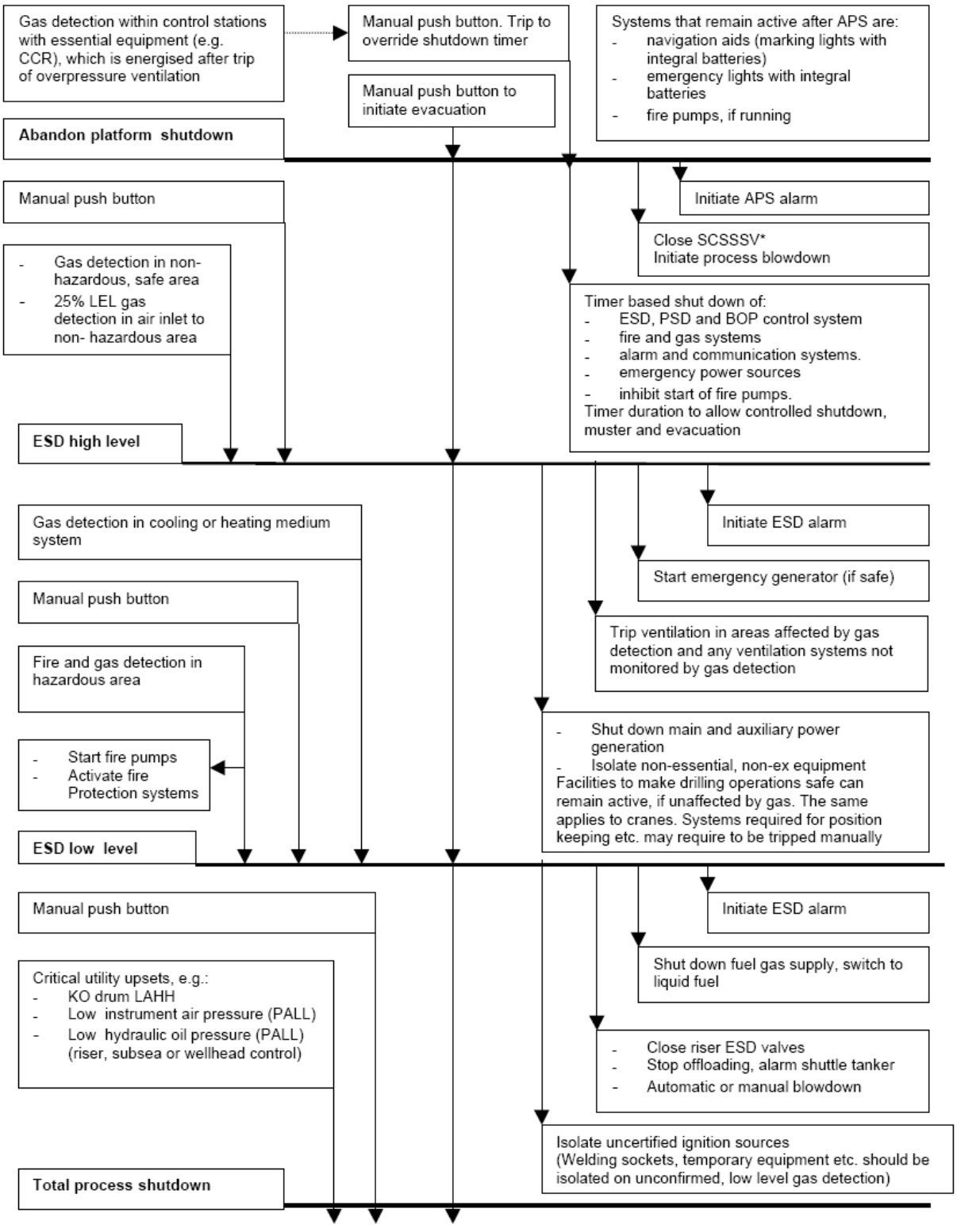
D102 A *shutdown logic* shall be implemented to determine the response to different degrees of emergency or upset condition. The shutdown logic should be as simple as possible. The shutdown logic given in the figure below shall be applied as a basis with additional due recognition of installation specific requirements.

D104 Shutdown shall not result in adverse cascade effects, which depend on activation of other protection devices to maintain a plant in a safe condition. The shutdown system shall be designed to ensure that any ongoing operations can be terminated safely when a shutdown is activated.

E101 Shutdowns shall normally be automatically initiated, however solely manually initiated actions may be provided where automatic action could be detrimental to safety, e.g. during drilling and dynamic positioning.

E103 In all shutdown systems, it shall be possible to manually activate all levels of shutdown at the main control station.

**remarked by the author*



*Surface controlled sub sea shutdown valve

Shutdown logic

Table E1 Location of push buttons for manual shutdown	
Shutdown level	*Location of push-button*
Abandon platform (APS)	— main and emergency control rooms — muster stations, lifeboat stations and helicopter deck — bridge connections between platforms
Emergency shut-down (ESD)	As for APS, plus: — process control room — driller's control cabin — exits from process, drilling, wellhead, riser areas etc. — along main escape routes
Process shutdown (PSD)	— main control room — process control room — exits from process, drilling, wellhead, riser areas etc. — along main escape routes
Manually activat-ed call point (MAC)	Readily available for use in all normally manned areas
It may be appropriate to limit the number of field installed pushbuttons for lower level trips (e.g. for PSD) in order to avoid confusion about their use.	

Section 8
Special Provisions for Drilling Units

E. Shutdown

E 100 General

101 International requirements for a simplified shutdown hierarchy may be applied on agreement between yard and owner. The principles of Sec.5 D remain applicable for areas that are vulnerable to an emergency originating from plant for well testing.

102 At least two emergency control stations shall be provided. One of the stations is to be located near the drilling console and the second station is to be at a suitable manned location outside the hazardous areas.

103 The control stations are to be provided with:

— manually operated contact makers for actuating the general alarm system.

— an efficient means of communication between these stations and all manned locations vital to the safety of the vessel.

— emergency shutdown facilities.

- **ABS**

7 Systems Associated with Drilling Operations

7.1 Emergency Shutdowns Facilities

7.1.1 Shutdowns Arrangements

Arrangements are to be provided for the disconnection or shutdown, either selectively or simultaneously, of all electrical equipment and devices, including the

emergency generator, except for the services listed under *4-3-5 / 7.1.2 from the emergency control station (see 5-3-1/7). Initiating of the above shut-downs may vary according to the nature of the emergency. A recommended sequence of shut-downs is to be provided in the unit's operating manual.

7.1.2 Operation After Shutdown

The following services are to be operable after emergency shutdown:

i) Emergency lighting required by 4-3-2/5.3.1 for half an hour
ii) General alarm
iii) Blow-out preventer control system
iv) Public address system
v) Distress and safety communications

All equipment in exterior locations which is capable of operation after shutdown is to be suitable for installation in Zone 2 locations.

** Part 4 – Machinery and Systems, Chapter 3 – Electrical Installations, section 5 – Specialized Installations; Item 7 – Systems Associated with drilling operations, sub-item 7.1.2 – Operation after Shutdown*

- **Lloyds Register**

SECTION 7

Emergency shutdown (ESD) systems

7.1 General

7.1.1 An ESD system is to be provided when any process presents a hazard which could affect the safety of personnel, the overall safety of the unit or the pollution of the environment. The system is to satisfy the requirements of 7.1.2 to 7.1.11.

7.1.2 The ESD system is to operate in association with those items of plant defined in Pt 6, Ch 1,1.2.3, as applicable, and is to incorporate levels of shutdown appropriate to the degree of hazard to personnel, the unit and the environment. The arrangements are to be derived using hazard analysis techniques.

7.1.3 The operation of the ESD system is to be initiated manually. In addition, operation is also to be initiated automatically by signals derived from the fire and gas detection system and signals derived from process and other equipment sensors. The shutdown of drilling equipment, required to make the installation safe, is only to be initiated manually.

7.1.4 Manual ESD actuation points for complete shutdown of the installations are to be provided at the main control station and other suitable locations, e.g. at the helicopter deck and the emergency evacuation stations.

7.1.5 Each manual ESD actuation point on the installation is to be clearly identified.

7.1.6 The ESD system is to be arranged with automatic changeover to a standby power supply in the event of failure of the normal power supply.

7.1.7 Failure of any power supply to the ESD system is to operate an audible and visual alarm.

7.1.8 The characteristic of the failure to safety operation for plant and equipment is the automatic reversion to the least hazardous condition upon failure of protective system, logic, sensors, actuators or power source. This requirement is normally realized by employing a de-energize to trip design. Special consideration is given to subsea christmas tree solenoid valves which are not normally energized.

7.1.9 Hydrocarbon related components are to be equipped with at least two independent levels of safety protection to prevent or minimize the effects of an equipment failure within the

process. Where provision of two diverse means of protection cannot be achieved, special consideration must be given to the design of the alternative means.

7.1.10 High level ESD is to be provided with local reset of each final element. Elements effected by low level ESD may be reset by means of a remote manual group reset operation from the central control room.

7.1.11 Software input inhibits and output overrides may be used for maintenance purposes. However, this method of applying inhibits and overrides must be restricted to some of the fire and gas systems and low level of shutdown functions only. Physical key switches are to be used for applying inhibits and overrides for high level, safety critical shutdown system.

7.1.12 Start-up overrides may be applicable to low trips during plant start-up. These overrides are to be cancelled automatically once the normal process condition has been reached or for a fixed period of time has expired.

7.1.13 Where arrangements are provided for overriding parts of an ESD system they should be such that inadvertent operation is prevented. Visual indication is to be given at the main control point when an override is operated.

7.1.14 Accumulators for pneumatic and hydraulic systems are to have sufficient capacity to perform one complete shutdown followed by reset capabilities without the need for recharging the accumulator.

7.1.15 Where ESD applications are to be implemented by programmable electronic instruments, a qualitative riskbased approach to the specification and design of these systems is to be adopted. Each measure to control or mitigate hazards is to be assigned an appropriate degree of risk reduction which contributes to the overall risk reduction. The risk reduction figure is to be translated into performance standards for each measure which will be specified in terms of functionality, safety integrity and survivability, *see* Pt 6, Ch 1,2.11.

7.1.16 The implementation of a programmable electronic system to perform high safety integrity level functions is not recommended. These functions are to be realised by simplistic and deterministic logic components which have high availability characteristics. Status, diagnostic and alarm information exchange executed by read-only soft links to remote digital systems for display purposes may be provided, as applicable, in addition to a matrix panel, *see* Pt 6 Ch 1, 2.11.8.

7.1.17 Mixing low safety integrity loops with high integrity level functions is to be avoided. The effect of this may lower the overall integrity of the protective system.

4- Existing configurations

Every DP-MODU has a standard to follow, the IMO MODU Code, but that is in general the only thing they have in common. Due to different shapes, control systems, power system, etc, only few units have the exact same system. On units under contract with Petrobras, we have in general the following configurations:

a) DP Semi-Submersible Rigs

The following information was taken from the rigs ESD F & G philosophy and are being used here only for the purpose of comparison between different systems installed on DP rigs under contract with Petrobras:

Rig "A" – class III

The Emergency Shutdown system is configured to operate with 3 shutdown levels:

- ESD Level 2 Service Shutdown
- ESD Level 1 Topside Shutdown (Preparation for Abandon)
- ESD Level 0 Abandon Vessel Shutdown (AVS)

Each ESD level will cascade down to lower levels.

For ESD Levels 0 and 1 there is a fixed set of responses to all sources of shutdown initiation.

The purpose of ESD Level 2 is to limit the tripping actions only to the affected systems. For ESD Level 2 there are therefore specific responses according to the source of the trip.

Level 0 is the highest level and is initiated from any of the dedicated Red coded Emergency Shutdown push-buttons located around the vessel (1 at each lifeboat and 2 at the helideck).

These can be activated after the decision has been made to abandon the vessel. Their function is to ensure that the abandoned vessel is electrically dead with the exception of the emergency support systems, which shall continue to operate until their individual UPS are exhausted.

The emergency support systems are:

- Navigational Aids (batteries for 4 days)
- Emergency lighting (batteries for 1hour 30 mins – 3 hours)

ESD Level 0 trips:

- Radio communications
- ESD and Fire/Gas panels
- Public Address and Public warning systems and integrated talkback system
- The following UPS:
  - F&G/ESD Workstations UPS
  - Blow Out Preventer UPS
  - Driller Equipment UPS (HITEC)

In the event of emergency drilling conditions, the operator can access the ESD screen page from a button on the background frame – this is always accessible by the operator.

The buttons are accessible to both the Bridge and Engine control rooms simultaneously. On pressing a button the operator will be prompted for confirmation prior to action being initiated.

It also shows discrepancy indicating if there is a difference between the commanded position of the damper and the actual damper position.

No additional password access is provided for these facilities i.e. once you are logged in at a level - any level (emphasis added) - you will have access to this screen.

Rig "B" – class II

The ESD system may be activated both manually and automatic. Manual activation is possible from the ESD & F&G matrix and from manual pushbuttons.

ESD level, Placement:

- AVS Lifeboat Stations, Helideck Entrance
- ESD 0 Nav Bridge, ECR
- ESD 1 Nav Bridge, ECR
- ESD 2 Nav Bridge, ECR, DCR
- ESD 3 Nav Bridge, ECR, DCR
- ESD 4 Nav Bridge, ECR

Manual ESD pushbuttons will be placed in AVS stations, where each AVS station will include 2 pushbuttons. Both pushbuttons must be pushed to activate AVS.

ESD 0 – 4 will be placed in the matrix panel.

Activation of AVS requires the mode selector key switch on the matrix panel, located in CCR, to be set to mooring mode (Both DP and Mooring Mode are available).

b) DP Drillship

The following information was taken from the drillships ESD F & G philosophy and are being used here only for the purpose of comparison between different systems installed on vessels under contract with Petrobras:

DS "A" (Class II)

Five pushbuttons for AVS are installed around the vessel: one on the bridge, two at the helideck and two on each lifeboat. After a total shutdown, an extra key shall be used for reset.

- ESD 1

All main engines stop
All main engine HV breakers open
Engine room fans trip
Engine room quick closing valves close
All engine PLC ACU's trip

- ESD 3A – 3B

Engines stop
Engine HV breakers trip
Engine room fans trip
Engine room quick closing valves trip
Fuel oil transfer pumps trip
Fuel oil service pumps trip
Fuel oil purifiers trip
Aft engine PLC ACU's trip

ESD 3 pushbuttons (Prepare for Emergency Response) are located on the Pilot House, Engine Control Room, Drillers Control Cabin, Forward Stbd Escape Way, Midships Stbd Escape Way, Aft Escape Way and shall be activated by nominated persons.

DS "B" (Class III)

The vessel is equipped with an emergency shutdown (ESD) system that is designed to allow a controlled and progressive shutdown of the vessel in the event of an emergency.

The ESD is provided with five emergency stop panels, located as follows:

- Bridge
- ECR
- Forward Emergency Headquarters
- Aft Foam Room

• Driller's Workstation

The ESD functions available from each location are shown in the table below:

ESD No	Description	Availability of ESD				
		Fwd Em HQ	Aft Em HQ	Bridge	DWS	ECR
1	Accommodation and non-DP related ventilation shutdown and damper closure	•	•	•	•	•
2	Automatic ventilation shutdown by fire or gas alarm					
3	Forward machinery space and forward thruster room ventilation shutdown, damper closure and QCV closure.	•	•	•	•	•
4	Shutdown forward and aft FO, LO and BO transfer pumps and valves	•	•	•		•
5	Topsides hazardous area ventilation shutdown and damper closure	•	•	•	•	•
6	Port engine room fans shutdown	•	•	•	•	•
7	Centre engine room fans shutdown	•	•	•	•	•
8	Starboard engine room fans shutdown	•	•	•	•	•
9	Aft thruster rooms, boiler room and IG plant ventilation shutdown and damper closure	•	•	•	•	•
10	Cargo pump shutdown and suction valve closure	•	•	•		•
11	Emergency generator shutdown and damper closure	•	•	•		
13	Port engines only shutdown	•	•			
14	Centre engines only shutdown	•	•			
15	Starboard engines only shutdown	•	•			
16	Port engine room total shutdown	•	•			
17	Centre engine room total shutdown	•	•			
18	Starboard engine room total shutdown	•	•			
19	Port engine room dampers and fans shutdown	•	•	•	•	•
20	Centre engine room dampers and fans shutdown	•	•	•	•	•
21	Starboard engine room dampers and fans shutdown	•	•	•	•	•

Failure Effects of the Safety Control System

- Failure to operate on activation of ESD pushbutton: This failure is not an issue for DP redundancy. However, failure of the ESD function to operate when required could compound a situation that is already extremely serious. The ship's staff should be aware of how to carry out the functions of the ESD by means of local controls.

- ***Spurious activation: The worst single act of spurious activation would be the activation of ESD 13, 14, 15, 16, 17 or 18, which would result in the shutdown of one engine room. This is within the design worst case failure.*** (emphasis added)

- Failure of Control PLC or Cabling due to fire: The ESD system control PLC could be destroyed by a fire and this could result in various input and output circuits becoming either short-circuited or broken. The circuits are designed to be immune to cable faults so there should be no false activation and thus no effect on DP. The ESD system functionality will be lost, however, and shutdowns will have to be initiated manually from local control stations

5- Potential Risks

The Well

A safety case prepared by DNV in 2008 for a new-built DP drillship reinforced that the primary action in case of blowout is to move the vessel off location, which means Level 0 ESD can not be applied.

The current MODU ESD rules increase the risks for DP MODUs. Among them, we have the following:

- total vessel blackout
- loss of position
- immediate termination of well control efforts
- vessel drifts uncontrolled until restoration of power

In addition, the fact ESD pushbuttons are required to be installed near to the helideck and lifeboats, we may have:

- opportunity for unintentional activation
- susceptibility to mechanical damage and/or water ingress in open locations
- human error

Human Error as Root Cause of DP Incidents

In 2007, DPPS, concerned about the human error problem, joint a workgroup especially dedicated to analyze the causes for that problem and also propose solutions. As a result, an action plan was put into practice.

As every major action from DPPS related to DP-operated vessels, this task was shared with Contractors and the result could not be better since fourteen causes were identified and twelve actions were proposed to be implemented by both Petrobras and Contractors. Among the causes, we had:

- Lack of specific procedures
- Stressful situations due to more activities and responsibilities
- Less experienced operators
- High turnover among companies or even within the same company
- Not enough time to be familiar with systems
- Few opportunities for practicing
- Ineffective on-job-training
- Lack of participation during commissioning
- Poor quality/Absence of manuals especially after upgrades
- Experienced people too much confident

- People relying on higher level of automation

As a consequence of human errors, an ESD can be activated for any of the above reasons. As variations of that famous law, we will have associated ideas, such as "If the operator has any way of making a mistake, he will." Or "If there's more than one way to do a job, and one of those ways will result in disaster, then somebody will do it that way."

Concerns

- Item 6.5.2. of the MODU Code refers to '*at least two strategic locations*' but it does not mention helideck or lifeboat specifically as a place to install emergency pushbuttons.
- On the item 6.5.3, the MODU Code says that '*the system's design should minimize the risk of inadvertent operation*'. On a DP MODU, 'minimize' is not enough. It should not be possible to operate the pushbuttons with a single and inadvertent action.
- Some of the Rigs Operating Manuals refer to a recommended sequence of shutdowns to be provided but there are no specific instructions guiding the operation of the ESD pushbuttons.
- The ESD system should be fail safe, redundant PLC's are required.
- An internal and/or external ESD system supply fault including voltage fluctuations should not generate any ESD tripping action
- The ESD system outputs should be de-energised (that means energised to trip) with output loop control.
- Maintenance operation should be possible without causing ESD tripping action
- In case of power on, power off and end of battery capacity of the ESD system no tripping action will be activated
- An ESD push button cable open or short circuit should not activate any tripping action.
- An ESD "0" or "4" (highest level) tripping order should generate immediately via the PA/GA system an alarm to inform all rig occupants the vessel abandon request
- At least 2 Fire and gas sensors will be required to generate an ESD trip.
- Special care should be taken on the engine air intake dampers so that in case of loss of dampers supply (air or electricity) no closing action should be generated.
- The ESD UPS supply should be instrumented at least with the followings:
  - Insulation fault
  - Battery charger current
  - Output voltage
  - UPS general fault

It was tested on the 'RIG A" that when the ESD is restarted it will default to the ESD level 0 (total blackout). To prevent the vessel to black out, a start up procedure has to be followed. It is recommended that the drilling operations are stopped and the well "made safe". Also, a preparation for a controlled disconnection is made before starting the ESD restart procedure. As in the event the procedure is not followed correctly, the rig will shutdown.

As expected, when the ESD system shut the power down, the power management system will not be able to start additional generators, as the "ESD in progress" contact is made. The instance of maintenance or ESD system failure the operators should be aware that the PMS is effectively disabled and that they will have to take the appropriate action.

FPSO DP – Another Concern

When a DP Shuttle Tanker is connected to an FSO or FPSO, oil, gas or condensate is being pumped at very high rates across the link between the two vessels. If a problem were to occur that could potentially end up with a major spill into the ocean, or endanger the life of the crew on either vessel then it is possible that the operator might be the first to see this occurring.

During the time taken for the operator to contact the FSO/FPSO by radio to stop the pumping process, considerably more damage may occur.

The operator on a DP Shuttle Tanker has the chance to interrupt operations simply by pushing a button on his remote device and then speed up this shutdown process. However, on a DP FPSO like the Seillean, which is hired by Petrobras for a long-term test on wells, the actions might be as different as the consequences of shutting down the vessel.

The Seillean has a specific configuration of class and that problem requires further investigations as well as a full study because the consequences of activating a ESD pushbutton, e.g. on the gas turbines, even at intermediate levels, are not yet determined. They are only being mentioned here to be subject of future discussions.

6- Incidents

At a first glance, an overview of the technical specification for ESD systems shows that the ESD philosophy meets the DP requirements for safety and redundancy of the system. That is because it is split along lines of the redundancy concept, is limited in its control system failure modes and is protected against inadvertent operation. However, even considering these factors, the results we got reinforce the need to keep a continuous evaluation of the system. The following examples are reminding us it is true:

- ABS +A1(E), “Drilling Unit”, +AMS, +ACCU, +DPS-3, NBLES, DLA, New Built (2009) 6th.Generation Deepwater Drillship: someone operated a ESD switch near a lifeboat and blacked the rig out.
- LR +100A1, +LMC, UMS, DP (AAA), PC, DRILL, OIWS: while waiting on the commencement of the contract, someone intentionally operated a ESD switch near the helideck and blacked the rig out. It took almost two hours to restore the power.
- DNV, STABILIZED UNIT DRILLING VESSEL, HELDK, DYNPOS AUTR, EO, DRILL: while performing a DNV test on one of the F & G emergency stations the operator made a mistake and pushed the wrong button blacking the rig out. Almost two hours later the power was restored.

Engine: Shutdown X Emergency Stop

The concept of ‘emergency stop’ should be applicable for DP MODUs instead of ‘Emergency Shutdown’. The reason is quite simple: when an engine needs to be stopped in emergency it is common to have an emergency stop button that is fitted for that purpose. Once the problem that caused the engine to shutdown is solved the engine is ready to be started. The same idea could be put into practice for a DP MODU – once the emergency situation that caused the vessel to completely shutdown is solved the vessel is ready to go back to the well location without spending a lot of time with a start up procedure.

In a DP vessel, ‘emergency stops’ are quite common for engines or propellers that pushing the wrong button is just a matter of opportunity. It is because the emergency stop buttons and the emergency shutdown buttons seem to be the same thing with the same function after all. Actually, they both have the same designation in most of the cases. Normally, a new-

built rig brings clear identification on the buttons but they remain in place only for a year or so. After that, only those who were working on the same vessel since the beginning would be able to know almost everything about that, especially their location and why they are there for. It means that a trainee can misconfuse the buttons while intending to 'help' especially because on his mind the idea of 'shutdown' is the same. Once pushed the button, there is no way back and the damage (or the cost) is irreversible.

There were many cases where the intention was not exactly to shutdown the engine or the propeller but it happened. After investigations, the following lessons were learnt:

- it should not be possible to accidentally activate critical items such as emergency shutdown controls;
- protective covers and other barriers to prevent accidental activation should be fit to avoid that;
- at least two separate actions should be required to activate any shutdown;
- emergency controls should be located at easy places to access but where no accidental activation should be possible.

Emergency Shutdown during Acceptance Trials – a case study

- LR +100A1, +LMC, UMS, DP (AAA), PC, DRILL, OIWS: during acceptance trials and while carrying out power systems tests a voltage drop caused the ESD system to activate blacking the rig out. By following the procedure to restore power, almost one hour was spent. Uncontrolled drift and lack of communication was noticed.

In 2001, when DPPS went onboard for acceptance trials in a class III DP rig, it was very strange to find out that rig could have a system that completely blacked her out. It was unacceptable because DPPS always understood a blackout could be the worst thing to happen in a DP vessel.

To make the situation even worse, there was a high risk of a second blackout after restoring the power if a correct procedure was not followed. Another important point observed was the amount of the available pushbuttons for emergency stops or emergency shutdowns in different levels around the rig. They were all unprotected pretending nothing wrong would ever happen regarding to inadvertent activations or sabotages.

7- It exists. How to deal with it?

Actions

It was included on DPPS checklist an item to check that out not only on Acceptance Trials but also on Annual Trials. The expected result is every button with similar functions to be covered and labeled. Proof of 'Handling the ESD' training for engineers, especially the new ones, that includes touching but not activating controls to simulate the required actions. Restrictions to those spaces where the buttons are located are also put in place and are part of the checklist.

DPPS agrees with different levels of shutdowns to increase safety levels and to keep control over the vessel. However, the places where they are located and their functionality must be well known and understood by everyone who is responsible for operating the equipments.

Isolation of levels I and 0 Shutdowns

This action requires approval of the certifying authority *(emphasis added)*

- Level 0 shutdown buttons

The level 0 shutdown buttons have a 5 minute delay after they are initiated. On initiation the PA fire alarm sounds immediately and the abort timer starts, the operator can abort the shutdown by initiating the abort button located on the bridge. These buttons can be inhibited on the Fire & Gas console.

- Level I shutdown buttons

There is only one of these buttons located next to the abort button on the bridge. This button can be inhibited on the Fire & Gas console.

Technical Specification

Since the first problem was found, DPPS tried to figure out a solution via its Technical Specifications for the bids. The first thing to be done was to do a research. The results, however, were not so good:

- there was no mention to emergency shutdowns on MSC/ Circ. 645;
- IMO MODU Code 1989 established emergency shutdowns for moored rigs;
- Classification Societies did not mention anything about emergency shutdowns on DP vessels.

The chapters related to the power systems only mention the emergency shutdown in case of explosions, mainly on the engine room, and they are not specific for DP Vessels.

Based on that, a technical specification was prepared and it brought the following text:

"If the unit has ESD (Emergency Shutdown) devices installed, they shall be permanently deactivated prior to the commencement of the Contract with Petrobras. That action shall be proven by tests and a certificate shall be issued by an IMO-recognized company to ensure that."

Of course there was a contradiction on that request because one of the first items of the technical specification has requested the contractor to follow the Class Society rules an all the applicable standards. At the same time, it was asking the contractor to forget that by inhibiting one of the safety devices! That was a very controversial thing that was later on corrected.

8- Future Actions

- MODU Code

Recommended changes, specific to DP MODU's are as follows:

- guidance note to raise awareness that current ESD rules may be unsafe for DP MODUs and should be carefully considered
- accept centralized RESET to minimize drift time without power if ESD was applied
- remove requirement for helideck and lifeboat stations for DP MODUs
- possible a new redaction for item 6.5, as below:

6.5 Emergency conditions due to drilling operations

6.5.1 In view of exceptional conditions in which the explosion hazard may extend outside the above-mentioned zones, special arrangements should be provided to facilitate the selective disconnection or shutdown of:

.1 ventilation systems, except fans necessary for supplying combustion air to prime movers for the production of electrical power;

.2 main generator prime movers, including the ventilation systems for these;

.3 emergency generator prime movers.

6.5.2 In the case of units using dynamic positioning systems as a sole means of position keeping, special consideration may be given to the selective disconnection or shutdown of machinery and equipment associated with maintaining the operability of the dynamic positioning system in order to preserve the integrity of the well. (emphasis added)

6.5.3 Disconnection or shutdown should be possible from at least two strategic locations, one of which should be outside hazardous areas.

6.5.4 Shutdown systems that are provided to comply with paragraph 6.5.1 should be so designed that the risk of unintentional stoppages caused by malfunction in a shutdown system and the risk of inadvertent operation of a shutdown are minimized.

6.5.5 Equipment which is located in spaces other than enclosed spaces and which is capable of operation after shutdown as given in paragraph 6.5.1 should be suitable for installation in zone 2 locations. Such equipment which is located in enclosed spaces should be suitable for its intended application to the satisfaction of the Administration. At least the following facilities should be operable after an emergency shutdown:

.1 emergency lighting under paragraphs 5.4.6.1.1 to 5.4.6.1.4 for half an hour;

.2 blow-out preventer control system;

.3 general alarm system;

.4 public address system; and

.5 battery-supplied radio communication installations.

Regarding to the items 6.5.2 and 6.5.4 above we suggest the following to be added or modified:

6.5.2 – “In the case of units using dynamic positioning systems (,,,) in order to preserve the integrity of the well ***and the maneuverability of the vessel.”***

Reason: when a DP vessel is working in a crowded area (possibility of collision) and, for safety reasons (e.g. a blowout) a shutdown is mandatory then a quick restoration of power when the shutdown is no longer necessary must be essential to maintain the control of the vessel.

6.5.4 – “Shutdown systems that are provided to comply with paragraph 6.5.1 (,,,) and the risk of inadvertent operation of a shutdown are (~~minimized~~) ***eliminated***.

Reason: it is unacceptable that in a DP vessel the risk of inadvertent activations of ESD devices are still present. It should be avoided by ensuring that a single action would cause no effects on the system.

- Petrobrás/DPPS Technical Specification (new)

The updated version for DP Vessels Class II and III is the following:

“4.2.2 Emergency Shutdown (ESD): the system shall be hierarchically integrated in such a way that the high levels are comprised of lower levels. Every actuator shall have clear identification of the equipments to shut down. It shall be protected against inadvertent activation by a mechanical protection. The highest level (usually Abandon Vessel Shutdown) shall not be activated by a single device, even if mechanically protected or activated by two independent

actions, unless special features such as a password are implemented. Any activation of the ESD system shall be followed by visual and audible alarms."

9- A Newbuild Configuration

SS Amazonia (Owner: Shahin Oil & Gas) (System designed by Kongsberg)

Since Schahin Oil & Gas has already a vessel under contract with Petrobras (the drillship Schahin Cury Lancer), the relationship between DPPS and its technical department made a new ESD design possible to be installed on their new-built DP rigs. Since the beginning, the major concern was to follow IMO specifications and Petrobras DPPS technical specifications at the same time. Schahin has obtained an important help from Kongsberg to design and built a system with those characteristics. In the end, the Schahin Amazonia levels of shutdown are as follows:

- Level 3 ESD3 (APS) Abandon vessel
- Level 2 ESD2 Rig Emergency Equipment Shutdown
- Level 1 ESD1 Fire & Gas Shutdown

Emergency shutdown level 3 – Abandon vessel

If a critical situation makes it necessary to abandon the vessel, **APS** shall be provided to ensure safe evacuation of personnel from the installation. It is only activated from dedicated manual push-buttons located at:

- CCR
- ECR

APS push-button sets shall have dual push-buttons mechanically latching in the emergency position and reset by manual operation. The APS PB's shall be clearly marked and protected against undesirable operation.

APS shall only be initiated by the Captain. *(emphasis added)*

Override provision of ESD system actions is available only for the CCR-operator. The override status lamp is available on the individual CAP-Panels.
After activation of APS, the equipment required by IMO regulations shall as a minimum be functional. Also, all electrical equipment left operational after ESD1 shall be certified for operation in zone 2 areas.

10- Conclusion

The purpose of this paper was to present an important issue that DPPS is dealing over the years. Since the first acceptance trials and, as consequence, the first problems related to blackouts involving ESD mechanisms, DPPS is trying to balance the IMO – MODU Code standard and the Classification Societies rules with its Class II and Class III Technical Specifications. The intention was always look for improvements on reliability of DP Vessels and we consider the existence of ESD mechanisms as something that can be a source of problems instead a solution.

For many years, the Classification Societies have been receiving objections to their requirements to have ESD blackout buttons at lifeboats and at helideck. As argument, the operators and contractors have a history of incidents that includes not only inadvertent acts that

blacked the rigs out, when the switches located on those places were operated, but also electrical problems that led to unexpected situations while trying to restore power. In general, people involved with this issue think that could be reasonable and responsible to consider those devices as a threat to DP. Most of that people also agree that the existence of those buttons, depending on how the configuration of the ESD system is, it should be considered a FMEA "A" recommendation like a single point failure.

Due to this fact, DPPS wants the institutions involved with analyses of regulations to come up with something that on one hand solve the problem and on the other hand can help Captains not to put in risk their obligations under the law.

By comparing the IMO standard and the rules of the Class Societies with its Technical Specifications, DPPS tried to focus on the need to join efforts in order to create a better and safer rule to be applied on DP Vessels. By bringing information about the problems we notice and the incidents data we have, this paper intends to reinforce the non-existence of ESD-related DP incidents since DPPS has included a request to have ESD buttons inhibited at the lifeboats and helideck and special features included on the system.

Based on DPPS technical specifications, new-built rigs are bringing new features for the ESD system. As an example, the newbuild DP rig Shahin Amazonia has requested to Kongsberg that the system should not allow a blackout without a double action taken by the Captain. Also, a key should be used in addition while the system pops a message up for confirmation of the shutdown action.

As a result of these actions, reliability on DP-operated vessels is being improved.

11- References

Petrobras – *Editais para Sondas DP – Adendo D, Seção A, Parte I – Relação de Itens Restritivos e Equipamentos Mínimos Exigidos* by Afonso André Pallaoro, DPPS

Machado, Gilberto Beduhn; Costa, Marcelo S. R. – *Analyzing DP Incidents, DP Conference*, Houston, 2006

IMO – **International Maritime Organization** – *MSC/Circ 645 – Guidelines for Vessels with Dynamic Positioning Systems*, 6 June 1994

IMO – International Maritime Organization, MODU Code – *Code for the Construction and Equipment of Mobile Offshore Drilling Units*, 2001 edition

CODE FOR THE CONSTRUCTION AND EQUIPMENT OF MOBILE OFFSHORE DRILLING UNITS, 2009 (2009 MODU CODE) *Draft Assembly Resolution, ANNEX 14 - MSC 86/26/Add.1, Page 65*

IMCA – **International Marine Contractors Association** - *Guidance on The Design, Selection, Installation and Use of Uninterruptible Power Supplies Onboard Vessels, IMCA M 196*, April 2009

DNV – **Det Norske Veritas** –*Rules for Classification of Ships – Special Equipments and Systems – Part 3-6, – Dynamic Positioning Systems* – January 2004

ABS – **American Bureau of Shipping** - *Rules for Building and Classing Steel Vessels – Part 4, Chapter 3, Section 5, Item 7: Systems Associated with Drilling Operations*, 2006

Lloyd's Register - *Rules and Regulations for the Classification of a Floating Offshore Installation at a Fixed Location*, May 1999 - *Safety Systems Hazardous Areas and Fire, Part 7 – Safety and Communications Systems, Section 7 – Emergency Shutdown (ESD) Systems*

Global Maritime – *FMEA 22451-0201-14307, Rev. 0*

Poseidon Maritime - *FMEA, PML/10797/Rep-002, Rev. B*

Kongsberg – *ESD and F&G Philosophy for SS Amazonia*, 2008

Alstom – *Emergency Shutdown Philosophy for Semi Submersible Drilling Rig*, 2003

http://en.wikipedia.org/wiki/Classification_society, page last modified in 24 Aug 2009

Public domain (Internet)

Contributions:

Afonso Andre Pallaoro, *Petroleo Brasileiro SA – DPPS*, Macaé

Pete Fougere, *Transocean Engineering and Technical Support*, Houston

GILBERTO BEDUHN MACHADO
gbeduhn@petrobras.com.br