DYNAMIC POSITIONING CONFERENCE
October 14-15, 2014

RISK SESSION

Fire & Gas Detection – ESD Design Philosophy and their impact on Asset Management. Analysis of risks ESD / AVS / APS systems create high risk for DP vessels.

By Harry van Rijswijk

Lloyd's Register Energy - Drilling

Return to Session Directory

1. Abstract

The biggest threat for station keeping in the last few years on the new build drill-ships is the designing of Fire & Gas and ESD systems without necessarily taking account the impact on other safety critical functions. In the past, the Fire & Gas Detection systems were alarm and monitoring systems, but in the new builds over the last 5 years we have seen Fire & Gas systems automatically shutting down engine-rooms (engines) and thrusters. The design engineers for these vessels cross the line of station keeping, rather than respecting equipment protection design boundaries.

The interpretation of class rules by automation engineers has led to a design philosophy of placing control capability where only condition monitoring should be used. One other system that is becoming over-engineered is the AVS (Abandon Vessel Shutdown) or APS (Abandon Platform Shutdown). This system does not belong on a DP vessel such as a (drill-ship or semi-submersible. This system will actually put more lives in danger through its operation. In history these systems were made for platforms (production) or MODU's to kill all systems and protect lives after a large gas kick or blowout. These rules were developed from common sense and industry practice however, many engineers inside and outside class are only using the rules to make their system the "best in the world" but are forgetting that this system is on a DP vessel.

Other station keeping threats include water-mist installations in 11kV switch board rooms and bridges. On top of the equipment issues there is the lack of DPO experience on the Bridge. (There are too many new builds and not enough DPO's with experience).
A recent incident occurred on a new 6th generation drill ship on 28-12-2011, in which a crew member accidently operated the AVS switch near a lifeboat and blacked out the vessel while it was drilling and connected to the well. After 8.5 hours the power was restored. The crew member confused the AVS switch with the reset button for the lifeboat davit. He had lowered the lifeboat about 1 meter and was trying to get it back. The total loss for the operator was 10 million dollars. The drilling contractor was lucky that the drill ship did not hit a nearby FPSO. This is the fifth known case of an AVS/APS causing unintended downtime.

There have also been incidents during blowouts in which the DP drill-ship did not use the APS-AVS button. In the MTS paper from October 2009 "ESD in a DP Vessel - For Safety, not for Blackout", the organization explains that DNV's safety analysis resulted in a similar conclusion, to not activate the AVS. Station keeping to secure the well should take priority over shutting down all rig systems.

The solution to this problem is to have IMO and all class societies (ABS, DNV, LR and others) make an exception for DP drilling vessels on the rule to install an APS or AVS or ESD zero system. Class has to consider that one rule can have a big impact to the design of these new systems. The fire & gas systems try to take out the human factor, but forget the overall risk for loss of station-keeping and therefore may present a larger environmental risk or risk to personnel. In this paper I intend to discuss the various scenarios and failure cases associated with using APS/AVS systems, and examine the impact of industry design best practices on the overall goal of drilling and completing wells safely.

Below is a statement from a study made by the Maritime College State University of New York

Another segment where there is increasing opportunity for our graduates is the offshore energy industries which are seeking more maritime professionals to crew offshore platforms, drilling ships, and off-shore supply vessels (OSVs). Dynamic positioning or "DP" is a rapidly maturing technology related to the off shore oil and gas exploration industry and research vessels.

DP is a computer-controlled system which allows the operator to very precisely maintain a vessel's position and heading by use of its own propellers and thrusters. In 1980 the number of DP capable vessels totaled about 65. It is estimated that today there are over 2000 DP vessels and the number will continue to grow. As such there will be an increased demand for certified operators. DP systems have become more sophisticated and complicated, as well as more reliable. As of January 2013, there are only seven certified DP centers and they are located in Louisiana and Texas. As reported in the International Dynamic Operators Association Spring 2012 journal: "With so many new OSVs coming equipped with DP, and many older ones having systems retrofitted, there is a high stakes race

developing to safeguard the supply and capabilities of qualified DP operators globally. Employers are left struggling to find the very best new people."

IMCA has on this moment 900 companies as member from 60 countries and they are the owners of these 2000 DP vessels.

2. Introduction

My first report on this issue is from November 2008 after the second Saipem 10K design vessel by Samsung, the West Capella (HN 1687). The West Polaris (HN 1657) is included as well, first of a new series of about 40 vessels build by Samsung Heavy Industries; what is known as the Saipem 10K / 12K design. The first Saipem 10K was delivered in 2000 and the new series started in 2007. In the first report about the design of the AVS (Abandon Vessel Shutdown) I already reported my concern about the design by Samsung and Kongsberg. Mainly because it was too easy to completely shut-down the vessel on several (3) locations on board the vessels by a single push button. This represented a single point failure. The design used the standard ABS 2001 part 4 chapter 3 section 5 item 7 (page 206) as guideline. There are several issues and treads for station keeping:

1. Name plates not clear or missing
2. Box with AVS push button station not locked
3. Only very few persons has knowledge of when to use this button
4. The activation needs better protection against accidental actuation (like key lock switch see Fig.1 below as example)

Fig.1 Kongsberg F&G and ESD panel

In this report the term AVS (Abandon Vessel Shutdown used by ABS) will also cover APS (Abandon Platform Shutdown used by DNV) and ESD zero or 1 or 3 (as highest level) for LR.
The first comment is that it would be recommended if the industry is using one term for the same function. The second comment is on the use by DNV using the word "Platform"; this is already the standard terminology for stationary Modu-s like fixed platforms, jack-ups and moored semi subs. This is not the case for DP vessels. See also the comment from DNV in chapter 12 "*So we do not expect that APS should be used normally for a DP vessel, but it is a safety backup if something goes wrong*." This comment shows the philosophy behind the DNV stance on APS and associated terminology.

3. Report 27-Nov-2008 from Samsung new build (2008) HN 1687

Below are some statements from a report made in 27-Nov-2008 on the inspection on the HN 1687;

The biggest concern with this system is when it can operate shutdowns and alarms automatically without input from personnel (see Cause and Effect Matrix).

Every alarm has to be **acknowledged before it can be reset** (all ESD and F&G outputs are latched and must be reset after alarm situation , see page 34 Kongsberg). Sometimes it will not reset from the Kongsberg console and has to be reset at the Fire alarm panel (Autronic).

ES-11 Port Engine Room total shutdown
ES-12 STBD Engine Room total shutdown
ES-82 Drilling Control Room (drillers cabin) - automatic
ES-83 UPS shutdown - automatic

One other major issue is the connection between the EDS system and F&G system in the case when it can shutdown the power-plant. It has to be investigated if there is a single point failure possible. ES-11 and ES-21 (Port and Starboard Engine room total shutdown) are manual shutdowns but there is a link with ES-82 and ES-83 (automatic shutdowns, ES-82 Drilling Control Room, ES-83 UPS shutdown)

The three (3) abandon rig push buttons are a separate system. Again, investigation is needed to determine if there is a **single point failure** possible. Drawings for the system have been requested, but not received at this time.

Recommendations:

- A strong recommendation is also mentioned in the DP FMECA. The ECR operator or DPO operator who is in charge of the 24 hour watch needs to have sufficient training on this very complicated system.
- It is a recommendation to have as much as possible involvement of the ECO (Engine Control Operator) during commissioning period.
- The interpretation of the ABS rule Part 4, Chapter 3, Section 5 / 7.1 for the design of this system makes sense for a moored rig or a platform, but not for a DP 3 drill-ship.
- The risk to trigger ES-82 and ES-83 (PS and SB engine rooms included) on software failure shutdown (FS-49 and 50) is a risk for station keeping. The risk of losing station by software failure is not acceptable.
- During the acceptance period, the effect of tripping ES-41 on station keeping should be tested.

References:

- Kongsberg Function Design Document ESD and Fire & Gas Detection System
- Samsung HN 1657 ESD and F&G Philosophy Rev G
- Samsung HN 1657 ESD and F&G Philosophy Block diagram A3
- Seadrill Operation Manual Volume III section 4 ESD and F&D System

4. MTS paper October 2009 from Mr. Gilberto Beduln

In 2009 Mr. Gilberto Beduln authored a paper on the same issue discussed in 2008. This paper highlighted the safety case done by DNV in 2009 not to use the ESD zero / AVS or APS in case of blowout with DP vessel. In his paper he also talks about 3 incidents with accidently actuations. The incident aboard the Samsung new build in Angola on December of 2011 adds a fourth instance.

5. Rules

IMO Modu-code (Section 4.12 and 6.5)
IMCA (M196)
DNV (Section 5 and 8)
ABS (Part 4 Chapter 3 Section 5 item 7)
LR (Section 7)
As basis for all class rules and IMCA rules are the IMO Moducode rules from 1979, 1989, 2009 and 2012 these rules are the minimum requirements for Mobile Offshore Drilling Units. In the beginning there were nearly no DP drilling vessels, mainly anchored and jack-ups and fixed platforms. For these units it was normal to have a total

shutdown pushbutton because when you shutdown all electricity, you could save lives after blowout or gas kick. These units did not have the issue of drifting away. It will be an improvement if the industry is using one name for this function. DNV is calling it APS (Abandon Platform Shutdown) a DP drilling vessel is not a platform. Kongsberg is using what the client ask, from ESD zero or ESD level 3 or AVS. AVS is the best because it is not confusing with all other ESD's on individual equipment. AVS is covering the function the best.

MODU Code 1989

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 abovementioned 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 radio communication installations.

MODU Code 2009

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.

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.

MODU Code 2012

D10.5 Emergency shutdown facilities

D10.5.1 Emergency conditions due to drilling operations

In view of exceptional conditions in which the explosion hazard may extend outside the areas defined in D8, special arrangements should be provided to facilitate the selective disconnection of shutdown of :
- Ventilating system
- All electrical equipment outside Zone 1 areas, except where of a certified safe type for Zone 1 applications.
- Main electrical generators and prime movers.
- Emergency equipment except those items listed in D10.5.2.
- Emergency generators.

Initiation of the foregoing shutdown of facilities will be the operator's responsibility. The initiated action may vary according to the nature of the emergency. A recommended sequence of shutdowns should be included in the Operating Booklet (see D1.3.

D10.5.2 Equipment to remain operational after emergency shutdown.

At least the following facilities are to be operable after an emergency shutdown.
Equipment which is located in spaces other than enclosed spaces and arranged to be operated after complete shutdown as given D10.5.1 is to be suitable for installation in Zone 2 locations. Such equipment, when located in enclosed spaces, is to be suitable for its intended application to the satisfaction of the society:

Emergency lighting required by D10.4.2 for half an hour;
Blow-out preventer control system;
General alarm system;
Public address system; and
Battery supplied radio communication installations.

6. Incident 28-Dec-2011 in Angola with Samsung new build (2010) HN 1702

See Attachment A and B, in this case the push button near the lifeboats was actuated and it took the vessel 8.5 hours to recover from the event. The vessel did perform a successful EDS (Emergency Disconnect Sequence). Total cost for the operator was 10 million dollars (recover time) because they were very fast to recover the part that fell in the well. For the same case it may be expected to cost up to 20 million dollars (recovery time).

7. Incident 28-Nov-2007 on old drill ship NRE (1977) in Brazil

In this case the vessel suffered from a gas blowout and got on fire that injured 6 men on the drill floor. In this case the AVS is not pushed. They try to get the well under control. You cannot do that by pushing the AVS. First you need to perform an EDS before pushing the AVS. Depending on wind and current, the vessel may accidentally drift towards a FPSO. In many cases a drill ship is working in close distance from an anchored FPSO or TLP. These are all considerations before drifting from a gas cloud. In theory there are some options but in real world there is only one option and do as fast as possible an EDS. The rig is on fire after an explosion 1 hour and 46 min (in this case) after the first gas alarm sounded. The fire stopped immediately after an EDS.

8. Test new AVS system after new build.

During commissioning the AVS is tested in the shipyard and sometimes later during acceptance on location. The industry is not completely aware of the impact of these tests for the effect on software and hardware. There are many studies done on the effect of loss of power on hard drives and memories. For this reason we have nearly all drives powered with uninterruptable power supply's (UPS's). When the AVS is actuated all batteries are switched off from the UPS's. This is a final kill for all systems. The industry need to make better procedures to test the AVS on the new builds without damaging the software and hardware. The test is only for the power supplies, not for the systems that are fed by them.

9. What damage can occur with testing or accidently actuating the AVS

Looking at all the different studies (see chapter 16 with all websites about this issue) there are many failures possible with the hardware as well with the software when the power is lost. (power failure). Special caution must be taken when they want to test the AVS. The best is to shut down as many possible systems by a normal power down of servers and computers. Test with the AVS if all batteries from all UPS's.

10. What can be done in the future?

- If we want to protect the people on board the DP vessels from blowouts we need to make the crew aware what can happen in the worst case and train these on simulators, similar to the approach of the aviation industry with pilot training. The USCG Safety Alert from June 17 2013 should be mandatory as well.

- Make a dispensation for DP vessels not to design a system that can kill all systems, it will make the DP drilling rigs less reliable and more dangerous.

11. Other threats for DP drilling vessels (station keeping)

- We have seen a DP vessel (semi submersible) that the Fire & Gas system can automatically shut down a thruster. The Cause and Effect matrix shows when the system is shutting down a thruster.
- High pressure water-mist systems in 11kV rooms, ECR's and Bridge's (IP not high enough).
- Because the many new builds in the last 5 years and the high need of experienced DPO's, we can see the that the minimum requirements are shifting towards less experience for DPO's

Note; the latest new build drill ship has for 24 hours DPO Bridge covering; 2 x 12 hours of 1 DPO with 3 years experience on supply boats and one or two assistant DPO's (zero experience) just from the Maritime Academy. This new build just arrived in the GOM in August 2013.

12. Single H2S sensor can shut down your DP vessel

A new build from 2013 arrived in Angola and during the acceptance on the first well we found by accident that the cause & effect was shutting down the DP system taking down UPS's and DGPS antenna's. The crew was testing all gas detection sensors from the vessel. Normal procedure was to inhibit the sensor before the test. But after the test there was still enough gas in the sensor head to trigger the high high (15 ppm) alarm, the direct effect was to activate an ESD (non critical users). But in this list of non critical users we found also many critical users for the DP system.

13. Conclusion

1. In 2009 in the paper of Mr. Gilberto Beduln; he made an proposal for future changes by IMO to make changes in the Modu-code:

   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 and the maneuverability of the vessel .

   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 ***eliminated.***

   In 2012 the latest Modu-code did show a different layout but no changes as above. They made the changes in 2009 but with small difference in wording. See above highlighted.

2. Implement mandatory simulator training for DPO's and Drillers (see item 10 and 11 in section 15 Websites; USCG Marine Safety Alert 17 June 2013)

3. Operators need to demand time for the annual DP trials to implement two blackouts each year, one time for each crew a year. This will make the client and DPO's and their maintenance crew more confident with their unit. To show the automatic recovery time of the system including thrusters back in DP. (At this time we stop the time when one fwd thruster is in DP and one aft thruster is in DP. This is used to compare all DP vessels). It is used as a fitness test of all systems. Also it has nothing to do if you run in a single or double split configuration.

4. The DP alert system is also using network A and B, in the past this was always an independent hard wired system. When the law of Murphy kicks in ……

5. More vessels need better WSOG and training between parties involved with the WSOG.

6. More and more DP vessels installing a Weather Doppler Radar (200 mile range) to have a better response on local bad weather. It will give the DPO's an extra "eyes and ears".

7. Implement one name that is used by the complete industry and class. Now we have ESD zero or 3 (LR), Abandon Platform Shutdown (APS from DNV), Catastrophic Shutdown (Converteam) and Abandon Vessel Shutdown (AVS from ABS).

14. References

Machado, Gilberto Beduhn – ESD in a DP Vessel - For Safety, not for Blackout, MTS 2009

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*, 1979, 1989, 2001 and 2009 edition

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** –*Offshore Standard OS-A101 – Section 5 – Emergency Shutdowns (ESD) Principles* – October 2005

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

ABS – **American Bureau of Shipping** - *Rules for Building and Classing Mobile Offshore Drilling Units – Part 4, Chapter 3, Section 5, Item 7.1.1: Shutdown Arrangements*, 2001

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*
Kongsberg – *ESD and F&G Philosophy for West Polaris drillship*, 2008
Petrobras – *Incident report 28-Nov-2007 Noble Roger Eason*

Total – *Incident report 28-Dec-2011 Saipem 12000*

Kongsberg – *ESD and F&G, Cause & Effect matrix*

Maritime College – *Strategic Plan 2013 – 2018, Analysis, Imperatives and Objectives – 25 July 2013*

15. Websites and links

1. Data Corruption
https://wiki.csiro.au/display/ASC/Data+Corruption

2. IDENTIFYING PLAUSIBLE CASCADING EVENTS IN
SYSTEM STABILITY ASSESSMENT
http://orbi.ulg.ac.be/bitstream/2268/5650/1/CIEM2007_2.pdf

3. Understanding the Impact of Power Loss on Flash Memory
http://cseweb.ucsd.edu/users/swanson/papers/DAC2011PowerCut.pdf

4. How To Corrupt An SQLite Database File
http://www.sqlite.org/howtocorrupt.html

5. Software Failure Rates:
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.75.2736&rep=rep1&type=pdf

6. Cascading failures of Blackouts:
http://www.ece.wisc.edu/~dobson/PAPERS/nedicEPES06.pdf

7. Software Insensitive Systems:
ftp://ftp.cordis.europa.eu/pub/ist/docs/fet/strat-6.pdf

8. Software Failures:
http://www.cs.vu.nl/en/Images/dissertation%20PN%20van%20der%20Spek_tcm75-256915.pdf

9. Data loss prevention / protection digital assets
http://www.mampu.gov.my/documents/10228/29588/Data+Loss+Prevention.pdf/39d34304-e463-4f5d-99a8-4e561ff53857

10. RECENT FAILURES OF DYNAMIC POSITIONING (DP) SYSTEMS ON
MOBILE OFFSHORE DRILLING UNITS, June 2013 USCG
http://www.naylornetwork.com/adc-advisory/assets/msib_modu_2005_13.pdf

11. DP Failures on Mobile Offshore Drilling Units
http://www.marinelink.com/news/failures-offshore355728.aspx

12. Marine Control Systems
http://www.marin.ntnu.no/~assor/publications/marcyb.pdf

13. Hardware in the loop testing 2006
http://www.mic-journal.no/PDF/2006/MIC-2006-4-3.pdf

14. Simultaneous faults on the 11 kV system of an offshore FPSO vessel
http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5936974&url=http%3A%2F%2Fieeexplore.ieee.org%2Fstamp%2Fstamp.jsp%3Ftp%3D%26arnumber%3D5936974

15. Dynamic positioning power plant system reliability and design
http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5936973&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Ficp.jsp%3Farnumber%3D5936973

16. Improving total efficiency and safety during DP-operations
http://www.marinepropulsors.com/proceedings/MB2-3-Halstensen%20-%20Improving%20Total%20Efficiency%20and%20Safety%20during%20DP-Ope.pdf

16. Contributions:

Keith Kruelskie, *WEST Engineering / LR – Engineer*, Houston

David Dugas, *WEST Engineering / LR – Systems & Controls Consultant*, Houston