



DYNAMIC POSITIONING CONFERENCE  
October 12-13, 2010

RELIABILITY SESSION

---

**FMEA Failed to Meet Expectations Again (Again?)**

**By (Doug Phillips, Brian Haycock, Steven Cargill)**

***(DP Expertise, BHDP Services, GL Noble Denton)***

---

## **Abstract**

In 2001 a paper was presented at the MTS DP conference discussing the adequacy of DP system Failure Modes and Effects Analysis (FMEA) - Fails to Meet Expectations Again. Since then many FMEAs have improved considerably, with those improvements being led by one major operator, one major vessel owner, one main DP FMEA supplier and IMCA guidance. All of which has 'raised the bar'. However, in the authors' combined experience of producing comprehensive FMEAs and reviewing 100 or more FMEAs as part of Shell's DP Vessel approval process, many FMEAs are problematic to produce and may overlook many potential single point failures. The paper will identify where in the authors' experience FMEAs have improved, but also present where the FMEAs still miss many failures modes and operational constraints.

## **Introduction**

The Failure Modes and Effects Analysis is an important part of the process of ensuring that a DP system is fault tolerant with the desired post failure DP capability. However, it is only one element in a process that involves classification societies, designers, equipment vendors, vessel owners and shipyards. Each member of this group has an important role to play in ensuring the integrity of the vessel's redundancy concept. Arguably, the FMEA should be the last line of defense. It is far better not to introduce single point failures in the first place than depend upon the FMEA to find and remove them.

This paper will first lay out some of the key impediments to the production of a good quality FMEA, then secondly discuss some of the more commonly overlooked failure modes in DP FMEAs.

## **Key Impediments**

**Key responsibilities** These are rarely defined but need to be

- The vessel owner must clearly define the Worst Case Failure Design Intent (WCFDI) and/or the desired post failure DP capability in the specification for the vessel.
- Designers must consider the WCFDI and post failure capability in the design of all DP related systems and develop a redundancy concept to ensure the desired post failure DP capability.
- The shipyard must understand the redundancy concept and communicate it to all parties that need to know.
- The FMEA provider must provide a competent FMEA and proving trials program.
- The classification society must confirm the design of the DP system complies with the requirements of the appropriate DP notation. They must confirm that the FMEA meets acceptable standards and reject any that do not.

## **No minimum standard for FMEAs**

There are many guidelines and standards for FMEAs and DNV is currently developing a 'recommended practice' for DP FMEAs. This document will go a long way to addressing the shortfall but it will only apply to vessels built to DNV class and even then, it may not be a rule requirement. The focus of this recommended practice is efficiency of the FMEA approval process.

### **Complexity of modern vessels**

The diesel electric power plants of modern DP vessels are becoming increasingly complex. PLCs, micro controllers and data communications networks, control and connect thruster drives, generators and switchboards. There may be several layers of control systems between the operator and the machinery under control. Modern redundancy concepts rely heavily on a whole range of sophisticated and sometimes bespoke protective functions particularly in vessels that normally operate with a common power distribution system.

Much use is made of the word 'redundancy' in relation to the design of DP Class 2 and DP Class 3 vessels. Redundancy is defined as an alternative means of providing the same function which can be interpreted as simply having at least two of every piece of essential equipment. In reality this is overly simplistic as what is really required is 'fault tolerance' which is the ability of a system to continue in operation following a failure. Typically, only a single failure is considered but means for detecting that such a failure has occurred should also form part of the FMEA process.

The ever increasing complexity of redundancy concepts makes it essential to have a multidisciplinary engineering team for all but the simplest vessel designs. A typical DP FMEA team should include:-

- Marine engineer
- Electrical engineer
- Control systems engineer

It is not always appreciated that the work involved in proving the fault tolerance of a DP vessel operating with a common power distribution system is significantly greater than proving fault tolerance in the case of a vessel which operates with two or more independent power systems. Vessel owners should carefully define the operating configurations they would like the FMEA to analyze. It is not unusual to request analysis for two configurations typically a common power system and two or more independent power systems. One configuration may be defined as the preferred configuration and it is usually the case that the vessel would spend much of its working life in this configuration. However, some vessel owners have requested five or six different configurations. The amount of rework created by changing the preferred operating configuration mid way through the analysis should not be underestimated.

At least one of the major classifications society states that they only consider a DP vessel to be in compliance with their requirements if it is operated in one of the configurations analyzed in the approved FMEA. That is not to say that the DP system is not fault tolerant in other configurations or with a major piece of equipment unavailable due to maintenance or repair. However, it may be prudent in such circumstances, to formally assess and document the effect of the configuration change on the redundancy concept and post failure DP capability.

### **Supporting studies**

It is clear that the process of proving fault tolerance depends heavily on being able to predict how the plant will respond to various fault conditions. This is particularly true in the case of vessels intending to operate with a common power distribution system connecting all generators and thrusters. Thus, there may be a requirement for additional studies to support the conclusions of the FMEA. Some of these studies may be provided to meet the requirements of main class rules but others may have to be specially commissioned to support the FMEA. Others may require an extension of their original scope.

1) Protection Coordination Study: A comprehensive protection study is required covering the full range of power plant failures, taking into account the action of any bespoke protection system. In this case, the emphasis should be on ensuring continuity of power supply to the thrusters and other essential systems. It should not just focus on equipment protection.

2) Power Plant Stability Study: A study demonstrating that a faulty generator connected out-of-phase, connected when stopped or which loses synchronism for any other reason such as severe mechanical failure will not cause failure effects exceeding the worst case failure design intent. This study might be extended to examine the failure effects arising from incorrectly synchronizing two bus sections together.

3) Voltage Dip Study: This is required to confirm worst case voltage dip magnitude and duration combined with verification of the ride through capabilities of drives, motor starters and other essential consumers. This may complement the protection coordination study in respect of delays required for under voltage release settings etc.

4) Harmonic Study: This is required to estimate the worst case harmonic distortion for all intended operating configurations. This would normally be backed up by measurements onboard to confirm its accuracy in at least a representative sample of configurations including worst case. The study should also demonstrate the effect on levels of harmonics resulting from the failure of a harmonic filter or other power factor correction equipment.

### **Commercial pressures**

DP consultancies are commercial organizations like any other and must produce a profit to survive. The cost of an FMEA is determined typically by the day rate being charged for the service and the number of days required to complete the work. Day rates are influenced by market forces but the number of days required to complete the work is largely determined by the complexity of the design and the depth of the analysis. There can be considerable variation in the depth of analysis considered necessary and it can be difficult for those placing orders for FMEA work to understand why this should be the case. To understand why one company should require more analysis time than another for the same vessel it is necessary to understand the standards being applied. It requires an informed purchaser to understand their own needs and the expectations of their potential clients.

Over the last ten years much has been learnt and published about the failure modes of diesel electric power plant and vessel control systems. These advances in understanding have driven the level of analysis required to prove fault tolerance to ever deeper levels. This process has now reached the point where some are beginning to question whether the term FMEA accurately describes the process of proving fault tolerance which appears more closely aligned to 'design verification' than the process outlined in standards for FMEAs. Not all FMEA providers consider it necessary to perform such detailed investigations and this is reflected in the cost of the service they offer.

Those FMEA vendors who do consider it necessary to offer a more detailed analysis depend upon the support of vessel owners who share this view. Varying standards will continue to exist as long as turnkey shipyards, classification societies and vessel owners are prepared to accept a less detailed level of analysis.

### **Lack of detailed information**

Lack of detailed information is one of the most significant problems encountered when developing DP FMEAs for newbuild vessels. Often there is considerable pressure to deliver a preliminary FMEA very early in the design process and long before there is sufficient detailed design to support all but the most elementary conclusions regarding redundancy. It is appreciated that shipyards and vessel owners want reassurance regarding the suitability and compliance of the redundancy concept but there are better ways to address this issue. Issuing a preliminary FMEA which is substantially incomplete and which raises more questions than it answers benefits no one. An improved approach is to create a redundancy concept document in the basic design stage to guide the development of the detailed design. The detailed design can then be monitored as it evolves by using a 'drawing review process' to provide feedback to the

Phillips, Haycock, & Cargill      Reliability Session      FMEA Failed to Meet Expectations Again (Again?)

---

builder and vendors. The preliminary FMEA can then be developed later with the confidence that sufficient detailed information is available to support conclusions regarding the fault tolerance of the design.

### **Limitations on testing**

DP FMEA trials are performed to confirm the conclusions of the FMEA in respect of the DP system's fault tolerance. This process is limited by traditional FMEA proving trials techniques such as wire break testing, shutting down equipment, injecting erroneous signals and applying severe step loads. Hardware in the loop testing provides a means to extend traditional FMEA testing techniques and provides a better platform to assess the reaction of control systems software. HIL is now finding application in the testing of dynamic positioning control systems, power management systems, drilling control systems, thrusters other things.

As sea trials time is considered to be expensive there is always pressure from shipyards to reduce the amount of testing carried out in FMEA proving trials. Although there may be an opportunity to carry out some FMEA proving trials in cooperation with other activities such as commissioning and customer acceptance tests the best result is obtained by performing the DP FMEA proving trials once all commissioning activities are complete. Experience confirms that failure to properly commission a DP vessel before starting FMEA proving trials simply leads to a large number of deficiencies being identified which must be corrected and retested leading to the potential for further extended delays.

### **Reliability of information from equipment vendors and designers**

DP system FMEAs rely on designers and equipment vendors to provide information about the design of their products and systems by way of manuals, functional design specifications, equipment FMEAs or answers to technical queries raised by the FMEA team. What level of proof should be accepted in cases where only the equipment vendor has access to the detailed knowledge, particularly in cases where the FMEA issues in question may have significant commercial implications related to non compliance? Proof by testing is the preferred method but in some cases properties such as voltage dip ride through capability are not easily tested by traditional DP FMEA proving trials methods. At least one of the major classifications societies now requires that protection systems and voltage dip ride through capability are proven by applying a real short circuit to the main power distribution system under controlled conditions. This test must be carried out on any DP vessel intending to operate with a common power distribution system. This test has often revealed significant design errors and flaws that would defeat the redundancy concept and the author recommends that vessel owners seriously consider including such a test in the specification for future new builds. It is however important to ensure that all possible precautions are taken to limit the risk of equipment damage and injury. At present, the majority of DP vessel power generation schemes are subject to testing which proves much but does not fully recreate the power plant conditions experienced during a severe fault. Performance under transient conditions is often taken on trust until a real fault proves whether the system was fault tolerant or not.

The overwhelming majority of designers and vendors take FMEA issues seriously and provide the assistance necessary to resolve them. However, the FMEA practitioner must be wary of situations where the responsibility for resolving design flaws is clouded by contractual uncertainties or poor vessel specification. In such cases it may be difficult to obtain the necessary level of confidence that issues have been satisfactorily addressed.

### **Competence of the FMEA provider**

Many sectors of the oil and gas industry face significant challenges in recruiting and training staff to meet demand. In the past, DP consultancies could rely on a source of highly experienced staff from within the marine sector but this is no longer capable of meeting current demands and companies must look elsewhere to fill their expansion requirements.

To fill this experience gap DP consultancies have had to review the level of training and internal guidance they provide to their staff and review and enhance their internal processes.

Clients of DP consultancies should expect that staff are provided with job specific training supported by internal guidance on how to perform DP FMEAs and new engineers and analysts are adequately supervised until they become proficient. It is also reasonable to expect that suitable quality assurance measures are applied to the product to be sure that FMEA teams are performing to expectations.

### **DP FMEA development tools**

DP FMEAs have traditionally taken the form of a narrative discussion of the DP system and redundancy concept with or without tables and such formats are routinely accepted by all the major classification societies. Such an approach is vulnerable to omission of important information or analysis if not carefully controlled. Tabular FMEAs provide a means to more carefully control the content but space constraints limit the room for expression of complex failure effects which risks oversimplifying the discussion.

This problem can be overcome by creating a detailed and structured DP FMEA report template to assist the analyst and guide them to address all the important issues. The template is routinely updated with new sections and information from lessons learned. Any organization which invests heavily in FMEA internal training, a defined standard of reporting through standardized templates and analysis techniques will eventually develop a product which can be clearly differentiated from others and which is recognized by the purchaser and the purchaser's clients.

The main headings from such a detailed template are shown in the appendix. The numbering reflects the standard numbering system applied in the report. There can never be a 'one size fits all' template but a well constructed and maintained template provides a sound base for any vessel specific adaptation required.

### **Key elements of the analysis**

Any DP FMEA should address five key elements but some analyses may overlook or omit some of these

- Failure modes and effects
- Hidden failures
- Common mode failures
- Configuration errors
- Acts of maloperation

Failure modes and effects: This section documents the effects of single failures on the DP system to prove redundancy.

Hidden failures: This section of the analysis identifies opportunities for hidden failures to defeat the redundancy concept. At this stage, the analyst may make recommendations for alarms or periodic testing to reveal such failures before they can compound the effect of another fault.

Common mode failures: This section examines the possibility that systems that appear to be redundant may not be fault tolerant. This condition may arise because identical redundant elements that make up the system all react adversely to a common stimulus.

Configuration errors: This section discusses ways in which fault tolerance can be removed by incorrectly configuring a system which has more than one possible operating configuration. Recommendations may be made to provide alarms to indicate when the incorrect configuration has been selected or to include a configuration check in the DP checklist.

Acts of maloperation: This section examines the possibility that a single inadvertent act may lead to a loss of position and/or heading.

### **FMEA management tools**

To properly manage the information flow in a complex DP FMEA it is necessary to have a range of management tools such as those given here but these or something similar is not always used:-

- Technical query form
- Technical query register
- Assumptions register
- Maintenance, testing issues register
- Concerns register
- Progress reports

Technical Query Forms (TQs): This form provides a structured means to request information.

The Technical Query Register: This register provides a means for recording the date that information was requested and when the answer was received and serves to demonstrate to the client whether the information required to complete the FMEA is being received in a timely manner. It also forms a useful reference for all the FMEA team members to quickly locate the information they need or to find out what project resource information has been requested by other team members and thus avoid repeat requests.

The Assumptions Register: The register records all assumptions on which the FMEA is based. In any analysis it will be necessary to make some assumptions about the way certain items of equipment work and fail and how the plant is configured and operated. It is important that such assumptions are recorded in such a way that they can be reviewed by designers and the vessel owner's team so that they can be challenged if considered incorrect or inappropriate.

The Maintenance, Testing Issues Register: This records any periodic maintenance or testing on which the integrity of the redundancy concept depends.

The Concerns Register: This register provides a means to log and categorize important issues arising from the analysis and proving trials at the time they arise rather than waiting to include them in the preliminary FMEA. The concerns register should be included in the progress report but can be issued more frequently as required

Progress Reports: These reports should be issued at agreed intervals during the FMEA process and provide a means to inform the client of progress and other important issues related to the conduct of the FMEA. They should contain the three registers discussed above with a summary of any significant issues such as outstanding TQs that may be delaying progress. This allows the client to act upon any deficiencies in the design and also address any problems with information flow or availability.

### Conclusions and recommendations

From the analysis, it is clear that there requires to be a conclusion section in the FMEA and also recommendations when required. The development of these recommendations would require an

acceptable categorization such that it is clear to the reader the impact and risk related to each recommendation. It has been apparent that a number of FMEA recommendations have been diluted due to external pressures and hence the analysis can become diluted from a reviewer's perspective. Conversely, recommendations that are the opinion of the author and / or subjective can also damage the validity and objectivity of the whole analysis. Hence these two sections are considered to form the basis on which a reader will establish the risk profile of the specific rig or vessel.

### **Key missing failure modes and features**

There are several areas in most FMEAs which could be improved by consideration of the following:-

#### The Safest Mode of Operation

As mentioned earlier, there may be several options for setting up configurations of the electrical power system, especially with more complex systems. There may also be options in, for example, deciding which pumps run in duty/standby pairs for thruster hydraulic servos, cooling systems, and so on. When not set up as per the safest mode of operation, the effect of a hidden failure (failure to changeover to the standby device) combined with the worst case failure (WCF) could easily lead to a failure mode greater than the WCF.

As an example, consider a diesel electric vessel with HV distribution supplying two bow thrusters and two stern thrusters. Each thruster has two hydraulic servo pumps, powered from opposite sides of the low voltage distribution. The safest mode of operation would be to select the duty pump to be that which derives its power from the same side as that thruster's main drive motor to remove dependence on a standby start.

However, it is often a condition of planned maintenance to alternately assign the duty pumps to the opposite side LV distribution to balance the running hours. During DP2 operations this configuration increases the risk that the worst case failure effect will be exceeded if the servo pumps fail to changeover (hidden failure as above). In such circumstances both bow thrusters and / or both stern thrusters could be lost (one thruster lost due to loss of HV and the other due to loss of the associated LV). If one accepts that duplicate pumps are provided to improve thruster availability in the event of pump failure (not power supply failure) then both thruster pumps should be supplied from the same side of the power distribution system as their respective thruster motor. Such an arrangement has no restrictions for planned maintenance.

Many DP vessels have the facility to cross feed auxiliary systems such as fuel oil systems, seawater cooling, fresh water cooling and compressed air. The intention of such cross feeds is to provide a 'get home mode' or to enable continued operation during maintenance. With complacency or poorly defined procedures, it is possible that essential systems could be left in a cross connected mode (a configuration error), increasing risk of exposure to a common failure mode and defeating the redundancy concept. The safest mode of operation should clearly define the correct configuration of auxiliary systems.

Other items that should be included in the safest mode of operation include:-

- Checking operation of changeovers
- Checking status of batteries and ability to switch over to them
- DP control system set up
- Power management set up
- Selection of PRS and sensors
- Ventilation and air conditioning
- Operation of manual controls and Independent Joystick

The FMEA should clearly define the safest mode of operation or give the information required to define it. The safest mode of operation should then be included in the DP checklists or added as an appendix.

#### AVR and Governor failures

Many AVRs have comprehensive protection and limiting functions built-in which are set during commissioning, but these need careful review by the FMEA practitioner. There are a number of essential considerations when setting this equipment, not just the protection and control of the individual generator. The setting of all components of the protection suite must co-ordinate with the vessel's protection and control systems.

For instance, should the AVR lose voltage sensing, it can force the output to maximum excitation, thus causing the affected generator to potentially force other connected machines into a loss of excitation condition. Unless correct coordination is achieved, this could lead to the loss of the healthy machines prior to the AVR tripping its associated circuit breaker on loss of sensing detection. The FMEA should examine how the AVR co-ordinates with the generator's under / over excitation protection. This is typical of information that is not available until after commissioning is complete, but should be verified before the FMEA is finalized. It should also be noted that a 'loss of sensing' function does not provide complete protection against all excitation system failures of this type and additional protective functions may be required.

The potential for a governor to fail to full fuel should also be examined. This can lead to a situation in which the engine with faulty governor takes the entire load, pushing healthy machines into reverse power. If there is insufficient base load, all healthy engines may trip on reverse power, followed by trip of the faulty engine on over speed or overload. The co-ordination of load reduction schemes for example, drilling phase back, should also be examined as the problem could be compounded by a reduction in load as the highest loaded (faulty) generator triggers the load reduction.

In modern systems, these types of problems can be dealt with by software functions in the power management system or dedicated systems that monitor each individual generator.

#### Full load capacity and load acceptance

At shipyard trials and possibly at commencement of a contract, engines and thrusters are normally tested at 100% load. However, with time, the ability of such machinery or its auxiliary systems to operate at full power can become severely degraded. If this condition remains uncorrected, an engine or thruster may trip on over-temperature or some other protective function if required to operate at high power levels. For this reason the safest mode of operation requires that thrusters, main generators, shaft generators etc. have been tested at 100% load at field arrival or within the last six months. It is assumed that this test is conducted in realistic conditions, simulating the power transition from below 50% to %100 at the rate demanded by the DP system or independent joystick system. The ability of engines to accept the maximum step load acceptance with worst-case loss of other online generators may also require consideration. It is generally accepted that rapid load shedding systems may be used to compensate for restrictions in load acceptance but the effectiveness of such functions must also be proven periodically.

In a typical DP vessel, with redundant thrusters, an allowable maximum thrust level can be defined which allows for the WCF to occur and the required thrust can be maintained by an increase on the remaining healthy thrusters and generators. In very simple terms, a vessel with two bow thrusters is considered fault tolerant up to around 50% thrust. Should one of the two thrusters fail, the required thrust would be provided by the remaining thruster increasing to 100%. If two out of three thrusters is a possible failure mode, the maximum thrust would be around 33%. Note that in practice other factors need to be considered and some allowance should be made for the lever arms of the thrusters and further reductions if one of the thrusters has a higher rating. It should also be remembered that in a diesel electric system the increase in load seen by the generators may be significantly higher due to the non linear relationship of thrust to power.

In more complex power systems, where many redundant configurations are available, the logic and capability of all practical or intended configurations should be analyzed to enable the maximum % thrusts and maximum % generator load to be defined in the safest mode of operation. This would allow for one or more generators or even switchboards to be taken out of service for maintenance.

#### Deficiencies in the Consequence Analysis

The consequence analysis function required by class for all DP2/3 vessels, is a useful tool in assisting computation of the maximum level of thrust referred to above, and alerting the DPO when levels are being exceeded. This is especially true for vessels with complex power system and thruster arrangements. However, the consequence analysis is not required to cover failure modes other than that normally defined as the WCF. For example, in vessels where the supply of fuel oil to engines is not a straight two way split fuel system problems may result in greater loss of generators than those associated with distribution system failure when certain combinations of generators are connected. Alternatively, if the high voltage switchboard is capable of a four way split, the consequence analysis may only consider loss of one section, even though, with one or more sections connected together, failure modes exist that could affect more than one section of bus.

In addition, several examples have been discovered where the allocation of inputs and outputs (I/O) to the DP control computer has not been made in line with the redundancy concept. In these systems, loss of a single I/O module could lead to a loss of equipment exceeding the WCF and the consequence analysis does not consider these failures.

Another common failing of consequence analysis is that it does not recognize 'Time to terminate' and no attempt is made to predict how fast position will be lost or in what direction. Also few consequence analysis designs consider the task appropriate mode, for example, in the case of drilling operations, does the system acknowledge that drilling load can be phased back? Such failings lead to inappropriate alarms resulting in the consequence analysis being "turned off".

#### Assignable Generators and Thrusters

Another problem encountered with allocation of inputs and outputs (I/O) to the DP control computer is with Diesel generator sets and thrusters that can be assigned to alternative bus bars. Since the I/O is allocated to one module only, the failure mode for loss of an I/O module will depend on how the equipment is assigned. The FMEA should analyze the possible configurations and capture the preferred assignment in the safest mode of operation.

#### Power system interface to DP / Blackout prevention

In a diesel electric system, the DP system is required to include a blackout prevention mode that reduces power demand of the thrusters when a shortfall of power occurs or is approaching an overload situation. To facilitate this function the DP interface would include the status of each generator and bus tie breaker and each generator's real power consumption. Clearly, failure of any of these signals can result in power limiting functions operating too late or too early. The requirements for FMEA should include checking that comprehensive cross checking of the signals is included in the DP software, that the system fails safe and an alarm is initiated.

Although everything possible must be done to prevent a blackout, this eventuality cannot be ruled out and robust plans should be in place for a rapid recovery. Optimization of blackout recovery should be part of FMEA, FMEA proving trials and annual trials.

#### Inclusion of propellers and rudders in redundancy concept

The use of propellers and rudders to provide lateral thrust at the stern of a vessel usually entails one propeller running astern and one ahead. The rudder behind the ahead running propeller provides the lateral thrust and the other propeller (running astern) is used to offset the unwanted ahead thrust.

There are many vessels in the field with shaft generators and a single stern thruster where loss of a main engine leaves the vessel with one bow thruster, one main prop and one rudder. In this situation, thrust at the vessel's stern is only possible from the remaining propeller and single rudder so the vessel can only DP into an ahead environment above a certain threshold (there is no way to get rid of the unwanted ahead thrust). Many FMEA's and even class have overlooked this problem.

#### Failure of tension interface or similar.

There are several DP applications where an external force is acting on the vessel in addition to the environment, such as the pipe tension in a pipe layer or the hawser tension in a shuttle tanker. It is normally possible to measure the external force that can be input to the DP controller and which operates as a feed forward term. This is similar to the concept of 'wind feed forward' using measured wind speed and direction to provide immediate reaction to changes in wind, rather than waiting for the model to learn it. Thus, the DP system can respond immediately to a sudden change in the external force. However, if the signal representing the external force fails, the DP system will command a greater or lesser force than is actually required, causing a drive off. This is another area that is not always explored in the FMEA.

#### Specific DP Applications

There are several other specific applications of DP where FMEAs do not consider the special requirements that need to be investigated. For example, heavy lift crane barges where as the load is transferred, the mass of the lifting vessel changes and an additional lateral force becomes evident via the crane. Similar situations exist for fire fighting modes with fire monitors; shuttle tanker offloading modes and the associated problems with fishtailing and surging.

#### Suitability of Position Reference Equipment for application.

The requirements for equipment classes 2 and 3 in MSC645 are that "at least three position reference systems should be installed and simultaneously available to the DP-control system during operation. When two or more position reference systems are required, they should not all be of the same type, but based on different principles and suitable for the operating conditions".

DP vessels have been operating in deeper water for some time now, where the use of position references may be limited to DGPS and Long Base Line acoustics. Typically, drilling vessels operating in open water will only have acoustics and DGPS based systems.

Often relative position reference systems based on laser or radar principle are employed on OSV's operating against a tension leg platform or Spar. These structures can be subject to significant movement within their anchor systems, which prevents the combined use of the relative position reference with DGPS on the OSV. Clearly, the intention in MSC 645 cannot be met in these situations. FMEAs do not always examine the implications for the loss of diversity which is implied in above and additional precautions that should be taken in mitigation.

#### Independence of Position Reference Systems (PRS).

Other areas which some FMEA's may omit to analyze, are the actual independence of the Position reference systems from their power supplies, input of sensors or input of the data to the DP controller via input/output (I/O) boards. It is not uncommon to find during annual trials that power supplies to the component parts of a DGPS system have been crossed over such that all DGPS systems are failed by the loss of one UPS output. This is due in part to the 'plug and play' nature of a typical DGPS system. Acoustic systems, especially for Ultra Short Base line, are dependent on the input of motion reference units (MRU) to provide pitch and roll data. Other systems require compensation for pitch and roll relative to height above centre of gravity and this is normally calculated in the DP. Sometimes changeover switches are supplied to enable selection of which MRU is fed to which system, which may then result in multiple PRS being dependent on one MRU.

### Back up DC supplies

A DP system may contain several items of equipment that have dual supplies, typically one at 230V and the other at 24Vdc. The 230V supply is normally converted to 24Vdc and connected to the other supply using blocking diodes. This arrangement is typical for some gyros, thrusters and engine electrical control units. The possibility of hidden failures due to one or other supply failing, or diode failure which is more difficult to detect, means that regular tests of the circuit should be conducted. Ideally, both supplies would be monitored and alarmed.

Of greater concern is an arrangement in which a single 24Vdc supply is used to provide the backup supplies to several redundant elements such as all the ship's gyros. The danger here is that all three gyros could be damaged should the 24Vdc fail to a high voltage level. This occurs because the blocking diodes always pass the highest voltage. The FMEA should confirm diversification and independence of supplies or at least ensure over voltage protection is designed into these circuits.

### Ventilation

FMEAs do not always consider the potential for common mode failures due to ventilation problems in common engine rooms. Stopping of individual fans and partial loss of forced ventilation does not generally limit engine power significantly but inadvertent closure of all engineroom fire dampers can have a severe effect and may also be a safety hazard.

In some engine protection systems there is a risk that inadvertent closure of the supply and exhaust dampers in an engine room, could cause spurious operation of the crankcase pressure sensors on all the engines in the same room. This creates a change of set point for atmospheric pressure. The negative pressure changes the baseline of the sensors and trips the engines.

Another engine related problem which can lead to multiple engine failures is the false operation of Oil Mist Detectors when all units are supplied from the same compressed air supply, and where the action on loss of the air supply is to trip the engines, not just alarm. Similar problems can be created by blockage of common crankcase breathers and the FMEA should ensure that crankcase ventilation is considered in the same way as any other auxiliary system.

### Location of DP Sensors.

Many FMEAs do not always check that sensors are located at the most effective position to obtain consistent measurements. For the most accurate measurement, MRUs should if possible be placed at vessel centre of gravity (C of G) but are normally most sensitive to height above C of G than lateral offset from it. Modern MRUs can be located in a convenient spot but be configured with lever arms to provide measurements corrected to C of G. Normally it is hard or impossible to actually install a MRU at true C of G anyway. It is worth noting that the roll center for a ship is not a constant spot so any location is a compromise since no location is always correct.

Wind sensors need to be clear of obstructions that can block the wind or cause turbulence around the sensor.

A recent incident on a semi submersible during a squall involved a false reading on two poorly sited wind sensors which outvoted the good measurement on a third wind sensor and caused a drive off.

The median value of three selected anemometers was used. Two of the anemometers recorded no change in wind measurement, so the anemometer which did see the wind speed and direction change was voted out. Because in this instance the median value of measured wind was significantly different to actual, an excursion took place.

### Operator errors.

IMO guidance and DNV rules require consideration of a single act of maloperation if such an act is reasonably foreseeable. The FMEA should check that such acts are guarded against or at least consider

the effects of such an act. However, this is no substitute for good training of operators and a full understanding of the effect of operation of each of the DP controls.

One example in a recent incident where a vessel had a temporary excursion, a DP operator pressed the 'present position' button three times during the incident which allowed the DP controller to relax and so the vessel continued to drift.

#### Systemic failure

A systemic failure is defined as one due to design, construction or use of a system which cause it to fail under particular combinations of inputs or under some environmental conditions. This can give rise to a failure of all equipment of the same type simultaneously. The risk of systemic failures in the DP hardware and software is kept low by rigorous testing. Mitigation by use of diverse hardware and / or software as used in other industries, has not been considered cost effective for DP control systems.

However, consideration could be given to providing diversity of sensors by installing different types or manufacturers. The FMEA process should highlight this possibility early enough to enable components to be specified and not when it is too late and they have already been purchased.

#### Capability plots not considering WCF

DP capability plots are calculated to meet class, and provide ESKI / ERN numbers etc. For example, to compute an ERN number, plots are made for the fully intact case, loss of most effective thruster and least effective thruster. Thus plots are not always calculated for the WCF and rarely ever for failures greater than the WCF as discussed above for failures to fuel oil systems, DP inputs/outputs modules, equipment down for maintenance, etc.

The DP software in many modern systems provides the facility for on line capability plots. Again, these should be verified against the theoretical plots and real situations whenever possible. As part of the overall FMEA process, theoretical capability plots should be checked whenever an opportunity presents itself. The format of plots should be as per a common standard such as defined by IMCA M140 so that a like for like comparison is possible.

#### Fuel contamination

Although it may be considered an operational issue, the FMEA does not always discuss the need for rigorous anti-contamination procedures in order to prevent water or microbiotic contamination of all fuel systems. These can be considered as hidden failures such as irregular or non-operation of settling tank sludge cocks or the continuous use of the high suction from service tanks with high and low suctions. Or configuration errors such as setting purifier throughput too high or operating with purifier gravity discs that do not match the specific gravity of the fuel in use.

#### Risk of Engine Room Fires

The FMEA should consider the risk of engine room fires and if all available preventative measures are in place. An inspection of the vessel considering the following points (from IMCA M04/04) should be conducted during the build stage or at least during FMEA proving trials.

- Fuel leaks should not only be considered for Class 3. If it is clear that a leak on a Class 2 vessel cannot be isolated such that a failure worse than the desired worst case fuel failure occurs, the fitting of additional valves should be considered.
- Fuel leaks with respect to fires should be considered on both classes of vessel. They should at least have double skinned high pressure piping, fuel leak detection and there should be no hotspots. The latter may be identified by thermographic survey.

#### Cooling systems, and thruster hydraulic systems header tanks

Fresh water cooling systems and thruster hydraulic systems often depend on header tanks to supply the required system operating pressure. Monitoring of the tank level is normally provided and is useful as the first indication that a leak may be present. Tank level sensors are not always installed and the FMEA should state explicitly if monitoring and alarms are provided or not.

Undervoltage trips of circuit breakers and motor starters

Severe voltage dips can be a source of common mode failure especially in the case of power plants operating with closed bus ties. Under voltage release may be installed on generators and service transformers for various reasons but if it is fitted there should be suitable delays to ensure the circuit breakers remain closed during the worst case voltage transient which will normally be associated with clearing a short circuit fault in the power distribution. The magnetic contactors in motor starters may also be vulnerable to the effects of voltage dips and contactors may open causing pumps and fans to stop. The FMEA should consider the effects of voltage dips on all power consumers and confirm their ride-through capability by reference to manufactures data or by suitable testing where practical. The FMEA may also consider if under voltage trips are necessary or can be removed.

DP/Manual/Independent Joystick changeover switch

It is accepted that some areas of otherwise redundant DP systems will have non-redundant connections between them. One such area is the changeover between manual, DP and independent joystick. Often all the thrusters are switched simultaneously by a single multi wafer switch. A better arrangement is individual switches for each thruster. One application for sensing the contacts of the wafer switches uses two 24Vdc systems connected by blocking diodes, which despite appearing to have good redundancy has a single failure mode at the common connection point, and is vulnerable to hidden failures. The FMEA should but doesn't always investigate the integrity of these changeover arrangements.

## Appendix

### **Suggested Section headings**

SUMMARY

TABLE OF CONTENTS

1. INTRODUCTION
  2. ENGINES AND AUXILIARY SERVICES
  3. POWER GENERATION
  4. POWER MANAGEMENT
  5. POWER DISTRIBUTION
  6. THRUSTERS - (Including main props)
  7. VESSEL MANAGEMENT SYSTEM - (Or similar titles e.g. IAS, ICMS IVCS)
  8. DP CONTROL SYSTEM
  9. SAFETY SYSTEMS
  10. PROTECTION AGAINST FIRE AND FLOOD – (DP Class 3 only)
  11. CONCLUSIONS AND RECOMMENDATIONS
- APPENDIX A ABBREVIATIONS

### **Headings in INTRODUCTION**

Within the INTRODUCTION section there are the following headings, drawings and associated discussion.

- 1 INTRODUCTION
  - 1.1 GENERAL
    - 1.1.1 Instructions
    - 1.1.2 Scope of work
    - 1.1.3 Conduct of the work
    - 1.1.4 Applicable rules and guidelines
    - 1.1.5 FMEA document history – (Reference to any previous FMEAs)
    - 1.1.6 FMEA proving trials – (Reference to test document)
    - 1.1.7 Software – (Reference to record of software installed at FMEA proving trials)
    - 1.1.8 Acknowledgements – (Optional)
  - 1.2 VESSEL PARTICULARS
    - 1.2.1 Description of vessel – and figure with general arrangement
    - 1.2.2 Principle dimensions
    - 1.2.3 Machinery and DP equipment list
  - 1.3 FMEA ANALYSIS
    - 1.3.1 Objectives of FMEA
    - 1.3.2 Limitations of FMEA
  - 1.4 FMEA PROCEDURE AND METHODOLOGY
    - 1.4.1 Method
    - 1.4.2 Structure of the FMEA narrative
    - 1.4.3 Management of the FMEA process
    - 1.4.4 Procedural and technical assumptions – (Reference to register)
  - 1.5 REDUNDANCY CONCEPT

- 1.5.1 Worst case failure design intent(s)
- 1.5.2 Overview of redundancy concept with figures for overall SLD and Thruster arrangement. – (Discussion of how redundancy is achieved in each subsystem)
- 1.5.3 Operational configuration of the DP system – (related to WCFDI , all subsystems, all modes)
- 1.5.4 Common points between redundant systems
- 1.5.5 Protective functions upon which redundancy depends
- 1.6 POWER AND PROPULSION CAPABILITY
- 1.6.1 Relationship between power and thrust
- 1.6.2 Effect of worst case failure on power generation and thrust capability

### Headings for each SUBSYSTEM

Within each subsystem there are the following headings. – Replace the word 'system' with appropriate name e.g. ENGINES AND AUXILIARY SYSTEMS. Replace 'subsystem' with the appropriate name e.g. FUEL OIL SYSTEM.

- 2 SYSTEM
- 2.1 SUBSYSTEM
- 2.1.1 Document reference
- 2.1.2 Description, and redundancy concept – (including simplified sketch of subsystem)
- 2.1.3 Location
- 2.1.4 Configuration for DP
- 2.1.5 Failure modes of the subsystem
- 2.1.6 Effects of subsystem failures
- 2.1.7 Hidden subsystem failures
- 2.1.8 Common mode failures
- 2.1.9 Configuration errors
- 2.1.10 Acts of maloperation
- 2.1.11 Worst case failure of the subsystem

### Headings within the CONCLUSIONS and RECOMMENDATIONS section

The conclusions and recommendations section has the following headings:-

- 11 CONCLUSIONS AND RECOMMENDATIONS
- 11.1 CONCLUSIONS
- 11.1.1 General – (Statement of the work done)
- 11.1.2 DP system configuration for analysis
- 11.1.3 Other system configurations
- 11.1.4 Worst case failure – (for configuration analysed)
- 11.1.5 Compliance with rules and guidelines
- 11.2 RECOMMENDATIONS
- 11.2.1 FMEA companion document - (Reference to, if provided)
- 11.2.2 Recommendation categories - (By severity in relation to the WCFDI)
- 11.2.3 Category A
- 11.2.4 Category B
- 11.2.5 Category C

**References**

FMEA – Fail to Meet Expectations Again? – Doug Phillips MTS DP Conference Houston 2001

IMCA M04/04 – Methods of establishing the Safety and Reliability of Dynamic Positioning Systems - March 2004

IMCA M140 - Specification for DP Capability Plots – Rev1 June 2000

PES - Programmable Electronic Systems in Safety Related Applications – HSE 1995

IMO MSC Circular 645 Guidelines for Vessels with Dynamic Positioning Systems – June 1994