

Marine Technology Society

Dynamic Positioning Conference

21 - 22 October, 1997

Session 4

Reliability and Risk Analysis

Reliability and Risk Analysis

By:

Howard Shatto

Shatto Engineering, Inc. (Houston)

Failure Modes and Effects Analysis (FMEAs)

By

Doug Phillips

Nautronix (San Diego)

Session Planner

Howard Shatto *Shatto Engineering (Houston)*

SESSION 4

Session Planner

RELIABILITY AND RISK ANALYSIS

Howard Shatto
Shatto Engineering

History of DP Reliability

Author

Early systems successes and failures
Enter Reliability Engineering
Their effect on MTBF

Howard Shatto

Failure Modes and Effect Analysis

Author

Background
Objectives of a FEMA
Scope of a FEMA
Level and Format of a FEMA
Problems with FMEAs of DP Systems
Examples of Failures

Doug Phillips
Nautronix

Reliability Analysis

Author

Reliability defined
Availability
Failure rates and MTBF
Series of subsystems
Redundancy effect
Weather's effect on reliability
Other factors influencing reliability
Power management system
Data logging and diagnosis
Operator training
System design and the misplaced incentives
MTBF goals and budgeting
Typical subsystem and device MTBFs
Need for better data
DP vessel failure records
Disclosure of records
Risk Analysis

Howard Shatto

RELIABILITY AND RISK ANALYSIS

History of DP Reliability

Early systems successes and failures

The world's first automatically controlled dynamically positioned vessel was spectacularly successful in spite of its appalling lack of reliability. Built by Shell to drill ocean floor core samples, she began operation in 1961. This little 400 ton 400 HP ship drilled several times as many core locations per day at her anchored rivals, and where they were limited to about 300 ft of water, the *Eureka* went to 4000 ft. See fig 1 over page. Her DP system was single thread all the way, with one azimuthing thruster forward and one aft, one taut wire, one gyro and one analog controller each for X, Y and yaw. Failure to hold position was surprisingly frequent. We didn't measure failure frequency, but down-time was over 20 percent for the first year.

Fortunately the cost for position failure was not very high; some bent drillpipe and the occasional loss of a bottom-hole assembly.

Eureka



Fig. 1

Ten years later, when Sedco built the 445 for Shell, we tried to have redundancy everywhere. See Fig 2

There were 11 lateral thrusters and six motors on each of the two main screws, taut wire and two acoustics processors, two gyros and two control computers. There were teething problems and unexpected single point failures which were eliminated as they erupted. But all in all she too was very successful as the world's first dynamically positioned riser drillship for oil exploration.

New DP drilling vessels built throughout the '70s were much the same in that they had a minimum of dual redundancy in all of the obvious places. By the early '80s the track record of some of the best contractors showed a fairly consistent average of about one position failure or disconnect every six months.

Sedco 445



Fig. 2

After some modifications to tackle 7500 ft water off the East Coast, the *Discoverer Seven Seas* started to drill for Shell in July of '83. See Fig 3. Addition of long base line acoustics probably improved reliability for the deep water, but we had little reason to expect much other than the average six months between failures. Two very expensive disconnects within the first three months of operation got our attention.

Both were single point failures even though the *Seven Seas* had been in operation on DP for about six years. Again the record showed that many of the past DP failures had been single point failures and that in each case a modification had been made so that that failure would be far less likely to reoccur. The fact that new ones had kept presenting themselves led to the conclusion that there were very likely a great many more that were still lying in wait.

Seven Seas



Fig 3

Enter reliability engineering, the first FMEA for DP Drillship

How to find single point failures? Where to go for expertise? Honeywell had built the DP controls and offered their help. They did a lot of work for the military and had some first rate reliability engineers. Thinking they might not find much fault with their own equipment we also got a proposal from Boeing. They had reliability engineers available but advised that it would take six months for them to learn enough about DP to do the job properly. Since speed was important, we went with Honeywell and were quickly impressed with their thoroughness and professionalism and impartiality.

This effort was to cover the whole DP system, that is everything that had to be working for the ship to hold station. However, to speed the process further, the decision was made to spend little or no effort in areas that were already clearly redundant. This included the engine/generators, thrusters and main propulsion motors and their power supplies. Honeywell's first act was to validate all of the system drawings by checking them on board with much help from the Offshore Co., now Transocean, team members. As drawings were cleared they were immediately studied by the reliability engineers.

Results were quick in coming. Within a few weeks from the start of the project, thirty single point failures had been identified, several within the Honeywell controls. A second phase was started concurrently to find means and make necessary changes to eliminate the potential failures as they were discovered.

The effect on Mean Time Before Failure or MTBF

As part of their analysis the reliability engineers had included for each failure a rough measure of its probable frequency of occurrence. From this it was estimated that by eliminating these single point failures, the total system MTBF was likely to improve from the previous level of about six months to a new level of about two years. Subsequent performance proved this prediction to be just about right.

Since both the drilling contractor and the oil company had much to gain through this exercise, the total cost of about \$130,000 was shared between them. What did they gain? The average cost of a disconnect at that time was estimated to be about \$1 million. Reducing the number of disconnects from four every two years down to one is a recurring saving of \$3 million every two years. What seemed rather expensive at the time turned out to be a very highly profitable project.

If time had been taken to study those areas that had been declared out of bounds for the sake of speed, it is possible that even more improvement would be seen. Later changes and the additions of Starfix and then DGPS have brought present system MTBF up to about five years.

Failure Modes and Effect Analysis of Dynamic Positioning Systems

Background

As already mentioned operators and charters of Dynamically Positioned (DP) vessels seek to have redundancy built into the system when the consequences of a failure are such that there may be a danger to life, and or there may be serious economic consequences, such as damage to equipment or vessel down time.

As Dynamic Positioning was used more for vessels performing saturation diving the desirability of fully redundant systems for this application also became apparent after some serious accidents or near accidents on DP vessels. These resulted in the UK and Norwegian authorities producing joint guide lines for DP diving vessels and then later DP drilling vessels. These addressed not only the DP control system but also its supporting systems, as well as the operational procedures the vessel personnel should follow and their training. These matters were also taken up by class initially by DNV then followed by Lloyds, ABS and others. The class rules generally only deal with equipment and do not deal with operator competence, training etc. To fill this gap and to help self regulate their industry the DP Vessel Owners Association (DPVOA) was setup and produce Guidelines for the Design and Operation of DP Vessels as well as guidance on the training of DP operators and associated personnel. These DPVOA documents have been adopted almost totally as part of IMO guidelines for DP.

It is all very well to have these rules and guidelines but how can the redundancy be checked? This is done by performing a Failure Mode and Effects Analysis (FMEA) on the DP system to find the single point failures that can cause position loss.

Objectives of a FMEA

The objective of an FMEA, as applied to a DP vessel, is to provide a comprehensive, systematic and documented analysis to establish the important failure modes with regard to station keeping. The analysis must seek to determine any failure modes that can affect the station keeping as a whole and cause a position loss. The possible modes of position loss are:

- Drive off
- Drift off
- Large excursion

The analysis seeks to find any single point failure in any of the total DP system that can cause any of the position losses stated. The FMEA of a DP vessel is based on a single failure concept under which each system's subsystems and parts are assumed to fail by one probable cause at a time.

It is also customary to include a single act of maloperation as a possible single failure. This is assessed when a mistake is easy to make due to system layout where a single act has severe consequences. 'Single act' is a subjective definition and is generally taken to mean the operation of a single button, lever or switch.

The analysis must also consider hidden failures, this is a failure of a back up or standby without an alarm so that a second failure is not realized until the initiating single failure has occurred. For instance a standby pump being faulty, or a UPS having a faulty cell and being unable to take load when required. It must also consider that on some vessels that are in continuous operation, such as drilling vessels, where some equipment may be down for maintenance for long periods of time.

Any failure mode, which may cause a catastrophic loss of position, should be shown by the analysis to be guarded against by system or equipment redundancy, unless the probability of such a failure is extremely low. For some failure modes it may be reasonable to accept corrective measures in lieu of redundancy. It may also be acceptable to have procedures in place that mitigate or reduce the probability of a potential failure going undetected. For example a DP watch keepers check list can be used to check say all acoustics are not on the same vertical reference unit; mobilization or field arrival trials can be used to check all back up pumps, back up battery supplies etc.

Scope of a FMEA

Originally, and to some extent even now, the term 'DP system' tended to mean just the DP control system, however the term is now used for all the vessel's systems needed to support and keep it on position. These include the power generation, power distribution, thrusters, and even the operators, as well as the DP control system itself. Systems to be covered should typically include:

Power Generation	prime movers, generators, fuel system, sea water cooling, fresh water cooling, lubrication, compressed air, ventilation.
Power Distribution	high voltage, medium voltage, low voltage ac, low voltage dc, control supplies,
Thrusters and Propulsion	drives, control system, cooling, lubrication, hydraulics, manual to DP changeover, DP interface

Power Management	load sharing, load shedding, load reduction, black out recovery, DP interface
DP Control System	input output system, data highways, position reference system processing, DP changeover, DP power distribution, UPSs, power limiting, control modes, operator interface
DP Sensors	gyros, vertical reference sensors, wind sensors
DP Position Sensors	acoustics, taut wire, DGPS, riser angle etc
Human Factors	capability plots, footprints, communications systems, operator competence, operator (DP and ECR) training, operator experience, working conditions, check lists, operations manuals, standing orders, man machinery interface

Level and Format of a FMEA

Most FMEAs of DP vessels are based on the functional and hardware partitioning of the system into descriptive and block diagram form. The level at which this partitioning takes place, i.e. to what component level, plus the form of the analysis determines the detail to which the analysis will be performed. The more detailed a study the lower the risk of missing a critical failure but the higher the cost. However the cost of the FMEA may be repaid many times over if it prevents an expensive incident.

Often though it is not necessary to proceed into the detailed FMEA of a particular item if it can be decided at the higher level that it is not critical and need not be investigated further.

The format also affect the cost and level of analysis. One approach is to provide a description, and possibly a block diagram, of each vessel system which is essential to the positioning of the vessel its method of operation and possible failure modes. This provides the rationale by which the failure effects can be established.

The format can be made more detailed by performing the analysis using a tabulated format. This forces the analysis into a more systematic approach and requires each part of the table to be considered. The more comprehensive the table format the more detailed the analysis will be. A typical simple set of table headings might be:

FAULT	SYSTEM EFFECT	BACK UP	SYSTEM/ALARM

A more detailed format might be:

ITEM NOS	COMPONENT	FUNCTION	FAULT	FAULT DETECTION	RESULTING ACTION	OPERATOR INFORMED BY	REMARKS

The tabulated format can just as well be presented in a fault tree type presentation where the sequence of events following a failure run from top to bottom of the ‘tree’.

The tabulated format is the more analytical but can restrict the freer thinking that may be necessary to find some of the single failures. The descriptive analysis is better for this, so generally a mixed approach is best. In addition the descriptive part should demonstrate the analyst’s full understanding of the DP system he is analyzing. The fault tree is the most easily read but may be too time consuming to do for every conceivable fault, it can however still be used in combination with the other techniques for specific very critical failures.

Other concepts that may want to be introduced are: criticality (or severity) and probability with this an attempt is made to grade the severity and probability of all the failures. The probability can be a simple classification into low (extremely improbable), medium (remote possibility) and high (frequent and reasonably possible). The severity can also be into categories based on consequences e.g. catastrophic, hazardous, major, minor. These may be a subjective categorization based on experience or be based on reliability figures from historical data or specific studies. A catastrophic consequence as a result of a extremely improbable failure may be accepted as reasonable. Similar minor consequences of a reasonably possible event may be acceptable. Other combinations will not.

Problems with FMEAs of DP Systems

Timing

To obtain maximum benefit from a FMEA is important that it is performed at the appropriate time in the design process of a DP system. This is however difficult to time because the design needs to be far enough along to have something to analyze. It must not though be so far along that it cannot be altered based on the findings of the FMEA. A FMEA can still be of great benefit even if it is performed on an existing system as it can reveal limitations and some solutions need not be major but still be worthwhile. The

optimum is to perform the FMEA at the design stage and continue enhancing it through the duration of the whole project, finally updating it after sea trials, and then revising it following future modifications to the system.

Design

An FMEA is often seen by designers of DP systems as a criticism of their design. However all designers of safety critical systems should and do design with failure in mind. The FMEA is simply a double check on this process. If the design is done with the FMEA in mind to begin with then the findings of the FMEA are going to be less influential on the design itself.

Software

It is difficult to FMEA the DP control system software as its failure modes should generally result in a watchdog trip or a total system crash. To check it for other failure modes all possible failure modes of its inputs need to be considered and the software's reaction to them can be used to realize the failure effects. Similarly any failure in the software would be similar to the possible failure modes of the DP control system's outputs.

Failures

Fundamental to the success and usefulness of the FMEA is the expertise and experience of the person or persons performing the analysis. A DP system encompasses many different engineering disciplines it may therefore require a multi discipline team to perform the FMEA. Experience of DP is also needed. Wide personal experience has to be drawn upon but another useful source of experience is the IMCA database of DP incidents. This is a collection of real DP incidents reported to IMCA, these have been collected over many years. These provide event trees of incidents that resulted in a position loss to the surprise of the operator. It is interesting to note that at least half of all such incidents are attributed to operator error, not just the DP operator but any person associated with the positioning of the vessel.

Confirmation

Initially the FMEA is a paperwork theoretical analysis and to meet class this is all that needs to be submitted. However IMO and DPVOA require proving trials to be conducted on the vessel to verify the findings of the FMEA (good and bad). The FMEA of the DP control system in particular should be used as a basis for the factory test procedures it is to meet. This can impact the cost and program for the DP system and the vessel itself, however the costs saved later when a fault may occur for real and expensive damage is done.

Examples of Failures

The IMCA database of DP incidents contains numerous examples of what can and has failed on DP vessel with a resultant position loss. These are categorized for different levels of seriousness. The more interesting of these are those where redundancy has been assumed and taken for granted but something very fundamental manages to circumvent it. Some would have been very difficult to imagine during a FMEA but are more obvious once the incident has actually occurred. The FMEA is therefore not the end of the checking of a vessel. When these incidents are read and issued each year every vessel operator should ask 'Could that happen here'. 'Has the FMEA covered that'.

Some examples of actual events on DP vessel are given below.

- 1) A vessel with split engine rooms and buses, running bus connected, had a fire in one engine room. The operator shut down the engines in the engine room that was on fire and the load of all the thrusters was then instantly placed onto the remaining generators and the system volts dropped and the vessel blacked out.

A similar thing occurred with a vessel running split bus when one side blacked out the DP control system lost half of its thrusters. A failure mode it was designed to cope with and the DP control system therefore increased the load on the remaining thrusters to compensate, this blacked out the remaining healthy. In addition when these types of things occur the voltage drop and transients in the power system are such that all the starters of ancillary equipment such as hydraulic pumps, cooling pumps trip, etc. and the system is lost by that means.

- 2) Some DP control systems have been designed to mix the measurements from the various position measurement systems on the basis of how noisy they have been in the past i.e. using their variance to establish their weighting. The less noisy a system the more credibility it gets. However a seemingly perfect system then gets full credibility. So on some vessels where a transponder had unintentionally not been fully lowered on the seabed it has been given maximum weight and then when the vessel is moved it is believed to the exclusion of the correct but seemingly noisier systems. The other seems are then rejected and the vessel is positioning of a non fixed transponder.

More recent systems have included a median test that gets around this 'perfect measurement' problem. However means of defeating this have also been found by settling the same transponder to come in through two different acoustic systems this then gets two channels of the DP. The same has been achieved using two riser angle measurements, both exhibited near perfect performance as they rarely moved in response to vessel motion. When it did move significantly the riser signals were believed and the good systems rejected.

- 3) Examples of operator error are numerous. Some examples are. The DP operator calls the Bosun and asks him to go and lift the port transponder up as it appears to be giving problems. He deselects that transponder and sets his closed circuit TV on the port transponder winch position. No bosun appears but suddenly the DP chases the starboard transponder because the bosun has lifted the wrong one and did not confirm with the DP operator before he commenced lifting.

Others are a fault in a bow thruster causes it to go to full the other bow thruster is driven in opposition by the DP to compensate and confuses the DP operator who then emergency stops the wrong one. Similarly a ECR operator asked to stop generator 4 and stops thruster 4 by mistake as the stops are next to each other.

- 4) Other minor examples of a more curious nature is the book that fell of the book shelf and landed on the DGPS keyboard causing the DGPS to hang up its signal to the DP.

An engineer decides to use the compressed air to weed clear the sea water inlets while on DP this resulted in the systems becoming aerated and the loss of sea water cooling.

- 5) The main areas of weakness around any DP control system are the changeover between the DP control and thruster manual control, and the signals from the power system. This is often an area where neither supplier takes full responsibility. A full class III vessel has been found with all the thrusters changeover on two relays on one power supply. The power interface can be such that all the generator running signals to the DP control system were on one supply. Loss of this caused the DP to assume that there was no power available for the thrusters and therefore set them all to zero.
- 6) Governor maintenance has been shown to be important. Incident s have occurred were one generator takes all the kW load and the remaining generators trip on reverse power before the faulty unit tripped on overload. Result blackout.

AVRs have been a problem where a faulty AVR causes a generator to become a kVAR load. The remaining generators have to supply the main kVAR load and the faulty generator. This trips all generators, result black out

Reliability Analysis

Reliability defined

We use the word reliability loosely at times. To reliability engineers it has a very specific meaning. Reliability means the probability that something with a known failure rate will not fail during a particular time period.

For example, if a derrick barge is going to be alongside a TLP for only one day. What is the likelihood that it will not have a DP failure during that time. Or what is the probability that a rig will make it through a one well contract without a disconnect.

The equation looks like this:

$$R = e^{-\lambda t} \dots\dots\dots(1)$$

Where R is reliability, e is the natural log base, λ is the failure rate and t is the time duration. Both the rate and time must be in the same units.

With low failure rates and short exposure times, the values for reliability are close to one, like 0.98. In this case doubling the exposure time, t , gives a reliability of 0.96, not a very meaningful difference.

Since failure rate, λ , is the reciprocal of $MTBF$, the expression for reliability may be rewritten as

$$R = e^{-\left(\frac{t}{MTBF}\right)} \dots\dots\dots (2)$$

Availability

Another measure used by the reliability engineers is availability. This is the fraction of time a thing or system is available for use; that is, not shut down by failure. The equation:

$$A = \frac{MTBF}{MTBF - MTTR} \dots\dots\dots (3)$$

Here *A* is the fraction of total time the system is available, *MTBF* is its mean time before failure and *MTTR* is the mean time to repair. With a long *MTBF* and a short *MTTR* the fraction of time available is again in the order of 0.99 and 0.98, and again not a very useful or expressive number.

Failure rates and MTBF

The most useful measures for analyzing DP systems are failure rates or their reciprocal, MTBF. Reliability engineers generally use hours as the common measure of time. MTBFs are given in hours and failure rates in failures per million hours. For MTBFs a measure of months or years is most meaningful. Just remember that in any of the equations you have to use the same units for both.

Series of subsystems

It is intuitively pretty obvious why it is difficult to make any complex system like dynamic positioning have a high reliability or a long MTBF. There are many subsystems that all have to work if the total DP system is to work. The major elements are familiar to everyone. As a minimum these must include a position sensor, heading sensor, control system, its power supply, a set of thrusters to control position and heading, and a power plant, its fuel supply, cooling system, etc.

There is an equation that puts this into perspective. It says that the failure rate for the total system, λ_T , is the sum of the failure rates, λ_n , for all of the series subsystems.

$$\lambda_T = \lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 + \lambda_5 + \lambda_6 + \lambda_7 + \lambda_8 \dots\dots\dots(4)$$

Again, since MTBF is the reciprocal of failure rate, equation (4) can be rewritten as

$$\frac{1}{MTBF_T} = \frac{1}{MTBF_1} + \frac{1}{MTBF_2} + \frac{1}{MTBF_3} + \frac{1}{MTBF_4} + \dots \frac{1}{MTBF_n} \dots(5)$$

Put some numbers in these equations, and the prospects for high reliability look dismal. With eight series elements and with each having a two year mean time before failure, the total system will have an MTBF of only 0.25 years or three months.

If you want a five-year MTBF, which is about the best that has been achieved in the recent past, then each of eight subsystems will have to have a 40-year MTBF. That assumes that all of the subsystems have the same failure rate. If some are lower, the others will have to be higher. But any one subsystem with a very low MTBF tends to dominate the result forcing all of the rest to be very much higher to get the same total result. For example if one of the subsystems has a 10 year MTBF then each of the other seven must have a 70 year MTBF to reach the five year desired total. Also, depending upon how your system is configured, you may have many more than eight series elements and therefore the need for higher MTBFs for all of the series elements.

Redundancy effect

Fortunately parallel redundancy has an even more powerful effect to improve reliability than series failures have to destroy it. To make a subsystem such as the control computers more reliable, additional control computers can be added in parallel redundancy.

The improvement comes from the probability that a second or backup computer will be operable in the event of failure of the first...and moreover that the backup will continue to run satisfactorily while the failed computer is being repaired. So long as the MTBF of each of the computers is much longer than the time it takes to repair a failed one, the improvement by adding a redundant computer can be very large. For two computers in parallel, the $MTBF_P$ of the pair can be estimated by the following equation.

$$MTBF_P = \frac{MTBF_S^2}{2(MTTR_S)} \dots\dots\dots(6)$$

Again, putting some numbers to the equation will help. If each of those two single computer control systems has an $MTBF_S$ of six months, or a half year, and an $MTTR_S$ of two days, or 0.00548 years, the resulting combined system MTBF is 22.8 years. A good reliability engineer has said that the true result is really even a little better than that, namely 23.3 years. The reason is that this equation includes only the improvement from redundancy but not the original starting MTBF of 0.5 years.

This awesome 46-fold improvement through parallel redundancy is obviously due to the fact that the numerator is squared. By comparison, the terms in the series element equation (5) are merely additive.

The reliability improvement is even more striking with triple redundancy. To explore this effect we need a slightly more general equation such as the one that follows.

$$MTBF_p = \frac{MTBF_S^{(n-r+1)}}{n(MTTR_S)^{(n-r)}} \dots\dots\dots(7)$$

Here, n, is the number of parallel elements in the system and, r, is the number that are required for successful operation.

Now if we try three computers, each with the same six month $MTBF_S$ and the same two day $MTTR_S$, the resulting parallel redundant set has a combined $MTBF_p$ of 1387 years. This constitutes another 60 fold improvement in going from two computers to three, or a 2700 fold improvement in going from one computer to three.

A word of caution. These simple calculations have assumed a purely parallel redundant configuration. The real relationship between control computers is often more involved, and the extent of that involvement can reduce the combined MTBF significantly. These equations also assume unrestricted repair. That is, no matter how many of the parallel elements have failed, they can all be repaired simultaneously. When that condition cannot be met, the $MTBF_p$ will be reduced accordingly.

Nevertheless, it is clear that redundancy has an enormous ability to extend MTBFs of parallel systems and thereby to improve total system reliability in spite of the difficulties offered by the string of series elements in a DP system.

Weather’s effect on reliability

Any vessel’s DP system can be modeled as a group of elements, some in series and some in parallel. It is difficult to find suitable failure rates and repair times for individual components. But if they can be determined or estimated at all well, then, a reasonable estimate can be made for the MTBF of the total system. Unfortunately there is not a simple, single solution except for a constant level of environmental forces. There is in fact a different level of reliability or total system MTBF for each level of weather. The rougher the weather, the lower the MTBF. It is only by finding and summing the failure rates for the duration of each level of statistically expected weather that a final single total system MTBF can be determined for the season or total time period in question.

Weather affects reliability in many ways. Severe weather stresses both people and equipment. Acoustic position sensing is particularly susceptible to the noises of wind, waves, rain, engines, propeller cavitation and bubbles in the water. These effects are hard to quantify.

years or one tenth the MTBF of a single engine power plant. Of course this stands to reason. The ten engine plant has ten times as many things that can go wrong.

It does not take long looking at these numbers to see that the high MTBFs are determined very strongly not by the number of engines in the plant but instead by the number of spare engines, those that are available but not required at the time to hold position.

Remember, too, that in the usual multiengine power plant on a drilling vessel at least one engine, and hopefully no more, will be shut down for servicing or repair for 15 to 25 percent of the time. During the time that an engine is out of service, the plant will be the equivalent of one with one less engine, and the MTBFs will be found one column to the left.

Ships are slow to turn and are therefore susceptible to being blown off position by unexpected severe squalls that may hit on the beam or a stern quarter. Enough thrust should be provided to hold against a strong beam wind for at least the time taken to get the bow into the wind. Normally a 20 percent margin is provided for control dynamics, so this design wind level should be held at 80 percent of full beam thrust. A design beam wind of 61 knots, without wave drift or current force, has been fairly consistently able to meet this contingency over many years at least in the reasonable weather areas such as the Gulf of Mexico. A power plant able to supply that load plus the hotel load with one engine out of service can have an MTBF comfortable for deepwater drilling. The Discoverers Seven Seas and 534 have both achieved periods up to five years between disconnects and have been used as models for these criteria. It is not necessary that all 61 knots be considered necessary for wind. Whatever is not used for peak wind provides added redundancy and reliability for the thrusters and power plant.

This single number for beam wind holding capability has much to be said for it. Most of the cases in which ship shaped vessels have been blown off location by the environment have been the result of a sudden, unexpected squall coming up on the stern or beam, many times with erratic wind direction. It is time spent with beam to the wind that causes the loss of position. The reason for not including wave drift force for a fully developed sea is that sea development takes much longer than a squall takes to blow a ship off location. Having enough power to hold a good beam wind will generally mean enough power to hold a much higher bow wind for survival in severe storms and also enough power for a respectable cruising speed.

Fortunately most of the time the environmental forces are low enough that the usual multiengine power plant MTBF is in the hundreds or thousands of years. It is the short periods of severe weather that represent the periods of high risk and low MTBF.

To find the average or composite $MTBF_C$ of the power plant for a year or for a winter season, start with a statistical measure of the fraction of that period of time that the wind, waves and current exceed various levels. For each of these levels of environment,

Other factors influencing reliability

Other than FMEAs and the eradication of single point failures, the profitability of which can hardly be overemphasized, there are a large number of things that affect reliability but which will not be discussed here. A few certainly worthy of mention in passing are maintenance quality, availability of spare parts to keep repair times short, and well developed procedures particularly covering emergencies. Another few will be mentioned more fully in this section.

As important as redundancy and elimination of single point failures are to achievement of high reliability, it must still be said that airplanes are safe and reliable even though their wings are not redundant. High reliability can be had even with the presence of non redundant elements, but only if they are very highly robust and have very long MTBFs.

Power management system

A DP system operator would be most content if all of the engines in his power plant were running and on line at all times. This would guarantee that full power would be available at any time the control system were to demand full thrust. But the DP load on its power plant is normally a small fraction of the plant's capacity, and diesel engines run poorly when lightly loaded. Early experience with the Sedco 445 made it clear that this process needed to be automated through the computer. Power management systems have been in use ever since.

Their principal function is to be sure that adequate power is available on line when needed, without risk of overload and blackout, while normally running with fewer engines on line than could be called for. To do this the PMS must work in cooperation with the DP controls. The DP system uses information from the power plant to avoid commanding any more thrust than there is running power to cover it. When a command is sent which gets close to the running power available, the PMS will automatically start another engine, bring it up to speed, synchronize its generator to the bus frequency and close its generator breaker, all within a few seconds. If the DP operator has advance knowledge of the need for more power, he can start another engine himself through the PMS.

Some power management systems are run in a mode which provides for automatically stopping an engine when unused capacity becomes excessive. To avoid the possibility of a malfunction of this capability shutting down more than it should, most operators prohibit automatic stops. In that case the PMS signal is used to advise the operator who will judge whether to shut the engine down manually.

For high reliability, power management systems must also be redundant. When power limits and equipment calibrations are prudently chosen and accurate, the power management system is a significant aid to reliability.

Data logging and diagnosis

Another great aid to reliability is a data logging system for continuous recording of all of the parameters that pertain to the DP system. Typically recording several hundred discrete and analog values at intervals of one half or one second, such loggers serve somewhat the same purpose as the airplane “black box” or crash recorder. Time based plots from these records often have provided the only definitive explanation of the root cause of DP system failures, including the events leading up to and following the failure.

Reports of incidents for which no such records are available are very often speculative about possible causes. This is not usually the case where records are taken. There also seems to be at least good anecdotal evidence that vessels with short MTBFs do not have data logging, and those with multiyear failure intervals do have them. This is probably not coincidental. A clear understanding of a failure is requisite to its elimination for the future.

Operator training

Among the most important contributors to DP system reliability are the aptitude, training and experience of the operators. Some data indicate that roughly half of the DP failures are caused by operator error. Others have countered that operators many times rescue an incipient failure through quick and appropriate action.

Much has already been said about operator selection and training, so little needs to be added here except to repeat that they are and will continue to be an important element in reliability.

System design and misplaced incentives

It should be said that many failures blamed on operators should rightfully fall on the system designers. Modern computers have the capability to help the operator avoid mistakes, and more use should be made of this capability. We have all been thankful when our computer reminded us to save a file before exiting. It seems likely that much more use could be made of that approach by offering the operator good advice when an error is about to be made. The new console displays are much better than the early ones, but here again much might be gained by a serious effort in man-machine interface engineering to present information in the most clear and intuitive and least confusing way.

Such an effort may be costly. The DP control system manufacturers at present are the only ones who have any significant ability to make such changes. Unfortunately they are very busy, and they are also very competitive. They complain that they can lose a sale for a few dollars of price difference while little attention is given to appreciating subtle improvements for operator assistance. At the same time their whole system is sold for less than the cost of a single disconnect. This disconnect cost is borne not by the manufacturer but instead it is shared by the vessel owner who buys the system and his client which is often an oil company. The client often has the most to pay for the disconnect and the least influence over the system selection, much less its detailed design.

There must be a way to channel or divert some portion of this risk of loss, now borne by the vessel owners and clients, into an effort to develop these system improvements. A team of experienced operators, reliability engineers, manufacturer's systems engineers, and owner and client representatives might make a productive mix with funding perhaps from a joint industry project. Maybe our new DP Committee might provide some useful guidance and help in evaluating the prospects of success.

Another word should be said regarding the need for contract provisions to give vessel owners strong financial incentive to improve DP reliability. There is typically a great deal that can be done by the vessel owner to upgrade the reliability of his DP system. This work costs much more than good will alone is likely to justify. Drilling contractors become much more proactive in this work when their contracts offer bonuses for reliable operation and a significant share of the cost of failures.

MTBF goals and budgeting

Vessel designs start with objectives in mind and then on paper...water depth, environment, variable deck load and the like. If it is to be dynamically positioned, these objectives should include a target MTBF. Like most objectives, to achieve high reliability requires planning and a dedicated effort throughout the project. MTBFs at the high end of the range have increased over the years to a present level of five years or so. The new DP vessels certainly have the potential to do better, but time will tell.

To get a higher MTBF will probably require not only commitment to a goal but also establishing a reliability team with that objective. Such a team should be led by a representative of the owner with participation by any principal client. It should also include members of the FMEA team which in turn should include a reliability engineer along with representatives from each of the key manufacturers as needed. This team including the FMEA members should be used regularly for design reviews, to keep a running tab on the state of the reliability estimate and finally to assist in sea trials.

Ideally, once the total goal has been set, values of MTBF and MTTR obtained from each of the suppliers should be used to form a reliability model of the system as it is configured. The reliability values should be requested from the manufacturers as a part of the original bid requests. They may be helpful in equipment selection and to confirm estimates of required redundancy.

Typical subsystem and device MTBFs

A few of these values covering some of the many of the elements of any DP system are gathered into the following Table 2. Accumulated over many years, they are still very sparse data which are almost obviously of doubtful accuracy. Most are manufacturers' stated values. A few were picked up from reliability engineers and others from rig records, albeit with a limited statistical sample. Values like 100,000 hours somehow look less like test results than they do fabrications of a sales department. And ranges of ten or twenty to one between minimum and maximum MTBFs also look like bad data.

The thruster MTBF for fixed axis, controllable pitch is from limited DP vessel records. The others in the reasonable column were expanded from that value on the guesses that pitch and azimuthing controls might have about the same failure rates. With neither controlled, the MTBF should be higher and with both, lower. The minimum MTBF of 944 hours for both is real data from one vessel with perhaps unusual thruster problems. The MTTR of 170 hours is a good estimate from a real vessel with onboard access to the whole thruster. If dry docking is required for access, repair time could be extremely long.

The computer control console numbers are understood to be calculated values from one manufacturer for his model just past. No MTBFs are yet available for the latest models.

Table 2 DP System and Component Reliability--MTBF and MTTR

Component	----- Minimum	MTBF-hrs Reasonable	----- Maximum	MTTR Hours
Control computer console				
Single	1700 (0.2 yrs)	7300 (0.8 yrs)	9,800 (1.1 yrs)	2
Dual		92,000 (10.5 yrs)		
Triple		1,600,000 (192 yrs)		
Acoustic position ref.		4000	23,900	2
Vertical Ref. Unit		100,000		100
Differential GPS		18,500		
Gyro	4000	25,000	48,000	30
Wind Sensor	8000	17,000	100,000	3
Unint. Power Suppl. UPS	5000	17,000	100,000	30
Engine Diesel		3500	20,000	30
Thrusters—fixed axis				
Fixed Pitch		12,000		
Controllable Pitch		9600		170
Thrusters—azimuthing				
Fixed Pitch		9600		
Controllable Pitch	944	7700		

Need for better data

There is no doubt that better component or subsystem failure and repair data would help make reliability models of total DP systems more accurate. This would be of great assistance in economically optimizing DP system designs. If total system MTBF could be calculated with acceptable accuracy, then valid risk analyses could be substituted for the present rather arbitrary guidelines for redundancy levels.

Manufacturers for the most part do not have access to records which could yield real failure rates. Their numbers are therefore usually calculated values. To improve their accuracy these values should be verified or adjusted or calibrated by comparison with records of real failures. This could be a large undertaking, but it may prove very worthwhile. Some efforts are currently underway to consider a pilot project to evaluate the prospects more thoroughly.

DP vessel failure records

Disclosure of records

Within the drilling industry, and perhaps a few others, the DP vessel owner's client, usually an oil company often assumes a very large part of the cost of a DP failure. This is true even after good efforts to adjust contracts to give the contractor more incentive to achieve high reliability.

In order to understand his level of risk it is necessary that the client be aware of the failure rate or MTBF of the vessels being considered. Responsible contractors have consistently made complete disclosure of their failure records for this purpose. Over time these records become fairly generally known. There has been no effort to hide their failure records. To do so would give the impression that there is cause for shame. On the contrary, some drilling vessel owners have been proud to see their MTBFs go from six months to five years.

This is a healthy trend that should be encouraged. The cloak of anonymity, which others have apparently found necessary in order to extract failure data, should not be necessary if open disclosure can be achieved.

Risk Analysis

It is difficult and time consuming to construct a reliability model of the whole DP system, and when it is done, the results are questionable; sometimes clearly too high or too low. Nevertheless the effort provides a useful framework to understand a system's strong and weak points and from which to assess and deal with failures. Experience gained with the system over time provides a rough calibration and a more believable total MTBF.

Such total system MTBFs can be used to assess the risk in a given operation. To do this one must also know the probable cost, C , likely to be incurred in event of a failure of the DP system and the probable duration, t , of exposure to such failure. The risk rate will then be the failure cost times the failure rate or $C/MTBF$. This will be the cost in dollars per year if the MTBF is in years.

Failure cost itself is not always an easy number to develop. It changes during an operation depending upon the activity at any particular time. For example, in drilling, the failure cost is lower while drilling a pilot or surface hole with bare drillpipe than it is while drilling a deep hole with riser. It is higher while drill collars are being run through the blowout preventers than not, and perhaps higher still while controlling a kick. These activities can be evaluated individually or given a weighted average value for the total duration of drilling a well or series of wells. The probable average failure cost for drilling is currently estimated to be about \$2 million. This includes rig downtime, possible damage, the possibility of a fishing job, and even the remote possibility of lost well control.

Using this \$2 million failure cost and a DP system MTBF of say five years, the risk rate is \$400,000 per year. The risk cost is for a period of time which then becomes, $(C*t)/MTBF$. For a three month well, the risk cost for DP failure would be \$100,000. For a five-year contract the risk cost would be \$2 million. And of course a rig with a six-month MTBF for a five year contract would have a risk cost of \$20 million.

These risk costs are still a small fraction of the total operation cost, but they could pay for an extremely thorough FMEA, a lot of software improvements to keep operators from making errors and a lot of operator training.

Similar risk analyses are most helpful to allow a vessel owner or his client to evaluate whether the addition of redundancy in a particular area is economically justified. An example will illustrate. A contractor was outfitting a DP vessel with redundancy throughout, including dual control computers, but planned to provide a single operator console. The MTBF of the single console is about 0.3 years or 3.6 months. Assuming an MTTR of two hours, the combined MTBF of two consoles in parallel redundancy, according to equation 6 is 184 years. If the failure cost while operating on DP is, say, \$300,000, then the risk rate resulting from operating with the single console is

\$300,000/0.3 or \$1 million per year. The risk rate resulting from dual consoles is \$300,000/184 or \$1,630 per year. The difference of \$998,000 per year times 1/10, the fraction of each year spent in work subject to that failure cost, is \$99,000/year. This is the yearly return for investing in the second console which cost about \$75,000. It was an easy decision.

It should be clear that one should not settle for a cheap and cursory FMEA or necessarily for the minimum redundancy called for in the Societies' guidelines, particularly for position sensors.

Bibliography

1. Morgan, M.J.: Dynamic Positioning of Offshore Vessels, The Petroleum Publishing Company, Tulsa, Oklahoma, (1978).
2. Shatto, H.L., and Van Calcar, H.: Improving Dynamic Positioning Performance in the Deep Water, High-Current, Rough Water Environment, Offshore Technology Conference, Paper 4749, Houston, (1984).
3. Shatto, H.L.: Dynamic Positioning Reliability—How Much Can We Afford?, The Society of Naval Architects and Marine Engineers, Offshore Station Keeping Symposium, Houston (1990).
4. Fugere, P., and Minge, J.: The upgrade and Performance of the Discoverer 534 Dynamic Positioning System, Offshore Technology Conference, paper 6959, Houston, (1992).
5. Inoue, K., and Wolff, C.V.: Development of a Semisubmersible Drilling Unit for 10,000 ft. Waterdepth, Offshore Technology Conference, paper 6272, Houston, (1990).
6. Shatto, H.L.: Dynamic Positioning System Evaluation, Offshore Technology Conference, paper 6962, Houston, (1992).
7. Karlsen, G., and J.D. Sikes.: Water Depth Upgrade of the Sonat Discoverer 534, SPE/IADC paper 21981 Amsterdam, (1991).