DYNAMIC POSITIONING CONFERENCE
October 13 –14, 1998

RELIABILITY

Classic Single Point Failures of Redundant DP Systems

D. F. Phillips, Eur Eng, B.Sc.(Hons), C.Eng, MIEE, MIMarE

Nautronix Inc. – San Diego (California)

Introduction

The control of a vessel's position by the use of thrusters rather than its anchors was originally conceived for positioning of drillships in deep water where deploying anchors was not possible. This positioning technique later became popular for diving support operations where minimum set-up time was required, or the deployment of anchors would be difficult due to location. This technique, known as Dynamic Positioning (DP), is now applied in many applications including crane vessels, cable layers, accommodation vessels (floatels), offshore off loading tankers, fire fighting vessels, work boats, cruise liners and even luxury yachts etc.

Initially the term DP system was used to describe only the control system. The term DP system is now used to describe all vessel control systems required to keep position. These systems include the power generation, power distribution, power management and the thrusters as well as the control system itself. Plus the DP operator has also to be considered as part of the system as he can be crucial to a DP system's operational success.

The industry trend is for dynamically positioned drillships to upgrade their DP systems with increased redundancy and hardware.

The examples described in this paper are from the DP industry's experience as a whole and are not reflective of any one DP control systems supplier.

The aim of this paper is to increase DP operators and owners awareness that regardless of the amount of hardware redundancy installed, all control systems could fail in an instant even if they were thought to be redundant. However, through operator awareness and proper set-up, the chances can be greatly reduced.

Holger Rokeberg of DNV has stated that "…the problem a lot of designers, operators and owners have is that they do not like to think failure." Mr. Rokeberg's comment reflects the attitude of many in that they are not comfortable with the idea that their redundant system might fail. They have an almost superstitious belief that – if they think failure – they will get failure. Contrary to their belief, it is imperative to think failure and never be too complacent about the reliability of the system. The examples within this article will show that any system can experience failure under certain circumstances.

What if? – should be a question frequently asked.

Types of Failures

During the 1997 MTS Dynamic Positioning Committee meeting the author of this paper gave a presentation on Failure Modes and Effects Analysis of DP systems. In the presentation examples were given of systems thought to be dual and triple redundant and still had single point failures. This paper will provide greater detail on these and other similar failures.

A definition of a single point failure often used is any failure that results in the loss of position. There are three possible scenarios of position loss:

- Drive off
- Drift off
- Large Excursion

The design should be such that no single failure can cause any of the above position losses. According to DNV rules and IMO guidelines, any single act of human error should be considered as a potential single point of failure. The system should also be protected against any hidden failures. A hidden failure is

when there is a dormant fault in a back-up system that may not be realized until the first failure occurs and the back-up or standby fails to take over and perform the required operations. Generally, systems that meet this redundancy criteria are called 'Class 2' systems.

In addition to loss of position, the design of Class 3 systems also provides protection against critical physical catastrophes such as a fire or flooding.

Redundancy for the vessel's DP control system invariably means additional identical hardware. It is rarely realized that the software is still also identical in each DP Control System installed making the systems prone to what is known as systematic faults. These faults can occur when a set of conditions arises which have not been tested or designed for. Such faults can cause software to crash or perform unexpectedly; therefore effecting all systems simultaneously regardless of the level of redundancy.

DP System Classic Single Point Failure Examples

The examples in this paper cover each DP sub-system and are all based on real occurrences stemming from the author's personal experience or from the IMCA DP incident database. The samples within describe single acts of human error, physical, hidden and systematic failures. They are not specific to any particular vessel or DP control system supplier and, in fact, have been chosen to give a fair distribution across all suppliers.

All operators and designers of DP vessels, systems and sub-systems should ask themselves:

- Could this failure or something similar happen on my system?
- Is this covered in the FMEA?
- Why is Doug Phillips such a pessimist and I am not?

Power Generation Failures

Physical/Hidden Failure

A vessel with split engine rooms running with a connected bus had a fire in one engine room. The operator shut down the engines located in the engine room with the fire, and the load of all the thrusters was then instantly placed onto the remaining generators. The system volts dipped dramatically and the vessel blacked out.

Unexpected fuel or cooling problems could also trigger the same occurrences resulting in a vessel blackout.

Single Point Failure

Some occurrences, such as this one, are much more obvious and preventable. This vessel had been fitted with an air inlet flap on each diesel engine. The flaps were to be closed in the event of a gas alarm. Unfortunately, the engines were air operated and required air to keep them open. Because, there was only one air supply available the air supply was lost and all diesels shut down in one instant.

This single point failure could have been prevented by supplying the flaps with additional air supplies; or as in the case excluding the feature entirely.

Power Distribution Failures

Hidden Failure

A power distribution failure occurred on one particular vessel that was running split bus. There was a blackout on one side of the bus. The DP control system then lost half of its thrusters. Since this was a failure mode the DP system was designed to cope with it increased the load on the remaining thrusters to compensate; this blacked out the remaining healthy side.

These types of occurrences are more likely with the bus tie connected. In the event of a high voltage switchboard short, not only does the DP transfer the thrust to the remaining thrusters as above, the voltage also drops. The transients in the power system are such that all the starters of ancillary equipment such as hydraulic pumps, cooling pumps, etc. can trip on under voltage and the whole power system can fail.

Hidden Failure

During this vessel's annual trials one-half of the 440V board tripped; this trip resulted in all the pitch pumps of the thrusters changing over to the assigned standby pumps on the other 440V board. Upon changing over, the pitch hydraulic pressure on each thruster dipped, and the ready signals to the dual DP control system were transiently lost, all thrusters were deselected and set to zero.

This is an excellent example of a hidden fault – the changeover to standby pumps failed. The vessel had been set-up to keep the running hours even by running all pumps on one board for one month, then all on the other boards the next month. The DP system failed to cope with the transient loss of the ready due to pressure dips. If the power distribution had been set up with the thruster's main pitch pumps split across the two 440V boards and the standbys had been set up on their respective opposite 440V board, the changeover would have been successful.

Hidden Failure

While producing the FMEA for a Class 2 vessel, all governors where found to be from the same power supply. The vessel had provision for a 24V back-up power supply through diodes; but the back-up power supply was not connected and its absence was not alarmed.

The technique of providing back-up power supplies using diodes is quite prevalent; however, it is not the preferred scheme. In fact many DP control system's input and output signals are powered through diodes to save having to fit dual signals.

It is quite unfortunate that because of unawareness, systems thought to be redundant might be dependent on the successful operation and reliability of a couple of diodes. In fact, this could be quite disastrous.

Power Management Failures

Single Point Failure

Governor maintenance has been proven to be extremely important. Incidents have occurred where a diesel with a faulty generator takes all the kW load, and the remaining generators trip on reverse power before the faulty unit tripped on overload. The result – blackout.

Single Point Failure

Faulty AVRs (Automatic Voltage Regulators) have caused generators to trip resulting in a blackout. Cases have been documented where a faulty AVR caused a generator to become a kVAR load. The remaining generators had to supply the main kVAR load and the faulty generator which also represented a kVAR load.

Thruster Failures

Single Point Failure

The use of thrusters for DP operations is required. In order to meet class the thrusters must either fail to zero or as is. However, in reality, if the pitch hydraulic sticks, the thruster can still fail to full pitch. The only way to prevent this is to trip a thruster when a significant discrepancy is detected between command and feedback. This arrangement is rare indeed, and in any case, produces other less desirable failure modes. Plus the detection of failure and getting the thruster to zero or frozen is not easy or fool proof.

Single Point Failure

A full Class 3 vessel that had been operating for many years was often used as a great example of how Class 3 should be done. It was found out that this vessel had the entire thruster changeover on two relays and on one power supply. This changeover lost all the ready signals for all the thrusters to the dual DP system. The back-up system was still operational, however the design of a Class 3 system is such that the dual system must withstand any single point failure as per a Class 2 vessel. The back-up system is only designed to withstand physical failures, not oversights in the design that miss a single point failure.

Human Error

Thruster failures caused by human error are quite common and, in general, the system and the operator cope. On some occasions, however, they do not. For example, a vessel had a fault in a bow thruster which caused it to go to full, the other bow thruster was driven in opposition by the DP to compensate. This caused major confusion for the DP operator, who in turn emergency stopped the wrong thruster.

In another episode a thruster failed to full due to a linkage break in its feedback mechanism. This meant that, even though it had failed to full, it only indicated to 35%. The other bow thruster, of course, went to 100% to compensate. The DP operator therefore shut the good 100% thruster down assuming that it had failed to full.

DP Control System Failures

Systematic Failure

A dual DP control system had all the generator running signals on one fuse, loss of this fuse caused the on-line system to assume that no power was available for the thrusters and therefore set them all to zero. The standby, however, did have valid signals but did not changeover on the basis of adequate generators.

Proper interfacing of the power system and the DP control system can fall between the cracks of two suppliers. If the failure modes are not covered properly then it is easy for the DP control systems to either power limit too early – or not at all. Newer DP systems include cross checks to prevent this from happening.

Systematic Failure

Another vessel had been operational for about four years and had undergone very detailed testing and FMEA procedures. However, one day a fault on one input channel of a digital input card failed low. Unfortunately, this was the center of rotation selection and the system therefore believed that no center of rotation was selected. The software, in both the on-line and standby system failed to compute correctly and effectively shut down.

The software had not been designed to default to display the vessel center if nothing was selected.

Systematic Failure

The Kalman filter in the DP control system models the vessel's behavior and therefore needs to include the thruster levels. There are two options for filtering: 1) To use the internally generated demand suitably delayed to model the thruster lags, or 2) to use the actual feedback from the thrusters.

The problem with the second option is that there was a common direct connection from the outside world into the heart of each channel of the DP control system. There have been several occurrences both during normal operations and annual trails where failure of this signal destabilized all the Kalman models in all the DP control systems installed.

In the meantime, this particular system had been modified to use the actual feedback unless there is a thruster mismatch alarm from a difference between the demand and the feedback. If there is a mismatch, then the internal demand is to be switched to instead.

Systematic Failure

On this system both dual DP systems crashed when each of the computer's operating system (which, of course, were both identical) attempted to automatically alter their clock over to Pacific Daylight Savings Time. The application part of the program had not been programmed for this and both systems failed due to this systematic fault. This fault was just lying dormant until its time came.

Position Reference System Failures

Systematic Failures

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 is, the more credibility it gets. Therefore, a seemingly perfect system gets full credibility.

There was one occurrence where a vessel's transponder had not been fully lowered on the seabed and had been given maximum weight. When movement of the vessel occurred it was believed, to the exclusion of the correct, but seemingly noisier systems. The other systems were then rejected and the vessel was positioned on the basis of a non-fixed transponder.

This type of failure has occurred in different forms on a number of occasions. Other examples include a frozen Artemis signal, a DGPS that continued to transmit the same position on loss of satellites and taut wires that have broken or whose inclinometers have been faulty.

More recent systems have included a median test that copes with this "perfect measurement" problem. However, means of defeating this problem have also been found by settling the same transponder to come in through two different acoustic systems and sends data to two channels of the DP system.

Another incident occurred where a vessel using two riser angle measurement systems exhibited near perfect performance as they rarely moved in response to vessel motion. When there was significant vessel movement, the riser signals were believed and the good systems were rejected.

Systematic failures are not confined just to the DP control system. In one incident a DPGS receiver's software crashed as soon as eleven GPS satellites became visible above the horizon. If the vessel had two such receivers in a supposed dual system, this event would have caused them both to fail. A particular combination occurred and the software reacted on both systems in exactly the same way.

Another potential systematic failure of GPS receivers world-wide is that they will have a roll over date at midnight on the 21st to 22nd of August 1999. It has not been proven that all GPS receiver's firmware can cope with this rollover. The rollover is caused by the fact that time zero for GPS was the 6th of January 1980. The GPS cycle is 1,024 weeks beginning 00.00 a.m. on the 22nd of August. This will not only affect the date displayed, but the accuracy may also be adversely affected.

System Sensor Failures

Systematic Failure

On a semi-submersible a minimum rate of change (non-movement) check on a gyro compass can be a nuisance as the heading control can be "so good" that the gyros may often fail the check. This particular system was operating with two gyros; it was decided to interlock them with the mismatch alarm. The idea was that if they were both in agreement then neither of them could be stuck. So the non-movement check was only performed following a mismatch alarm hoping to diagnose if the mismatch has been caused by a stuck gyro. However, what happened was that the gyros did mismatch because they not aligned at a particular heading. Because the heading control was "so good" both gyros were deselected by the non-movement check on both DP control systems.

Single Point Failure

Before there were easy serial interfaces to gyros, and even now on conversions, the DP control system had to be interfaced using the gyro's digital repeater interface. This interface counted the phase transitions of the three phase square waveform. But, if one phase fails then the DP control system only counts up – never down. This effectively puts a positive feedback on the system, even with two gyros it is difficult to work out what is happening and serious heading and position loss can occur.

It is also rarely appreciated that incorrect gyro information results in incorrect position measurement. Computations of position error calculations require the use of the vessel's heading at the instant the position measurement is made.

Human Error

A vessel undergoing DP trials was operating the LBL/SBL acoustic positioning system in SBL mode in approximately 1000-meter water depth. One of three VRUs could have been selected for use by the system to compensate the acoustic measurement roll and pitch. There was a four position manual switch, with a position for each VRU and an off position. As part of the tests VRU #3 was to be selected. The switch labeling was poor and there was the parallax between the actual switch position and the off position –the off position was selected by mistake. This mistake resulted in an apparent large shift in position that the DP control system chased applying a large amount of thrust. This error caused the vessel to heel significantly which, because there was now no VRU compensation in the

acoustics, in turn caused the position to apparently shift even more – resulting in more thrust – and so on. Fortunately, the operator realized what the problem was and selected the correct switch for VRU #3.

However, the operator did learn that the off position of the VRU selector was a great way to get the Captain, the Off-duty DP Operator, the Drilling Superintendent and the Charter Representative on the bridge in record time.

Operator Errors

Human Error

Examples of operator errors are numerous and are generally due to simple human mistakes. At least 50% of reported DP incident are attributed to operator error. This statistic is often thought to mean the DP operator. However, an operator error can be caused by any person that can affect the DP system; i.e. DP operator, ECR operator, deck crew, etc.

The following examples show how operator errors (single acts of mal-operation) can result in a single point of failure.

A DP operator called a member of the deck crew and asked him to go and lift the port transponder up because it appeared to be giving problems. He deselected the transponder and selected his closed circuit TV on the port transponder winch position. Nothing appeared – but then suddenly the DP control system chased the starboard transponder because the wrong transponder had been lifted in error. On this occasion, there was no confirmation with the DP operator before the lifting was commenced.

An engineer decided to use the compressed air to weed clear the seawater inlets while operating on DP. The cooling systems became aerated and failed to cool. This incident brought the vessel dangerously close to losing all power generation.

A human error was discovered when a DP control system was being operated with apparent problems in the Artemis and taut wire system. What had happened, as it turned out, was that the Artemis fix station had been set up 180 degrees out of phase and was effectively giving positive feedback. Apparently, the vessel had run out of spare steel taut wire weights and it was decided to make one from concrete. Unfortunately, the difference in the specific gravity of concrete compared to steel was not realized. The weight was measured in air and not in water – thus the weight would have rarely, if at all, been on the seabed.

On another occasion an alarm went off in the ECR warning of hydraulic oil problems with the port azimuth thruster. The engineer then checked the thruster and discovered that oil was leaking under pressure. He returned to the ECR and promptly stopped the starboard thruster by mistake, the faulty unit stops soon after.

Conclusions

Prepare for failure!

Although not always comfortable, it is advisable to think failure. Plan for it and always be prepared. Single point failures can and do happen – no DP system is totally immune to them.

Be careful not to be complacent because there is a lot of hardware redundancy fitted – this does not guard against a systematic failure. All DP systems are equally vulnerable to the majority of single point failures

and all systematic software failures. All that is gained is immunity to rarer single point physical failures such as fire and flood.

The only way to avoid single point failures is to perform a thorough FMEA and perform tests to confirm its findings. FMEA should be conducted by someone with extensive experience who will perform the toughest analysis possible. Proper operating procedures should be in force including checklists, operator training, annual trials, consequence analysis and situation assessment. All procedures should be periodically reviewed and updated.

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. Other areas worth concentrating on are the way the power generation is set up and proper governors maintenance. Also all standby systems, including UPS units, should be checked regularly for correct operation. Paying attention to these areas will help avoid some of the more common single point failures.

Ultimately, all systems must undergo very comprehensive testing procedures in the proper environment. Delays in the program may impose pressure to deliver certain components of the DP system before testing is completed or to reduce the testing time to try to maintain the overall program schedule. If either occurs, the risk of system failure is drastically increased. Post sea trial modifications made due to new vessel requirements or past system problems must also always undergo comprehensive testing procedures.

References

1. Dynamic Positioning System's Incidents, IMCA
2. Software Failures, Follies and Fallacies, Les Hutton, IEE Review March 1997
3. Loss of Redundant DP Control Systems from Systematic Faults, Doug Phillips, IMCA 1998
4. The Dynamic Positioning of Ships: The Problems Solved?, Doug Phillips, IEE Control 96
5. Failure Modes and Effects Analysis, Doug Phillips, MTS DP Conference 1997
6. DP Systems Consequence Analysis, Doug Phillips, MTS DP Conference 1997

About the Author

Doug Phillips has an honors degree in Computer and Control Engineering and has worked with Dynamic Positioning for 24 years. The first 19 years with GEC/Cegelec designing, building and commissioning DP and anchor assist control systems. Initially as a project engineer, and then later as the manager of a team of project engineers and project managers. Then for 3 years in consultancy with Global Maritime performing FMEAs, trials etc. on total DP systems on vessels with DP control systems from all suppliers including those from Simrad and ABB. During this time he also worked on DP Incidents and research for IMCA. For the past 18 months Doug has been the Vessel Controls Product Line Manager for Nautronix mainly involved in the development of their ASK5000 Series Dynamic Positioning Systems.