DYNAMIC POSITIONING CONFERENCE
October 17 – 18, 2000

RELIABILITY

DP Systems – Fail to test or test to fail?

Doug Phillips – American Global Maritime

and

Blake Miller - Nautronix, Inc

INTRODUCTION

To fill out the title of this paper it should read – Are you failing to test properly if you do not test for failures? Comprehensive tests of DP Control Systems; in the factory, on the vessel, at acceptance trials, and during annual trials, are fundamental to the reliable, robust and continued operation of any DP vessel.

This paper will demonstrate that it is to not important only to test a system for the functionality a DP control system was designed to meet; but to go far beyond that and to 'think failure' and test for the failure modes. Nautronix have learnt the hard way that thorough testing during design and at integration in the factory pay great dividends in reduced on site time and less post commissioning problems. A subjective estimate is that it might take four times longer to fix and retest a fault in the field than it does to fix it in the factory. The use of a simulator to exercise the system contributes greatly you this. Of course the reduction of faults found on the vessel during warranty saves the vessel owner, valuable time, aggravation and money.

Examples from both the author's experience will be given of the fundamental tests that need to be conducted. As well as identifying where the weak points in a design are likely to be. The main source for deciding the actual failure testing is the Failure Modes and Effects Analysis (FMEA), the technique of FMEA will also be discussed and further reading on this referenced.

The paper will assist any owner of any DP control system in ensuring that their DP system has been fully tested and is fault tolerant. It should also convince them of the importance of FMEA and subsequent failure testing.

The subject of systematic failures is also broached; these are software failures that can shut down all systems if they have common software. Examples of systematic failures from all DP control system suppliers will be given.

DEFINITION AND CONCEPT OF TESTING

It is useful to go back to first principles and define the meaning of the word test. One definition that seems the most applicable for this paper is:

"To subject to a procedure that ascertains effectiveness, value, proper function, or other quality".

The Thesaurus gives some more clues:

"Proof, trial, try out, experiment"

The effectiveness and proper function we are testing is the positioning of the vessel under the control of the Dynamic Positioning Control System. Basically the vessel should stay on station and not be subjected to:

- A drift off
- A drive off
- An unacceptably large position excursion.

WHEN TO TEST?

There are obvious times during when a DP control system needs to be tested. These tend to be the Factory Acceptance tests and Sea Trails. These are generally thought of as the main ones as they are part of getting a customer to accept the system prior to leaving the factory. However there are more places were testing should take place, some of which are quite subtle and rather informal. In fact testing is rather more than just attaching a multi meter to something. It is anything that subjects that design to a procedure that is checking the effectiveness and proper function of the design.

During Design – this should be a mental exercise were the designer tests his design in his mind as he designs it. This is a process of what if? What if this happens, what if this happens? This is of course fundamental to the design of redundant systems that need to meet 2 and class 3

Class 3 systems take an extra level of design and review. The loss of compartment is difficult in the early stages, especially when equipment locations may not be known. This also stems into problems when shipyards or clients wish or require to move or re-located equipment in the middle of design stages.

At the same time, caution must be taken to not over-design a system or arrangement. In larger Class 2 or 3 systems, one must always keep in mind "what is the largest, or most destructive failure possible." I.e. If you have 4 generators in 2 engine rooms, you wouldn't be required to design a system with 4 PLC's (2 in each engine room) as the failure of one engine room would take down both PLC's anyway. However, if there were other requirements, or if a client wishes to pay for such added redundancy, there is nothing prohibiting this practice.

Design Review and FMEA – Design Review is similar to what the designer does mentally but is a formal check on the design by others; generally more experienced designers, other interested parties and peers. The FMEA itself is a formal way for an independent person to check the design. This is a systematic approach to go through all the 'what ifs' and documenting the expected results. These results then need to be validated both by the designer(s) and by testing.

Module Testing

Any design is to some extent modular whether in hardware or software. Any module that makes up the whole can be tested individually to increase confidence in the effectiveness of the overall design once it is all put together at integration.

Hardware can and should be individually tested. Individual cabinets with built in redundancy (dual power supplies, etc.) should be tested individually prior to the integration testing.

Engineering Acceptance Testing (E-FAT)

This an internal test generally conducted by experienced and independent engineer(s) who test the integrated system in the factory against a written agreed and approved procedure. This test procedure is designed to validate both the functionality and failure modes of the system. These tests can only go as far as that which can be simulated adequately in the test area. To make this as valuable as possible a comprehensive trainer simulator is built for each system that allows the control system to be exercised against. This testing should always attempt to test every alarm.

Also the engineer who is conducting the tests needs to be encouraged to go outside the bounds of the test procedure. Too often the criteria for a successful test is 'did it pass the test procedure' – without reference to the adequacy of that procedure. The engineer must be encouraged to go beyond this and follow up on things that might pass but seem strange, or if other unexpected things occur. Any additional tests conducted should be annotated to the test procedure results.

Quality Acceptance Testing (Q-FAT)

This is an independent rerun of the E-FAT by the QA department as an independent check on the system prior to Customer FAT.

Customer - Factory Acceptance Testing (C-FAT)

This is generally a demonstration of the functionality of the system and should show that the system meets the Customer's requirements, as far as is possible without actually being in control of the vessel. The level of detail that this goes into here often depends on the level of expertise of the Customer. The results of the Q-FAT are available for the Customer's perusal if required. Some customers send far too many personnel to witness the C-FAT others send none.

Sea Trials

This basically a repeat of the C-FAT but with the system actually connected to the actual and operational systems on board (thrusters, power system, position reference systems, sensors, etc) and in full control of the actual vessel in real environmental conditions. These trials are sometimes called DP Performance trials. They should concentrate on the "performance" of the control system and all of it's auxiliaries. It should not be interlaced with Failure Mode testing, as this should be conducted during FMEA Proving Trials. Most of the time, Performance Trials and FMEA Proving Trials are conducted within the same sea trial period.

FMEA Proving Trials

The majority of DP vessels have the whole DP system (i.e. everything that supports the vessel's positioning – from seawater cooling through to the operator) is subjected to an FMEA, often by independent consultant(s). The analysis is initially largely theoretical. These trials are designed to prove whether the FMEA is correct or not. As such they necessarily involve the DP control system. These also serve as useful training for operators to see how the system and vessel behave during failures that they might not normally see. Or will only see if they happen in real life.

One important point during FMEA testing is the requirement for a full set of willing and competent test personal to witness, record and later review the results. Failure mode testing always involves a large number of equipment and/or machinery that gets shut down, many alarms and subsequent operations and events that must be duly witnessed and recorded. It is crucial for all test personnel to fully understand exactly what is supposed to occur upon the failure. Unfortunately, there always exists arguments and/or differences in what he or she saw or what actually happened. This results in poor test review or in re-testing the event.

Mobilization Trials

Following Sea Trials and FMEA proving trials, and any re tests as a result, the vessel is ready to work. Mobilization Trails are conducted before each job to check that the system is operational before going to work. Generally these trials do not take long and mainly check basic functionality. One of their main uses is to check all standby systems, that might have a hidden failure, are operational. For example UPS batteries, pitch standby pumps, etc. This minimizes the chance that they will not operate should they be called to do so.

Annual Trials

In these trials a sub set of the Sea Trials and FMEA Proving trials are repeated broadly on a yearly basis. The purpose of this is mainly to check that the system is still as designed and that there have been no modifications that have affected the system. These also serve as useful training for operators to see how the system and vessel behave during failures that they might not normally see. Or will only see if they actually happen in real life. This is a good training opportunity for new operators and those on the vessel to learn more

Tests following Modifications

To often a system is modified to correct a problem and inadequate testing performed. There is always pressure to a vessel back to work as soon as possible. Often though, without due care, a modification causes another problem else were or changes the system such that some of the original design criteria are

no longer met. Thorough testing can only check this for. The FMEA should be modified to reflect the modification and any relevant failure modes tested for.

Examples will be given later of modifications to DP control systems that have resulted in failures. Often modifications are made to DP control systems under great pressure to get the system working as quickly as possible for various economic reasons – ***'production pressures'***. This only makes the chances of a mistake being made and going untested all the greater. Especially as the vessel owner and his client rarely understands the extent of the modification being

Those interested in the consequences of ill conceived, under tested modifications that have circumvented most of the original designs intent should refer to date published on the Piper Alpha and Flixborough disasters.

HOW TO TEST?

Testing must be for failures as well as functionality. Why? This is fairly simple answer; the primary requirement for a redundant DP control system is that it will still be operational after a single fault. The testing must therefore include checking for the effect of all possible single faults. Including any single inadvertent act by an operator.

It is important that tests are conducted in a systematic and controlled fashion. It is the nature of most DP control system tests that they take time. It is all too tempting, to try and conduct more than one test at once – often though the result is total confusion.

At sea trails in particular, were the overall vessel program has slipped it is tempting to try and save time on the testing of the DP system, which tends to be the last thing to be tested. This is a serious mistake – time spend now will be paid back many fold in the future.

Exact methodical recording of the important parameters affecting the test is critical to ensure that the test conditions can be repeated if necessary should there be a problem.

WHAT TO TEST AND CHECK?

The short answer is everything – however as an owner with what seems to be a reasonably functioning system. What tests and checks should you consider to really confirm the robustness of the design. The testing must be designed to try and make the system fail, all to often designers do not like to do this.

FMEA Check

The FMEA supplied by the DP Control System supplier must be at a suitable level of detail. All to often it is obvious that they are a simple confirmation of the functionality and do not seek to really test the robustness of the design.

The FMEA of the DP control system must be very detailed. For instance, for a digital input card, the possibilities of all input failing to high and all failing to low, plus each individually failing high and low should be considered. Similar for analogue signals – failure high, low and freeze (as is). For a serial line, total failure, miscommunication and hang up mid message must be considered. Those who have actually written, or are sufficiently familiar, with the software, should review the results of the analysis. Then the testing should be based on the FMEA to validate its findings.

Combinations

Often a system breaks down when particular combinations of items are in operation that has not been tested for. All combinations of thrusters, generators, switchboards, position reference systems, sensors etc should be tried. Often it is difficult or far to time consuming to test absolutely all combinations – those that cannot be checked should be tried in simulation mode especially during FAT against the full simulator.

Thruster Changeover

Where and how the control of the thrusters is switched between DP and Manual control is an area were often neither the DP control system supplier nor the thruster supplier is responsible for it's design. Or were there may have been a misunderstanding on how this should integrate. This is often a weak link in the system and should be tested extensively.

Power system interface

Similar to the thruster changeover this is an area that can be neglected in the design or implementation. The input of the power system interface is extremely crucial, and the placement of interfaces can be overlooked, so on-board performance and FMEA testing focusing in on these interfaces is required.

Common Interfaces

Items that provide an interface to all the DP control systems the vessel might have are a source of systematic failures. These are discussed later in the paper. Typically though these are all position reference systems, sensors, power system interface, thruster feed backs, BOP system interface. Anywhere were a common interface can hang up all the supposedly redundant systems.

Alarms

Each and every DP control system alarm should be demonstrated. This really checks over the whole system and is a must.

Limiting Conditions

Often a design will break down at limiting conditions – e.g. during power limiting, maximum surge, sway and yaw demands and in combination, maximum range of position reference system etc. These should be tested for.

Redundancy

All conditions that can cause a change over between redundant DP systems must be tested for. In conjunction with FMEA Proving trials, redundancy testing can take a large amount of manpower and a close inspection of the results is required. A full understanding of the system's design and operation is a must for redundancy testing.

Hidden failures

If the design has back ups in that are meant to cut in then this must be monitored to ensure that they will operate should they be called into operation. These back ups must be tested and also tested for what happens if they are already failed when called upon.

FAILURE MODES AND EFFECTS ANALYSIS

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 DP control 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 mal operation 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, or being able to set the system up and defeat the redundancy.

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 example; 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.

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 the entire 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.

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 however the more detailed the more expensive and time consuming it will be.

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 affects the cost and level of analysis. One approach is to provide a description, and possibly a block diagram, of each vessel system that 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 is the more analytical but can restrict the freer thinking that may be necessary to find some of the single failures. A 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.

Further detail can be obtained from reference one.

SYSTEMATIC FAILURES

While the hardware of a DP Control System is relatively easily made redundant the software is identical in each DP Control System installed – no supplier or operator has opted to have different software in each system. This makes the systems prone to what are known as 'Systematic Faults'. These occur when a particular set of conditions arises, that have not been tested or designed for. These cause the software to either crash or do something unexpected - **on all the systems simultaneously.**

It is imperative that the FMEA and failure testing seeks to find these systematic faults as they are definite sources of single failure that can cause all systems to fail.

Generally, hardware will not suffer from systematic errors if it is at least duplicated. Systematic hardware faults needs to be something that can affect all systems at once, such as radio interference, earth faults etc. However for the purposes of failures of DP control systems, the failures will largely be limited to software – a hardware event may initiate the failure, but it is the software's reaction to it that creates the problem. There have been a few exceptions to this, as in the case where substandard chips in all three processors failed simultaneously when a voltage spike occurred. Also where a telex transmission caused the wind sensors to erroneously register 100 knots and the DP control systems reacted accordingly, driving the vessel rapidly off station.

It should also be noted that this problem applies to any system that is part of the DP control system that runs software. For example, redundant position reference systems (dual DPGS / dual Acoustics), DP control computers, and certain dual sensors (gyros and VRUs). If identical units are purchased – they will have identical software running in them.

EXAMPLES OF SYSTEMATIC FAILURES IN DP CONTROL SYSTEMS

The following examples of systematic failures are based on both of the authors' personal experience and the IMCA DP Incident Database.

After about seven weeks operation each DP control systems crash in close order

In this incident each of the three DP control systems installed failed within minutes of each other. The fault was found to be a millisecond counter that had filled its register at FFFFFFFF. At 429497.296 seconds (49.7 days) after the last reboot the register fill and the system crashes. As each system had been rebooted at around the same time they all crashed at around the same time.

Reboot of Power Management System causes both DP Control Systems to fail

The DP control System had been interfaced to the vessels power management system (PMS) over a data highway. This was used to send information about the generators running, power being consumed etc. These signals were backed up with direct-wired signal and the failure modes of the single PMS were

covered. However at some stage in the commissioning it was decided to synchronize the DP control system time setting to that of the PMS as the data highway had that information available. This worked fine until the PMS was rebooted causing the time sent to be a random setting. The DP software had no protection or checks on the time information and both DP systems crashed

DP control system mistakenly assumes manual control has been selected.

In this incident this vessel had a single multi-pole switch that changed over control from the manual thruster controls to the dual DP control system. Each DP control system sensed a contact of the switch. The input to the on-line system was lost so it assumed that the switch had been set to the manual position. It then set all its thruster demands to zero, told the standby system that manual was selected (so that it followed suit) and no changeover took place. As the switch was, in reality, still in the DP system position, all thrusters went to zero. The problem was easily fixed.

DP control system assumes there is no power available for the thrusters.

This dual system had the entire 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 set them all to zero. The standby did have valid signals but the changeover was not designed to take place on the basis of adequate generators. Subsequent systems now include certain cross checks to prevent this happening again.

A similar event occurred on another dual system where the power available for DP was a single signal from the power management system to the DP control systems. This signal failed and both DP systems assumed that there was no power available for the thrusters and set them all to zero. Future systems with this type of arrangement had a check and alarm included. If the signal is suspect then the power-limiting feature of the DP control system is suspended.

DP system sits in a wait loop for the rest of a serial message that will never arrive.

This triple redundant system had all three system interfaced by serial line to them for the communication of the riser angle over the BOP Mux system. The software for handling this serial line had been written and tested in the factory. It was however necessary to modify it on the vessel as the telegram was not exactly as per the design information. The modification was rushed and not tested thoroughly enough. Then on one occasion the serial line transmission stopped in mid message leaving all three systems waiting for the rest of the message and not doing anything else useful – like keeping the vessel on station for instance.

DP control system believes that a faulty position reference system is 'perfect.'

This is classic of older systems that weighted the position reference systems on the basis of their noise content. The less noise – the higher the rating. This works very well until something happens that makes a faulty system seem perfect. Examples are a transponder that is not actually on the bottom, a taut wire touching the vessel side or giving out a nearly fixed signal because the wire has broken or the signal is lost. In these cases, the faulty system actually gets the majority of the weighting and the healthy alternative position reference systems get largely ignored and even rejected. This has occurred on a

number of occasions – examples other than a transponder not on the seabed or a faulty taut-wire, include a frozen Artemis signal and a DGPS that continued to transmit the same position on loss of satellites. This effect would occur on all DP control systems in any redundant set. It is over come on more recent systems with the use of median checks and 'voting.'

DP control system assumes that no center of rotation means gives up control.

This vessel had been operational for about 4 years and had undergone very detailed testing and FMEA. However one day a fault on an input 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 and the software in both the on-line and standby failed to compute correctly and effectively shuts down. The software had not been designed to default to the vessel center if nothing was read as being selected.

DP control system assumes all its gyros have failed.

On a semi-submersible a minimum rate of change (non-movement) check on a gyrocompass can be a nuisance as the heading control can be so good that the gyros may often fail the check. On this system with two gyros it was decided to interlock them with the mismatch alarm. The idea being 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 were less well aligned at a particular heading. Then, because the heading control was so good, both gyros were deselected by the non-movement check on both DP control systems.

Failure of a thruster feedback signal upset the DP control system's Kalman model.

The Kalman filter in the DP control system models the vessels behavior and therefore needs to include for what the thrusters are doing. There are two options here: 1) either use the internally generated demand suitably delayed to model the thruster lags, or 2) the actual feedbacks from the thrusters can be used. One supplier opted for the latter – the others have always opted for the former. The problem with the latter is that there is a common direct connection from the outside world into the heart of each channel of the DP control systems. Failure of this signal nicely messes up all the models in all the DP control systems installed. Since realizing this, the system has been modified to use the actual feedback unless there is a thruster mismatch alarm caused by a difference between the demand and the feedback. If there is then the internal demand is switched to instead.

Display scale selection fails a dual system.

This fault was present in many systems. Here changing the shared display's scale with certain other conditions present, caused both DP control systems to crash. This fault was subsequently corrected on all systems in the field.

REFERENCES

1) Failure Modes and Effect Analysis (FMEA) – Doug Phillips – MTS Houston 97
2) Loss of Redundant Systems from Systematic Faults – Doug Phillips IMCA Rio 98
3) Classic Single Point Failure of Redundant DP Systems – MTS Houston 98
4) Software Failures – follies and fallacies, Les Hutton, IEE Review March 1997
5) Explosive Lessons, Matthew Bransby, Computing and Control Engineering Journal – April 1998.
6) "Are N average software versions better than 1 good one", Les Hutton – IEEE Software – Dec 1997
7) The Dynamic Positioning of Ships: the problems solved? – Doug Phillips – IEE Control 96
8) IMCA Station Keeping Incidents
9) Normal Accidents – living with high risk technologies - Perrow

ABOUT THE AUTHORS

Blake Miller has a Bachelors of Science degree in Marine Engineering Systems from the U.S. Merchant Marine Academy (Kings Point). He worked at National Steel and Shipbuilding Company (NASSCO) for 3 years as a Test Engineer where he was responsible for the operation and testing of shipboard systems prior and during Sea Trials. Blake joined Nautronix in 1997 as a Project Engineer responsible for the design and technical aspects of DP and Vessel Control projects. Blake led the development, from a technical standpoint, Nautronix's 5000 Product Line of Vessel Control Products and has recently taken on the role of Engineering Manager of the Nautronix, San Diego office.

Doug Phillips has a Bachelors Honors Degree in Computer and Control Engineering and has worked with Dynamic Positioning for 26 years. The first 20 years with what is now Alstom designing, building and commissioning DP and anchor assist control systems. Initially as a project engineer, 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 3 years he was been the Vessel Controls Product Manager for Nautronix mainly involved with the development of the ASK5000 range. He has recently rejoined Global Maritime heading their DP effort in Houston.