DYNAMIC POSITIONING CONFERENCE
October 09 - 10, 2018

UNWANTED THRUST SESSION

Thruster Fail-Safe – Effective Validation and Verification

By Steven Cargill

DNV GL Noble Denton marine services

Abstract

Despite the downturn in DP vessel activity in the last few years there has been a persistent and disappointingly high number of DP loss of position incidents associated with thrusters failing in such a way that they produce excess thrust or thrust in the wrong direction. The effect of this is either to drive the vessel off position directly or destabilize the DP control system to the point where large position excursions develop (surging). Some of these incidents occurred on Diving Support Vessels and it is largely due to chance that the consequences were not more severe. The failure effects have been most severe in the case of vessels with controllable pitch main propellers but tunnel thrusters and azimuthing thrusters with fixed and controllable pitch propellers have also failed to non-fail-safe conditions.

Clear and unambiguous guidance on the fail-safe condition of thrusters was established in IMO MSC 645 and further refined in MSC 1580 but traditional verification and validation processes (intended to confirm the requirements in the guidance is complied with) have failed to prevent all the incidents.

This paper discusses:

- Why thrusters fail in ways that do not comply with fail-safe requirements.
- Why traditional verification methods fail to detect these unacceptable failure modes.
- Why traditional mitigations are not fully effective in preventing drive-off.
- An alternative approach to the design and analysis of thruster control and protection systems which ensures thrusters fail-safe.

Abbreviation / Definition

CPP Controllable Pitch Propeller
DNV Det Norske Veritas
DP Dynamic Positioning
DPO Dynamic Positioning Operator
DPSI DP Station Keeping Incident
FMEA Failure Modes and Effects Analysis
FPP Fixed Pitch Propeller
IMCA International Marine Contractors Association
IMO International Maritime Organisation
LFI Learnings From Incidents
MSC Maritime Safety Committee
MTS Marine Technology Society

Introduction

In the IMCA station keeping review for 2017 (DPSI28), thruster and propulsion related incidents, were the largest single cause of DP incident reports accounting for more than a quarter of all reports in that year. The percentage of thruster related reports (thrusters only) in the Half Yearly IMCA DP incident report for 2018 was similar. Not all of these incidents concerned thrusters that failed in a non-compliance way but some of them did. The prevalence of thruster incidents means that faulty thrusters are something that a DPO can reasonably expect to experience at some point in their career. DPOs may also be relied upon to react in the correct manner to prevent the effects of the thruster failures leading to a loss of position. This paper focuses specifically on failures that do not comply with fail-safe requirements. Such failures have the potential to cause a loss of position.

Figure 1 shows a much-simplified representation of the control system for an azimuthing thruster with a controllable pitch propeller. It consists of two closed loop control system one for azimuth and one for pitch each with a feedback potentiometer. The DP control system performs open loop control of the Pitch and Azimuth controls system but monitors feedback through its own electrical independent potentiometers.

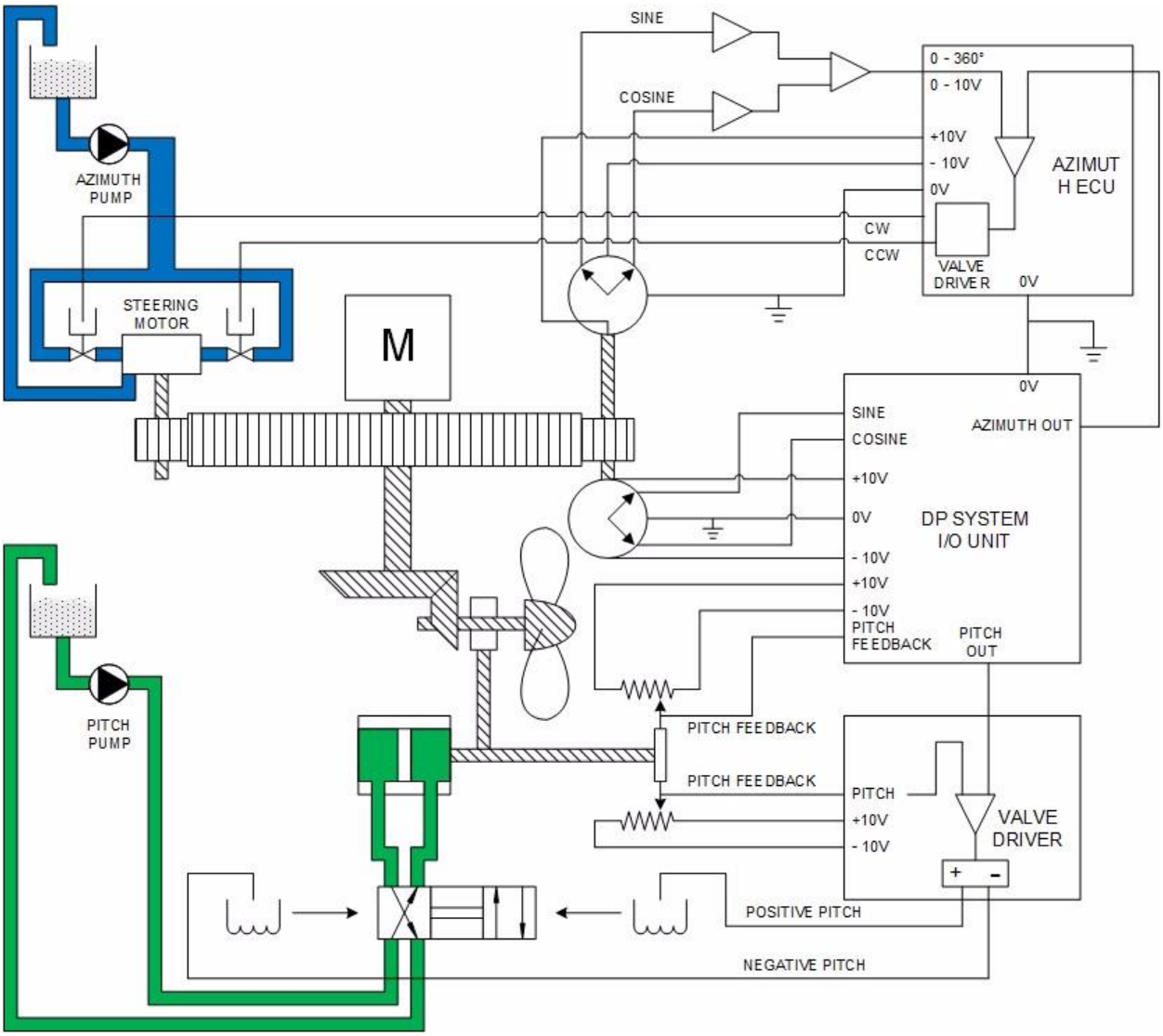

Figure 1 Basic Elements of an Azimuthing Thruster with a Controllable Pitch Propeller

Why thrusters fail in ways that do not comply with fail-safe requirements

There are at least two reasons why such failures occur:

- The thruster has not been designed to be fail-safe for all modes of failure and the verification and validation process has not detected these deficiencies.
- The thruster design may or may not be fully fail safe but there are hidden failures which compound the effects of a subsequent failure. The periodic testing process has not revealed these faults in time to prevent escalation.

Open Loop Control - Thrusters are a closed loop control system under open loop control from the DP control system. Generally, the DP control system will only alarm (takes no action) if it has reason to believe

it is not obtaining the thrust magnitude or direction it has requested from the thruster control system. As thruster feedback is used by the DP model, the DP control system may switch to estimated feedback to prevent the model being affected by erroneous data. To initiate this changeover, the DP control system monitors the feedback signal to detect if it has gone out-of-range in some way. This may prevent faulty feedback, from an otherwise healthy thruster, influencing the model but it cannot prevent a faulty thruster from destabilising station keeping.

A basic thruster control system employs closed loop control with negative feedback. That is to say, the difference between the set-point (command and feedback) is measured and used to drive an actuator which reduces the difference between command and feedback until it falls within an acceptable dead band.

A closed loop controller will continually attempt to minimise the error as the set point changes. However, if the feedback from the sensor fails the system will continue to drive the actuator in the direction that would minimise the error. For example – if the thruster is being commanded to go to half pitch when the feedback fails to zero the thruster controller will continue to drive the pitch up in the hope that the thruster feedback will eventually get to half pitch. In practice, this means the thruster is driven to full pitch and a drive off or position or excursion may ensue.

Thus, at a fundamental level, a basic closed loop control system does not fail in line with the guidelines (example - engine speed controller failing to full fuel). Other features must be added to make it fail safe.

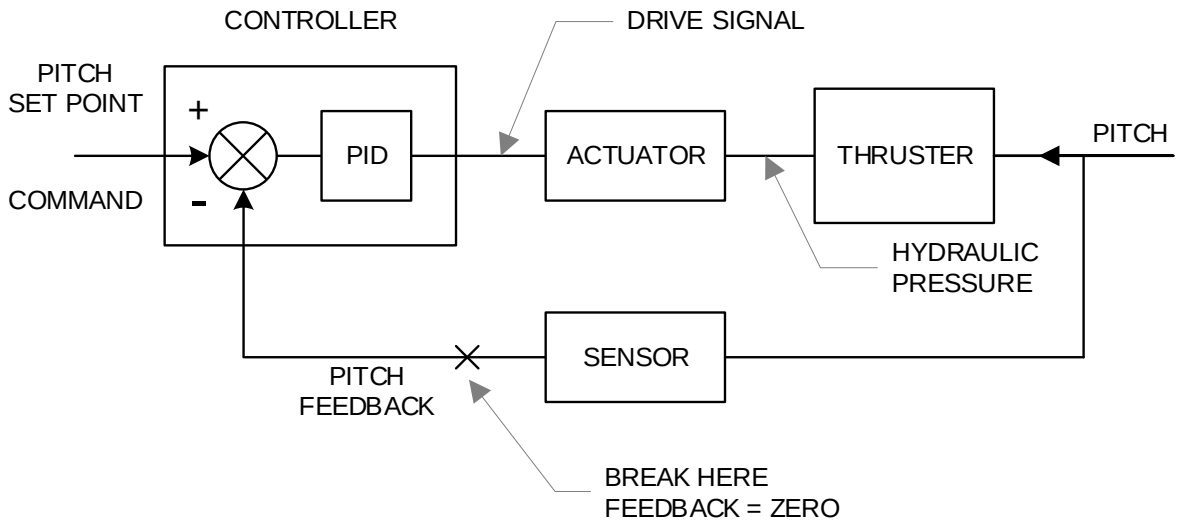

Figure 2 ~ Basic Closed Loop Control

Early in the history of DP vessel development, is was quite common for wire break tests to cause CPP thrusters to fail to full pitch. Results such as these usually initiated in some kind of modification that allowed the thruster to pass the wire break test. Early DNV rules were silent on thruster fail-safe. When the rules for fail-safe were developed, allowances were made for older vessels if the rate of failure to full thrust was slow and there was a credible period of time for operator intervention.

In thrusters that rely on tachometers for propeller speed feedback it was not unusual to find that failure of the tachometer to zero speed feedback would cause the drive output to increase to full speed.

Even in the case of DP vessels in service today it is still possible to find thrusters that do not pass this basic test. This may be because:

- A protective function or feature intended to address the simulated failure mode has not been installed or is not working properly.
- The test method has been changed and revealed a previously unrecorded deficiency in the design.
- Fail-safe attributes have been modified by hidden failures. For example, hydraulic circuits may inherently fail to the last ordered position when the command fails because actuator valves close locking the hydraulic fluid in place, fixing the pitch position. However, if there are leaks in the system, the blades may slowly advance to the full pitch position. Annual DP trials do routinely detect this type of failure on CPP thrusters.

Figure 3 shows an example of a failure mode which has happened on several occasions. The azimuth thruster in question has a single mechanical drive for three potentiometers on a common shaft. The coupling became loose and over a period of time causing the true thruster azimuth angle to diverged from the angle indicated by the potentiometers. Because all potentiometers agreed the closed loop control system was able to turn the thruster to give the DP control system the azimuth angle it requested there was no alarm until station keeping performance deteriorated to the point where a position warning was generated. The azimuth indictors on the manual thruster control panel also gave no indication that anything was wrong.

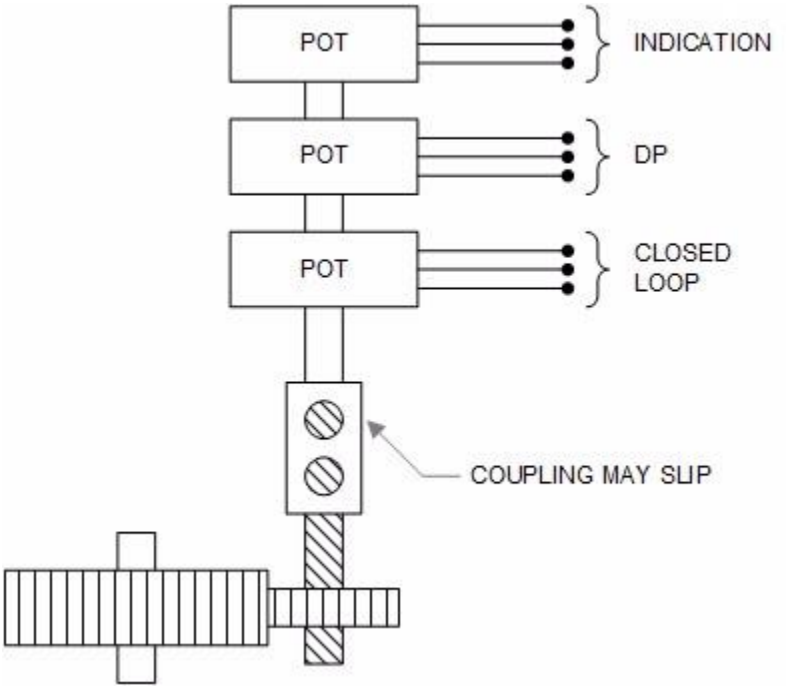

Figure 3 ~Common mechanical drive to rotation transducers

Mechanical failures are not the only way this type of failure mode can manifest itself. Figure 4 shows a much-simplified representation of a closed loop control system. In this design, there is a common feedback signal for closed loop control and for feedback to the DP control system. There is a separate signal for indication which shares the mechanical drive. The signal from the feedback pot is conditioned before it is applied to the summing node. If this amplifier develops an offset the true thruster azimuth angle will deviate from the indicated angle at the manual thruster control panel but the DP control systems will not alarm because the closed loop control systems will be able to turn the thruster to the angle the DP control system requests. As in the previous example, station keeping performance deteriorates because there is significant thrust in the wrong direction leading to surging. In this case. It would have been possible to observe the divergence on the azimuth indictor on the manual thruster control panel when compared with the DP control

systems but there is no alarm to draw the attention of the DPO to the manual controls and focus tends to be on the DP control system screen when station keeping is deteriorating.

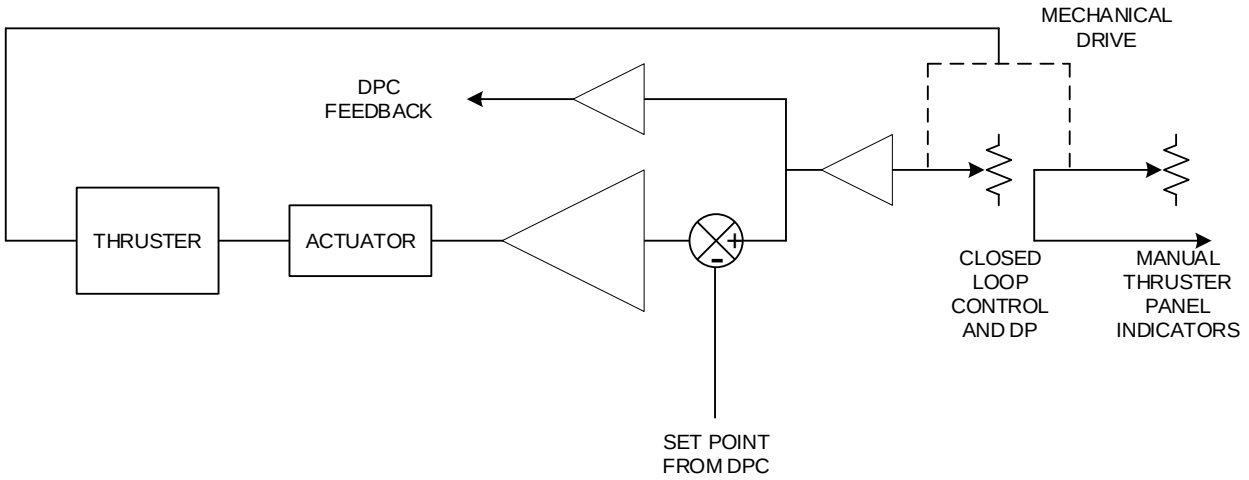

Figure 4 ~Vulnerabilities of common mechanical drive and feedback

Why traditional verification methods fail to detect these unacceptable failure modes.

Although there are requirements to comply with rules for thruster fail-safe there is no requirement for the thruster manufacturers to demonstrate that these requirements have been met by way of established methods such as Failure Modes and Effects Analysis. Some manufacturers do this voluntarily but there is variability in the scope and depth of these analyses. The bulk of the verification process falls upon the overall DP FMEA provider and is in practice a relatively small part of the scope.

Traditional verification methods employed at DP FMEA proving trials and annual DP trials test a very limited number of failure modes. Such tests are often developed from past-experience of what is normally accepted and not from a detailed understanding of the thruster's design, fail-safe features and protective functions upon which a satisfactory failure response depends.

Wire break tests will, for example, test the failure effects of control loops to open circuit faults. There may be protective functions monitoring the loop to detect an open circuit and freeze the actuator output. However, the zone of detection may be limited to the external wiring of the feedback loop. Other failures internal to the controller or its sensors and actuators may have the same effect but are not detected and may have unacceptable results. In the worst case, such designs could be considered to be 'test-proof' rather than fail-safe.

Even within the very limited scope of control loop testing there may be significant variability.

- Some tests programs only break the signal wire
- Others programs may break the ground wire and the signal wire
- Some test programs will fail power supplies to potentiometers and not just the signal output
- It is less usual to find control loops being tested for ground faults and short circuits which have caused thruster to fail to full thrust in the past. Reluctance to allow such tests to be carried out is often driven by fear of equipment damage.

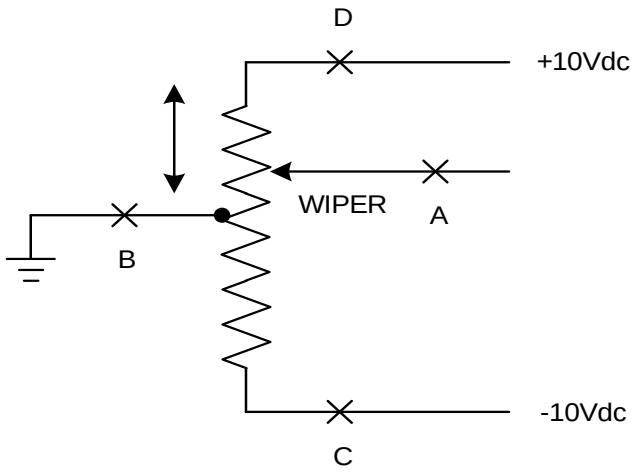

Figure 5 Potentiometer with center ground tap

The operating point of the thruster at the instant the tests is carried out may also influence the result. Figure 5 above shows a typical potentiometer used to provide feedback. Although there are many modern options available for displacement transducers the potentiometer is still widely used. In the example above, the pot wiper is shown in the upper part of the resistance element – if point C is broken there will be no effect on the feedback signal. If point D is broken the feedback signal will go to zero. This will create a difference causing the closed loop control system to operate the actuator to try and reduce the error. The thruster will no longer be delivering the thrust magnitude or direction required.

- The thruster control system may have loop monitoring capable of detecting if the signal wire is broken at point A but, in this example, zero is a valid signal level.
- Thruster may appear to fail in a compliant manner when the wiper is broken.
- The thruster may not fail safe when a power supply connection to the resistance element is broken (wiper on the supplied element).
- The thruster may appear to fail safe when a power supply connection to the resistance element is broken (wiper not on the supplied element).

It is not unusual to find thruster failure effects reported as ‘Not as Expected’ when all that has happened is the initial conditions prior to the test were different from those at the previous set of trials. The expected effects are often based on the observed performance of supposedly healthy thruster and not on an understanding of the thruster’s detailed design.

Essentially, much of the verification process is based on a traditional understanding of what is accepted by approval authorities and other stakeholders and not on a detailed understanding of the thruster’s design and the protective functions which ensures it fails safe. A detailed knowledge of protective functions and features is required to confirm whether they provide comprehensive cover and also to develop periodic test plans and monitoring to ensure there is a high probability that they will operate effectively on demand.

There is no doubt that carrying out wire break tests without knowing what function or attribute is being tested is not a good use of vessel time particularly where a thruster could not actually fail any other way. This is not to say that wire break tests are entirely without merit. They often detect unacceptable failure modes, particularly in CPP thrusters. But they are not sufficient on their own to confirm the fail-safe condition of a thruster. Figure 6 and Figure 7 illustrate a problem that occurred on more than one occasion with dual-element pitch potentiometer designed for use on DP Class 3 designs having an analogue interface between the DP Control system and the thrusters. In this design the pitch-pot has two resistive elements –

one is powered from the main DP systems and the other from the back-up DP systems. What is not always appreciated with this design of potentiometer is that it is possible to install it onto the thruster with the shaft displaced by 180° from the wanted position. The thruster functions perfectly well but a very significant common point is created by powering the pitch-pots for the main DP system from the Backup DP system If the installer is unaware of this possibility, then the laws of probability dictate how many thrusters are incorrectly wired. This can in practice vary between all of them and none. Performing wire break test will at least reveal those that are incorrectly wired as the alarms appear on the backup DP control system when the main DP system is failed. Commissioning should be the primary means by which such errors are identified but commissioning tends to focus on proving that equipment performs to expectations not that it fails in line with the DP redundancy concept.

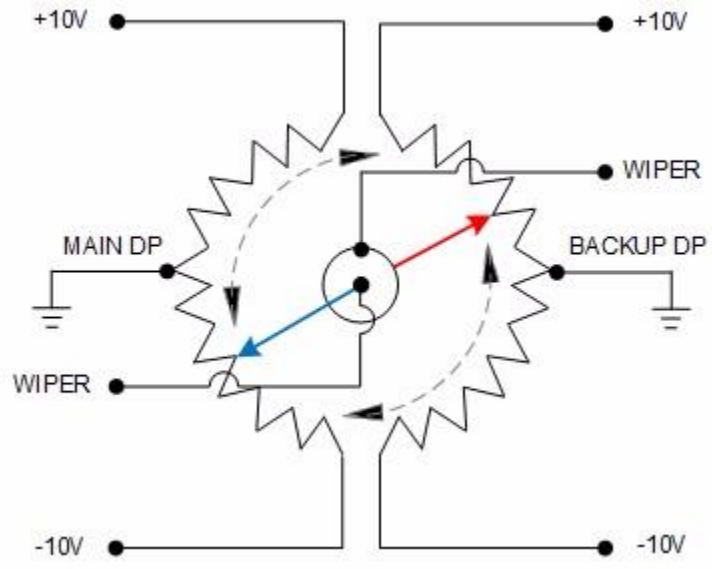

Figure 6 Dual Element Potentiometer for DP Class 3

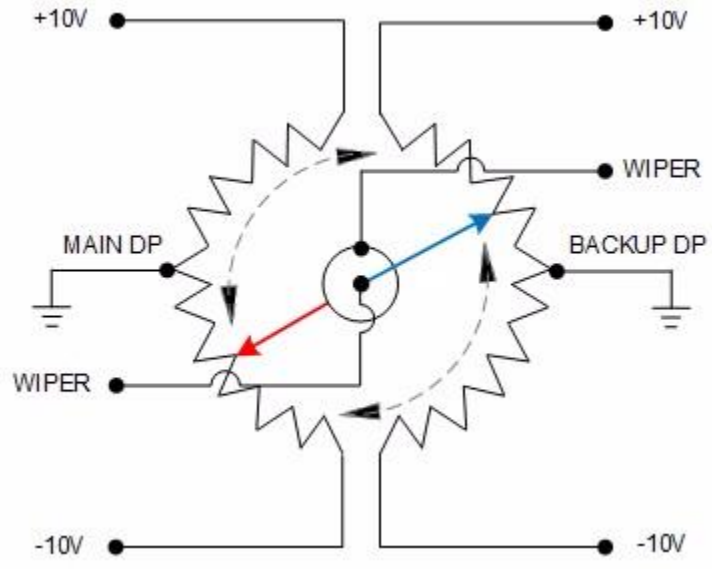

Figure 7 Dual Element Potentiometer for DP Class 3 – Incorrectly installed

One of the easiest ways to investigate whether a thruster has a protective function other than wire break detection is to simulate a stuck valve or an active valve drive output by manually operating one of the hydraulic valves and observe if the thruster rotates in azimuth or changes pitch. In the case of azimuth control, some thruster control systems will detect the deviation from set-point and remove the DP ready signal, this has the effect of also setting the thrust command to zero and will prevent thrust being developed in the wrong direction. In the case of pitch control failure, removing the thruster ready signal to the DP control system may have no effect on the pitch as the control loop is considered to have failed in some way and unwanted thrust will develop. Unless the thruster control system has the facility to stop the prime mover the possibility of developing unwanted thrust exists. Similar concerns exist in relation to the speed and toque control loops for FPP thrusters.

Other reasons why traditional testing practices fail to reveal unacceptable failure modes is because there is uncertainty about which indicators are actually providing an accurate representation of the thruster's response during testing. Typically, indicators on the manual thruster control panel are the most reliable when testing the closed loop and DP loop signals but this should be confirmed. Having someone physically confirm the actual response of the thruster in the thruster compartment provides the highest level of confidence. It's not uncommon to find that the DP feedback has gone to full thrust but the manual indicators confirm the thruster is still following the command.

Figure 8 shows a popular angle transducer used to indicted the direction of thrust from Azimuthing thrusters. Other types of transducers include inductive types such as Synchros & Resolvers and digital types including encoders of various designs.

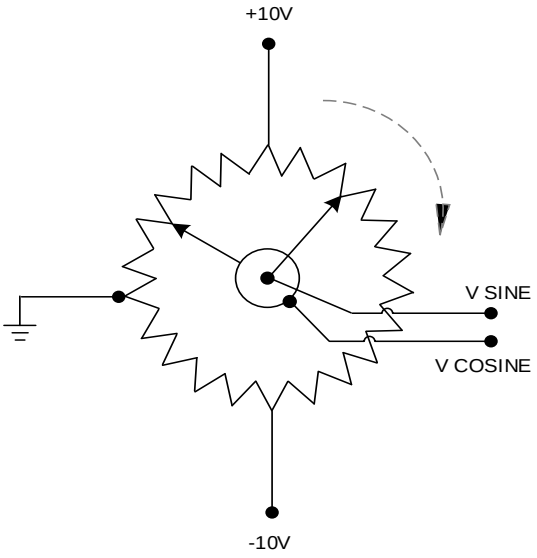

Figure 8 ~Independent Rotation Transducers Protection Concept

The sine-cosine potentiometer has resistance elements with a tapered resistance distribution which produces an output voltage proportional to the sine of the angle of rotation. A second wiper displaced by 90° provides an output proportional to the cosine of the angle. It's not possible to derive an absolute position from one signal alone because there are two possible angles for every voltage. Knowledge of both sine and cosine voltages as shown in Figure 9 allows a unique angle to be resolved.

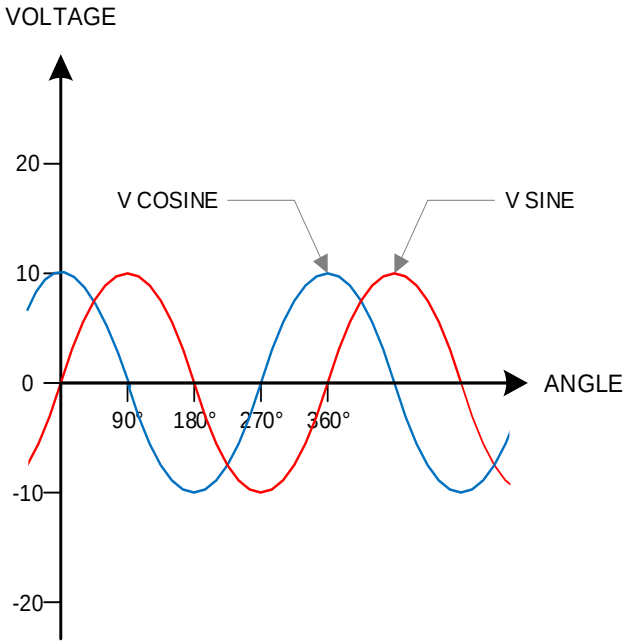

Figure 9 ~Azimuth Angle Determination by Sine / Cosine potentiometer

1. if V_sin ≥ 0 and V_cos > 0	angle = arctan (V_sin / V_cos) / (2*pi) * 360
2. if V_cos = 0 and V_sin > 0	angle = 90
3. if V_cos < 0	angle = 180 + arctan (V_sin / V_cos) / (2*pi) * 360
4. if V_cos = 0 and V_sin < 0	angle = 270
5. if V_cos > 0 and V_sin ≤ 0	angle = 360 + arctan (V_sin / V_cos) / (2*pi) * 360

Algorithm 1 – Resolution of Azimuth Angle

The failure modes of the sine - cosine potentiometer are interesting and may depend on how the conversion from voltage to angle is coded. One method of conversion is given in Algorithm 1. Figure 10 shows the two voltages derived from the wipers on the potentiometer. Figure 11 shows the azimuth angle derived from these voltages against the true thruster direction as the thruster completes one revolution. As expected, the indicated feedback matches the true angle of rotation.

Figure 12 and Figure 13 show the effect of one of the two channels failing to zero voltage. In the case of the sine channel, the feedback from the thruster toggles back and fore between 0 and 180° as the thruster completes one revolution. In the case of the cosine channel the feedback toggles between 90° and 270°.

If the feedback is used by the DP control system, then it should indicate a prediction error and possibly indicate failure of the loop as well. However, if 4-20mA convertors are used for the purpose of providing line monitoring they may not detect failures in the transducer itself if these results in valid signal levels. In the case of sine - cosine potentiometers it may be possible to detect faulty channels using the relationship in

Equation 1.

$$\mathrm{Sin}^2 \mathrm{A} + \mathrm{Cos}^2 \mathrm{A} = 1$$

Equation 1

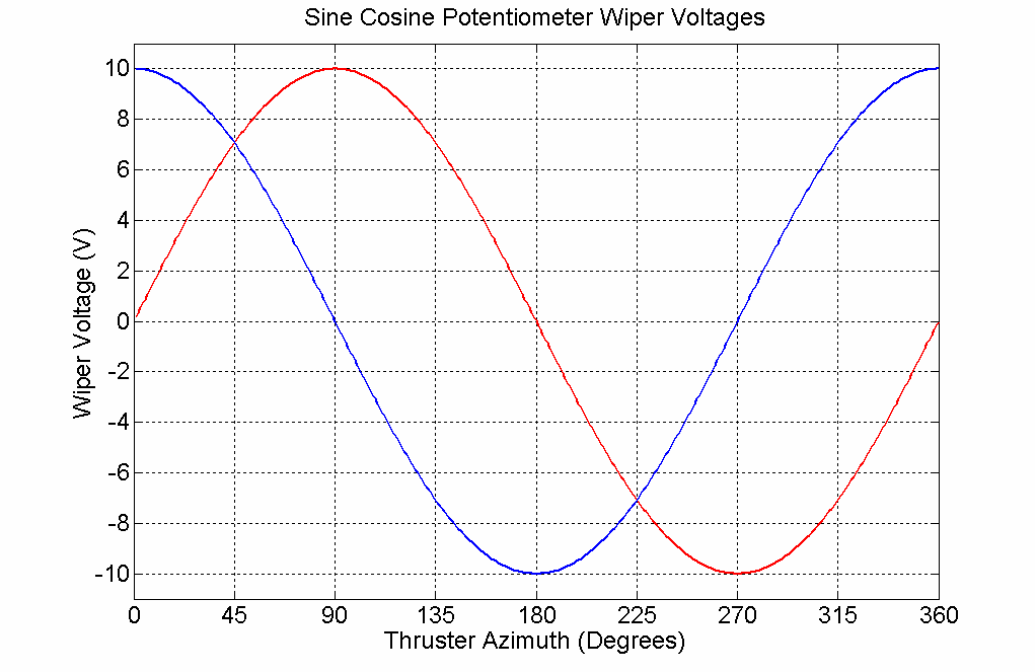

Figure 10 wiper voltage against Azimuth angle

Figure 11 Resolved Azimuth value as thruster rotates through 360°

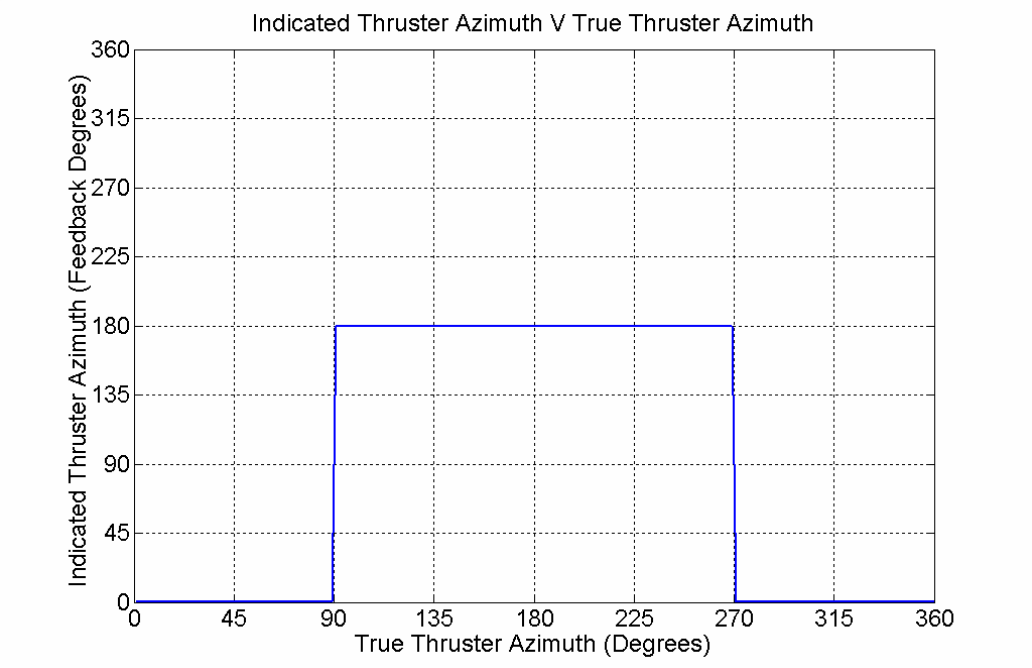

Figure 12 Indicated thruster angle when Sine channel is faulty (failed to Zero Volts)

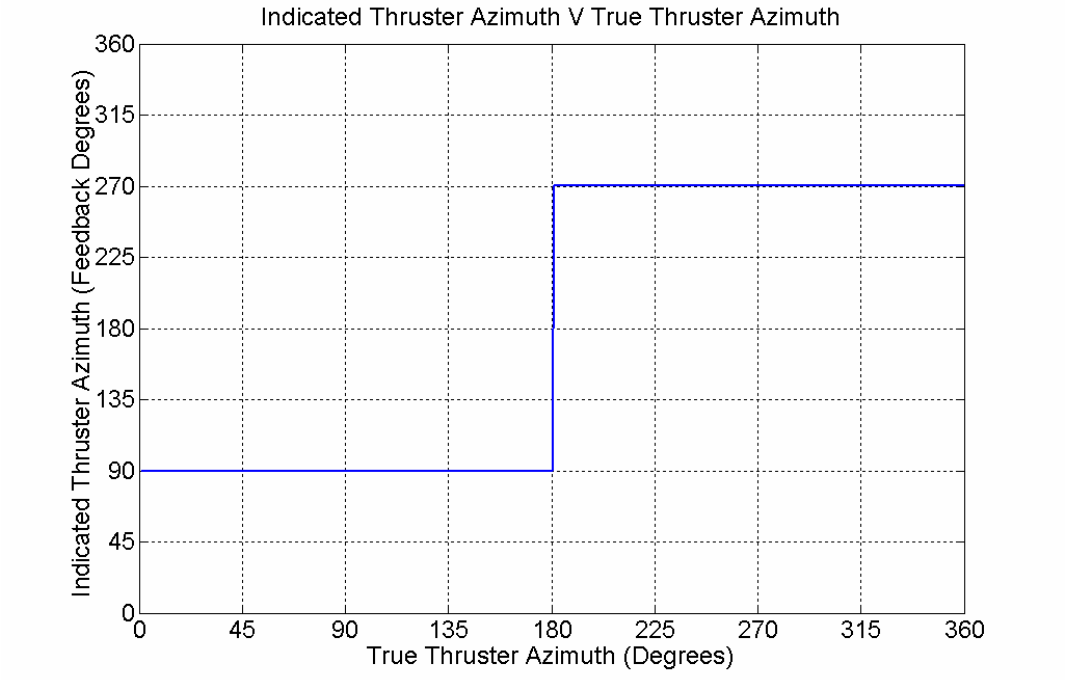

Figure 13 Indicated angle when cosine channel is faulty (Failed to Zero Volts)

Digital communication is increasingly used for thruster command and feedback. The serial lines used for this purpose generally fail in a predictable manner but this may mask the fact that there is analogue circuity at the transducer that may not fail to a safe condition.

Why traditional mitigations are not fully effective in preventing drive-off.

There are requirements in the overall DP system FMEA (Refer to DNVGL RP-D102 – FMEA of Redundant Systems) to consider Drive-Off as a possible failure mode and thruster failures to non-fail-safe conditions are a potential cause of such a mode of failure. Even when the analysis indicates that there is a possibility that the thruster may not fail to a safe condition it is often accepted as meeting requirements if it passes the most basic of wire break tests.

The provision of an emergency stop is often cited as the means by which 'Other Risks' are addressed. Reliance on operator intervention to mitigate non-compliant failure effects has its own challenges and it is unusual to find any basis for confidence in the assumption of an effective operator response:

Effective operator intervention may be comprised in various ways:

- The DPO requires a clear and unambiguous indication that the thruster has malfunctioned. Regrettably, this is not always provided, particularly in the case of shared sensors for DP feedback and closed loop control.

- The operator must act quickly and effectively under stressful conditions. A recent MTS LFI 17-3 on unwanted thrust provides evidence that this is not always the case.

- The operator must understand the effects of a faulty thruster providing thrust in the wrong direction and shut it down before it can cause instability in the DP control system.

- The ergonomics of the emergency stop buttons may impede effective decision making.

Thus, a great many assumptions may be made, unconsciously, regarding the efficacy of operator intervention as a risk mitigation with very little basis for confidence in their credibility.

More could be done to help operators take appropriate action in stressful conditions. The DP control system is often able to identify a faulty thruster and alert the operator to this by way of a 'Thruster Prediction Error' indicting that the thruster is not behaving as expected. That prediction error could be used to illuminate the corresponding emergency stop button to reduce the risk of accidentally stopping the wrong thruster which is likely to make the position deviation significantly worse. The efficacy of this concept relies on ensuring that thruster malfunction is reliably detected. Unfortunately, this is not always the case so it may assist but is not a solution.

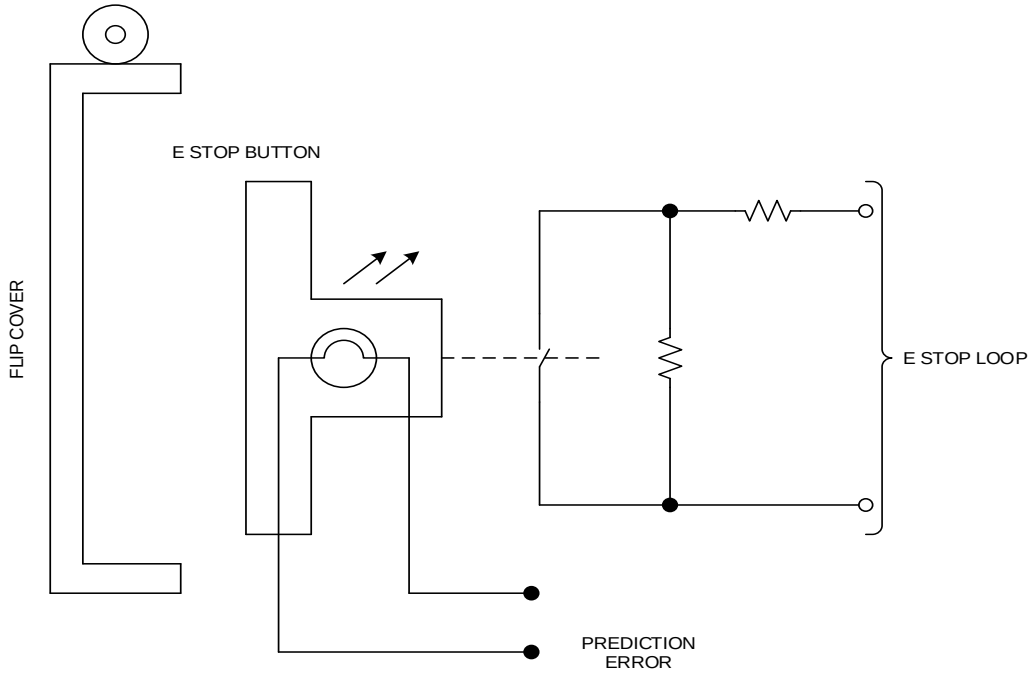

Figure 14 Decision Support

It is good practice to ensure that the Emergency Stop is independent of the thruster control system so that a malfunction in the thruster control system (that requires the use of the emergency stop) cannot also disable the emergency stop. Where the emergency stop trips the prime mover's main circuit breaker, or operates a clutch, there can be reasonable confidence that the two functions are independent. However, in the case of FPP driven by variable speed drives it is common for the emergency stop to be an input to the drive controller – Proving the independence of these functions is more challenging.

An alternative approach to the design and analysis of thruster control and protection systems which ensures thrusters fail-safe.

The fail-safe condition of thrusters relies almost entirely on ensuring there are protective functions able to detect the onset of a thruster malfunction and take appropriate action. Those elements of the verification process that relate to thruster fail-safe in FMEAs and proving trial tend to be limited in scope and depth and fall short of establishing whether the thruster fails-safe for all identified modes of failure.

It is difficult to create a truly fail safe system by addressing a few specific failure modes and even more difficult to verify the fail-safe condition without detailed knowledge of the control system and assorted auxiliary systems, particularly if control and protection function are closely integrated. It is understandable that manufacturers wish to protect their intellectual property but vessel owners and charterers need to protect their assets and personnel from the consequences of a DP drive-off.

Maintaining the independence of functions for control, monitoring and protection is a long-established principle but the advent of integrated automation systems has made it easy to blur the boundaries and essential protective functions may be integrated in to the control system in a manner that compromises their independence and further complicates the verification process. If a thruster system does not include a function that allows it to shut down the prime-mover it must fail-safe be able to guarantee there is no failure that can cause excess pitch or speed and this can be difficult particularly in the case of hydraulic or mechanical elements of the control system. It is proposed that thrusters and their control systems should have a completely independent protective system that is capable of stopping the thruster if it malfunctions

in a non-fail safe way. That is to say, it produces excess thrust over that ordered by the DP control system or thrust that is significantly in the wrong direction. The verification process will then be focused on ensuring that the protective function provides comprehensive protection, does not cause spurious tripping and is fully operational.

Such an independent protective function must not reduce the reliability of the thruster or introduce common mode failure with other thrusters or it will fail to achieve its objective and potentially increase the station keeping risk. Adherence to established principles of independence segregation, autonomy and differentiation can reduce the risk of comprising the DP redundancy concept. Practical measures include:

- Correlation between various, measurements – motor current, pitch, speed, azimuth, hydraulic pressure etc.
- Differentiation in measurement methods (Different type of transducers)
- Model based protection
- Independent measurements for control, protection and monitoring
- Multiple rotation transducers with physical separation
- Autonomous operations with very little connection to other thrusters

Figure 15 provides an outline concept showing how such a protective function might be implemented. In addition to having an independent mechanical feedback it applies algorithms and mathematical models to other data available from the thruster to create a much higher degree of confidence in the thruster's performance. Such model based protection has been used successfully in the protection of fault-tolerant DP power plant for more than ten years and thus the principles and methods are well understood.

Figure 16 illustrates the principle of maintaining segregation between azimuth feedback used for control, DP feedback and monitoring. Diversity could be applied by using the zero-point selector to periodically confirm the calibration of the other transducers.

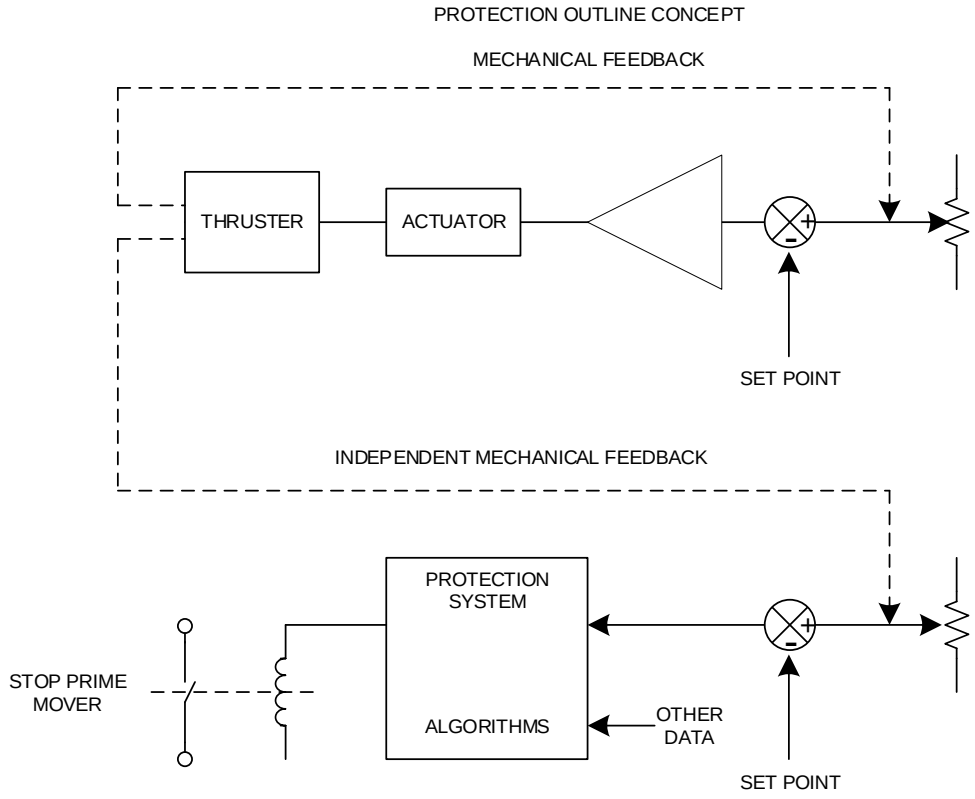

Figure 15 Outline Protection Concept

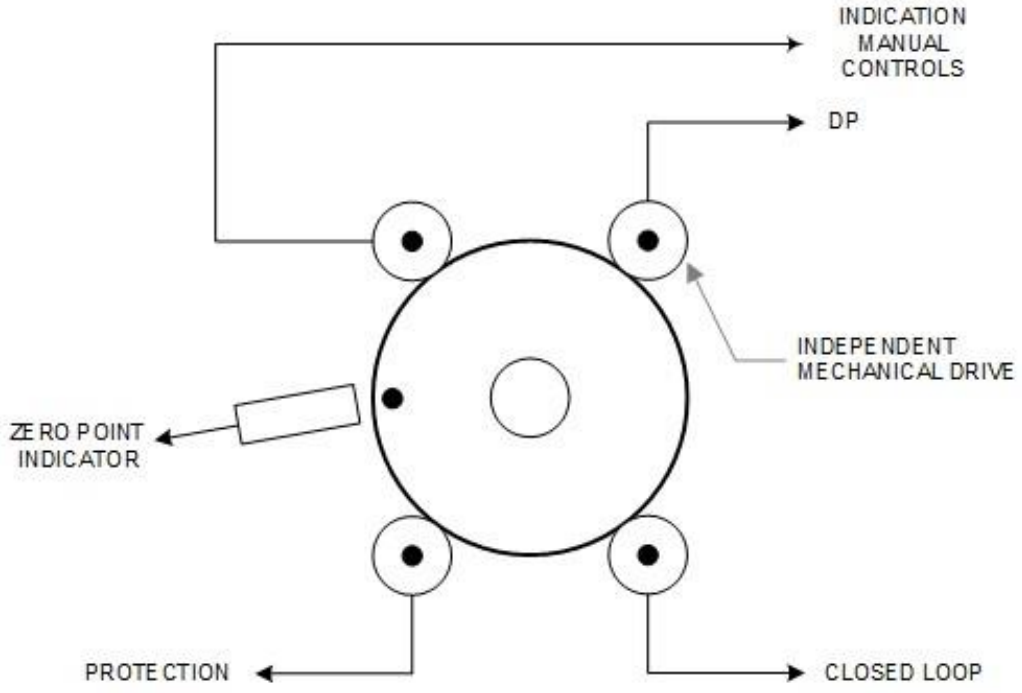

Figure 16 ~Independent Rotation Transducers Protection Concept

Conclusion

DP drive offs caused by unwanted thrust vectors may have significant consequences for life, property and the environment yet the practice of proving thrusters fail in line with industry guidelines has lagged behind developments in other fields of DP system verification. Proving fail-safe is more challenging than proving the fault tolerance of redundant systems. Much of what is currently done as part of DP FMEAs and proving trials is based on limited analysis and testing which provides what is traditionally accepted as indicating compliance and not on a comprehensive engineering analysis. Although there is no formal assessment or record of how many thrusters have some vulnerability it is suspected that the number is significant and that some degree of non-compliance with industry guidelines may in fact be the norm.

Proving fail-safe requires:

- Access to detailed design information which is not normally available including control systems software.
- Test methods that are more comprehensive and more sophisticated than simple open circuit wire-break tests.
- An analysis and testing effort which is significantly beyond what is traditionally practiced in DP system FMEAs and proving trials.

By their very nature, basic closed loop control systems tend not fail to a safe condition. They require the addition of protective functions that can detect anomalous behaviours and act to prevent the thrusters developing excess thrust or thrust in the wrong direction. Typically, there is no comprehensive list of the protective functions upon which fail-safe functionality depends and nothing which would allow them to the verified and periodically tested. Those protective functions that do exist may be closely integrated with the control system and it is difficult to prove their independence and demonstrate that they are not subject to a common cause of failure.

In the case of existing designs, it is not difficult to postulate failure modes that cause thrusters to fail to non-fail-safe conditions. In some cases, it can be relatively straightforward to demonstrate that there are insufficient protective functions to cope with all possible failure modes. Given the challenges of proving a particular design is fail safe it may be more practical to assume that it is not fail-safe and provide an independent protective function for each thruster dedicated to protecting the vessel against drive off. A similar approach has already proved successful in protecting power systems operating with closed busties from blackout.

There is some evidence to suggest that the DP community's trust in reliance on operator intervention may be misplaced. The credibility of operator intervention as a mitigation is typically not validated or verified in a manner which provides a high degree of confidence. Indeed, failures have occurred where no warning or indication of thruster malfunction was provided, save that which indicated the vessel was losing position. There was nothing that would assist the operator in remedying the situation. Furthermore, thrusters which have caused drive offs have often undergone all the tests that are traditionally performed and have passed these tests without comment.

Traditional wire-break testing is not entirely without merit and can detect a limited range of non-compliant failure effects but cannot be considered as comprehensive mitigation of the risk. Although there are improvements that could be applied the challenges of improving on traditional verification methods in a piecemeal way are significant and such an approach lacks the system thinking necessary to achieve success. it is therefore proposed that verification and validation process be refocused on proving the efficacy of an independent protective function which can be applied to any thruster and which is capable of detecting anomalous behaviour and taking appropriate action in a robust and reliable way.