



UNWANTED THRUST !

“HAVE WE DONE ENOUGH?”

Suman Muddusetti

PRINCIPAL MARINE OPERATIONS ENGINEER - MARINE RISK TEAM LEAD

SHELL INTERNATIONAL EXPLORATION AND PRODUCTION (Projects and Technology)

Outline

- Leveraging MTS LFI on Unwanted Thrust
 - Introspection and Reflection
 - Dilemmas
 - Developing Clarity
- A Systems Approach to implementation of the LFI
- Actions
 - Internal
 - External
- Predictable Outcomes - Can We do More?

Leveraging MTS - LFI



Diving Vessel Drive-off - Propeller Failure to Full Pitch

Target audience for this LFI

- Vessel Management and Operations Teams on DP Vessels
- DP Technician Support Function (Vessel Owners/Contractors)
- DP Assurance Teams of Operators/Charterers
- Vessel Designers, DP Equipment Vendors,
- FMEA Providers
- Classification Society DP Approval Authorities

What happened

A significant loss of position event was experienced. (Position excursion of around 70 metres in approximately 74 seconds). The potential consequences triggered an incident investigation using the guidance and tools provided by the MTS Techop on DP Incident Investigation.

[TECHOP ITEM 03 \(Conducting Effective and Comprehensive DP Incident Investigations\)](#)

Vessel Particulars

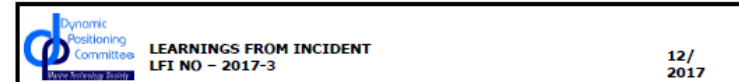
- DP Class 2 - Mono-hull diving support vessel
- Main propulsion provided by engine driven Controllable Pitch Propellers (CPP)
- Electric tunnel thrusters driven by shaft generators

Events

At the time of the failure, the vessel was taking stores from a small harbour boat and preparing to commence diving operations. The vessel was operating on DP and in accordance with the ASOG.

- The vessel was observed to drive off position in the ahead direction
- The port propeller pitch indicator was observed to be at full pitch ahead
- Black smoke was observed from the vessel
- A 'Port Pitch Reduction Error Alarm' was enunciated on the DP control system
- The Port CPP Fault Indication Light illuminated in the ECR and on the bridge.
- A position excursion of 70m was experienced
- The Senior DPO selected manual control mode.
- The Operator of the vessel used the emergency stop to shut down the port main engine approximately 74s after the port pitch alarm was activated.

MTS DP COMMITTEE THANKS THE SUBMITTER OF THIS LFI ON BEHALF OF THE DP COMMUNITY. LFIs ARE PUBLISHED ON THE MTS DP COMMITTEE WEBSITE TO PROMULGATE LEARNINGS FROM INCIDENTS WITH A VIEW TO ENABLE PROACTIVE MANAGEMENT OF SUCH VULNERABILITIES AND MINIMIZE POTENTIAL FOR DP LOSS OF POSITION INCIDENTS.



Lessons learned

Current industry practice to analyse and prove the fail-safe condition of thrusters falls short of achieving the objectives in established industry guidance and classification society rules.

- Verification and Validation Processes for the Fail-Safe Condition of Thrusters needs to be more robust.
- The effectiveness of MOC processes must be validated.
- Activities to undertake self-assurance must be in place. (Undue reliance should not be placed on Charterer's 3rd party assurance)- (Example for assurance activities attached as appendix)
- Reliance on Operator Intervention and Human Performance is not a reliable method of limiting the severity of a drive off.
- Data capture following an incident is key. Procedures with sufficient level of detail must be developed and implemented. Training in execution should be provided to personnel key to the delivery of DP operations.

Recommendations

Vessel Owners should evaluate their vessels to establish whether they are vulnerable to this type of failure. In particular, they should review the design of their thruster control systems and any associated protective functions to determine whether they address all possible failure modes leading to failure effects that produce significant quantities of unwanted thrust in both magnitude and direction.

Short term remedial actions

- Verify DP operator familiarity with procedures and response capability to identify and address unwanted thrust through documented drills and exercises.
- Seek ways to relieve the cognitive burden on the DPO.
- Review and confirm emphasis on guidance in this case through ASOGs, vessel specific procedures and Master's standing orders etc.
- Developed verification and validation process for addressing configurable settings and performance of equipment. (Attached as appendix)

Medium term remedial actions

Engage with manufacturers, DP FMEA providers and classification societies to ascertain and establish that verification and validation processes are adequate to satisfy requirements to prove the fail-safe condition of thrusters.

Long term remedial actions

Engage with relevant stakeholders to seek ways to eliminate the hazard (downrated thruster) design.

NOTE:- There appears to be growing consensus that the fail-safe condition for thrusters while on DP should be to fail to Zero Thrust.

- Verify DP Operator familiarity with procedures and response
- Seek ways to relieve the cognitive burden
- Place additional emphasis on awareness through ASOG
- Develop verification and validation process for configurable settings
- Engage with manufacturers and classification societies to satisfy requirements
- Engage with relevant stakeholders to eliminate hazard by design

Introspection and Reflection

A LOOK BACK!

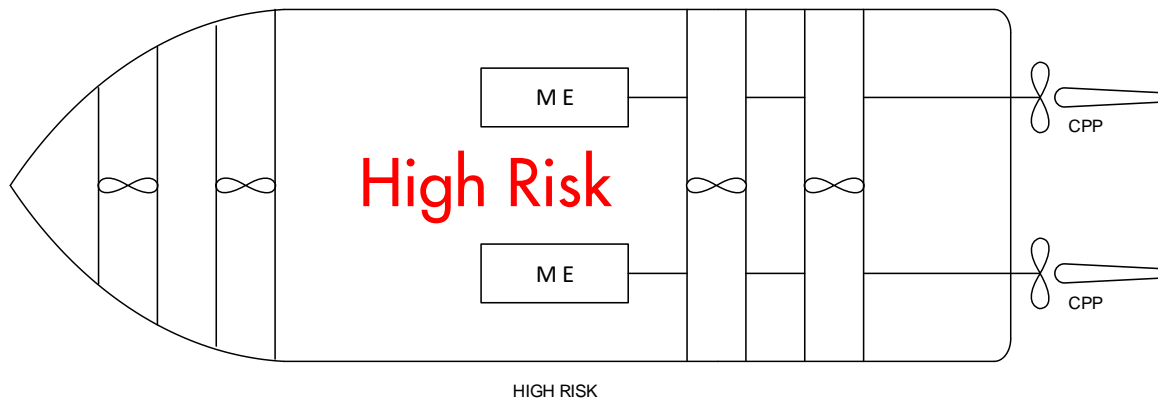
- Similar Incidents had been experienced, albeit on Logistic Vessels
 - No Consequences- Incidents had occurred outside the 500 m zone
 - Operator intervention was accepted as a credible mitigation
 - Incorporated in ASOG's

OPPORTUNITIES

- A Gift
 - Implement Learnings adopting a Systems Thinking Approach
 - Address through lens of Design Operations People and Process
 - Process Improvements
 - Stakeholder engagement
 - Classification of Incidents

Identification - (Classification of Vessels – **TYPE 1** or **TYPE 2**)

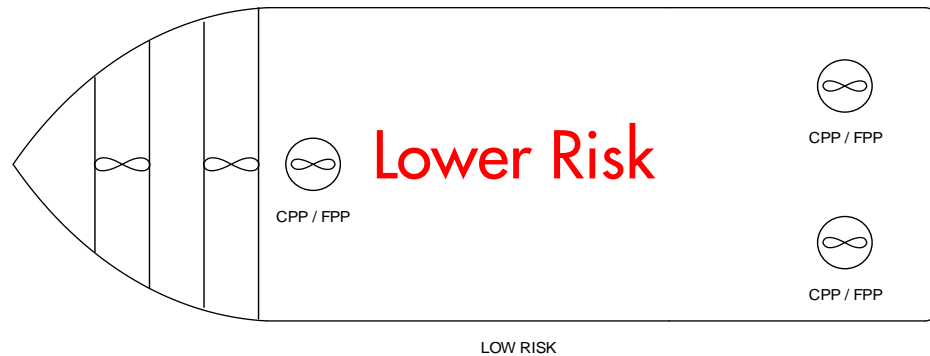
TYPE 1 VESSEL



TYPE 1 VESSEL

- **MECHANICALLY DRIVEN CPP'S (USUALLY SHAFT GENERATORS PART OF CONFIGURATION)**
- SWAY BY TUNNEL THRUSTERS
- **SURGE AXIS ONLY BY MAIN PROPS**
 - PROPS EFFICIENCY IN AHEAD DIRECTION
 - CPP'S FAILURE MODES
 - USUALLY HIGHER THRUST CAPABILITY
 - LIMITED COUNTERACTING CAPABILITY FOR UNWANTED THRUST IN SURGE AXIS
- **HIGH RELIANCE ON OPERATOR INTERVENTION TO ADDRESS UNWANTED THRUST**

Identification - (Classification of Vessels **TYPE 2**)

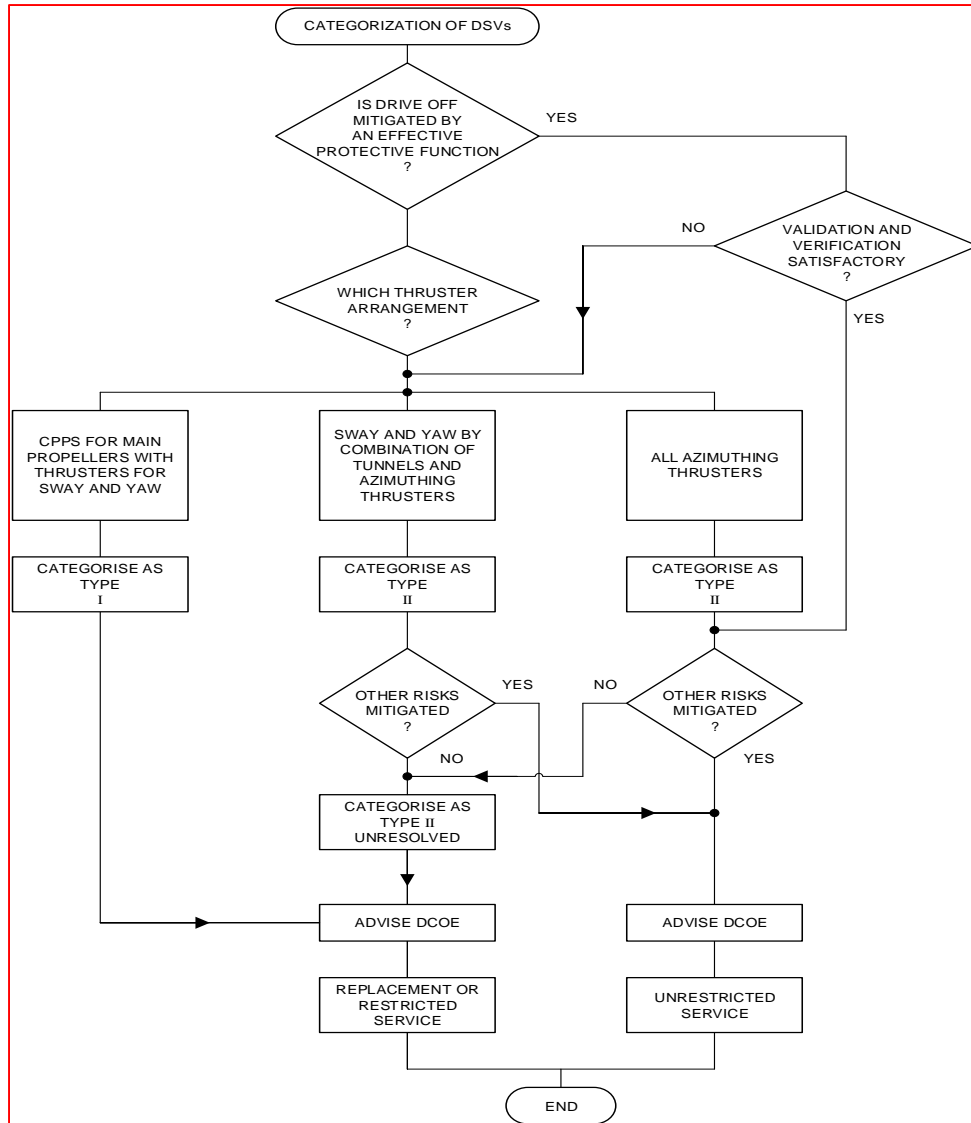


TYPE 2 VESSEL


- AZIMUTHING THRUSTER
 - Could be CPP's or FPP's
 - FPP's not immune to unwanted thrust-Directionality Failures of Azimuthing Mechanism.
- LOW RISK AND MEDIUM RISK VESSELS
 - Differentiator – Counteracting Ability
 - Number of Propulsors available for counter acting
- **UNRESOLVED IDENTIFIED VULNERABILITY LEADS TO RECLASSIFICATION OF TYPE 2 TO TYPE 1!**

Early Identification and Notification Enables Planning!

Categorisation



Notification



TECHNICAL NOTE

DATE:	07 FEB 2018	MRT REF:	MRT_DPDSV_DCOE NOTIFICATION-DATE
PROJECT:	GENERAL	BUSINESS:	GROUP
ATTN:	PTE DIVING/BUSINESS FOCAL POINT (INSERT NAMES)		
FROM:	Suman Muddusetti	CHECKED:	N/A
SUBJECT:	DP DSV (INSERT NAME) - IDENTIFICATION AS DP DSV TYPE 1 AND OR TYPE 2 VESSEL WITH POTENTIAL VULNERABILITIES THAT NEED RESOLUTION		

BACKGROUND

Learning from a significant High Potential near miss with a DP DSV has been incorporated into assurance process currently being undertaken by the Marine Risk team. One of the actions arising out of the follow through with the investigation was the commitment to notify DCOE and the Business Focal Point of identification of a vessel as a Type 1 DP DSV.

TYPE 1 DP DSVs are those that have a potential vulnerability for a rapid loss of position due to specific configurations of the propulsion system. TYPE 1 DSVs rely on operator intervention as a barrier to prevent the consequences of certain failure modes. Learning from incidents have concluded that such reliance on operator intervention alone is not a dependable barrier. Additional focus will be required on the management of station keeping risks as well as planning for the conduct of the diving operations.

While not common, in some cases DP DSVs identified as TYPE 2 may also need additional focus to resolve identified vulnerabilities.

Notification will be made to the DCOE and business focal point immediately if a vessel has been identified as a TYPE 1 vessel or a TYPE 2 vessel with vulnerabilities that need resolution.

It is understood that if a TYPE 1 vessel and or a TYPE 2 Vessel that has not been able to satisfactorily resolve identified vulnerabilities cannot be substituted with a suitable alternate vessel, will result in significant impacts to the business/project. Examples of some such impacts are:

- Additional tasks associated with the assurance activities
- Potential for precluding the conduct of certain diving activities (e.g. confined space diving) and/or development of additional mitigations/responses to a loss of position.
- Potential for cost increases (assurance tasks, non-productive time etc.)

STATEMENT

Please be advised that the DP DSV has been identified as a (TYPE1/TYPE 2 With need for Resolution)

Notification is being made as part of the agreed protocols.

TYPE 2 (WITH NEED FOR RESOLUTION)

The following are the vulnerabilities identified on this TYPE 2 Vessel.

S.No	Issue	Potential Impacts	Remarks

The undersigned or designate is available for further discussions as needed. Please keep us advised of the path forward that you would like us to pursue. Your prompt action on providing the steer to the Marine Risk Team is greatly appreciated.

Suman Muddusetti
 Marine Risk Team Lead
 Projects and Technology (PTP(D))
 Shell International Exploration and Production Inc.
 150 North Dairy Ashford, Houston, Texas 77079-1197, USA
 Tel: +1 832-337-6278 Fax: +1 713-423-0679 Cell Phone +1-281-224-5393
 Email: suman.muddusetti@shell.com
 Room No Wck Building D- 8th Floor "Dynamic Desk"

Implementing The LFI - Verification Activities of the Fail Safe Condition Of Thrusters

LFI Addendum

Addendum to LFI 2017-3

EXAMPLE VERIFICATION ACTIVITIES FOR FAIL SAFE CONDITION OF THRUSTERS

PURPOSE OF ADDENDUM: -

This document outlines an example verification process to address self-assurance activities for fail safe condition of thrusters. This may be used to document and make available the outcome of verification activities.

BACKGROUND: -

THRUSTER FAIL-SAFE REQUIREMENTS:

IMO, classification societies and industry bodies all have clear requirements that thrusters should fail safe as follows:

- **IMO 1580 Section 3.3.5** 'Failure of a thruster system including pitch, azimuth and/or speed control, should not cause an increase in thrust magnitude or change in thrust direction.'
- **ABS Guide for Dynamic Positioning Systems**. Feb 2016, Section 4, Thruster System, Part 3 Thruster Capacity, 'A single fault in the thruster system, including pitch, azimuth or speed control, is not to result in unintended operation of pitch, speed and direction.'
- **DNVGL-RU-SHIP** July 2017, Part 6, Chapter 3, Section 1, 7.3.3, 'A single failure in the thruster control system should neither cause significant increase in thrust output nor make the thruster rotate.'

NOTE:

- The most recent rule references have been provided above but the same requirements date back to at least 1994 in IMO MSC 645.
- The requirements to prevent unwanted thrust direction also apply to rudders.

VERIFICATION

The following Information pertinent to the fail-safe condition of thrusters is documented.

- Documented evidence of verification activities in a suggested format.
- Statement of Verification.

DOCUMENTED EVIDENCE OF VERIFICATION ACTIVITIES

Complete tables below:

For Each Azimuthing Thruster				
	Ahead	Port	Starboard	Astern
Confirm mechanical zero and electrical zero align – Then confirm azimuth angle at DP and all other indicators.				
Confirm angle by observation of thruster wash				
	Pump 1	Pump 2	Pump 1 & 2	
Record turning speed CW for Time for 360°				
Record turning speed CCW Time for 360°				
For Each Fixed Pitch Propeller				
	Motor current (A)	Motor current (%)	Motor Speed (RPM)	Motor Speed (%)
Set manual Levers to 100% Forward – Record Motor current and RPM				
Set manual Levers to 100% Reverse (where available) – Record Motor Current and RPM				
Using manual levers record ramp time from 0 to 100%				
Note ramp time for ramp 100% to 0				
Confirm thrust direction by observation of thruster wash				
Thrust Allocation - Excursion on Change of Allocation Mode				
For vessels with the potential to use different thrust allocation modes such as Bias and Free, orient the vessel beam on to the prevailing conditions and provoke a change of thrust allocation mode. Record the maximum position and heading excursion.				
For Vessels with Variable Speed / CPPs ('Combinator Mode'), clear statement to be provided whether DP operations are to be carried out with fixed speed or variable speed. DP documentation to be provided substantiating stable DP capability (footprint plots, statement from OEM that vessel is tuned and stable station keeping ability has been validated etc.) if variable speed is permitted for DP station keeping.				

Azimuth Thruster & Fixed Pitch Propellers

- Confirmation of Mech and Elec Zero
- Confirm azimuth feedback at 0° 90° 180° and 270°
- Confirmation of angle by thruster wash
- Turning rate CW and CCW
- RPM at 100% Forward and Reverse
- Ramp time 0 - 100% RPM
- Confirmation of direction by thruster wash

Thrust allocation

- Excursion between mode changes
- Confirmation of use of combinator mode

Implementing The LFI - Verification Activities of The Fail Safe Condition of Thrusters

Main Engine Driven Props - CPPs

Motor Driven Props - CPPs

For Main Engine Driven CPPs – Including Combinators						
Item	Description	Port ME Ahead	Stbd ME Ahead	Port ME Astern	Stbd ME Astern	Remarks
Load and speed settings (ahead and astern)	Load settings on the engine will be tested, verified and documented.	(kW, RPM)	(kW, RPM)	(kW, RPM)	(kW, RPM)	
Pitch stroke setting	Pitch stroke setting to be measured and documented	(%)	(%)	(%)	(%)	
Full Ahead / Full Astern (Pitch Stroke vs ME Load)	ME loads at Full Ahead and Full Astern to be documented	(%, kW, RPM)	(%, kW, RPM)	(%, kW, RPM)	(%, kW, RPM)	
Mid-range ahead and astern (pitch stroke vs ME loads)	ME loads at mid-pitch stroke to be documented	(%, kW, RPM)	(%, kW, RPM)	(%, kW, RPM)	(%, kW, RPM)	
Zero pitch stroke vs ME loads	ME load at Zero pitch stroke to be documented	(%, kW, RPM)		(%, kW, RPM)		
Vibration	Subjective test to document vibrations when main props are full ahead and full astern	(Vibration)	(Vibration)	(Vibration)	(Vibration)	
Verify configurable settings in ECR on main prop for alignment with ASOG	Verify settings are as demonstrated and documented at tests.	(%, kW, RPM)	(%, kW, RPM)	(%, kW, RPM)	(%, kW, RPM)	

For Electrically Driven CPPs – Including Combinators						
Item	Description	Port CPP Ahead	Stbd CPP Ahead	Port CPP Astern	Port CPP Astern	Remarks
Load settings	Settings to be verified and documented	(kW, A, RPM)	(kW, A, RPM)	(kW, A, RPM)	(kW, A, RPM)	
Pitch stroke setting	Settings to be verified and documented	(%)	(%)	(%)	(%)	
Full Ahead / Full Astern (Pitch Stroke vs motor Load & Speed)	Motor load, current, speed and pitch stroke at full ahead and full astern	(%, kW, A, RPM)	(%, kW, A, RPM)	(%, kW, A, RPM)	(%, kW, A, RPM)	
Mid-range ahead and astern (pitch stroke vs motor load and Speed)	Motor load, current, speed and pitch stroke at Mid Stroke	(%, kW, A, RPM)	(%, kW, A, RPM)	(%, kW, A, RPM)	(%, kW, A, RPM)	
Zero pitch stroke vs motor load & Speed	Motor load, current, speed and pitch stroke at Zero Pitch	(%, kW, A, RPM)		(%, kW, A, RPM)		
Vibration	Document vibrations when props are full ahead and full astern	(Vibration)	(Vibration)	(Vibration)	(Vibration)	
Verify configurable settings on props for alignment with ASOG	Verify settings are as demonstrated at tests.	(%, kW, A, RPM)	(%, kW, A, RPM)	(%, kW, A, RPM)	(%, kW, A, RPM)	

Main Engine and Electrically Driven CPP's

- Load and speed settings ahead and astern
 - Pitch stroke settings
 - Pitch stroke V ME load (Full - ahead and astern)
 - Pitch stroke V ME load (Mid - ahead and astern)
 - Zero pitch stroke V ME Load
 - Vibration
 - Verify configurable settings for main props for alignment with ASOG
- Load setting
 - Pitch stroke settings
 - Pitch stroke V motor load and speed (Full - ahead and astern)
 - Pitch stroke V motor load and speed (Mid - ahead and astern)
 - Zero pitch stroke V motor load and speed
 - Vibration
 - Verify configurable settings for main props for alignment with ASOG

EFFECTIVE STAKEHOLDER ENGAGEMENT

INTERNAL

- OPERATING COMPANIES/DIVING CENTER OF EXCELLENCE (DCOE)/PROJECTS
 - ACTIVITIES/PROJECTS IN EXECUTION
 - DISSEMINATION OF LFI
 - CENTRALIZED ACCOUNTABILITY AND ENABLER!
- BUSINESS IMPACTS
 - MANAGED EFFECTIVELY
 - WORK SCOPE ADJUSTMENTS
 - FOCUSED VALIDATION/VERIFICATION BASED ON RISK IDENTIFICATION

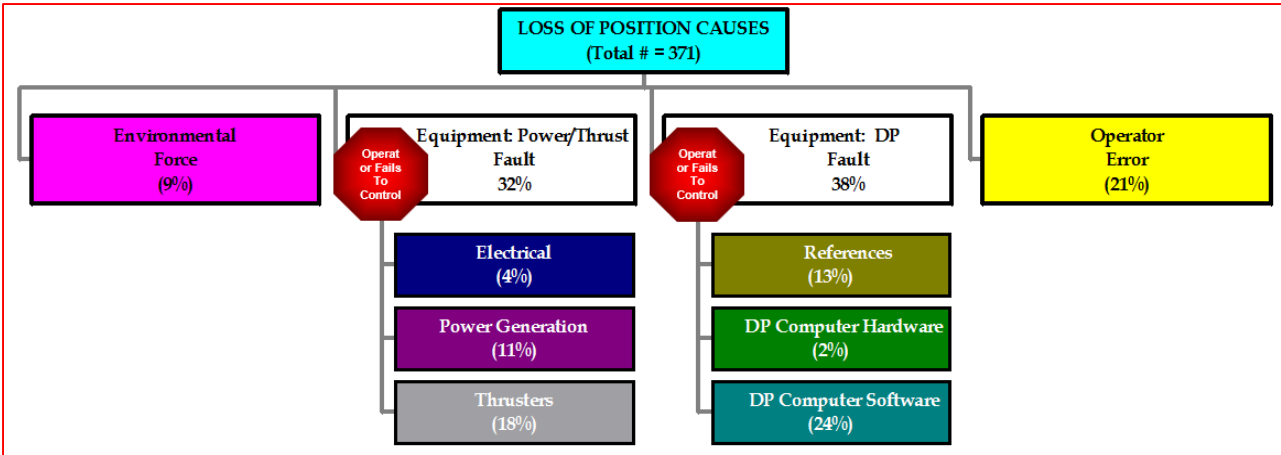
EXTERNAL ENGAGEMENT

- PARTNERS IN SAFETY (CONTRACTOR/VESSEL TECHNICAL OPERATORS AND 3P CONSULTANTS)
- DP COMMUNITY (OEM VENDORS/CLASSIFICATION SOCIETY)
- VERIFICATION AND VALIDATION EFFORTS
- ADDRESSING LONGER TERM MEASURES_ “DESIGN IT OUT”
- MTS DP COMMITTEE WORKSHOPS

Overview of Causal and Contributory Factors of Loss of Position Then and Now!

DISTRIBUTION 9 : 32 : 38 : 21

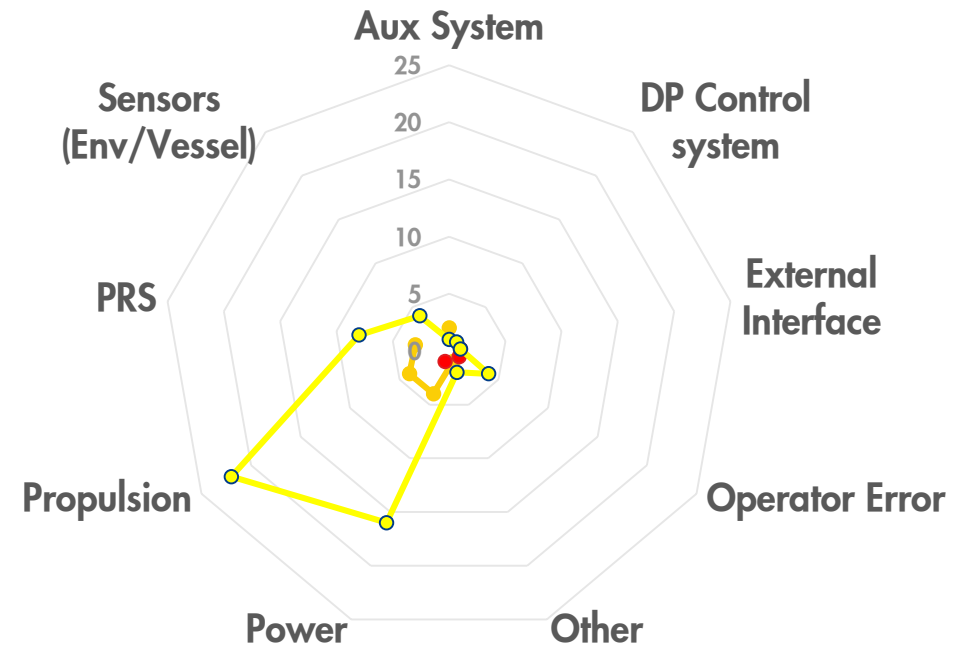
Information From Yellow And Red Tracker



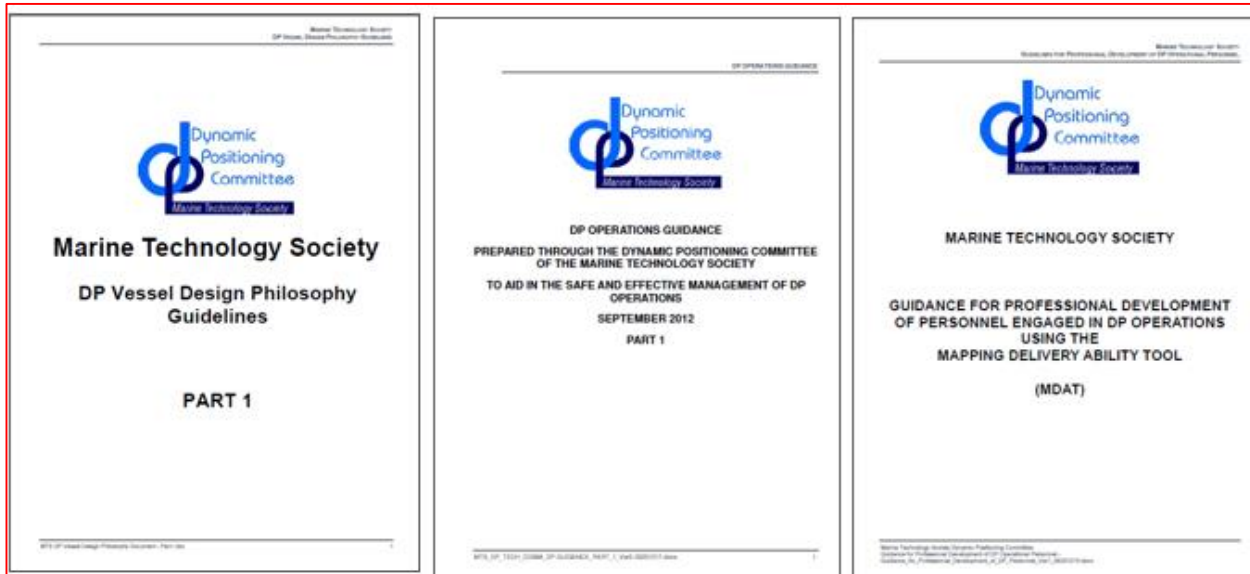
Environment **9%**
 Power Thrust **32%**
 DP Control **38%**
 Operator **21%**

Issues Reported by Category

—●— Advisory —●— Red —●— Yellow



Leveraging MTS Products!



- Design philosophy guidelines
- Operations guidance
- PDDP2 (formerly MDAT)
- IPV



Dynamic Positioning Committee
Marine Technology Society

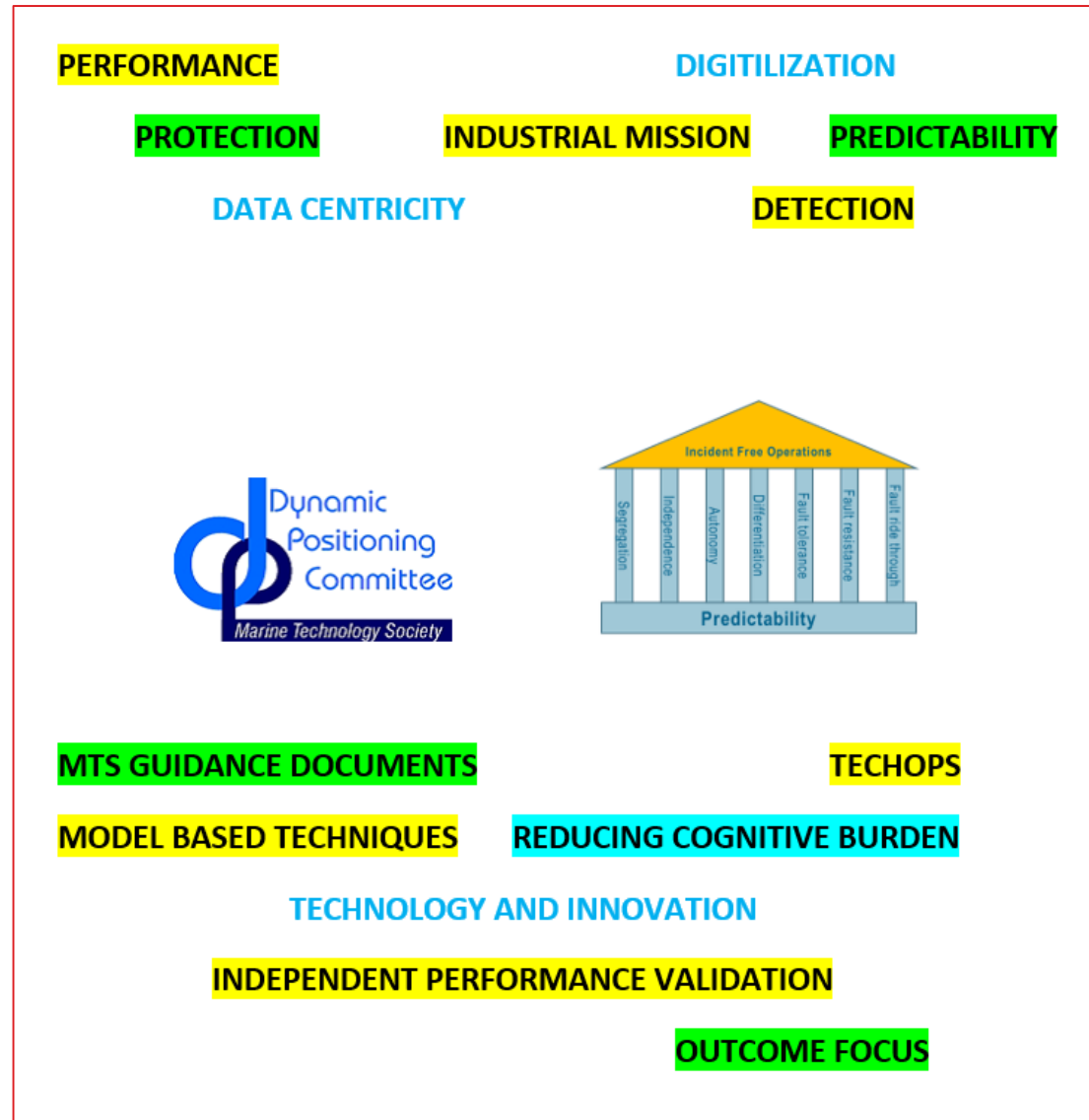
Independent Performance Validation for Robust and Resilient DP Systems

Steven Cargill* Chunying Li**
***DNV GL Noble Denton marine services**
**** Aspin Kemp & Associates**



marine technology
SOCIETY
Opportunity runs deep™

Leveraging MTS DP Committee Products!



Addressing Unwanted Thrust - (IPV) - Functional Specification

Specification for Independent Protective function



TECHNICAL NOTE

DATE	2 nd July 2016	REF/REF:
PROJECT:		SUBJECT:
ATTN:	ALL STAKEHOLDERS	
FROM:	Simon Hubbard	ISSUED:
SUMMARY:	Prevention of Unwanted Thrust - Functional Specification for Domestic Pumps	

INTRODUCTION

This technical note provides the functional requirements for a protective function intended to prevent faulty thrusters developing unwanted thrust in magnitude or direction. It is proposed that this is a function specification. Axioms provide the outline the team are permitted provided effective means of verification and validation, including substantiating discussion, are submitted.

BACKGROUND

- IMO classification societies and industry bodies all have clear requirements that individual thrusters should fail safe as follows:
- IMO MSC 98 Section 3.3.4 Failure of thruster systems including pitch, advance or speed control, should not make the thruster cease to go in uncontrolled full pitch and speed.
- IMO MSC 180 Section 3.3.5 Failure of thruster systems in steady state, which may require adjustment, should not cause an increase in thrust magnitude or change in thrust direction.

- ASB Guide for Dynamic Positioning Systems, Feb 2016, Section 4, Thruster System, Para 3 Thruster Capacity, a single fault in the thruster system, including pitch, advance or speed control, is not to result in uncontrolled operation of pitch, speed and direction.
- DNVGL-RU-SHIP July 2017, Part 6, Chapter 3, Section 1.7.3.3, A single failure in the thruster control system should neither cause significant increase in thrust output nor make the thruster cease.

NOTE:

- The most recent sea referenced have been copied above for the same requirements state that the most recent IMO MSC 180 Section 3.3.5 requirements are not being satisfied by current industry practice.
- IMO MSC 180 language is an improvement over ILO MSC 98.
- Most operators operating in CP are considered to be robust.

Despite the above requirements, incidents experienced in the industry reveal a failure to enforce the requirements that being to occur. There is lack of a common understanding of the issues, incidents being experienced in industry continue to demonstrate the inability of current industry practice. Reference is made to the LFI attached in Appendix A as an example.

Such incidents have resulted in consequences which have caused them to be assessed as high potential.

NOTE:

- Operator Intervention and Emergency Stops have been often offered as mitigations. Incidents have proven that operator intervention is not an effective or dependable barrier. This is not intended to negate the need for emergency stops or crew protective operator intervention.
- Conventional methods of mitigation, verification and validation (example: write-down tests, load monitoring and feedback loops) which reduce some loss of position incidents, have not succeeded in eliminating them. This has been attributed to limiting the need to write down and load monitoring of feedback loops and not addressing the need in the entire control system.
- Note: Write down tests are often considered without the full appreciation of the objective. It is meant to test a protective function or detect a hidden failure. Write down tests are not effective in uncovering all failure modes.
- The test may reveal hidden failures (example: internal leaks in hydraulic systems).
- Lack of an unambiguous or unprejudiced outcome provides a false sense of security about the failure condition of the thruster.
- The test does not reveal the lack of a protective function.
- It is acknowledged that there are tests that could be done to demonstrate the lack of a protective function but these are either restricted in practice (example: manually operating the pitch or advance controls) or to force uncontrolled changes in thrust magnitude or direction.

- It is acknowledged that vessels have implemented some mitigations. However, such mitigations, while seeking to assist current verification and validation practices do not achieve the objective of demonstrating that the thruster is fail safe from a CP perspective.
- It is acknowledged that the consequences of such failures are more serious on vessels with propulsion configurations where thrust in the Surge Axis (for DP and Turret) is provided by Conventional P&S Propellers. There have been numerous such incidents reported in industry but vessels will shut down in any proportion.

NOTE:

- The CP status and/or segment of the industry has provided mitigations in the form of Zero Pitch System. Due consideration is required to evaluate adaptability to address the issue of unwanted thrust.
- There are no technical reasons why similar mitigations cannot be designed and applied to vessels in the offshore and other industry segments.

INTENT

- This functional spec has been developed to require independent protective functions in thrusters to achieve the intent of IMO MSC 180 ILO 98.
- It is acknowledged that the failure modes of such functionality could result in the loss of a single thruster. Such an outcome is acceptable as long as it does not exceed the Worst-Case Failure.

DESIGN

Thrusters will be fitted with individual, independent, automatic, autonomous and robust protective functions which will generate warning alarms and, if necessary, shut down a thruster if the thruster develops significant amounts of unwanted thrust in magnitude or direction when operating in CP.

NOTE:

- Alarms shall be provided to obtain the protective function in conformity with requirements when the vessel is not operating in CP. The fact that it has been inhibited will be clearly visible to the DP or the main DP station and included in the vessel's alarm and monitoring system. The fact that it is inhibited from operating should NOT make the alarm that indicates the thruster is not following commands.
- This functional specification is limited to addressing unwanted thrust. It is not intended to be applied to automatic thruster recovery systems or thrusters with fault ride through strategies to address power plant disturbances. Protective concepts designed as mitigations to address unwanted thrust should not compromise or delay major automatic thruster recovery systems or fault ride through strategies in any way. Similarly, automatic thruster recovery systems or fault ride through strategies should not compromise protective function for unwanted thrust. This should be verified through appropriate testing.

The protective functions shall achieve the following:

- Shall not be dependent upon operator interventions.
- Design of the protective function shall incorporate the build-to-run philosophy and built-in test requirements functionality.
- Have applicable classification society / statutory requirements.

NOTE:

- The built to run philosophy is intended to ensure that essential structures and protective functions can be covered by 'black box' testing. Equipment should be designed to accommodate, without detrimental effects, unforeseen stress is required to prove the efficacy of functionality by testing.

- The above should facilitate carrying out essential tests without the fear of equipment damage.
- Each thruster shall have its own individual protective function which is independent of those for other thrusters.
- The protective function will be autonomous in so far as it will have all the necessary sensor and computing capability in order for its function not rely on external command control.

NOTE:

- This does not preclude the protective function utilizing control signals from other systems provided that can be documented and demonstrated that such utilization does not result in unacceptable failure effects, including common cause / mode failure. Changes in frequency of data communications can only be a passive warning and not able to broadcast or override thruster control under normal operation and failure modes. Hardwired monitoring of control signals will not increase noise or influence the original signal etc.

- Some designs have backup control functions activated upon failure of the main control function. Where thrusters have a backup control function intended to take over from the main function or failure of the main function it is acceptable to allow one for the backup-control function to take control providing that, in no case, does not

violate any other part of the specification. It is permissible for the protective function to be part of the backup control system provided:

- The backup control system is completely independent of the main control system.
- The protective function is not inhibited by the backup control system means or effectively isolates the above mentioned requirement is part of the design.

- The design of the protection system hardware circuits should be such that operation or failure of these circuits will not affect the thruster (example: prevent isolation high impedance sensors, etc).

- The activation of a protection function resulting in a shutdown shall be clearly and unambiguously indicated at all control stations (example: DP, P&S, VMS and manual thruster controls).

- It is suggested that the functionality of the protective function shall be based on a mathematical model of the thruster. This requires the modelling techniques to be designed to assist with location and validation. Alternative methods, if proposed, shall have some equivalent robustness of model based techniques.

- It is anticipated that extended mathematical models of the thruster will be used to confirm whether it is healthy or not and that the model will be able to produce accurate real-time representations of expected thruster performance for all static and dynamic conditions.

- The model may include such features as are required to meet the intent of this specification and may include, but are not limited to:
- Hydraulic effects
- Hydraulic system
- Mechanical system
- Electrical systems
- Control systems

- The protective function will stop the thruster before the deviation from the wanted thrust magnitude and/or direction reaches levels that could cause a loss of position and / or heading.

NOTE:

- This is not to be interpreted as implying that it is acceptable for position to be maintained by means that are not designed to do so by the factory etc. The use of heuristics to confirm that the thruster will be maintained in the event of a position is defined performance condition will be considered. Where tests are defined, they should be easily verifiable such as percentage pitch or thrust for example.

- The magnitude of unwanted thrust or deviation from desired thrust direction to trigger alarms and shutdown shall be determined by suitable calculations, reviewed data for healthy system and validated by a comprehensive test program. Stability of the protective function in dynamic conditions must be ensured (ie: uncontrolled shutdown).

- The design of the protective function must not introduce potential common mode or control plane failures with other thrusters including the effects of excessive acceleration / vibration / trip outputs etc.

- Example - The protective function should be robust and not susceptible to equivalent operation in extreme environmental conditions where when it is known that the vessel and DP thrusters provide full loss to recover.

- Example - Deviation of one more thrusters due to 'ventilation' (thruster coming out of the water due to vessel motion).
- Example - Excessive thrust allocation by the DP system must not be interpreted as a fault or multiple thrusters:

- It is expected that protection strategies depending solely on sea-ice change responses will be challenged to meet the above functionality.
- Example - Vessels have been forced in position due to uncontrolled counter-rotary responses by multiple quadrants (example: thruster order, DP/CP, vector, drive manufacturers and vessel management teams) all implying that safety margins.

- Suitable strategies will be used to ensure the decision-making (example: cause and effect) process that issues orders and shut-down the thruster is robust and not prone to causing spurious alarms or shutdowns.

- The protective function should alert, but not stop, a thruster that is providing less thrust than demanded. The protective function should only stop a thruster if it is producing significant amounts of excess thrust or thrust in a significantly wrong direction.

- The design of the protection function should consider, and be resilient to, the effects of the calibration, maintenance or fitting of sensors.
- The design of the protection against unwanted thrust in the wrong direction will consider and be resilient to the effects of changes in loading speed or pitch control associated with a reduced number of sensors or pitch purges caused by loss of a part of the power distribution system or other causes.

- The protective function will have sufficient internal diagnostics and test features to allow it to reliably indicate when the protective function itself is faulty.
- The independent protection function shall have comprehensive internal data logging functions for the following post event analysis:

- The protective function will have its own instructions and not share those with the DP or thruster control systems (and engineering practice is not to combine control, protection and monitoring functions).

NOTES:

- Thrustorder will be separated to the maximum practical extent including the use of independent protective stops.
- The goal for the protective function utilizing control signals from other systems provided that can be documented and demonstrated that such utilization does not result in unacceptable failure effects, including common cause / mode failure.
- Confirmation should be sought if there is any doubt about how to achieve this as an engineering principle including redundancy or, necessarily, requirements for simplicity.

- If such separation cannot be achieved the design should be subject to a comprehensive system engineering analysis to identify the consequences and how effective mitigations which are robustly implemented operator intervention.

- The protection of command and feedback loops in sea-ice during the thruster behaviour. Comparison of command and feedback above or in line is sufficient to meet the intent of the specification.
- The protective function will not cause alarms or shut-down the thruster in response to valid thruster orders by external systems to reduce thrust such as P&S pitch-back or motor overload protection. Any such system will reduce the DP control system that they are acting in changing the thruster set point.

- Protective functions with strategies to shut-down prime movers shall assess impact using a Systems Engineering approach and maintain loss of functionality / capability of other equipment.
- For example, when the prime mover for the thruster also drives a shaft generator used to power other thrusters or essential systems. For such systems, the reduction gear should be arranged so that it is possible to shut-down the main propeller without stopping the engine and thruster.

- Such functions must be assessed for understandability and potentially be implemented in a separate system: in general, such issues should be designed out of the system on a system level.

- Thrusters which have been stopped by the protective function should not be locked out from start and should be available to be restarted by all provisioning methods. The design of the protective functions should consider the effects of, and be resilient to, the cause spurious shutdowns (power plant disturbances such as voltage and frequency excursions and fluctuations).

- Change of control mode from DP to manual and / or LIS (for example) will not cause spurious tripping of the protective function.

- The above requirements are equally applicable to rudders when used in conjunction with propulsion to provide thrust. This requirement and specifications assume that the vessel is designed in such a way that it can manoeuvre position and heading with one propeller. A rudder gets protruding so that, i.e. it is not possible to stop the unwanted propeller and maintain position and heading. Where rudders are not in use there should be monitoring that the rudders remain in the mid-range position.

VERIFICATION AND VALIDATION

- A Systems Engineering approach shall be applied and documented (example: FMEA and Flowing Trials) in the development of the protective function.
- Any dependencies with other parts of the DP system that are introduced to provide advantages must be clearly identified and fail in both conditions.

- Analysis should be comprehensive and accompanied by robust verification and validation program.
- None:

- Analysis is deemed to be comprehensive when it covers all aspects of design and intended functionality.
- The conclusions arrived at from the analysis shall be transparent.
- The basis of the conclusion and mitigations are clearly articulated and independently verifiable.
- Analysis and conclusions shall support the objectives of the testing required to satisfy verification and validation activities.

- Testing and analysis should consider a comprehensive range of all relevant failure modes including design, regression and hidden failure modes. The failure mode identification should incorporate built-in and built-in test capability requirements.
- Design failure modes are often characterized by failure in some inactive state. For example, cessation of a function, failure to start against or power, failure to log, loss of power or to log, light.

- An aggressive failure mode is one where the item fails in an active way, i.e. full speed or power or to log, light.
- A hidden failure mode is one which may cause an unacceptable failure effect if it occurred both during when the hidden failure is present. Measures to reveal such hidden failures should be part of the design and may include alarms, diagnostics and test procedures.

- Introduction
- Background
- Intent
- Design
- Verification and validation

Key Salient Features Of IPV - Unwanted Thrust

GENERAL

- IPV is a principle not a product
- It can be applied to any system but is a good fit to DP system designs built to the seven pillars
- It is intended to provide superior DP system integrity
- It is intended to be more time efficient than traditional verification methods.
- Data logging
- Confidence indicators
- Robust model based protection
- Shut down prime mover if thruster produces **excess thrust** or thrust in the wrong direction
- Adherence to the seven pillars (in particular)
 - Autonomy
 - Independence (One per thruster - No commonality)
 - Segregation
 - Differentiation
- Attention to internal and external common cause failures
- Basis of confidence
 - Built to test
 - Test on demand
 - Healthy to operate

CONCLUSION

- UNDUE RELIANCE ON DPO INTERVENTION NOT PRUDENT.
- HIERARCHY OF CONTROLS
 - **Eliminate (Remove the Hazard)**
 - Substitution (Replace the Hazard)
 - Engineering Controls (Isolate People from the Hazard)
 - Administrative Controls (Train People and explain procedures)
 - PPE (Protect the worker)
- WE ARE ACCOUNTABLE!

