OIL & GAS

Thruster Fail-Safe

Effective Validation and Verification

Dr S. Cargill

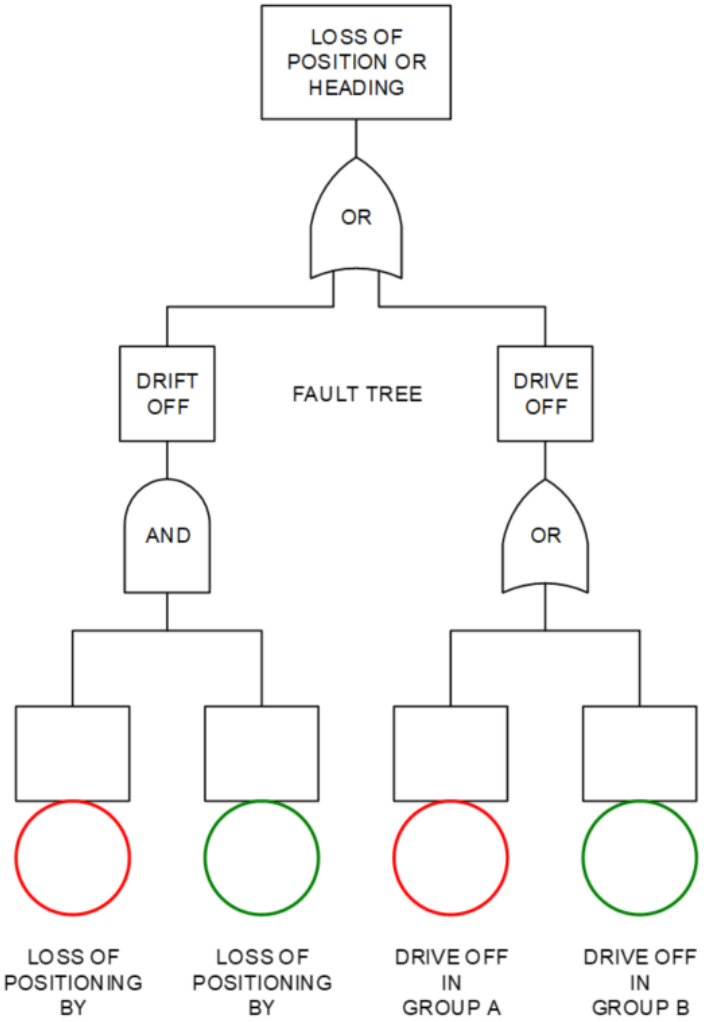
9th October 2018 - Houston

Ungraded

This presentation

- Introduction to the guidelines for thruster fail-safe.
- 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.

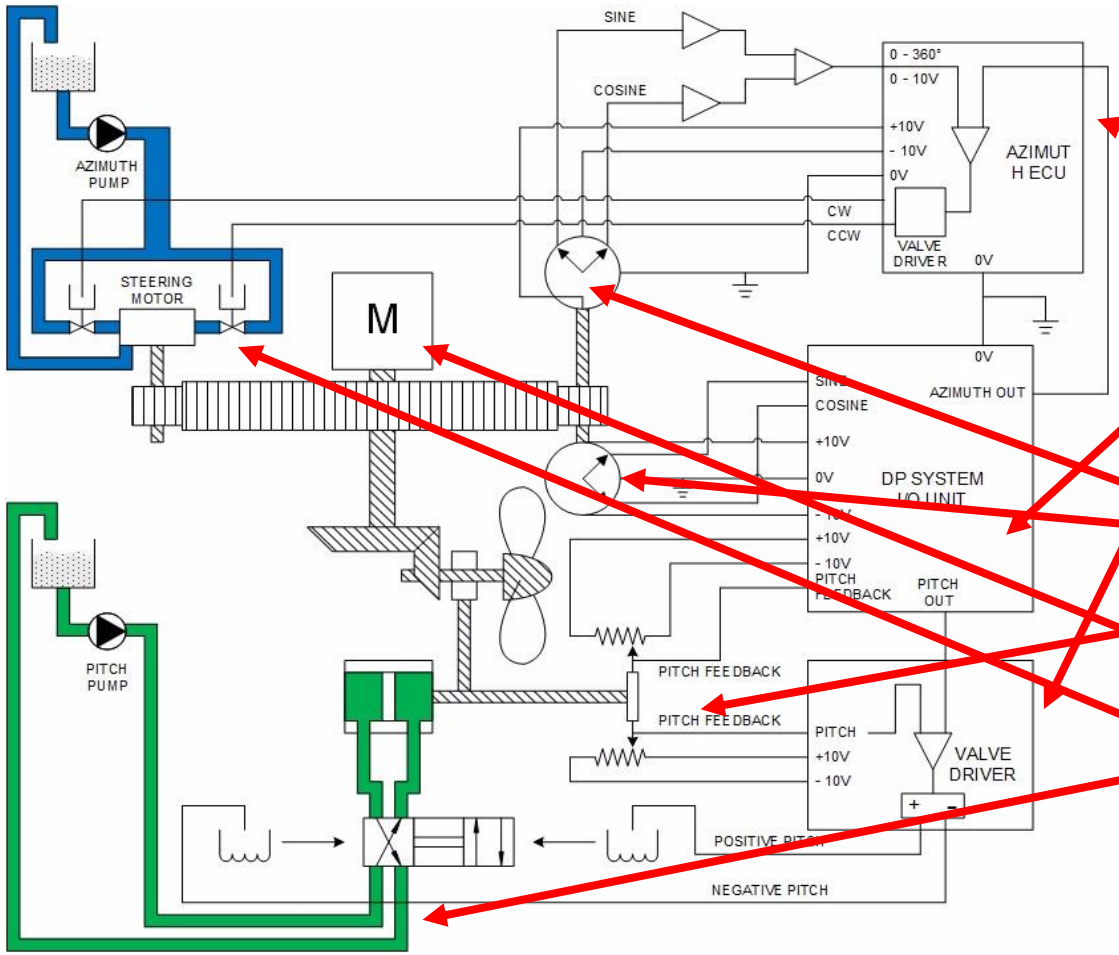
Two ways to lose position as the result of a failure



- Both redundant DP equipment groups have to fail to get a drift off
- Only one redundant DP equipment group has to fail to get a drive off

Ungraded

Azimuthing thruster with Controllable Pitch Propeller(CPP)



- Two closed loop electro-hydraulic control systems
  - Azimuth
  - Pitch
- Open Loop control from DP control system – monitoring and alarm
- Feedback
  - Azimuth 'Sine–Cosine' potentiometers
  - Pitch 'Linear' potentiometers
- Fixed speed motor
- Hydraulic systems

Guidelines for thruster fail-safe

IMO Guidelines for the fail-safe condition of thrusters

IMO MSC 645

3.3.4 Failure of thruster system including pitch, azimuth or speed control, should not make the thruster rotate or go to uncontrolled full pitch and speed.

IMO MSC 1580

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.

IMO MSC 1580 - Definition of thruster system

1.2.23 *Thruster system* means all components and systems necessary to supply the DP system with thrust force and direction. The thruster system includes:

.1 thrusters with drive units and necessary auxiliary systems including piping, cooling, hydraulic, and lubrication systems, etc.;

.2 main propellers and rudders if these are under the control of the DP system;

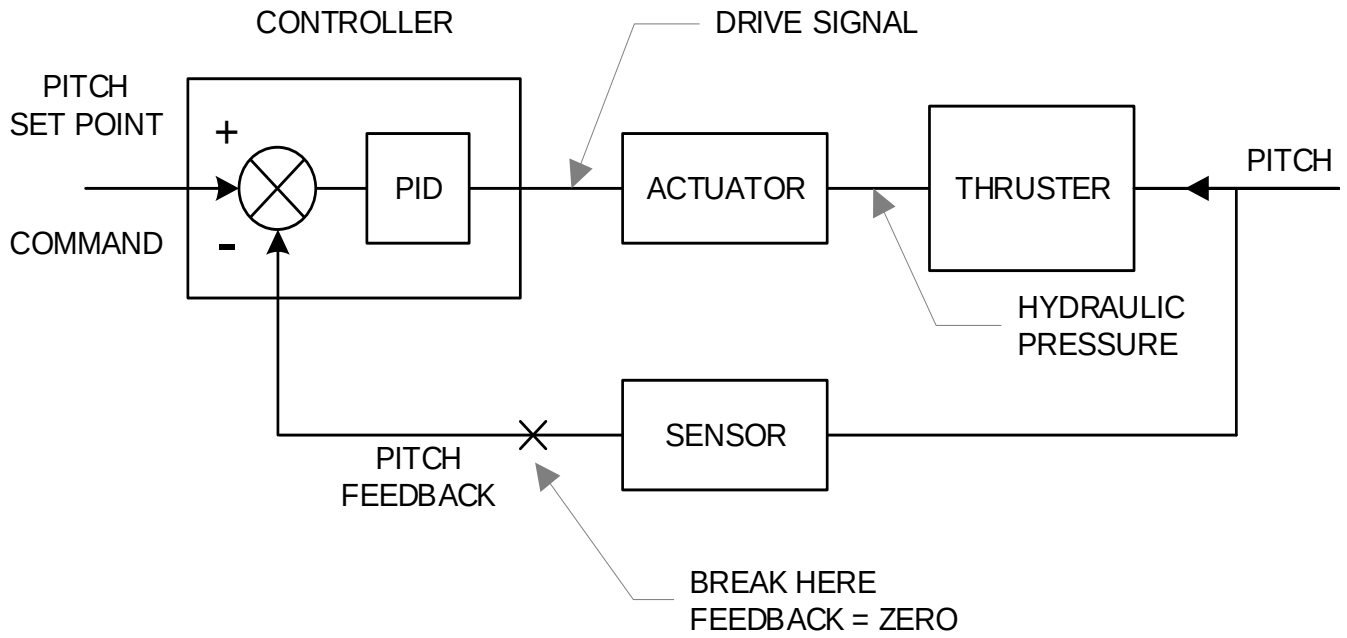
.3 thruster control system(s);

.4 manual thruster controls; and

.5 associated cabling and cable routeing.

- Applies to DP Class 1, 2 & 3
- Similar in MSC 645

Closed loop controllers



- Not inherently fail-safe in DP applications.
- Require protective functions.
- E.g. electronic engine governor has wire-break detection on magnet speed pickup
  - Without that function the governor fails to full fuel on loss of speed feedback.

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

At least two possibilities

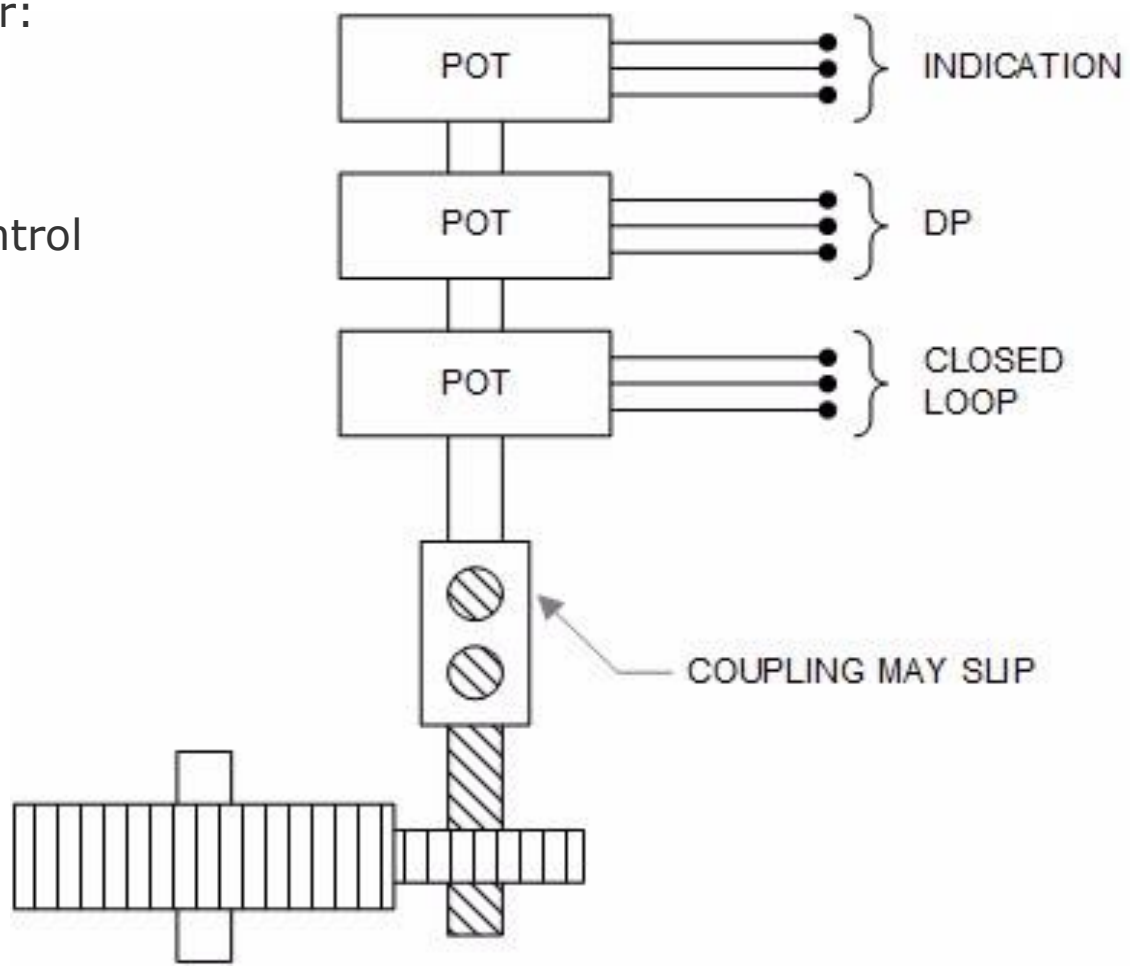
- Design Flaw - The thruster has not been designed to be fail-safe for all modes of failure and the verification and validation process has not detected these deficiencies.
  - Some aspects of the design might be considered exempt for certain acceptance criteria.
  - May be insufficient protective functions
- Hidden Failures - 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.

Importance of independence

- Long established engineering principle
- Independence between functions for:
  - Control
  - Protection
  - Monitoring
- If Control fails the protection will still work and the system can be monitored.
- If Protection fails the system is still under control can be monitored.
- If Monitoring fails the system is still under control and is still protected even if it can’t be monitored.
- When these functions are integrated, it becomes increasingly challenging to prove that the protection will still work if the system goes out of control because of a failure.

Common cause failures in azimuth feedback arrangements

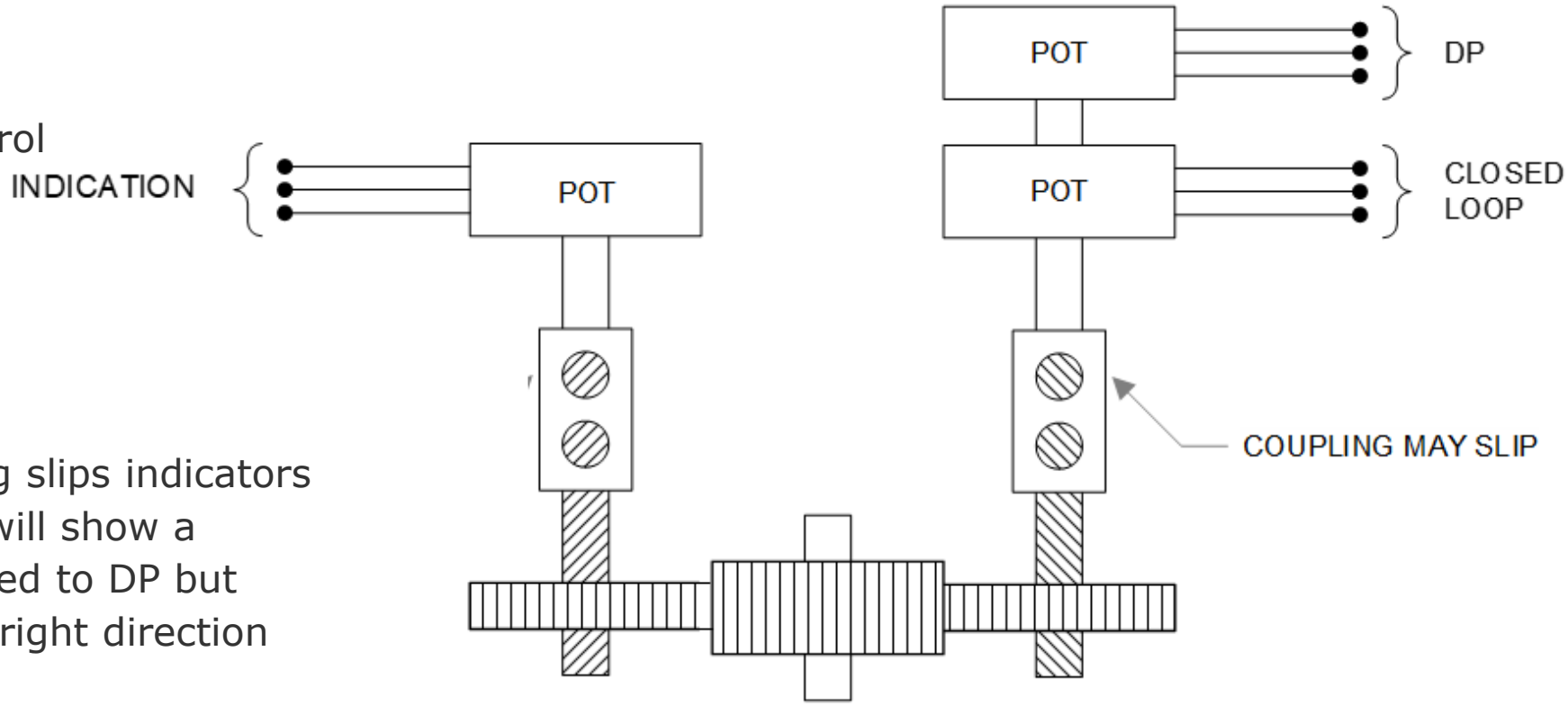
- Common drive for:
  - Indication
  - DP feedback
  - Closed loop control



- If coupling fails completely then DP will never get what it commands and will alarm
- If coupling only slips a little at a time control system can turn thruster to satisfy DP command but will be pointing in wrong direction. Offset accumulates
- There will be no alarm from DP and Manual Thruster Control indicators will agree with DP

Independent azimuth indication

- Common drive for:
  - DP feedback
  - Closed loop control

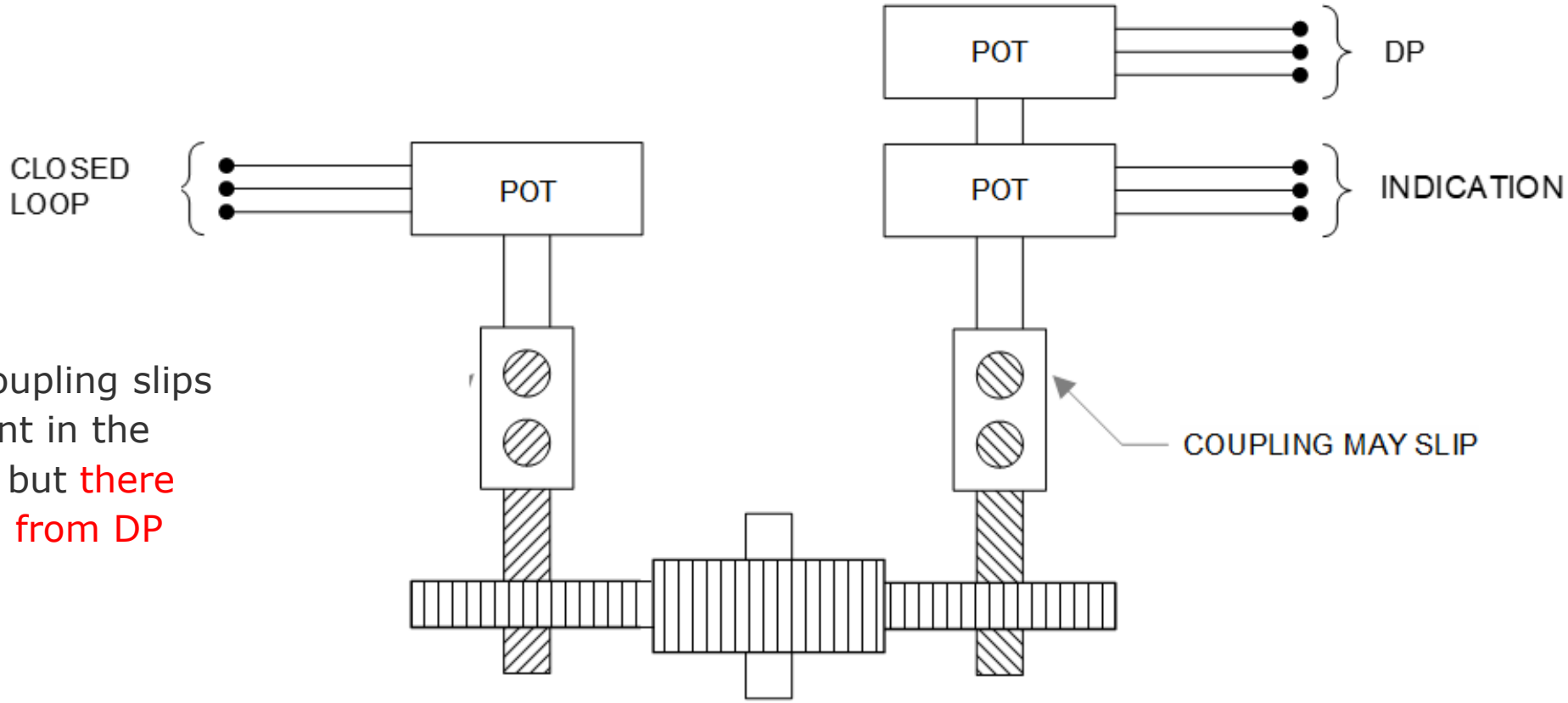


- If indication coupling slips indicators at manual controls will show a discrepancy compared to DP but thrust will be in the right direction
- If common coupling for DP and closed loop control slips then the thruster will point in wrong direction
- Azimuth indictors will show a discrepancy but there will be no alarm

Independent closed loop control feedback

- Common drive for:
  - DP feedback
  - Indication

Splined drive an option?

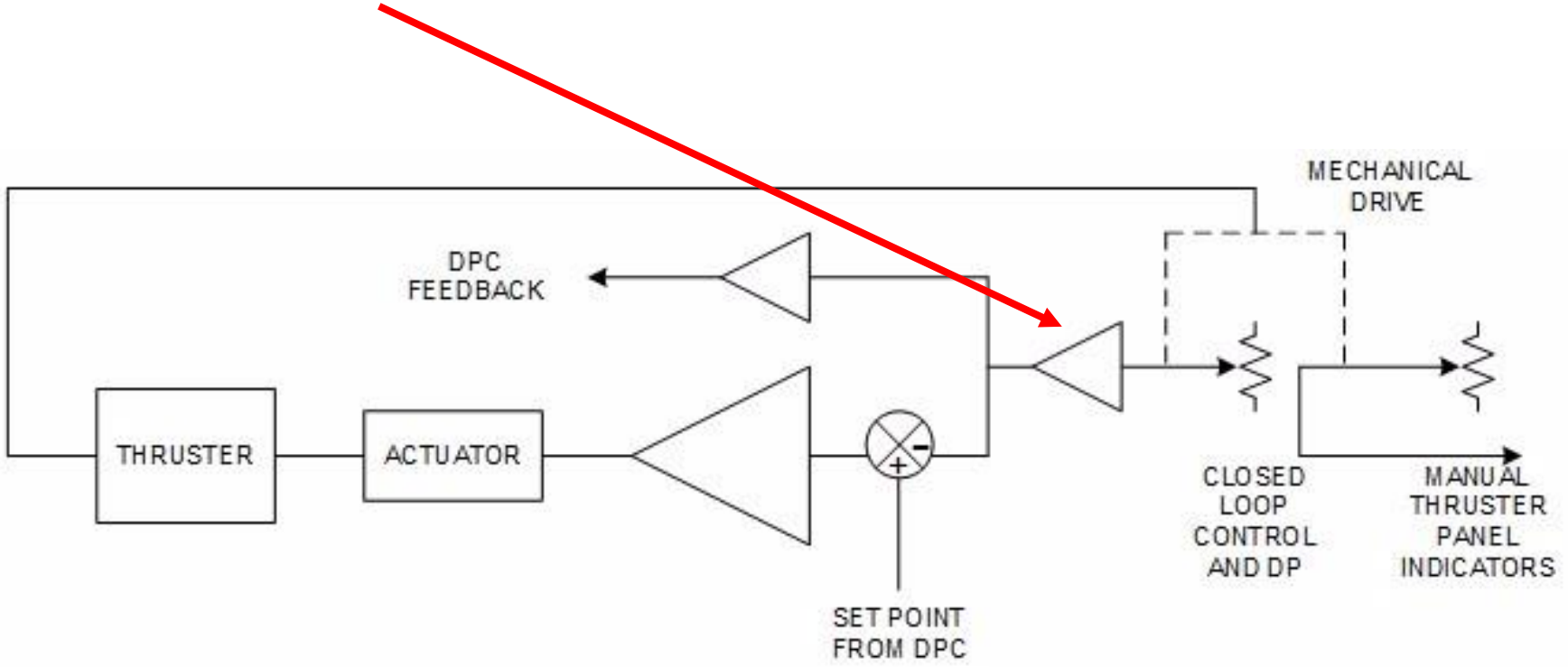


- If closed loop coupling slips thruster will point in the wrong direction but there will be an alarm from DP

- If DP and Indication coupling slips, thruster will point in the right direction but there will be an alarm because DP will never get the azimuth feedback it has ordered.

Offset can be electronic not mechanical

- If an azimuth offset develops here the thruster will point in the wrong direction but there will be no alarm from DP.



- Azimuth indicators will disagree with DP but there will be no alarm

Why traditional verification methods fail to detect non-compliant failure modes

Commonly encountered problems

- Most incidents and trials findings involve CPPs or Azimuth control systems.
  - CPPs failing to full thrust as a result of failure or wire break tests
  - Azimuth control systems causing thrust in the wrong direction and poor station keeping – often feedback issues.
- Not unsual to find a fix is already available.
- Suspicion that thrusters may be 'test-proof' not 'fail-safe'.
- Example – CPP - Tunnel thruster tested for wire breaks and passed without comment – A few weeks later the thruster failed to full thrust when a ground fault developed on solenoid valve wiring.
- TESTING is a vital part of validation and verification but you can't test a bad design into a good one.
- TRADITIONAL methods based on what is accepted not what is required.

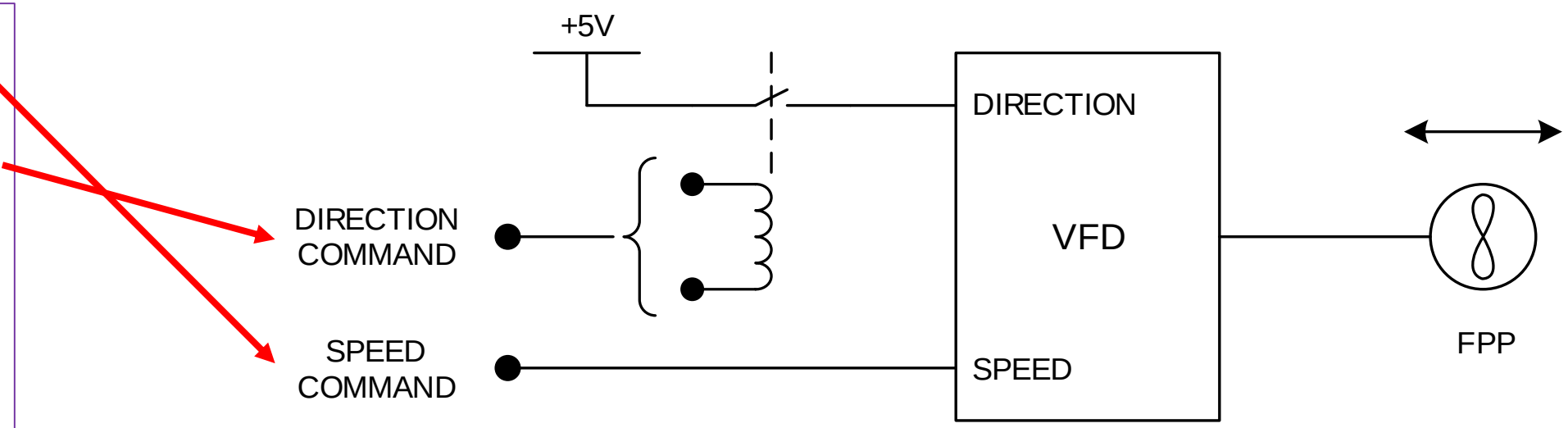
Traditional verification (DP assurance) process - Wire-break tests

- Traditional testing and analysis by DP assurance providers is typically limited in scope and depth
- Wire break tests on control loops are not without merit and do detect non-fail-safe effects in CPPs and Azimuth controls and auxiliaries (inc hidden failures)
- Even within the very limited scope of control loop testing there may be significant variability:
  - Some test programs only break the signal wire.
  - Other 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 thrusters 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.- 'BUILD TO TEST'.
- ESSENTIALLY – Just because a thruster can't be made to fail to a '*non fail-safe condition*' with the limited tool-box of tests and analysis that is traditionally applied does not mean it's fail-safe – as evidence by DP incidents.

Case study – FPP tunnel thruster – loss of heading

Test Results

- Fail Speed Command (O/C) – Speed goes to Zero
- Fail Direction Command (O/C) - Thruster reverses direction and increases speed – heading lost
- **End Effect** - DP control system senses loss of heading and increases speed creating even more thrust in the wrong direction.

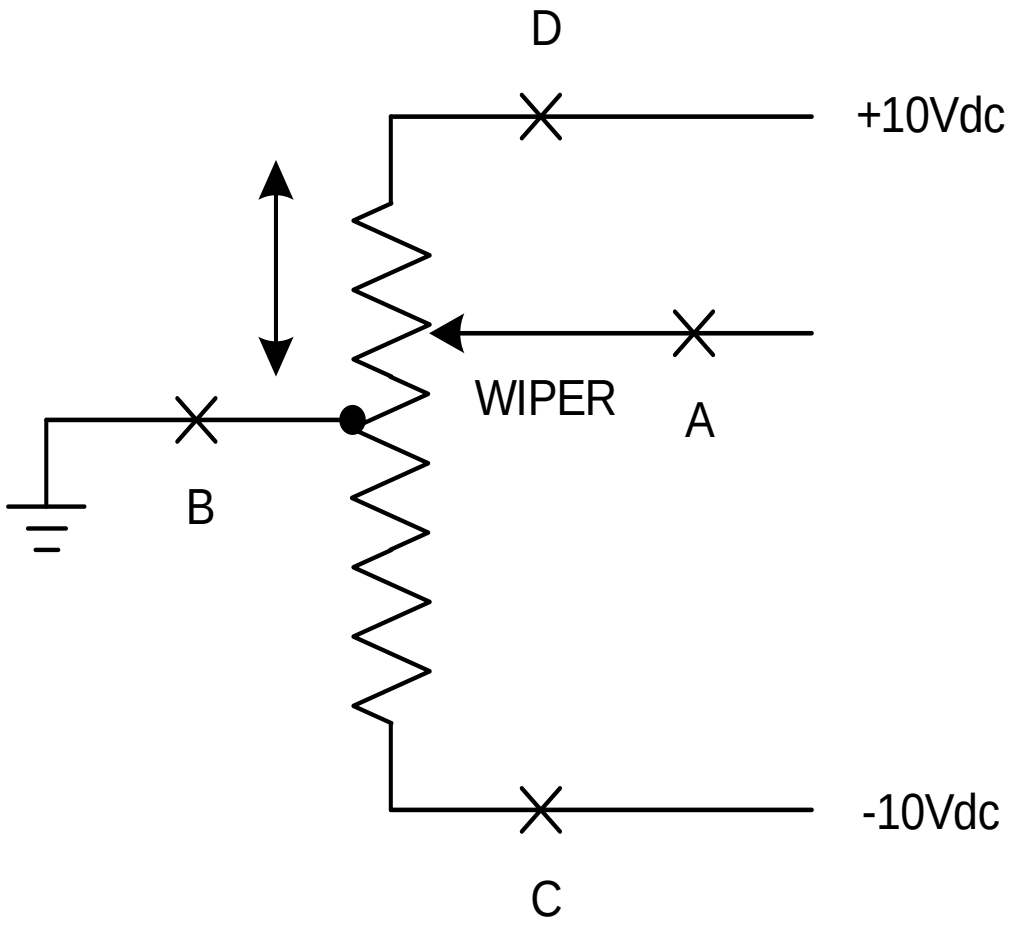


- Annual DP trials finding after the vessel had been in service for several years – Why?
- Direction control circuit design:
  - Failure of the circuit has **no effect** if is thrusting in one direction.
  - Causes **direction reversal** if it is thrusting in the other direction.
- A blind test may record that 'direction failure' caused the thruster to fail 'as set'.
- Is this 'Bad Luck' or inadequate verification and validation?

Variable speed drives

- Very few, if any, reports of modern VFDs failing to full speed (unlike older generation dc drives).
- VFDs tend to have a large range of protective functions.
- Protective functions intended to protect the drive against damage.
- If anything – problem with VFDs is spurious shutdown / ride-through rather than run-away – COMMON CAUSE FAILURE.
- Never-the-less – if the failure effects depend upon the correct operation of protective functions then there should be an understanding of what they are so that they can be proven to be effective (periodically - after control system updates for example).
- Should not assume that every design will fail-safe – BUT how much time is being wasted doing blind tests where there is no other outcome? – 'Apple Tree Test'.

Pitch feedback

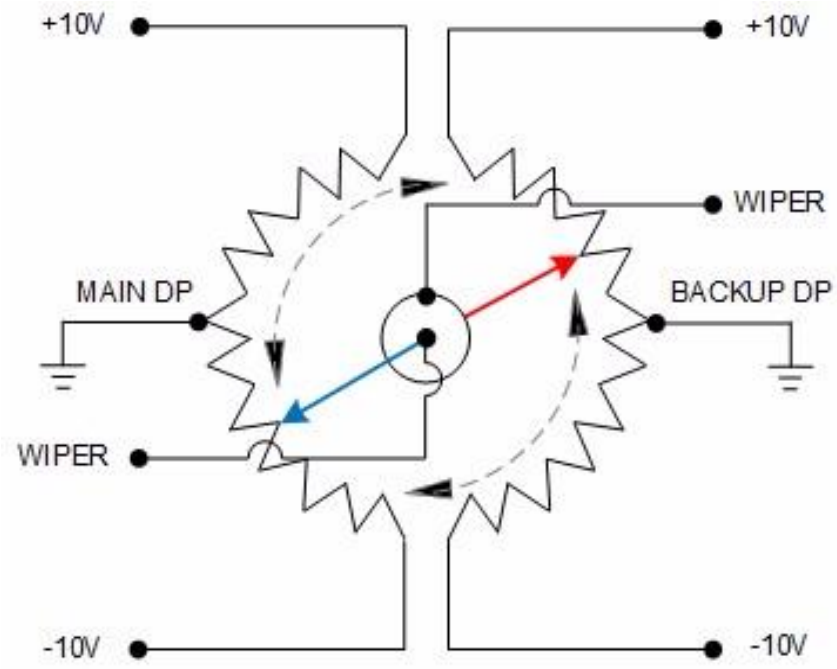


- Different failure effects are possible depending on which wire breaks
  - Wiper
  - Ground
  - Negative power supply
  - Positive power supply

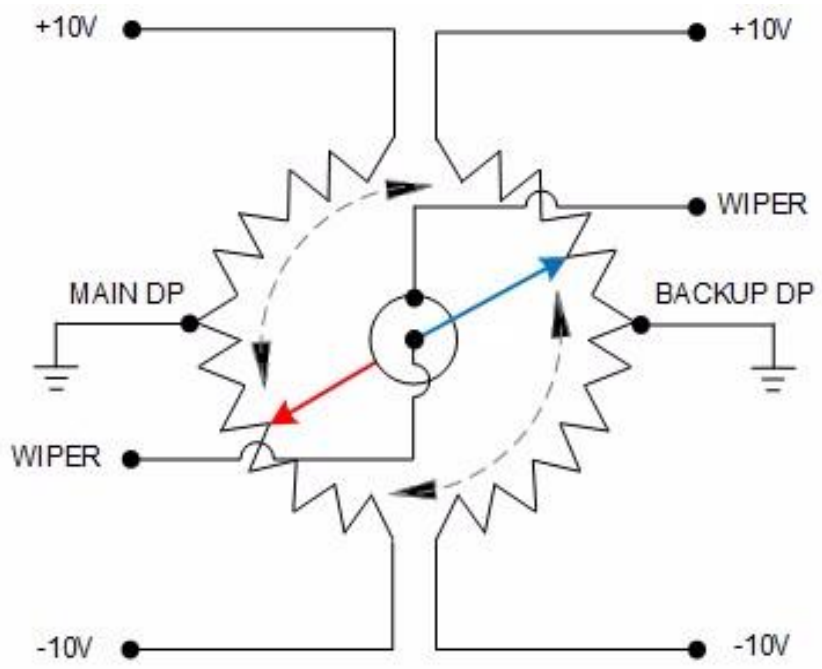
  Need to ensure an acceptable failure effect for all possible modes of failure.

Case Study – Maintenance induced failure – DP class 3 - CPPs

- Backup DP control system may become a common point.
- Possible to install rotor of dual element pitch-pot 180° out such that non redundant backup control system is powering the feedback signals for the main DP system. Functions without issue until back-up DP control system fails.

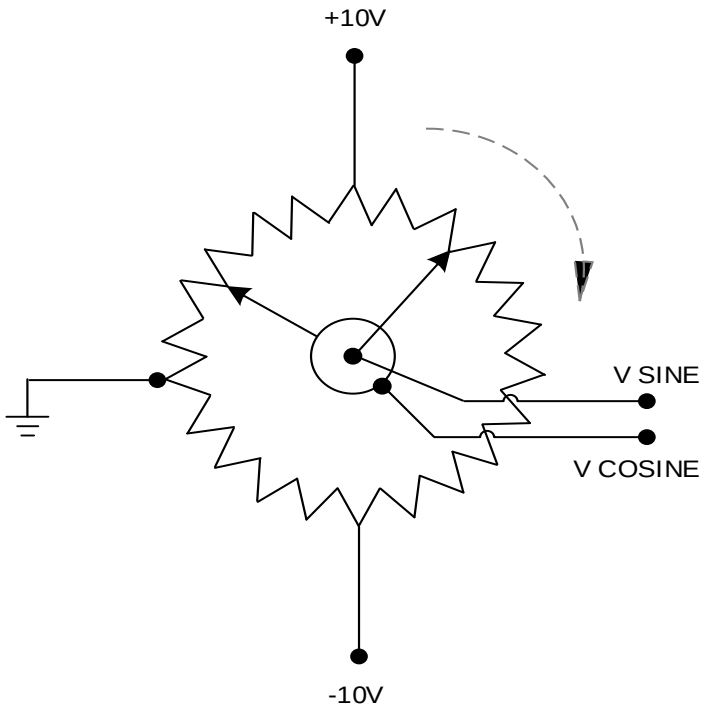


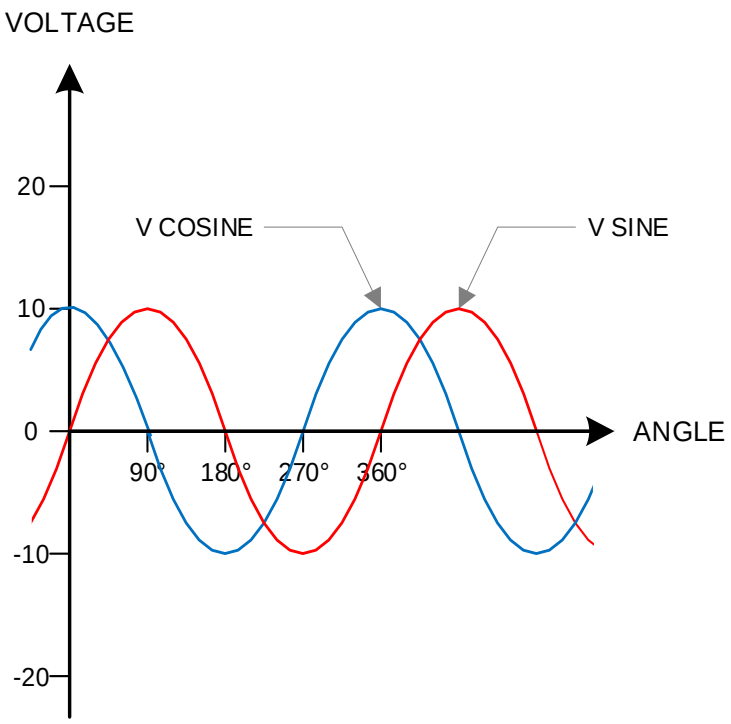
Correct



Incorrect

Sine – cosine potentiometer for rotation feedback

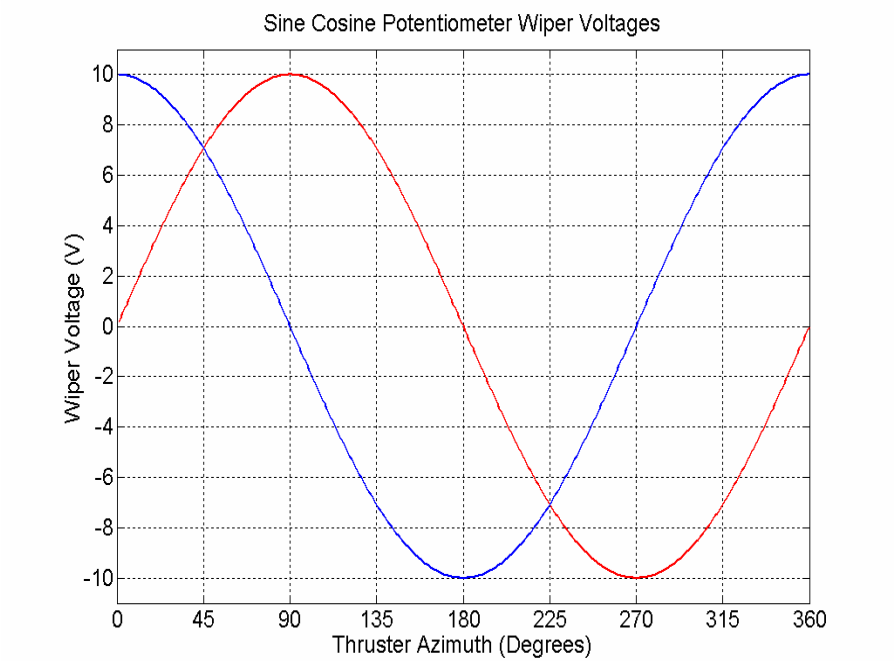


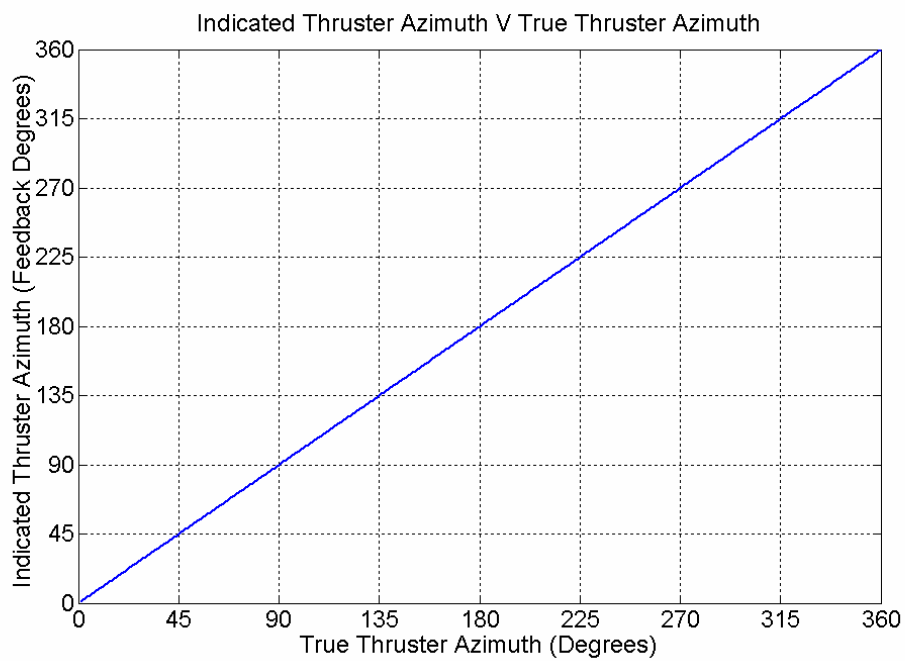


- Tapered resistance elements
- Two wipers
  - Sine of the angle
  - Cosine of the angle
- Can’t resolve an angle from one channel because there are two possible voltages for every angle
- Digital encoders now popular for feedback

Angle is resolved by using inverse Tan function (arctan)

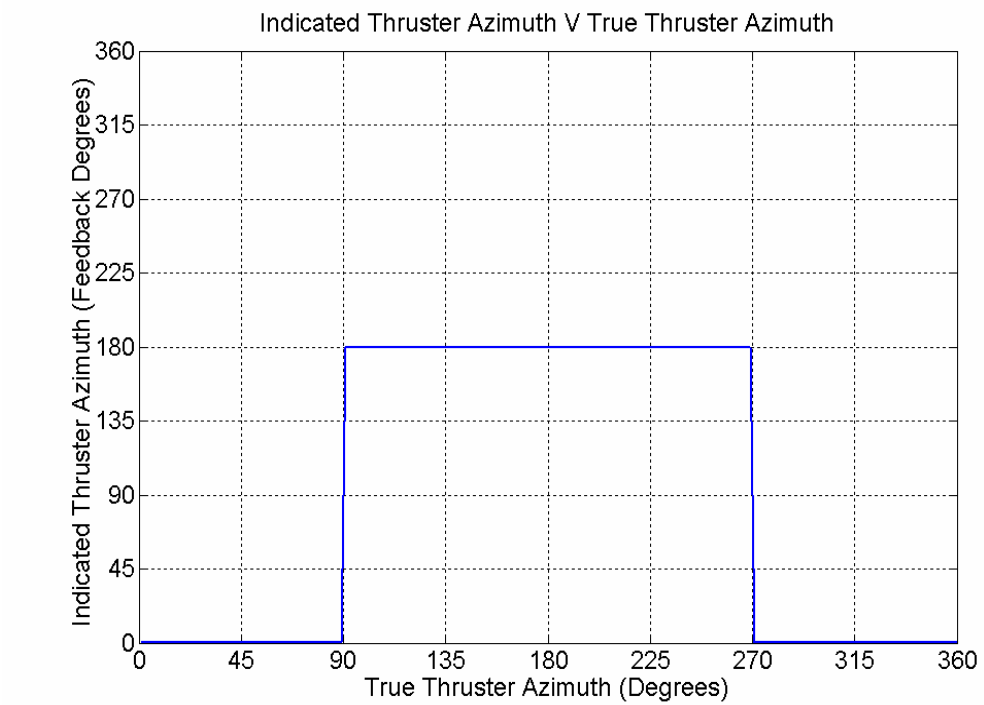
- if V_sin ≥ 0 and V_cos > 0 angle = arctan (V_sin / V_cos) / (2*pi) * 360
- if V_cos = 0 and V_sin > 0 angle = 90
- if V_cos < 0 angle = 180 + arctan (V_sin / V_cos) / (2*pi) * 360
- if V_cos = 0 and V_sin < 0 angle = 270
- if V_cos > 0 and V_sin ≤ 0 angle = 360 + arctan (V_sin / V_cos) / (2*pi) * 360

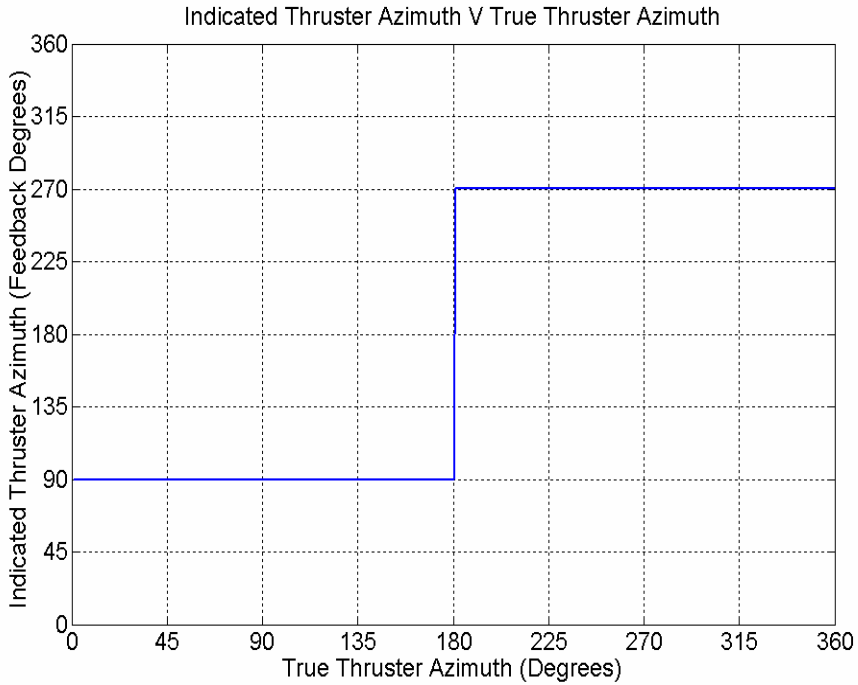




Failure effects

- With this particular algorithm:
  - Failure of the sine channel to zero Volts cause the feedback to toggle between 0° and 180°
  - Failure of the cosine channel to zero Volts cause the feedback to toggle between 90° and 270°





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

Emergency stops

MSC 1580

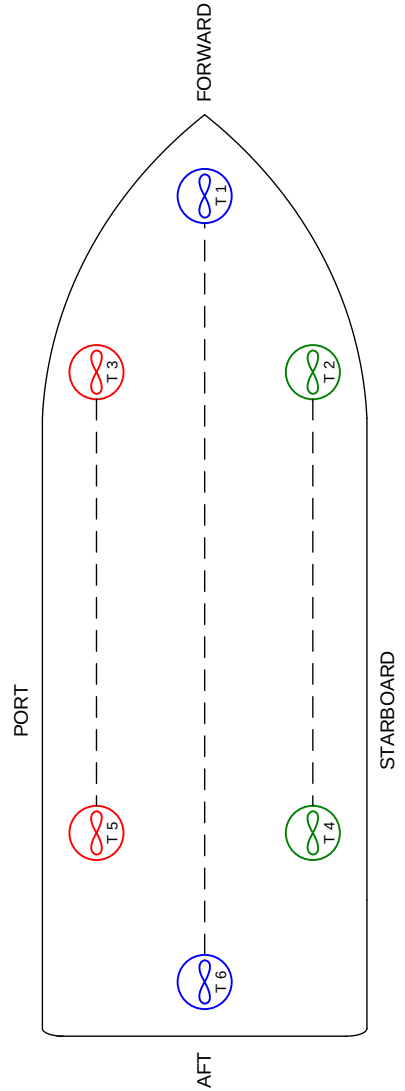
3.3.6 Individual thruster emergency stop systems should be arranged in the DP control station. For equipment classes 2 and 3, the thruster emergency stop system should have loop monitoring. For equipment class 3, the effects of fire and flooding should be considered.

- There will be an independent emergency stop for each thruster.
- It's prudent to have a fall-back to help mitigate the UNKNOWN.
- DP power plants are not supposed to BLACKOUT – but it's prudent to have an automatic Blackout Recovery function.
- Thrusters are not supposed to develop UNWANTED THRUST - but it's prudent to have an Emergency Stop
- Problems occur when the fall-back becomes a substitutes for effective validation and verification of the fail-safe properties of the thruster system.

Effective operator intervention may be comprised in various ways

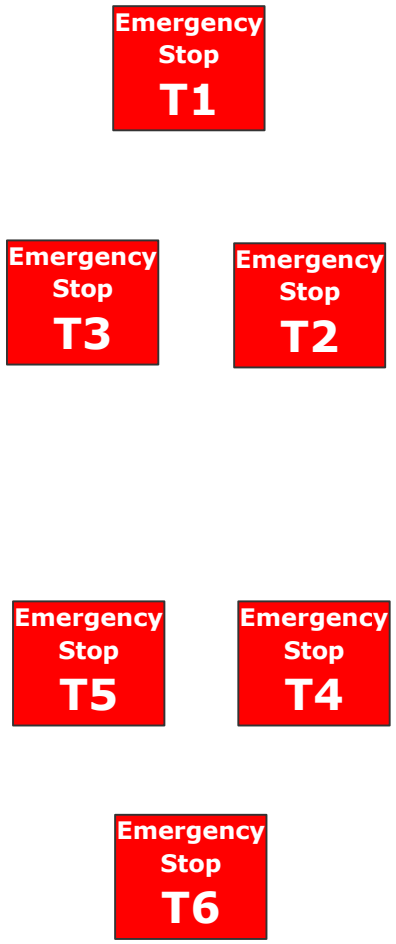
- The DPO requires a clear and unambiguous indication that the thruster has malfunctioned. Regrettably, this is not always provided, particularly in the case of shared sensors for DP feedback and closed loop control.
- The operator must act quickly and effectively under stressful conditions. A recent MTS LFI 17-3 on unwanted thrust provides some evidence that response is not always optimal. (an expectation that DP control system would take care of the drive off – not unreasonable – intended to be redundant and fail safe)
- The operator should 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.

Ergonomics



Layout 1

Layout 2



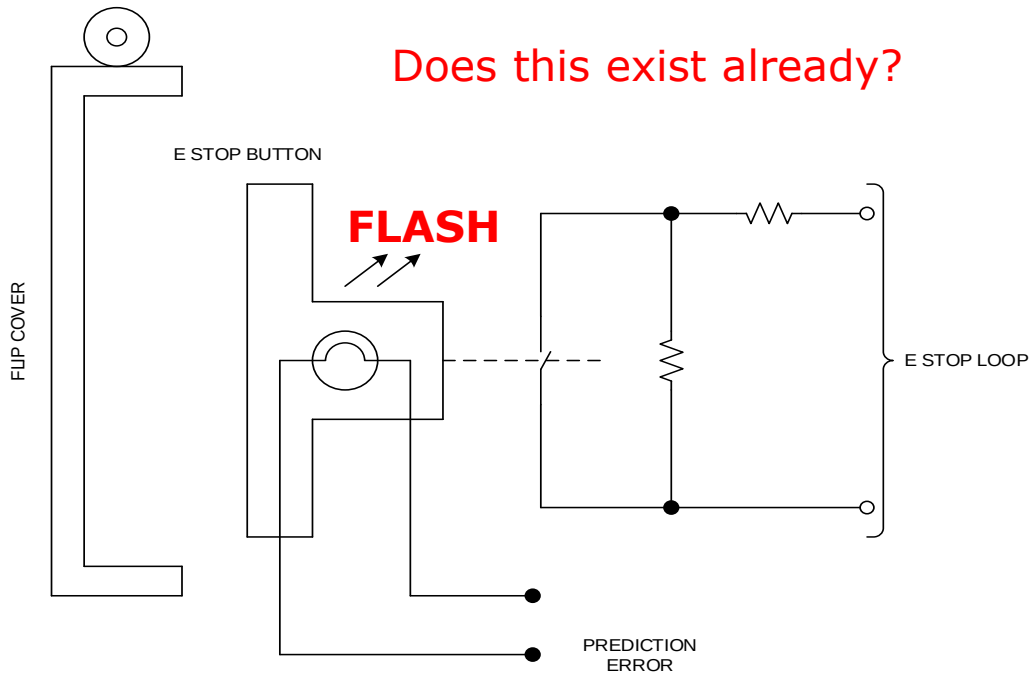
- Operators are sometimes blamed for not 'Saving the Day' but do we give then any chance of succeeding?
- Which layout of the Emergency stop buttons is likely to be most helpful?
- DP systems are supposed to be redundant and fail-safe why should there be a need for operator intervention?

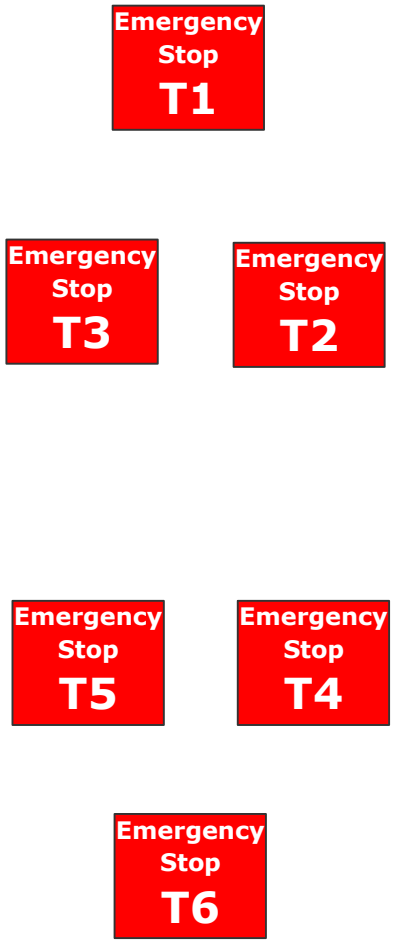
Ungraded

Methods to assist operator intervention

For example:

- Illuminated emergency stop buttons
- DP control system can flash button for thruster which has a prediction error.
- Depends on reliably detecting anomalous thruster behaviour





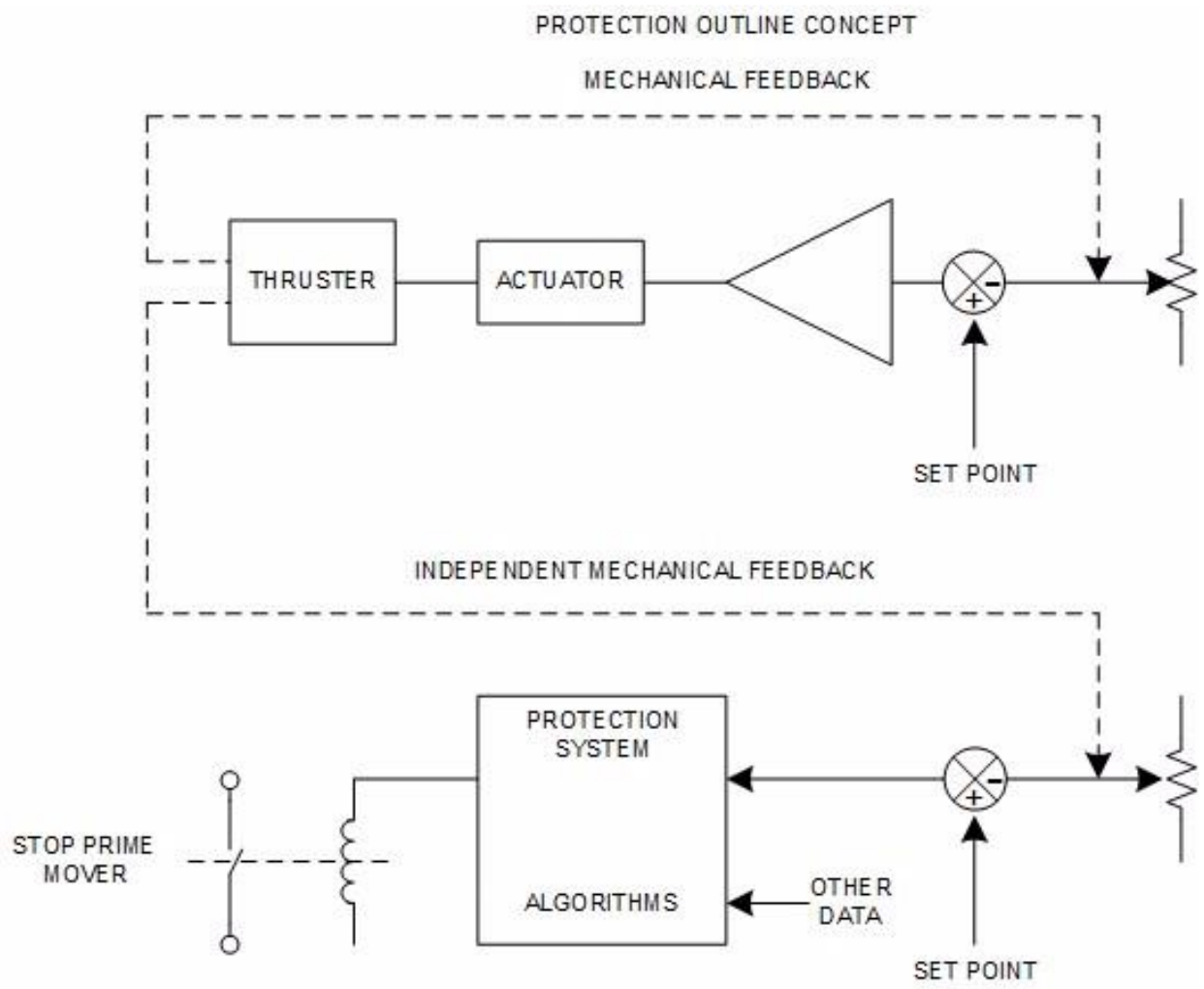
Ungraded

An alternative approach which ensures thrusters fail-safe

Existing challenges and an alternative approach

- Challenges in proving a design is fail safe – Methods have not developed in many years
- No well defined list of protective functions upon which 'fail-safe' depends
- Access to detailed design information – including software
  - Confidentiality
  - Intellectual property
  - Perhaps manufacturers better placed to do it themselves
  - Transparency – trust issue for stakeholders
- Protection and control often integrated – burden of proof too great
- Limited testing tool box
- Rather than struggle to overcome the challenges of proving a particular design is fail safe – why not adopt an alternative strategy, assume it is not fail-safe
- Add an independent protective function to make sure it does.
- Put the effort into validating and verifying the protective function.

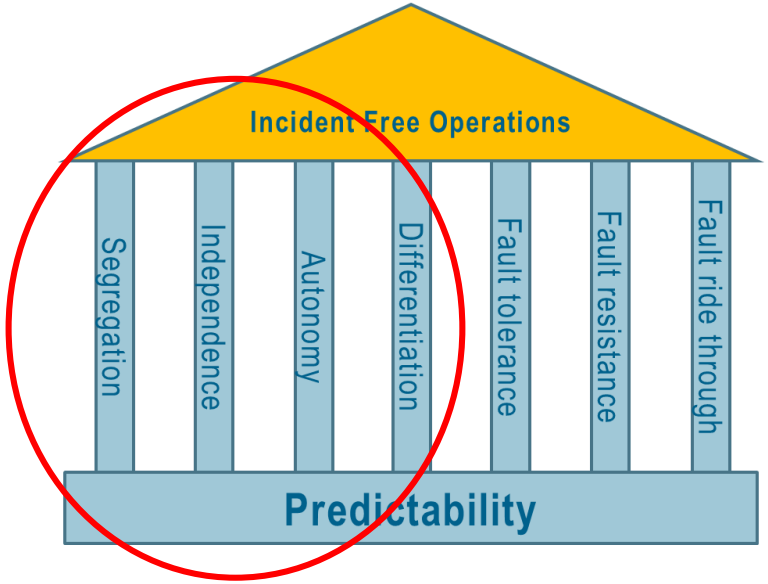
An independent protective function - Outline



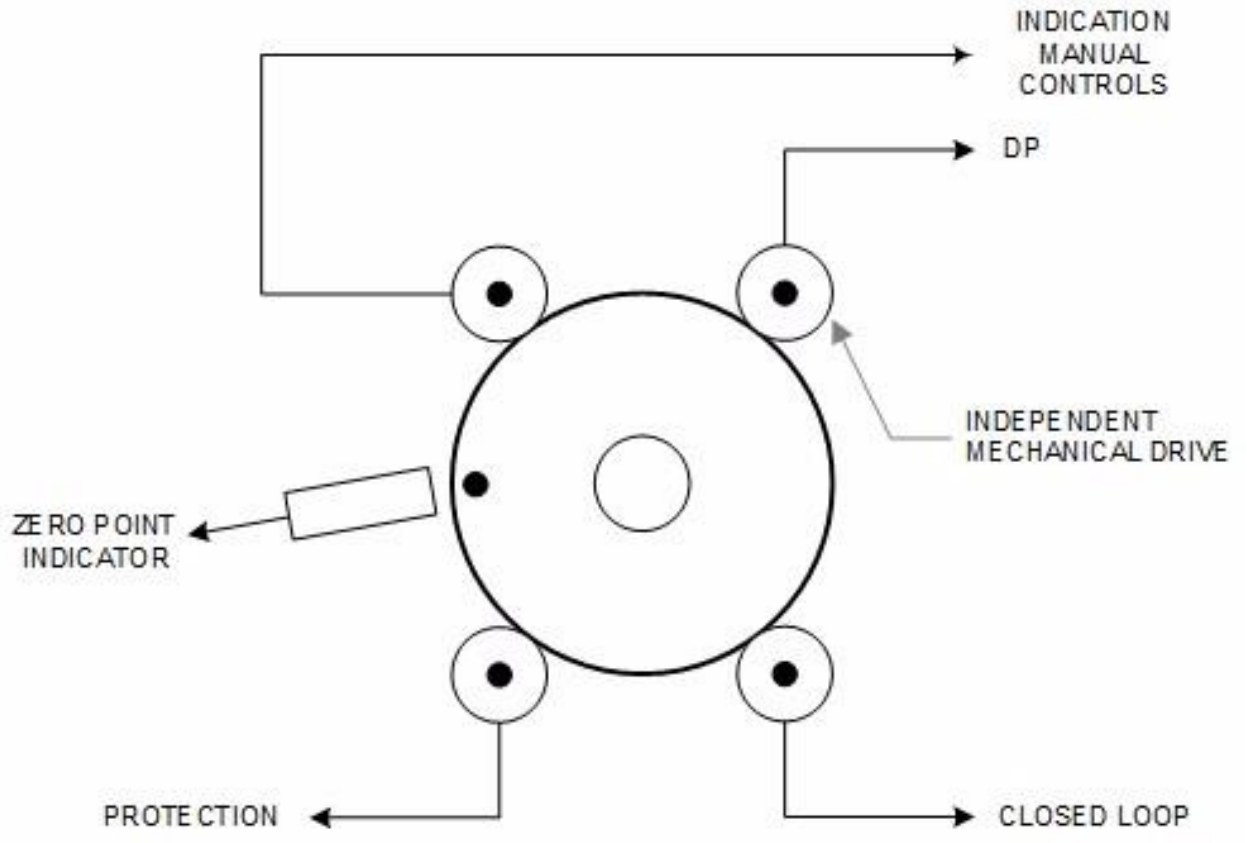
- Monitors the thruster's performance.
- Shuts down the prime mover if thruster produces:
  - Excess thrust.
  - Thrust in the wrong direction
- Robust – model based protection considering a wide range of performance indicators.
- Avoid spurious tripping – maintain reliability.
- Avoid confusing DP control system (ready signal – estimated feedback).
- Stop prime-mover and / or declutch CPP.
- Zero-pitch system – return to zero or trip.
- 'BUILT TO TEST'
- Other benefits – data logging etc.

Design attributes for independent protection

- Adherence to Seven Pillars with particular attention to:
  - Autonomy
  - Independence
  - Segregation
  - Differentiation
- Correlation between various, measurements – motor current, pitch, speed, azimuth, hydraulic pressure etc.
- Differentiation in measurement methods (Different types of transducers)
- Model based protection.
- Independent measurements for control, protection and monitoring
- Multiple rotation transducers with physical separation.
- Autonomous operations with no connection to other thrusters – some commonality for data collection (V&V).



Independent and well segregated transducers



- Independent mechanical drive
  - Indication and manual levers
  - DP feedback
  - Closed loop control
  - Independent protective function
- Well segregated physically
- Differentiation in measurement method to reduce risk of common mode failure

Conclusions

Effective verification and validation

Depends on:

- Understanding the un-mitigated failure modes and effects of all parts of the thruster system and the control systems in particular:
- Developing, validating and verifying a comprehensive and independent set of protective functions to convert non-fail-safe effects to safe ones.
- Developing test methods to prove those protective functions are effective and remain effective through the thruster's life cycle
- Systems must be 'built to test' - fear of testing means protective functions are not proven.
- Minimise the need for operator intervention but also validate that it is a credible mitigation. Give the DPO a chance!
- The challenges of verifying that integrated protective functions are independent, comprehensive and effective are such that it may be more effective to refocuses effort on developing, validating and verifying an independent protective function to ensure thrusters fail-safe.

Thank You and Questions

Dr Steven Cargill
Steven.Cargill@dnvgl.com
Direct +44 2038164365

www.dnvgl.com

SAFER, SMARTER, GREENER

Ungraded