This section contains information on the following topic areas as defined by the Nautical Institute.

DP Testing & Trials
FMEA
FMEA - purpose, class & guidance requirements, class involvement, specific guidance, objectives, failure types (single, common, hidden, etc)
FMEA Proving trials - guidance, purpose, requirements, what should be demonstrated (redundancy concept, effectiveness of protective functions, stability of the system over full range of load conditions, monitoring functions, degraded and failure condition, etc.)
FMEA 5 years proving trials - purpose, requirements, guidance, what should be demonstrated, etc
DP Annual Trial
IMCA M190, purpose, class & guidance requirements, class involvement, specific guidance, objectives, IMCA DP Practitioner Accreditation Scheme
Field Arrival Trials
Guidance, purpose, requirements, what should be demonstrated
DP Networks (Move to DP System)
DP Network system - overview & the risks, guidance available
DP Network system - Operational & Failure considerations
DP Network system - Lessons learnt from DP Events DP Network system

FMEA – PURPOSE, OBJECTIVES, CLASS & GUIDANCE REQUIREMENTS, CLASS INVOLVEMENT, SPECIFIC GUIDANCE

Vessel FMEA (Failure Modes and Effects Analysis) is a systematic methodology used to identify potential failure modes and assess the risks and effects associated with them. It is a risk assessment tool that considers the vessel's DP systems and components, as well as the potential consequences of failure, to prioritize areas for improvement and minimize the risk of vessel downtime and other negative impacts. The FMEA process helps to identify design, operational, or maintenance-related issues that could lead to equipment failure, and it is used to improve safety, reliability, and efficiency in DP vessels.

IMO MSC/Circular 1580 defines an FMEA as:

> *1.2.13 Failure Modes and Effects Analysis (FMEA) means a systematic analysis of systems and sub-systems to a level of detail that identifies all potential failure modes down to the appropriate sub-system level and their consequences.*

And it requires that

> *5.1.2 For equipment classes 2 and 3, an FMEA should be carried out. This is a systematic analysis of the systems to the level of detail required to demonstrate that no single failure will cause a loss of position or heading and should verify worst-case failure design intent. This analysis should then be confirmed by FMEA proving trials. The FMEA and FMEA proving trials result should be kept on board and the FMEA should be kept updated so that it remains current*

An FMEA is a document, usually a large document, prepared by an FMEA contractor and approved by the classification society for the vessel. Without an FMEA the classification society will not allocate a vessel notation as DP class 2 or 3.

The FMEA is a means of proving the redundancy concept of the vessel to ensure safe and reliable DP operations. OCIMF (Oil Companies International Marine Forum) have produced a document Dynamic Positioning Failure Mode Effects Analysis Assurance Framework Risk-based Guidance (2020) that is useful when analysing the contents of an FMEA.

It states that FMEAs are performed to

- *Verify the redundancy design intent (RDI) of the vessel.*
- *Prove that redundant equipment groups are independent and fail-safe.*
- *Identify common points that compromise independence between redundant equipment groups.*
- *Assess common points to determine the effects of failures (both benign and aggressive) that propagate through common points, as well as the effectiveness of mitigations for unacceptable effects.*
- *Develop a proving trials program to validate the analysis.*

IMCA offer a flow chart of the Failure Modes Effects Analysis process that demonstrates how technically involved and iterative the process is. It also demonstrates the technical and commercial depth of the FMEA team required.

The FMEA, during the design phase, can be an iterative process if proposed designs are found to have flaws. Note that the FMEA produced for the offshore industry does not evaluate based on the likelihood or the severity of the faults. If any perceived fault causes a greater failure than the defined WCF, then it must be eliminated.

A simplified flow diagram is presented on the following page.

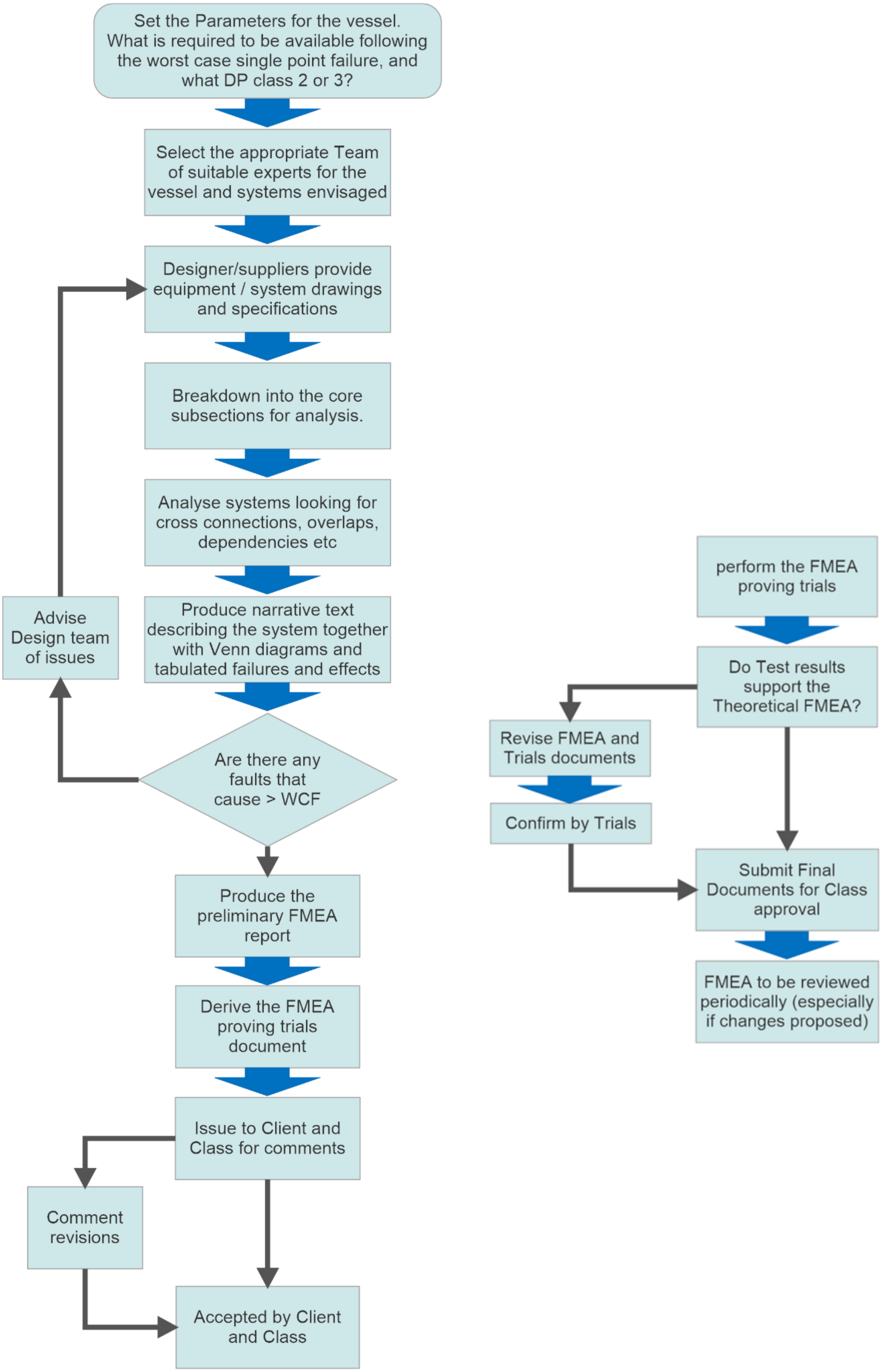

FIGURE 8 - The Basic FMEA Flow During Design and Construction and Confirming Trials

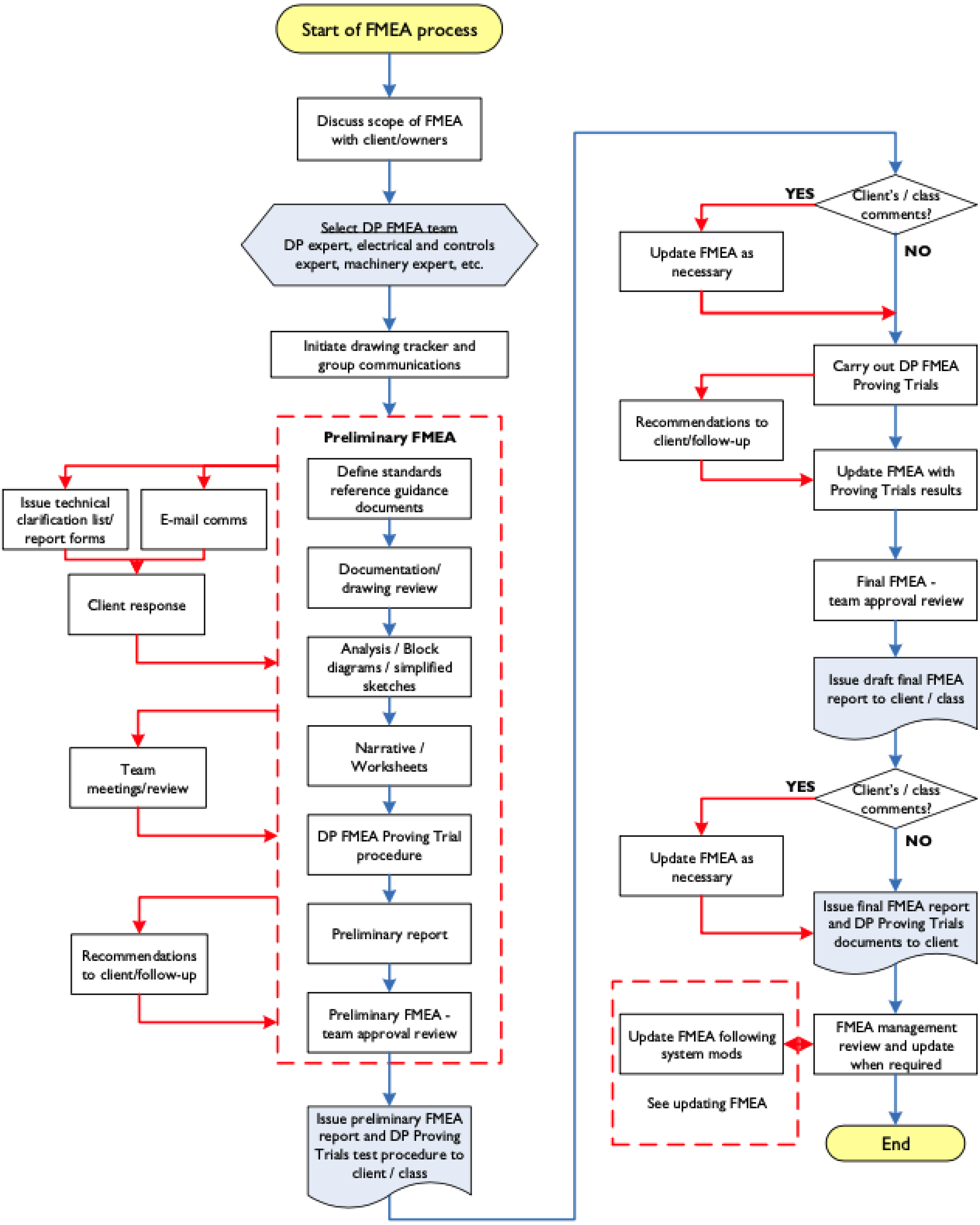

FIGURE 9 - IMCA M 166 REV. 2 - IMCA M 166 REV. 2

An FMEA is intended to be an exhaustive examination of all the systems on board the vessel that are directly or indirectly associated with the DP system function. MTS have produced a 'Gap analysis tool'. This document allows an assessment of the FMEA by asking questions based around the major systems involved with a DP vessel. By posing questions it allows the user to capture a snapshot of the FMEA. It is easy to analyse a system and to recognise for instance that there are no cross connections but then not state that fact in the FMEA. The GAP analysis asks if it is not stated was it because it was missed or just not confirmed. Because it covers the most complex vessels it can seem a little heavyweight but for any FMEA it is a useful aide memoire if nothing else.

The various GAP analysis tools are available on the MTS website by clicking **here**

Think about the difference between the redundancy upon which the DP concept is based and the redundancy within some systems that contributes to availability.

A typical example is a duty/standby FW pump arrangement for a single thruster. If a pump has failed the other allows the thruster to carry on, but it still has not reduced the overall redundancy. Why? Because there are still single failures that can stop the thruster.

On sea chests we often have dual strainers for exactly the same reason.

Think about the systems on your vessel what is critical to supporting the redundancy concept.

IMO MSC/Circular 1580 defines redundancy as

> *1.2.21 Redundancy means the ability of a component or system to maintain or restore its function when a single failure has occurred. Redundancy can be achieved, for instance, by the installation of multiple components, systems or alternative means of performing a function.*

This is normally achieved by placing more than one of any component onboard, for example two different types of position reference system. Or by or setting up integrated components (systems) up as complexly separate groups.

Consider the two completely separate redundancy groups in the thruster diagram below.

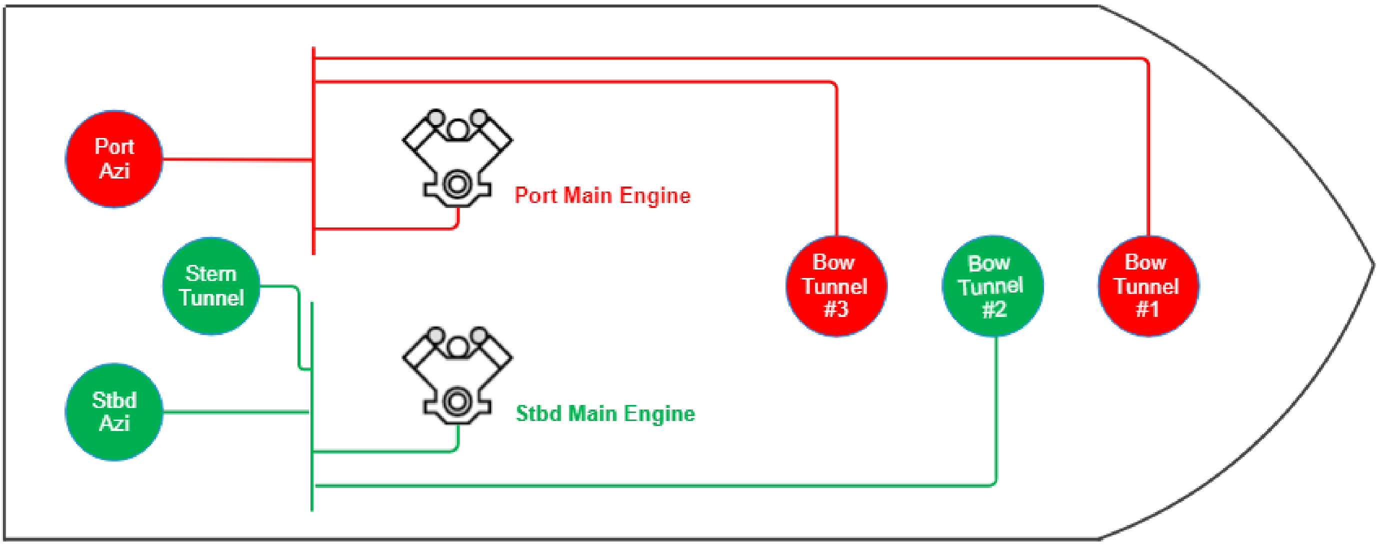

FIGURE 10 - TYPICAL DP2 VESSEL LAYOUT

A ***single failure*** in the context of the redundancy definition means a fault that could lead to a **worst case failure.** IMO MSC/Circular 1580 defines a worst case failure as:

> *1.2.25 Worst-Case Failure (WCF) means the identified single fault in the DP system resulting in maximum detrimental effect on DP capability as determined through the FMEA.*

The ***detrimental effect*** referred to here is the reduction in power / thrust due to the fault but which the remaining equipment is still able to maintain position and heading.

IMO MSC/Circular 1580 has designated three equipment classes. Each equipment class is defined by the level of redundancy (the installation of multiple components) needed to protect the DP system worst case failure (loss of a loss of position and/or heading) and it defines what is considered a single fault in each case.

> *.1 For equipment class 1, a loss of position and/or heading may occur in the event of a single fault.* (i.e. there is no redundancy)

> *.2 For equipment class 2, a loss of position and/or heading will not occur in the event of a single fault in any active component or system. Common static components may be accepted in systems which will not immediately affect position keeping capabilities upon failure (e.g. ventilation and seawater systems not directly cooling running machinery). Normally such static components will not be considered to fail where adequate protection from damage is demonstrated to the satisfaction of the Administration. Single failure criteria include, but are not limited to:*

>> *.1 any active component or system (generators, thrusters, switchboards, communication networks, remote-controlled valves, etc.); and*

.2 any normally static component (cables, pipes, manual valves, etc.) that may immediately affect position keeping capabilities upon failure or is not properly documented with respect to protection.

.3 For equipment class 3, a loss of position and/or heading will not occur in the event of a single fault or failure. A single failure includes:

.1 items listed above for class 2, and any normally static component assumed to fail.

.2 all components in any one watertight compartment, from fire or flooding; and

.3 all components in any one fire sub-division, from fire or flooding.

NOTE: the difference between equipment class 2 and equipment class 3 DP vessels is that ANY static component must not fail (rather than only those static components that *may immediately affect position keeping capabilities*) AND the separation of components by fire and flood protection. It is a common misnomer that DP vessels need more components or systems, they don't; they just need to protect them more.

Case Study – Vessel Degraded Capability

FMEA FAILURE TYPES (SINGLE, COMMON, HIDDEN, ETC)

IMO MSC/Circular 1580 defines a failure as:

1.2.12 Failure means an occurrence in a component or system that causes one or both of the following effects:

.1 loss of component or system function; and/or

.2 deterioration of functional capability to such an extent that the safety of the vessel, personnel or environment protection is significantly reduced.

And redundancy as

*1.2.21 Redundancy means the ability of a component or system to maintain or restore its function when a **single failure** has occurred. Redundancy can be achieved, for instance, by the installation of multiple components, systems or alternative means of performing a function.*

MTS DP Vessel Design Philosophy Guidelines gives some practical examples of possible failures and their consequences.

3.2.6 Failure analysis vocabulary

- *Failure modes: The mode of failure describes the way in which a component or system fails. For example, a diesel engine may fail to over speeding, hunting rpm or stop. The cause of this failure mode could be a clogged filter.*
- *Failure effects: The effects of a component or system failure can be defined at several levels in the DP system architecture including the local effect and the end effect:*
    - *Local effects: The local effect is the effect on the system at the failure point itself. Using the same example of a faulty cable, the local effect of a short circuit would be high current in the cable followed by operation of the upstream overcurrent protection to isolate the fault.*
    - *End effects: The end effect is the effect at the level at which the top event is defined (Typically loss of position and / or heading) Using the cable example above, top event of the cable short circuit may be a voltage dip that causes all thruster drives to malfunction leading to loss of position and / or heading. The effect of the open circuit may be less severe. Typically, loss of one generator or a thruster becomes unavailable. In the case of the ground fault the end effect may be an alarm with no greater effect on position or heading.*

Note that in the last paragraph if the 'End Effect' is a loss of position or heading then the outcome of that fault is not acceptable and must be mitigated so it will not result in anything worse than the defined 'Worst Case Failure'.

In a typical FMECA (Failure Modes, Effects and Criticality Analysis) failures are analysed and categorised according to how serious their consequences are (Criticality), how frequently they could occur (Likelihood), and how easily they can be detected (or even if they can be detected).

At present the industry requires an FMEA and does not discriminate and assumes all faults can occur and the system cannot subsequently degrade beyond the defined worst case failure.

SINGLE FAILURE

We know the Vessel will be assigned its DP Classification based on the effect of a single failure (or single fault).

> *.1 **For equipment class 1**, a loss of position and/or heading may occur in the event of a single fault.*
>
> *.2 **For equipment class 2**, a loss of position and/or heading will __not__ occur in the event of a single fault in any __active__ component or system. Common static components may be accepted in systems which will not immediately affect position keeping capabilities upon failure (e.g. ventilation and seawater systems not directly cooling running machinery). Normally such static components will not be considered to fail where adequate protection from damage is demonstrated to the satisfaction of the Administration. **Single failure criteria include**, but are not limited to:*
>
> > *.1 any **active** component or system (generators, thrusters, switchboards, communication networks, remote-controlled valves, etc.); and*
> >
> > *.2 any **normally static component** (cables, pipes, manual valves, etc.) **that may immediately affect position** keeping capabilities upon failure or is not properly documented with respect to protection.*
>
> *.3 **For equipment class 3**, a loss of position and/or heading will __not__ occur in the event of a single fault or failure. A single failure includes:*
>
> > *.1 items listed above for class 2, and any normally static component assumed to fail;*
> >
> > *.2 all components in any __one watertight compartment__, from fire or flooding; and*
> >
> > *.3 all components in any __one fire sub-division__, from fire or flooding (for cables, see also paragraph 3.5.1).*

The vessel's worse case failure (WCF) used in the consequence analysis (FMEA) is determined using this equipment class single failure criteria. See section Redundancy Concepts for more information on worse case failure (WCF).

HIDDEN FAILURE

A hidden failure is defined by IMO MSC/Circular 1580 as:

> *1.2.15 Hidden failure means a failure that is not immediately evident to operations or maintenance personnel and has the potential for failure of equipment to perform an on-demand function, such as protective functions in power plants and switchboards, standby equipment, backup power supplies or lack of capacity or performance.*

The MTS DP Vessel Design Philosophy Guidelines state that *Hidden failures have the potential to defeat the redundancy design intent.* They explain that failure of dormant or on demand functions such as standby redundancy and protection systems are examples of potential hidden failures. For example, all interlocks are potential hidden failures. Critical interlocks should be tested non-destructively and periodically to confirm their effectiveness.

COMMON FAILURE

Common connections between systems, intended to provide redundancy, create the paths by which a fault in one redundant system may affect another independent system.

MTS DP Vessel Design Philosophy Guidelines remind us that:

> *In any system based on redundant elements there can be internal and external **common cause failure** that are capable of defeating the redundancy design intent.*

and that

> ***Independence** between equipment groups intended to provide redundancy ensures they are not subject to a common cause of failure*

Conversely "dependencies" is the term used to describe the relationship between one component and another. Dependencies between redundant equipment groups may cause them to be vulnerable to a common cause of failure.

It is really important that you understand what an FMEA is and that you understand exactly what your vessel's FMEA is telling you, and how it supports your role onboard a DP vessel. MTS DP Operations Guidance states:

> *4.3.10 Key DP personnel, including the vessel master, DPOs, engineers and electricians should have a detailed knowledge of the DP FMEA and should use the information provided to be fully informed about the capabilities and limitations of the vessel's DP system.*

PRACTICAL ONBOARD EXERCISE

Find your vessel's FMEA.

Is it colour coded?

What failure modes does it document and what are the consequences of these failures?

It is useful to take a step back at this stage an consider the end goal: *the delivery of incident free DP operation.* This is a concept that MTS define as ***predictability***.

MTS's DP Vessel Design Philosophy Guidelines provide us with an *Integrated Thinking* model that looks incredibly complicated at first glance but which, when explored it will improve your understanding of key DP concepts.

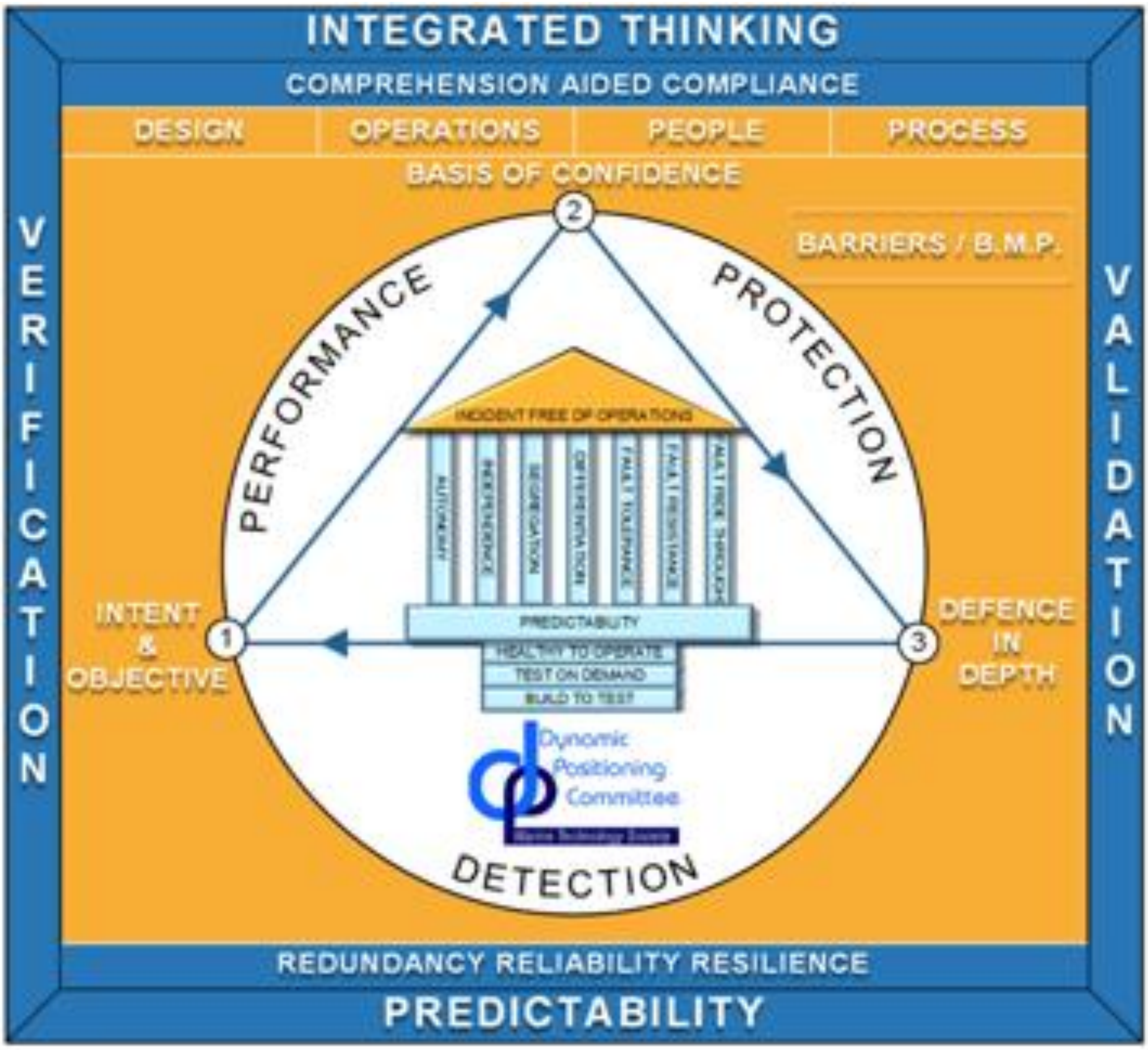

FIGURE 11 - MTS THINKING MODEL

MTS state that there are three essential attributes of any fault tolerant system based on redundancy

***Performance**: Elements of the system intended to provide redundancy must have equivalent performance in all redundancy groups.*

***Protection**: In any system based on redundant elements there can be internal and external common cause failure that are capable of defeating the redundancy design intent. Protection systems are required to limit the end effects of failures to the redundant group in which the failure occurred or protect the overall system (all redundant groups) from such influences.*

***Detection**: Fault tolerant systems based on redundancy are only fully fault tolerant while all redundant groups and the control and protection systems on which they depend are fully operational.*

Consider the role of performance, protections, and detection in the diagram below taken from MTS's DP Vessel Design Philosophy Guidelines

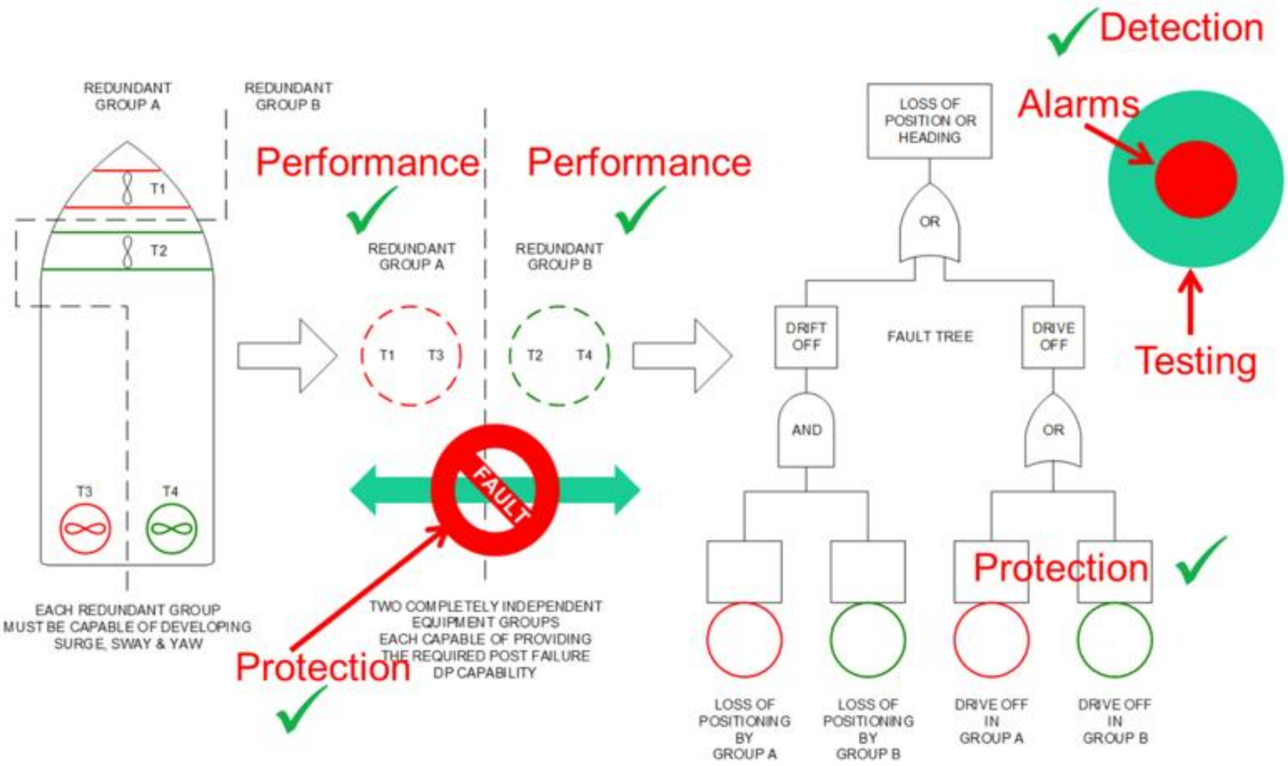

FIGURE 12 - MTS COMBINED ICONOGRAPHY INTEGRATED THINKING

- Redundancy concept,
- Effectiveness of protective functions,
- Stability of the system over full range of load conditions,
- Monitoring functions,
- Degraded and failure condition, etc.

DP FMEA proving trials are intended to establish the level of redundancy and fault tolerance provided by the DP system and confirm the analysis in the FMEA. The DP system of DP class 2 and DP class 3 vessels must be single fault tolerant in respect of defined failure criteria. At DP FMEA proving trials a large number of tests and failure simulations are carried out to prove that equipment and systems intended to provide redundancy have the necessary performance, protective functions and monitoring systems to ensure the integrity of the DP redundancy concept.

IMO MSC/Circular 1580 defines FMEA proving trials as *means the test program for verifying the FMEA.*

In Section 5 Surveys, Testing and Dynamic Positioning Verification Acceptance Document (DPVAD) it states that

> *5.1.2 For equipment classes 2 and 3, an FMEA should be carried out. This is a systematic analysis of the systems to the level of detail required to demonstrate that no single failure will cause a loss of position or heading and should verify worst-case failure design intent.* ***This analysis should then be confirmed by FMEA proving trials. The FMEA and FMEA proving trials result should be kept on board and the FMEA should be kept updated so that it remains current.***

MTS DP Operations Guidance - Part 1 states that DP FMEA proving trails are to be:

> *conducted to prove initial DP FMEA and at other times to prove modifications and additions to the DP system. DP FMEA Proving Trials should be repeated every five years. Findings and recommendations to be addressed in accordance with their criticality. All records to be kept on board.*

IMCA M103 goes further and states that FMEA proving trials are:

additional to commissioning and owner acceptance trials

And that proving trials should be:

> *properly documented and the results made available to operators, owners, charterers, surveyors and responsible authorities, to remove the necessity of repetition of design related trials during the vessel's working life and as input into operational manuals and vessel familiarisation procedures.*

In section 2.4 DP System Trials, Tests and Checks IMCA M103 states that DP FMEA proving trails should confirm the worst case failure design intent (WCFDI) and worst case failure (WCF) see section Redundancy Concepts , and should also

- *identify the subsystems and equipment and modes of operation;*
- *identify all potential failure modes and their causes;*
- *identify single point failures;*
- *identify potential hidden failures;*
- *identify potential configuration errors;*
- *evaluate the effects on the DP system of each failure mode.*

IMCA M 247 identifies over forty (40) potential failure modes and other considerations associated with DP systems and sub systems. It is impossible to discuss every potential failure mode presented in this document, and as IMCA state themselves this list is not exhaustive. However, we suggest that you cross reference your vessels FMEA with the section 4 *Identification of Failure Modes* as an above and beyond task.

However, we do highlight here two sections, one engineering based -Lubricating oil, and one deck (DPO) based - Computers and Consoles to illustrate how a Failure Modes Effect Analysis will test the effectiveness of protective functions, the stability of the system over full range of load conditions, monitoring functions, and degraded and failure conditions (as required by the Nautical Institute CPD revalidation criteria "Annex K").

> ***4.1.2 Lubricating Oil***
>
> *The FMEA should look for common failures, which affect not only running engines but also those on standby. The alternator bearing system should be included. The engine may also have subsidiary lubricating oil (LO) systems such as those for rocker arms. In the vast majority of cases, failure of an LO system is limited to one engine.*
>
> *LO storage and transfer facilities may be assessed, but the FMEA of this system normally starts at the sump. The sump level alarms and frequency of checking sump level should be identified. If there are online purification facilities, the interlocks and procedures to prevent pumping LO from one sump to another, which could lead to a low LO pressure shutdown or potentially a crankcase explosion, should be analysed.*
>
> *The use of pre-LO pumps, engine driven pumps and electrical main and standby pumps should be analysed. In particular, the pre-LO pump power supplies, pre-LO pump failure warnings and engine start logic should be reviewed to ensure that a standby engine or set of engines is not inhibited from starting when required by the PMS.*
>
> *There should be a clear understanding of the levels of LO pressure and temperature for warnings, starting standby engines, controlled shutdown and immediate stop. Such functions may be performed by one system or several different systems, e.g. engine management system, PMS, load sharing/ synchronising system, network, etc. Which system initiates breaker opening and closure should be determined. The effects of oil mist detector alarms or failures should be reviewed to determine if there are any conflicts between engine safety and the requirements of DP. The design of the LO alarm system on alternators should be treated as seriously as that on a diesel engine, as alternator bearing failure leading to serious alternator misalignment could cause a generator short circuit, catastrophic failure and significant power instability.*
>
> *The alarms available for filter differential pressure should be confirmed. The common failure of automatically cleaned filters should be considered.*

and

> ***4.7.2 Computers and Consoles***
>
> *All the DP system vendors provide a range of products as well as a large number of options to suit the widely varying activities of the DP vessel fleet. The specification stage of design needs to focus on ensuring that all the required functions are provided and also that unnecessary hardware and software is not installed. The layout of consoles, computers and reference sensors also needs to be confirmed.*
>
> *For common operator system consoles, it has been common practice to recommend soft shutdown of the console before carrying out power failure tests. In such situations, there is usually a bumpless transfer to the back-up system when power is failed. However, during UPS trials, a different failure mode has been reported when UPS batteries expire unexpectedly, and half the DP system crashed. In this case, there was loss of control over all thrusters and DP control on the backup system had to be forced manually.*
>
> *Considerable attention may need to be paid to the design of 'fire backup' switches and other such changeovers between main and backup DP systems, and also between various DP systems and manual thruster control. Normally, it will be necessary to perform an FMEA of the changeover logic to be satisfied that all requirements are met in relation to open circuit, short circuit, loss of power, alarms for hidden failure or misalignment of switches. Similar attention should be paid to bridge engine controls and emergency stops.*

More recently, classification societies have made specific requirements in relation to the failure modes of e-stop functions and the provision of wire break detection.

Although the DP system is by design a redundant system, a separate independent joystick system (IJS) is required for DP equipment class 2 and 3. IJSs require failure consideration and the FMEA should detail a description of the system and its redundancy concept. Detail of sensors interfaced to the system and the independence of the system requires analysis and testing during FMEA proving trials.

PRACTICAL ONBOARD EXERCISE

Find your vessel's FMEA. What failure modes does it document and what are the consequences of these failures?

Consider and discuss the two examples above in what way do the various 'failures' impact the redundancy concept? What are the possible performance, protection and detections functions available to the crew?

ABOVE AND BEYOND

Dynamic Positioning Failure Mode Effects Analysis Assurance Framework Risk-based Guidance (2020)

IMCA M 166 – Guidance on failure modes and effects analyses (FMEAs).

IMCA M 247 November 2018 Guidance to Identify DP System Components and their Failure Modes

IMCA M190, PURPOSE, CLASS & GUIDANCE REQUIREMENTS, CLASS INVOLVEMENT, SPECIFIC GUIDANCE, OBJECTIVES,

IMO MSC/Circular 1580, section 5.1 Surveys and testing states that:

> *5.1.1.3 an annual survey should be carried out within three months before or after each anniversary date of the Dynamic Positioning Verification Acceptance Document. The annual survey should ensure that the DP system has been maintained in accordance with applicable parts of the Guidelines and is in good working order. The annual test of all important systems and components should be carried out to document the ability of the DP vessel to keep position after single failures associated with the assigned equipment class and validate the FMEA and operations manual. The type of tests carried out and results should be recorded and kept on board.*

As most classification societies use the IMO MSC/Circ. 645 or IMO MSC/Circ. 1580 principles as the basis for their own DP rules it will be a condition of class that the vessel has conducted DP annual trials.

MTS DP Operations Guidance - Part 1 gives further guidance and details on when annual trials should be conducted and what they should test:

> *4.8.4 Annual DP Trials:- A series of tests of fault and failure conditions relevant to the DP System. The tests should be designed to prove system redundancy, as defined in the DP FMEA, system and equipment functionality, to validate repairs and preventive maintenance, and test the operation of protection and detection devices and responses so as to demonstrate that the vessel's DP system remains fit for purpose. Annual DP Trials should be performed at a specific once a year within 3 months of the anniversary of the previous year's trials. Annual DP Trials also provide the opportunities for training of the vessel's crew and enhancement of their knowledge of failure modes and their effects.*

However it is IMCA's document Guidance for Developing and Conducting DP Annual Trials Programmes IMCA M 190 Rev. 2.1 January 2020 (paywall protected) that offers the most comprehensive description of the development, conduct and management of DP annual trial programmes for all types of vessels equipped with DP systems meeting the requirements of IMO equipment classes 1, 2 or 3. IMCA M190 states that the aims of annual DP trails should be to:

- *Demonstrate that the DP system is fully functional, performing as intended with full power and thrust availability;*
- *Verify the level of critical redundancy established by the FMEA;*
- *Verify the effectiveness of essential protective functions and alarms;*
- *Verify that the failure modes and effects of any modifications or upgrades are fully understood and incorporated into the FMEA and operational procedures;*
- *Meet the testing and survey requirements of IMO Guidelines for vessels with DP systems*
- *Meet the requirements of the classification society for annual and periodical renewal survey (as appropriate);*
- *Be an effective tool for verifying, updating and generally managing the FMEA, thereby avoiding the need to redo the FMEA.*

IMCA M190 further explains the methodology of an annual trials programme carried out on redundant systems as an attempt to prove that the three elements of

Performance;
Protection; and
Detection.

are present where required.

It should be noted that the guidelines in IMCA M190 allow for annual trials testing to be undertaken on an incremental basis throughout the year, providing the tests are completed within a twelve- month period. IMCA have recently released an Information Note (IMCA Information Note 1496) to clarify this position. IMCA notes that:

> *IMCA has become aware that some vessel owner/operators are undertaking a fixed percentage of an overall trials programme per year on the basis that over 5 years the full programme has been completed. This is not in compliance with IMO and IMCA guidelines Guidance for developing and conducting DP annual trials programmes (IMCA M 190).*

And reminds us that a DP annual trials programme is the overall programme of tests to satisfy the **annual** survey requirements of IMO MSC/Circ. 1580

IMCA DP PRACTITIONER ACCREDITATION SCHEME

IMCA M190 states that

> *5.2 Independent verification of testing intended to prove the integrity of systems where the consequences of failure can be severe is desirable.*

and tells us that the independent witnesses

> *should be sufficiently removed from day-to-day operational control or responsibility for the DP system and vessel. They should also be familiar with the vessel or type of vessel and with the DP annual trials programme.*

Further, IMCA M 190 recommends that the independent witness is accredited according to the IMCA DP Practitioner Accreditation Scheme.

GUIDANCE, PURPOSE, REQUIREMENTS, WHAT SHOULD BE DEMONSTRATED

MTS DP Operations Guidance - Part 1 defines field arrival trials as,

> *A series of checks and tests that confirm satisfactory performance of the DP system and verify the set up mode of operation and DP functions.*

and IMCA M103 states that

> *These checks should be carried out on arrival at the field and conducted outside the 500 metre safety zone. The checks should be repeated when the vessel returns to the field after an absence of more than 24 hours.*
>
> *The purpose of these checks is to ensure satisfactory operation of the DP system. The checks should include full functional checks of the operation of the thrusters, power generation, auto DP and independent joystick (IJS) and manual controls. The checks also ensure that the DP system is set up correctly and that the manning is adequate.*

IMCA issued a freely available *Information Note* in December 2022 offering guidance on what should be tested or checked during field arrival trials. This includes:

- ***Configuration/Location Checklist*** *– It is critical that the vessel configuration is verified as configurations can change during periods of transit. Many station keeping events reported to IMCA can be traced back to errors in power & DP systems configuration set-up, where if they had been checked prior to entering the field could have been avoided. The configuration should match the analysis of the vessels FMEA and the ASOG.*
- ***Generator and Thruster Testing*** *– Sufficient tests to ensure that equipment is operating as intended and be able to reach their rated capability.*
- ***UPS Load Function Test*** *– UPS is operating as intended and set up correctly. UPS function testing (i.e., taking load for 30 minutes) will have been completed at annual trials and/or as part of planned maintenance system.*
- ***DP Controller Change****-over – To verify that transfer of control does not affect the position and heading keeping ability of the vessel. This should preferably be carried out whilst the vessel is making a position change.*
- ***Operator Station Change****-over – To verify that transfer of control does not affect the position and heading keeping ability of the vessel.*
- ***Independent Joystick*** *– To ensure the control station is set up correctly and in the optimum location. All operators can competently take control of the IJS and manoeuvre the vessel. A practise regime for the IJS should already exist to ensure that all operators are capable of switching to and configuring the IJS for immediate use.*
- ***Thruster Manual Lever Check*** *– Function test the changeover to manual and levers. All operators are able to competently take control of the manual lever control and manoeuvre the vessel.*
- ***Backup DP Control*** *– If one or more remote operator terminals exist, they should remain connected, ready for use and frequently tested. Switching between main and back-up DP control station should be part of the field arrival check list.*
- ***E-Stops from Bridge*** *– Function test the (thruster) e-stops from the bridge, the stops should be located close to the operator.*

- ***Testing of PRS'S Selected*** *(where possible) – The vessel can conduct a rotation check to observe any unacceptable divergence of the available position reference systems and that they are not rejected. Blind spots in communications satellite links (providing differential corrections) are also confirmed and recorded.*

- ***DP Model Test*** *– When the vessel has been stable on DP under the control of the main DP system for thirty minutes (or reduced where considered not to have detrimental effect on the DP model), all position references are deselected from the main DP system and the mathematical model test is conducted. Position deviation over a period of 5 minutes to be logged, by observing the DGNSS systems. Critical alarms noted. This can be carried out on a similar heading that the vessel will be working in the upcoming DP Operations.*

- ***Communications*** *– All communications methods should be tested between all control and mission control stations, including back up communications. Test of DP Alert status where applicable.*

- ***Mode Changes*** *– Testing the various functionality of the DP system, in particular that which is relevant to the industrial mission.*

- ***Reset of Controllers and Operator Stations*** *– It's natural for a computer to start running more slowly if it has been left on for a long time and restarting it will usually speed things up and help fix potential emerging issues. A reboot will reset the software and flush the computer memory.*

DP Operations Guidance - Part 1 tells us that

> *DP Field Arrival Checklists to be kept on board for the period set by the owner/ operator and, where relating to a DP incident permanently stored in retrievable archives.*

DP NETWORKS (VARIOUS YEARS ACCORDING TO SECTION)

IMO MSC/Circular 1580 states that a DP control system means all control components and systems, hardware and software necessary to dynamically position the vessel *including networks*.

IMO MSC/Circular 1580 states that for equipment class 2 and equipment class 3 vessels

> *Single failure criteria include, but are not limited to:*
>
> *.1 any active component or system (generators, thrusters, switchboards, **communication networks**, remote-controlled valves, etc.); and*

DP NETWORK SYSTEM - OVERVIEW & THE RISKS, GUIDANCE AVAILABLE

A vessel management system (VMS) is a remote control, monitoring and alarm system which includes a range of automatic functions, and which may incorporate the PMS. In a centralised VMS all field connections are brought to a single point, typically in the engine control room. A centralised VMS may be appropriate for smaller less complex DP vessels but for larger DP vessels such as MODUs and construction vessels the use of distributed VMSs is now almost universal. (Note that unless a DP system is standalone, then most DP systems utilise the redundant VMS network to communicate with the thruster field stations to effect control and feedback of the thrusters.)

IMCA states that s distributed VMS offers many advantages including:

- *reduced control cabling;*
- *reduced failure effect;*
- *diversity of control locations;*
- *ease with which system can be split to match the redundancy concept.*

In a distributed VMS the hardware and software which controls / monitors equipment is in field stations positioned close to the equipment, reducing the length of cable runs. Each field station is connected to two separate communications networks via network hubs or switches. These switches connect together to form the network 'backbone'. Operator stations provide the human–machine interface (HMI) and are connected to the network in the same way as the field stations.

IMCA M103 states that the data communications network for a VMS is generally designed to be dual redundant and that,

> *The networks should be provided with a high degree of mechanical protection, particularly in areas of higher risk. In DP equipment class 3 designs there are requirements for physical separation and appropriate fire protection, including watertight integrity being maintained between the cable routes for each network. Some classification societies require similar physical separation for DP equipment class 2 designs.*

The use of industrial ethernet as a communications protocol is almost universal, typically utilising fibre optic connections. IMCA M103states that the advantages of fibre optic connections compared to copper wire are,

- *externally coupled noise immunity;*
- *bandwidth;*
- *preventing the transfer of electrical faults including those created by the effects of fire and flooding.*

Although triple redundant systems can be used, evidence suggests that those few incidents that have defeated the redundancy of dual networks would also have defeated triple redundant systems. The emphasis should therefore be to protect dual redundant networks against internal and external common cause failures rather than adding additional communications redundancy.

Vessel downtime associated with failure of Ethernet links can be addressed by carrying critical spares such as network switches and interface cards and by including spare fibre optic cores in the backbone cables which are already terminated and ready for use.

The vast majority of faults will be network switches failing (internally or power supply). This testing is easy to accomplish by the crew and should assist with fault diagnosis if a real fault should occur during active operations.

DP NETWORK SYSTEM - OPERATIONAL & FAILURE CONSIDERATIONS

Communication network failures have been identified in high profile incidents involving DP vessels over the years. The cause of several of these network failures was specifically attributed to a **netstorm.**

MTS – TECHOP ODP 08 Annual trials GAP analysis states that

> *"Network storms are a potential common mode failure capable of causing a drift off. All modern networks are fitted with protection against this type of failure. This protection must be checked periodically to confirm it is operational and that alarms to indicate that it is operating are working."*

A netstorm is an excessive amount of traffic, or more specifically, a flood of packets on the network. In a control system network scenario, the vastly increased number of packets can cause controllers to become overloaded, unable to handle their normal tasks – such as controlling a thruster (DP), monitoring shutdown conditions (ESD), or providing switchboard protection (PMS).

Netstorm hinders valid data packets on an Ethernet network in the same way. Successful delivery cannot be guaranteed under netstorm conditions. Packets can be lost or delayed to the point they are worthless. Such delay is not acceptable in a real-time control system.

A netstorm could affect different control systems in the following ways:

- A netstorm on a DP control system has the potential to cause a loss of position, this can occur due to reference system signals not being received by the controller, or thruster/rudder command signals not being delivered.
- A netstorm on a Thruster Control System (TCS) has the potential to cause a loss of position, this could occur due to a thruster field station stopping if the controller became overloaded.
- A netstorm on a Power Management System (PMS) has the potential to cause one or more generators to shutdown unintentionally, thus causing a partial or full blackout. This could result in a loss of position while on DP.
- A netstorm on an Emergency Shutdown System (ESD) system has the potential to cause unwanted shutdowns or inhibit a genuine shutdown command. This could result in a loss of position while on DP.
- A netstorm on an Integrated Automation System (IAS) system has the potential to cause loss of position while on DP, due to the integrated nature of systems, many signals can be affected, or not correctly processed if the controller became overloaded.

MTS – TECHOP ODP 08 Annual trials GAP analysis advises that

> *Comprehensive tests for a network storm should be carried out during FAT and FMEA proving trials to ensure that such an event cannot fail both networks."*

Note that while the switches have a possibility of malfunction and causing a netstorm this would be likely to occur on one of the two networks. The clients on the networks are generally controllers, HMI PCs etc and they are transmitting and receiving data from the networks. If they malfunction, then this could affect both networks simultaneously. It is important that all active nodes are checked/tested and that if any software updates are made, that netstorm resilience is also confirmed following such a change.

Netstorm testing is normally carried out by the supplier of the DP/VMS system.

However, there are several independent companies that offer such testing but often the DP suppliers will push back against such testing.

DP NETWORK SYSTEM - LESSONS LEARNT FROM DP EVENTS DP NETWORK SYSTEM

DP Event Bulletin	ITEMS
IMCA DP Station Keeping Bulletin 01/19 February 2019	Event 3: Planned investigation resulted in DP incident

PRACTICAL ONBOARD EXERCISE

Referring to MTS DP Techop D-12 Management of intermittent faults (TECHOP (D-12 - Rev1 - May23) MANAGEMENT OF INTERMITTENT FAULTS)

Consider the network storm examples 1 and 5 (3.5.1 and 3.5.6) and discuss if a similar event could occur on your own vessel.

Discuss what might be an appropriate course of action in the event of a total thrust loss in the event of a network storm, are there any other ways to control the vessel that are not reliant on the networks?

Find out when a Network Storm test was last done on your vessel.

ABOVE AND BEYOND

Review the document IMCA M 259 DP System Network Storm Guidance September 2022