MARINE TECHNOLOGY SOCIETY

DP VESSEL DESIGN PHILOSOPHY GUIDELINES

APRIL 2021

This Dynamic Positioning Guidance was created by the Dynamic Positioning Committee of the Marine Technology Society.

The guidelines have been developed from regulations, codes, guidance and industry practice existing at the time of publication, and their purpose is to aid in the safe management of DP operations. This publication was designed and intended as a resource for dynamic positioning professionals. For any other use beyond personal, research or educational purposes, please contact the Marine Technology Society.

DISCLAIMER AND LIMITATION OF LIABILITY

The information presented in this publication of the Dynamic Positioning Committee of the Marine Technology Society ("DP Committee") is made available for general information purposes without charge. The DP Committee does not warrant the accuracy, completeness, or usefulness of this information. Any reliance you place on this publication is strictly at your own risk. We disclaim all liability and responsibility arising from any reliance placed on this publication by you or anyone who may be informed of its contents.

IN NO EVENT WILL THE DP COMMITTEE AND/OR THE MARINE TECHNOLOGY SOCIETY,

THEIR AFFILIATES, LICENSORS, SERVICE PROVIDERS, EMPLOYEES, VOLUNTEERS,

AGENTS, OFFICERS, OR DIRECTORS BE LIABLE FOR DAMAGES OF ANY KIND UNDER ANY LEGAL THEORY, ARISING OUT OF OR IN CONNECTION WITH YOUR USE OF THE INFORMATION IN THIS PUBLICATION, INCLUDING BUT NOT LIMITED TO, PERSONAL INJURY, PAIN AND SUFFERING, EMOTIONAL DISTRESS, LOSS OF REVENUE, LOSS OF PROFITS, LOSS OF BUSINESS OR ANTICIPATED SAVINGS, LOSS OF USE, LOSS OF GOODWILL, LOSS OF DATA, AND WHETHER CAUSED BY TORT (INCLUDING NEGLIGENCE), BREACH OF CONTRACT OR OTHERWISE, EVEN IF FORESEEABLE.

THE FOREGOING DOES NOT AFFECT ANY LIABILITY WHICH CANNOT BE EXCLUDED OR LIMITED UNDER APPLICABLE LAW.

CONTENTS

TABLES

FIGURES

APPENDIX A EXAMPLE FMEA SPECIFICATION

ABBREVIATIONS

ABS	AMERICAN BUREAU OF SHIPPING
AC	ALTERNATING CURRENT
AFC	APPROVED FOR CONSTRUCTION
AI	ASSET INTEGRITY
AODC	ASSOCIATION OF OFFSHORE DIVING CONTRACTORS
API	AMERICAN PETROLEUM INSTITUTE
ASOG	ACTIVITY SPECIFIC OPERATIONAL GUIDELINES
AVR	AUTOMATIC VOLTAGE REGULATOR
BOP	BLOW OUT PREVENTER
BV	BUREAU VERITAS
CFD	COMPUTATIONAL FLUID DYNAMICS
CMF	COMMON MODE FAILURE
CP	CONTROLLABLE PITCH
CPP	CONTROLLABLE PITCH PROPELLER
DGNSS	DIFFERENTIAL GLOBAL NAVIGATION SATELLITE SYSTEM
DGPS	DIFFERENTIAL GLOBAL POSITIONING SYSTEM
DNV	DET NORSKE VERITAS
DP	DYNAMIC POSITIONING
DPCS	DYNAMIC POSITIONING & CONTROL SYSTEMS
DPO	DYNAMIC POSITIONING OPERATOR
DPS	DYNAMIC POSITIONING SYSTEM
DPVOA	DYNAMICALLY POSITIONED VESSEL OWNERS ASSOCIATION
DSV	DIVING SUPPORT VESSEL
EARTH	GROUND
ECR	ENGINE CONTROL ROOM
ER	ENHANCED RELIABILITY
ESD	EMERGENCY SHUTDOWN SYSTEM
F & G	FIRE & GAS
FAT	FACTORY ACCEPTANCE TEST
FMEA	FAILURE MODES AND EFFECTS ANALYSIS
FMECA	FAILURE MODE EFFECT AND CRITICALITY ANALYSES
FOG	FIBRE OPTIC GYROS
FPP	FIXED PITCH PROPELLER
FPSO	FLOATING PRODUCTION STORAGE OFFTAKE
FSVAD	FLAG STATE VERIFICATION & ACCEPTANCE DOCUMENT
FW	FRESH WATER
GA	GENERAL ALARM
GNSS	GLOBAL NAVIGATION SATELLITE SYSTEM
GPS	GLOBAL POSITIONING SYSTEM
GROUND	EARTH
HAT	HARBOUR ACCEPTANCE TEST
HAZOP	HAZARD AND OPERABILITY
HDOP	HORIZONTAL DILUTION OF POSITION
HIL	HARDWARE IN LOOP
HMI	HUMAN MACHINE INTERFACE
HSE	HEALTH, SAFETY AND ENVIRONMENT
HSI	HUMAN SYSTEM INTEGRATION
HV	HIGH VOLTAGE, GENERALLY VOLTAGES OVER 1000 VOLTS

ABBREVIATIONS

HVAC	HEATING VENTILATION AIR CONDITIONING
I/O	INPUT/OUTPUT
IAN	INERTIAL AIDED NAVIGATION
IEC	INTERNATIONAL ELECTROTECHNICAL COMMISSION
IJS	INDEPENDENT JOYSTICK
IMCA	INTERNATIONAL MARINE CONTRACTORS ASSOCIATION
IMO	INTERNATIONAL MARITIME ORGANISATION
IRM	INSPECTION REPAIR AND MAINTAINABILITY
LBL	LONG BASELINE
LCI	LOAD COMMUTATED INVERTER
LIFE	LOW IMPACT FAILURE EFFECT
LLRC	LOW LOSS REDUNDANCY CONCEPT – See LIFE
LRS	LLOYDS REGISTER OF SHIPPING
LUSBL	LONG ULTRASHORT BASELINE
LV	LOW VOLTAGE, GENERALLY VOLTAGES BELOW 1000 VOLTS
MOC	MANAGEMENT OF CHANGE
MODU	MOBILE OFFSHORE DRILLING UNIT
MOU	MOBILE OFFSHORE UNIT
MRU	MOTION REFERENCE UNIT
MSC	MARITIME SAFETY COMMITTEE
MTBF	MEAN TIME BETWEEN FAILURE
MTS	MARINE TECHNOLOGY SOCIETY
MTTR	MEAN TIME TO REPAIR
NMD	NORWEGIAN MARITIME DIRECTORATE
OIM	OFFSHORE INSTALLATION MANAGER
OSV	OFFSHORE SUPPORT VESSEL
PA	PUBLIC ADDRESS
PLC	PROGRAMMABLE LOGIC CONTROLLER
PMS	PLANNED MAINTENANCE SYSTEM
PRS	POSITION REFERENCE SYSTEM
PSU	POWER SUPPLY UNIT
PWM	PULSE WIDTH MODULATION
QCV	QUICK CLOSING VALVE
RAO	RESPONSE AMPLITUDE OPERATOR
RCA	REDUNDANCY AND CRITICALITY ANALYSES
RCU	REMOTE CONTROL UNIT
RESTRICTED EARTH FAULT PROTECTION	DIRECTIONAL EARTH FAULT PROTECTION
RIO	REMOTE INPUT OUTPUT
ROV	REMOTELY OPERATED VEHICLE
RPM	REVOLUTIONS PER MINUTE
SAT	SEA ACCEPTANCE TEST
SCE	SAFETY CRITICAL ELEMENTS
SIL	SAFETY INTEGRITY LEVELS
SIMOPS	SIMULTANEOUS OPERATIONS
SMO	SAFEST MODE OF OPERATION
SOLAS	SAFETY OF LIFE AT SEA
STCW	STANDARDS OF TRAINING CERTIFICATION AND WATCH KEEPING

ABBREVIATIONS

SW	SEAWATER
TAGOS	THRUSTER AND GENERATOR OPERATING STRATEGY
TAM	TASK APPROPRIATE MODE
TCPC	TRAINING, CERTIFICATION & PERSONNEL COMPETENCE
THD	TOTAL HARMONIC DISTORTION
TTT	TIME TO TERMINATE
UKCS	UK CONTINENTAL SHELF
UPS	UNINTERRUPTED POWER SUPPLY
USBL	ULTRA SHORT BASE LINE
VAr	VOLT AMPERE REACTIVE
VCB	VACUUM CIRCUIT BREAKER
VFD	VARIABLE FREQUENCY DRIVES
VRU	VERTICAL REFERENCE UNIT
VRU	VERTICAL REFERENCE UNIT
WCF	WORST CASE FAILURE
WCFDI	WORST CASE FAILURE DESIGN INTENT
WSOG	WELL SPECIFIC OPERATIONAL GUIDELINES

1 INTRODUCTION

1.1 PURPOSE

1.1.1 This document has been generated by the MTS DP Technical Committee and has been provided to industry as a guidance document to aid in the design of DP Vessels.

1.1.2 This document is not meant to replace any rules, regulations or guidelines that are in existence. It is a compilation of experiences, practices and information gleaned from various sources in industry, some of which are not in the public domain. It is expected that compliance with applicable Class Rules will be ensured.

It is acknowledged that requirements for DP class notations are governed by class rules for DP systems which address DP system redundancy. However, these rules do not address the industrial mission of the vessel nor the overall performance and operational capability. Consequently, vessels designed to satisfy minimum requirements for a DP class notation alone may not achieve the post worst case failure capability that could be achieved by establishing and adopting philosophies that minimize loss of DP capability after failure and also enhance reliability.

1.1.3 This is not intended to be an all-encompassing document covering all aspects of DP vessel design. It attempts to provide guidance on a number of themes which have not been adequately defined by DP class rules or are subject to interpretation. Incorporating the guidance provided in this document during design should result in a vessel with enhanced capability to perform its industrial function and which meets class rules for the desired DP class notation.

1.1.4 Enhanced vessel capability, as implied in this document, means a more fault tolerant / fault resistant DP system which minimizes loss of positioning capability post worst-case failure. This in turn translates into greater operational uptime and the ability to carry out its mission within a larger operating envelope.

1.1.5 The focus areas of this document have evolved from industry experience of technical failures. Addressing these vulnerabilities during design will result in a robust vessel capable of conducting its industrial mission. Exposure to environmental conditions is addressed by focusing on capability and sizing of thrusters and power plants. Technical failures are addressed by designing fault tolerant and fault resistant systems. Some technical faults require operator intervention to prevent escalation. It should be recognized that undue reliance on operator intervention should be avoided as it is not as effective a barrier or control mechanism as designing the fault out. Ergonomics and ‘decisions support tools’ aid operator intervention.

1.1.6 Implementation of the guidance during design phase rather than later in the lifecycle is expected to lower the cost of a ‘fit for purpose’ DP vessel.

1.1.7 The guidance provided in this document is not directed towards any particular category of DP vessel. It is intended to apply to any Class 2 or Class 3 DP vessel operating in support of offshore oil and gas activities (many principles will be applicable to other industries). Examples include MODUs, MOUs, construction and logistics vessels where dynamic positioning is used for, or aiding, station keeping.

The principles may be implemented as appropriate on DP Class 1 vessels.

1.2 GENERAL GUIDANCE

1.2.1 The guidance provided in this document is intended to aid in the design of a fault tolerant, fault resistant DP vessel. It is intended to apply to any class of DP vessel operating in support of offshore oil and gas activities. The goals of the guidance are to promote designs that:

1. **Prevent loss of position.**
2. **Prevent loss of redundancy***

**limit the potential for the vessel to become non-fault tolerant and have to suspend operations.*

The objectives of the above are to maximize operational uptime while meeting class requirements.

1.2.2 The industrial mission of DP vessels varies. Examples as follows:

1. DP MODUs.
2. Project construction vessels.
3. Logistics vessels.

1.2.3 Fault tolerant power systems can be achieved by the use of sophisticated protective functions or by configuring the power plant as two or more independent systems (open bus). Design should always facilitate predictable incident free operations in all power plant configurations (open and / or closed bus operations).

1.2.4 It is acknowledged that the level of sophistication and complexity required to achieve fault tolerance, fault resistance and uptime for DP MODUs and project construction vessels is likely to be higher than that normally applied to logistics vessels with conventional power plants due to the nature of their industrial mission.

1.2.5 Hybridization of power plants may require closed bus configuration to maximize its benefits. Designs which rely on closed bus configurations should address verification and validation of attributes of fault tolerance, fault resistance and fault ride-through and not rely solely on the attributes of resilience that is provided by hybrid power.

1.2.6 It should be recognized that power plants need a larger level of integration than other components of DP systems. Care should be exercised in the concept and design phase of power systems to clearly establish the needs of the industrial mission, requirements of the Regulatory/Classification bodies and to define the system for all aspects of the project life cycle.

1.2.7 All vessels should be operated within their post failure DP capability as determined by their Worst-Case Failure (WCF). The WCF that was used as the basis of design is termed the Worst-Case Failure Design Intent (WCFDI) .

1.3 LAYOUT OF THE DOCUMENT

1.3.1 Previous revisions of this document were in two parts. Part 1 was a high-level guide for managers explaining why each theme is important. Part 2 contained additional details on how to address these themes along with anecdotal examples. This format has been replaced by a single part document in this revision.

1.3.2 The level of detail in the sections on power (generation, distribution and power management / vessel management) is deliberately and consciously greater than that provided in other sections. A well thought through power system design delivers a robust and capable vessel and enhances the ability of the vessel to perform its industrial mission.

1.3.3 Note: *The term ‘power system’ includes auxiliary systems and related pipework.*

2 DEFINITIONS

2.1 GENERAL

1. **Reliability:** The probability that an item can perform a required function under given conditions for a given time interval.
2. **Redundancy:** The existence of more than one means of performing a required function.
3. **Full redundancy:** A system comprising two or more redundant elements each of which is capable of performing the function.
4. **Partial redundancy:** A system containing three of more redundant elements which are capable of performing the function in combination (e.g. Any two-out-of-three)
5. **Availability:** The ratio of the total time a functional unit is capable of being used during a given interval to the length of the interval.
6. **Single fault tolerance:** The ability of a system to continue its function, following a single failure, without unacceptable interruption.
7. **Autonomy:** The ability of items of main machinery such as generators and thrusters to make themselves ready for DP without the need for hierarchical control. The use of the word autonomy here should not be confused with its use in applications such as self-driving ships and vehicles.
8. **Independence:** With reference to main machinery such as generators and thrusters. Auxiliary and control functions should be provided in a manner that makes the machinery as independent as practical to minimize the number of failures that can lead to the loss of more than one main item of machinery.
9. **Segregation:** With reference to systems or equipment intended to provide redundancy. Reduce the number of connections between systems to reduce the risk that failure effects may propagate from one redundant system to the other.
10. **Physical separation:** With reference to DP Class 3 vessels, fire and watertight subdivisions required to support the worst-case failure design intent in respect of DP 3 failure criteria.
11. **Monitoring:** Alarms and indications required to reveal hidden failures. Monitoring should be of a design and implementation that positively identifies a fault or degradation of functionality in the system e.g. lack of flow not just loss of pressure.
12. **Critical redundancy:** Equipment provided to support the worst case failure design intent.
13. **Non critical redundancy:** Equipment provided over and above that required to support the worst-case failure design intent. Its purpose it to improve the reliability and availability of systems.
14. **Industrial Mission:** The industrial mission is the primary operational role of the vessel, typically applicable to MODUs and Project and Construction vessels. (e.g. Pipe-lay/Heavy-lift). (Note Industrial mission by definition for Logistic Vessels is to support logistics).
15. **Diversity:** The property of introducing differences into redundant elements to avoid common mode, common cause failures. Different levels of diversity are possible such as specifying different manufacturers for redundant GNSS systems. Even greater diversity can be achieved through orthogonality which requires redundant elements to operate on different principles.

16. **Orthogonality:** With reference to redundant systems, the secondary means of providing a function should be based on completely different principles to reduce the risk of common mode failures. (e.g. Gyros-spinning mass versus Fibre Optic Gyros (FOG), anemometers (ultrasonic versus mechanical).
17. **Differentiation:** A method to avoid common mode failures by introducing a change in personality of redundant systems based on the same principle. (e.g. use of Inertial Aided Navigation (IAN) on one of the two redundant GNSS systems)
18. **Suitability:** In this document 'suitability' pertains to the vessel having the appropriate position reference sensors to undertake its industrial mission.
19. **Position/heading keeping:** The ability of the DP system to maintain a desired position and/or heading within the normal excursions of the control system and environmental conditions.
20. **Loss of Position**: The vessel's position is outside the limits set for carrying out the industrial activity in progress as defined in the WSOG/ASOG.
21. **Thruster Phase back:** A method utilized to temporarily reduce power consumption following an event, to stabilize the power plant and avoid a black-out.
22. **Critical Activity Mode of Operation (CAMO / CAM):** This is generally a tabulated presentation of how to configure the vessel's DP system, including power generation and distribution, propulsion and position reference systems, so that the DP system, as a whole is fault tolerant and fault resistant. The CAMO table also sets out the operator actions should the required configuration fail to be met. The term Safest Mode of operation (SMO) has been previously used to describe CAMO. CAMO is often shortened to CAM in practice.
23. **Systematic failure:** Failures due to flaws in the system. Systems subjected to the same conditions fail consistently.
24. **Wear out:** Specific class of failure when an item of limited life has worn out.
25. **Random failure:** Failure due to physical causes such as corrosion, thermal stressing. Statistical information can be derived from historical data.
26. **'Task Appropriate Mode' (TAM) is a risk based mode:** Task Appropriate Mode is the configuration that the vessel's DP system may be set up and operated in, accepting that a failure could result in effects exceeding the worst case failure such as blackout or loss of position. This is a choice that is consciously made. This mode may be appropriate in situations where it is determined that the risks associated with a loss of position are low and where the time to terminate is low. (Not to be confused with Thruster Assisted Mooring)
27. '**Active redundancy':** Redundancy wherein all means for performing a required function are intended to operate simultaneously.
28. **WCFDI:** The worst-case failure design intent (WCFDI) describes the minimum amount of propulsion and control equipment remaining operational following the worst-case failure. The worst-case failure design intent is used as the basis of design. Single fault tolerance is to be achieved by the provision of redundant systems. In a successful design WCF = WCFDI.
29. **Time to Terminate:** Time to safely terminate (operations) means the amount of time required in an emergency to safely cease operations of the DP vessel.

3 FOUNDATIONAL ELEMENTS OF DP SYSTEM DESIGN TO ACHIEVE PREDICTABLE OUTCOMES

3.1 DP DESIGN ICONOGRAPHY

3.1.1 The development of the MTS guidance documents and TECHOPs has been an evolutionary process which incorporates elements which address the themes of:

- Design
- Operations
- People
- Process

3.1.2 The evolutionary process revealed that the objectives of delivering predictable incident free DP operations requires a holistic view. This view is underpinned by integrated approaches, including systems thinking and systems engineering. However, it became apparent that the terms referred to above had different connotations which inadvertently fostered preconceived notions. The use of the terms in this document is explained in more detail in the sections that follow.

3.1.3 A form of iconography resulted from this evolutionary process which has proved effective in communicating foundational principles.

3.1.4 The terms that have become an integral part of the vocabulary are:

- Integrated thinking (Communicated as ‘three pegs’ thinking).
- The seven pillars (essential attributes to be addressed in DP design).
- Performance, protection and detection.
- Basis of confidence.
- Defense in depth.
- Effective verification and validation.
- Pragmatic and effective risk management (Barriers and Barrier management philosophy).
- Comprehension aided compliance.

3.1.5 The iconography depicted in the figures that follow has been used to visually communicate the evolved vocabulary.

3.2 DESIGN FUNDAMENTALS

3.2.1 **Predictability:** Predictability is one of the foundational tenets that has been found to aid in the delivery of incident free DP operations. It has not been necessary to adapt the definition of predictability as the dictionary meaning ‘behaving or occurring in a way that is expected’ is appropriate.

In order to achieve the desired outcomes i.e. predictable incident free DP operations, immediate failure effects, intermediate failure effects and end effects (with reference to generators and thrusters) should be predictable. This facilitates the development and implementation of effective and verifiable mitigations.

3.2.2 The phrase 'the three Rs' have been adapted to DP to mean:

- Redundancy
- Reliability
- Resilience

Redundancy: The ability of a system to restore or maintain its function following a failure

Reliability: The ability of a system to remain in operation for a specified period of time without malfunction.

Resilience: The ability of a system to withstand a failure and to continue in operation following failure. It may include the ability to recover from a failure without suffering significant damage.

Cautionary note 1. An oft observed vulnerability in designs is the presence of cross connections between redundancy groups. Introductions of such cross connections are usually well-intentioned attempts to enhance fault tolerance. However, the potential for such cross connections to serve as fault propagation pathways (capable of failure effects exceeding the severity of the worst-case failure design intent) is often not recognized or understood and this is reflected in the lack of comprehensive analysis, verification and validation.

Cautionary note 2: The temptation to equate the term robustness to the three 'Rs' should be avoided. Equipment performance indicators may mask the potential for equipment to fail catastrophically beyond a point where resilience is compromised, and failure effects exceed the worst-case failure design intent with no possibly of recovery. (example, automatic blackout recovery)

3.2.3 **Control, monitoring and protection:**

Good engineering practice promotes the concept of maintaining clear segregation between systems intended to provide:

- Control
- Monitoring
- Protection

Control system failure - The rational for the practice of ensuring independence of protection and control systems is to ensure that there are no common cause failures that can cause a system to become 'out-of-control' and, at the same time, disables the protection intended to mitigate the effects of such a control malfunction. Example, an engine governor requires 110Vdc from the protection system power supply. If the 110Vdc power fails, the governor fails to full fuel and the generator incomer and bustie circuit breaker lose their ability to trip the faulty generator offline or open the bustie. The entire power system blackouts out on over frequency.

Protection systems failure - Similarly, if protection systems have failed, it is imperative that there are no dependencies that also cause the control systems to fail.

Monitoring system failure - If the monitoring system fails it may not be possible to observe its operation but at least the system remains under control and protection systems remain operational to isolate the effects of any malfunction.

These objectives require additional engineering resources, greater attention and caution to validate and verify when the control, monitoring and protection systems are heavily integrated in hardware and / or software.

3.2.4 **Performance, Protection and Detection:** These are essential attributes of any fault tolerant system based on redundancy and the significance of proving these attributes throughout the life cycle cannot be under estimated. See Figure 3-1:

- **Performance:** Elements of the system intended to provide redundancy must have equivalent performance in all redundancy groups. Where equivalent performance is lacking, the overall system capability (intact and post failure capability) is determined by the system that has the lowest performance. It is imperative to detect loss of performance in all systems contributing to redundancy so that the effects on post failure DP capability can be understood.
- **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. It is imperative to detect faulty protection systems that are designed to prevent fault propagation before the faults they are designed to isolate occur.
- **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. Station keeping risk is typically managed by suspending DP operations when the DP system loses its fault tolerance. Each redundant DP equipment group must be sufficiently reliable to ensure that the risk of a failure in the surviving redundant groups is low enough to have a high degree of confidence that there will be no further failures in the time it takes to bring the DP operation to a safe conclusion.

3.2.5 **Independence and fail safe**

These attributes are a fundamental objective of fault tolerant systems based on redundancy.

- Independence between equipment groups intended to provide redundancy ensures they are not subject to a common cause of failure. In the context of this document, this essentially means no drift off.
- In the context of this document, ‘Fail safe’ refers to a post failure state that does not lead to a drive-off.

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 overspeeding, 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.

- **Hidden failure:** Hidden failures have the potential to defeat the redundancy design intent. Failure of dormant/on demand functions such as standby redundancy and protection systems are examples of potential hidden failures.
- **Means of detection and compensating provisions:** Compensating provisions are barriers to escalation of failure effects and must be maintained as part of the principle of defense in depth.
- These terms describe elements of the FMEA process that describe the way in which the documented failure effects are prevented from becoming more severe. Using the cable fault example:
    - The compensating provisions in the case of a short circuit fault would be existence of the redundant DP equipment group, the correct operation of the overcurrent protection and the fault ride-through capability of all the other DP essential consumers exposed to the voltage excursions associated with clearing the fault.
    - In the case of the open circuit the compensating provision would be the presence of the redundant equipment group and the alarm and monitoring that indicated the loss of the equipment in which the fault occurred.
    - In the case of the ground fault the compensating provisions are the alarm and monitoring functions that indicate the presence of one ground fault. Without these provisions, this detection system a second ground fault may occur on the other phase creating a short circuit. The effects of a short circuit are more severe and the compensating provision for that failure mode must be effective.

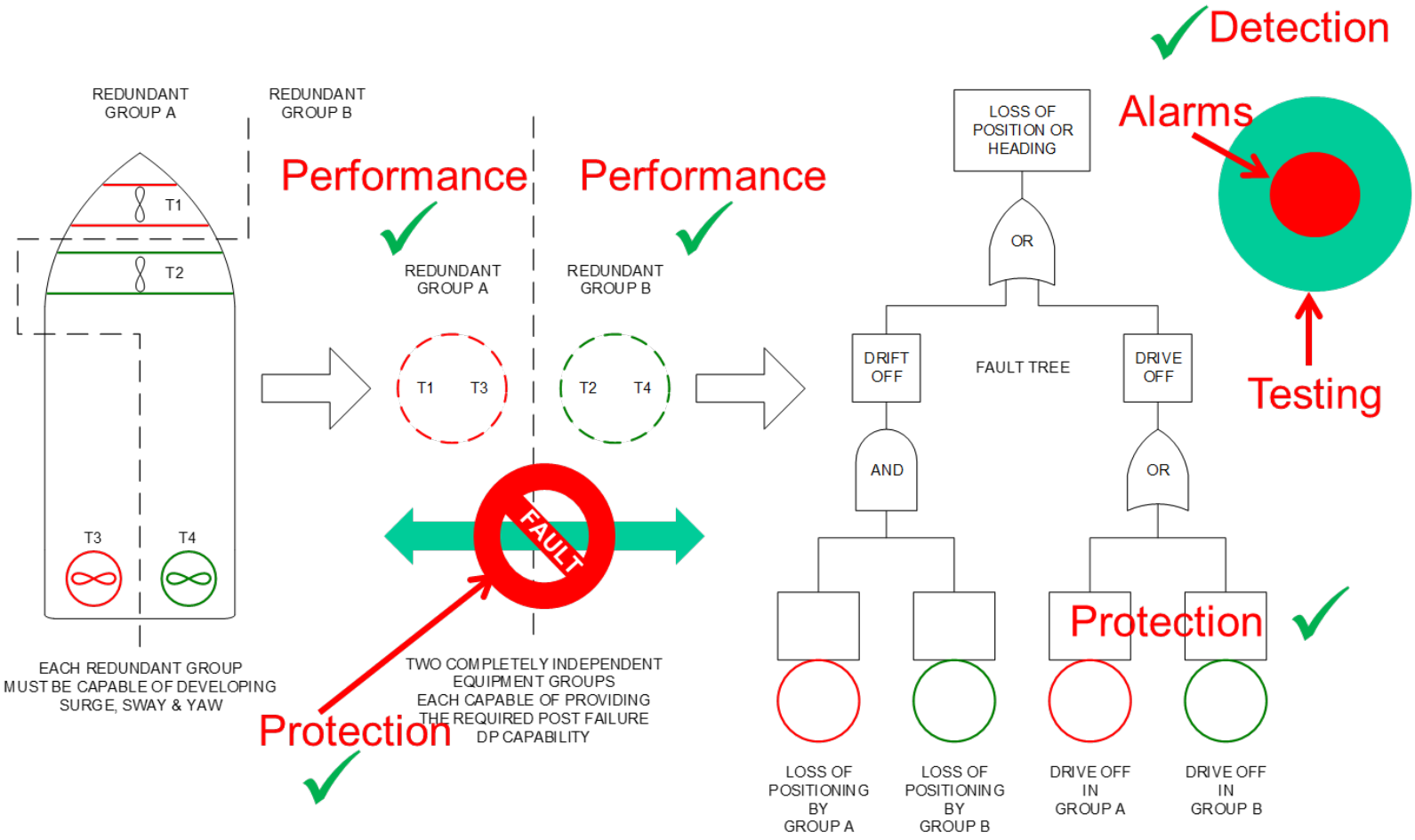


Figure 3-1 Key Elements of Redundancy Concept

3.3 THREE PEGS THINKING

3.3.1 Three pegs thinking or the concept of 'the three pegs' has been developed to provide a system engineering based approach to the verification and validation process. The concept can be adapted and applied through various methodologies that satisfy each peg.

3.3.2 The three pegs are:

1. Intent / Objective
2. Basis of Confidence
3. Defense in Depth

3.3.3 These have been developed as a means to intuitively communicate the following concepts:

- The intent and objective including:
  - The need to emphasise and maintain an objective and outcome focus.
  - The means to augment hitherto compliance-based approaches with comprehension to achieve desired outcomes i.e. predictable incident free DP operations (comprehension aided compliance).
- Integrated thinking (the basis of confidence is established on comprehensive, intuitive and transparent verification and validation)
- Pragmatic and effective risk management relies on adopting robust and effective barriers and establishing an achievable barrier management philosophy.

3.3.4 Three pegs thinking has been adapted to achieve desired outcomes predictably in areas other than DP.

3.3.5 Figure 3-2 below graphically represents 'three pegs' thinking:

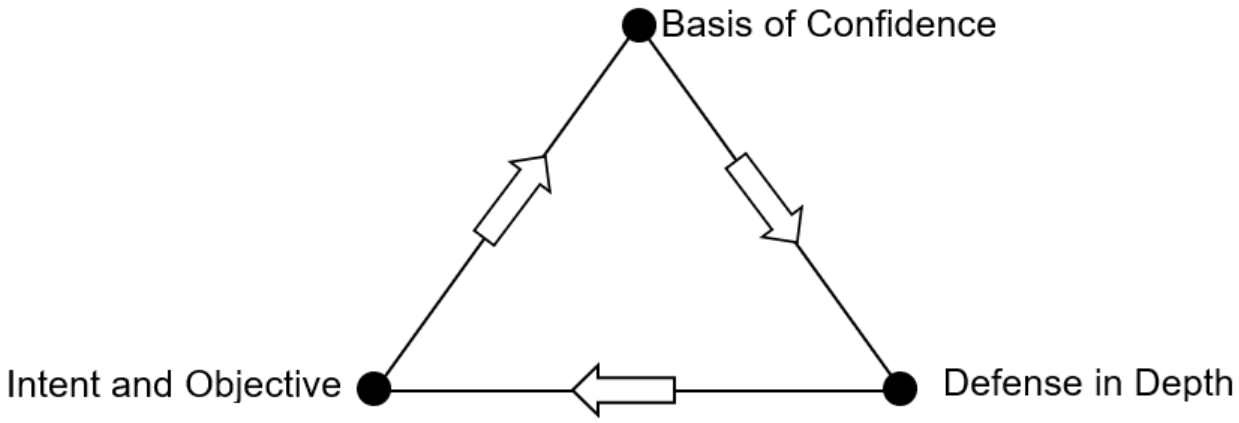


Figure 3-2 Three Pegs Thinking

3.3.6 The ‘three pegs’ as applied to DP is described as below:

3.3.7 **Intent and objective**

The intent is defined as ‘delivering incident free DP operations’:

- Objectives are to be focused on as ‘leading indicators’ to help ensure that the DP system is:
  - Reliable
  - Robust
  - Resilient
- Efficiency (e.g. no non-productive time)
- Unreasonable cognitive burden should not be imposed on operational teams (data / information presented should be intuitive and not lead to erroneous decisions).

3.3.8 **Basis of Confidence**

Basis of confidence as applied in a DP context is everything that is done to provide reasonable confidence that the objective will be achieved. Effective verification and validation are essential to establish the basis of confidence. Activity / focus area examples to which verification and validation are to be applied:

- Good vessel and DP system design (industrial mission focus maintained).
- Fault tolerant DP systems.
- FMEAs and supporting studies (including proving trials).
- Periodic verification (Example annual trials, post failure verification and validation activities).
- Periodic drills for operator intervention evaluation.
- Effectiveness of procedures, processes, decision support tools (enablers to supplement personnel ability to deliver predictable incident free DP operations).
- Identification and effectiveness of the barriers to loss of position.

3.3.9 **Defense in depth**

Defense in depth is the term applied to keeping the barriers strong. The term has been introduced to ensure that people are cognizant of the need for barriers to be strong if they are to be depended upon as compensating measures.

It is also essential to recognize that merely increasing the number of barriers may not be effective if attention is not devoted to keeping those barriers strong. Additionally, an increase in the number of barriers will increase the burden of ensuring ’defense in depth’ of those barriers. Care should be taken to ensure that the barriers themselves are not reliant on a number of dependencies. Care should be taken in design of barriers to ensure that the barriers themselves are robust and resilient to failures and acts of maloperation.

Examples of applying barriers and barrier management philosophy to verify and validate the strength and resilience of barriers include:

- Periodic Inspection and survey
- Field arrival trials
- Annual DP trials
- Renewal trials
- Planned maintenance.
- Gap analysis – new knowledge and learnings from incidents
- Embedment of the 'healthy to operate philosophy' by design.
- Crew familiarization and training (vessel specific and industrial mission focused).

3.3.10 Barrier management philosophy may appear to be an abstract term. It is to be recognized that there is a hierarchy of effectiveness in barriers. The hierarchy is described in the following sketch.

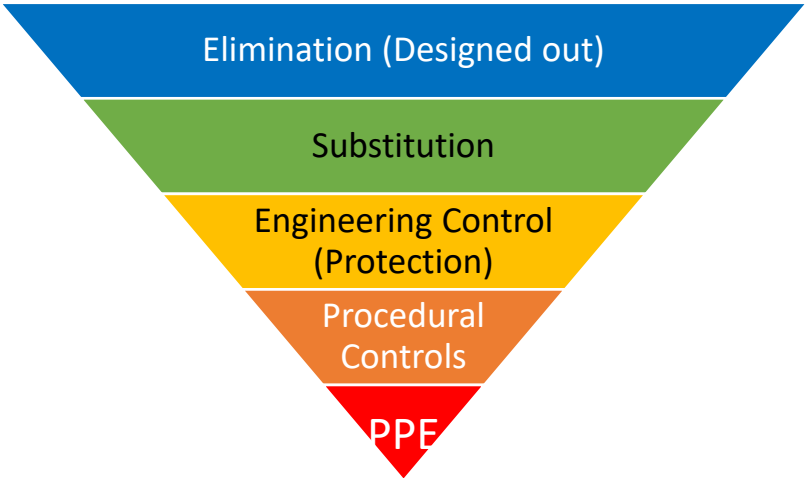


Figure 3-3 Hierarchy of Controls

3.3.11 An example of application of an effective barrier management philosophy is the conscious enhancement of the built-to-test philosophy to achieve the 'healthy-to-operate' outcomes. This is depicted in the iconography as the 'staircase'.

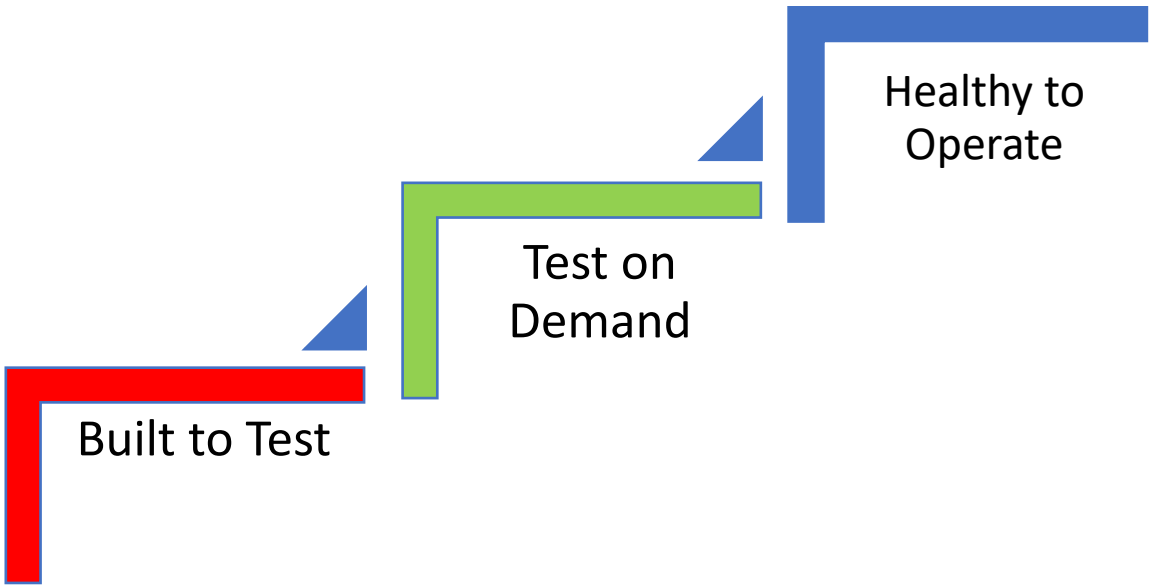


Figure 3-4 Stairway to DP Heaven

3.3.12 Design / build to test

Testing is an essential part of effective verification and validation. The ability to achieve effective verification and validation is often compromised by the fear of testing and typically justified by citing fear of damage to equipment.

Such concerns (real or imagined) should be addressed. Equipment deployed for use on DP vessels should be designed and built to be tested (Initial acceptance testing and periodic verification & validation testing over lifecycle).

3.3.13 Test on demand capability

Experience from conducting testing as a part of effective verification and validation has established that there is a burden associated with such activities. Resistance to carry out such testing is to be expected particularly If the burden of testing requires time away from industrial mission operations and / or imposes a burden on the resources required to conduct the testing.

Data centric approaches and Built In Test Equipment (BITE) have been developed and implemented to alleviate the burden of testing. Such approaches have been termed as test-on-demand capability.

3.3.14 Healthy to operate

Technological advances in sensors and communications / data loggers, accompanied by improved cost effectiveness, have overcome barriers / legacy thinking to foster more data centric approaches. The ability to analyses vast amounts of data in almost real time and provide a level of insight not achievable before has opened up opportunities to move away from scheduled based maintenance and verification & validation carried out on a periodic basis either to establish the basis of confidence or restore the basis of confidence following an unpredicted event or failure. Condition based monitoring and maintenance schedules based on condition-based monitoring are increasingly becoming the accepted norm. The ability to continuously monitor performance characteristics and identify divergences to provide insights are not being leveraged to develop and implement the concept of healthy to operate. The healthy to operate philosophy uses self-diagnosing capability to establish a higher level of confidence as divergences from the nominal conditions are made visible. A dip in confidence levels will trigger a response, usually in the form of additional verification and validation activities to restore confidence.

This progression from design / 'build-to-test' to 'healthy-to-operate' has been characterized as the 'staircase' in the iconography. Implementation of the staircase methodology along with the seven pillars has demonstrated the ability to enhance the hierarchy of controls from engineering controls to designing it out.

3.4 SEVEN PILLARS

3.4.1 The Seven Pillars is the term given to a series of seven desirable attributes. These are shown in Figure 3-5 and described in more detail below.

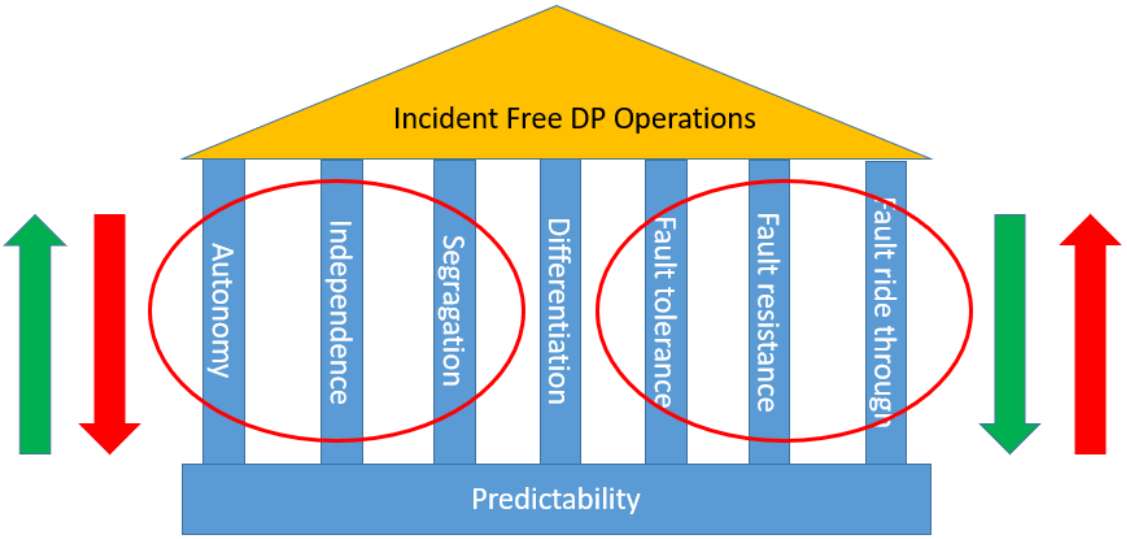


Figure 3-5 Seven Pillars

3.4.2 It is apparent, when considering the influence of the various pillars, that they fall into two distinct groups. The three pillars on the left are dominant in designs with very few cross connections and therefore fault propagation paths between equipment groups intended to provide redundancy. The three pillars on the right are required when there are fault propagation paths to be mitigated. Focus on the left diminishes the need for the attributes on the right. But the reverse becomes true when cross connections are introduced. The attributes on the right (fault resistance, tolerance and ride-through) also introduce an additional Lifecyle test burden to prove they are still effective.

3.4.3 **Autonomy**: Modern DP vessels are complex machines with several layers of automation. Experience suggests that there are benefits to be derived from making generators and thrusters independent in the provision of auxiliary support services and control functions. Designs should be resistant to internal and external common cause and common mode failures. Designs in which the control function has been decentralized are considered to be more fault tolerant. In such designs, each major item of machinery is responsible for making itself ready for operation and ensuring that all necessary services are online. In addition, control system failure effects are less likely to exceed loss of the associated engine or thruster. In a centralized system, it can be more difficult to prove that the effects of failure do not exceed the worst case failure design intent. This is an important consideration when choosing a control system topology for fault tolerant systems. There is still a requirement for a remote-control system in decentralized designs, but the functions of this control layer are limited to scheduling and remote manual control.

3.4.4 **Independence:** Items of main machinery should be provided with all the control systems, services and auxiliary systems they require so that failure effects of support services are limited to the loss of one item of main machinery (typically one generator or one thruster).

3.4.5 **Segregation:** DP system design should ensure Independence between redundant DP equipment groups. The number of connections between redundant equipment groups should be minimized.

3.4.6 **Orthogonality, Diversity and Differentiation:**

3.4.7 Diversity can improve the fault tolerance in system designs based on redundancy. Different degrees of diversity are possible such as choosing equipment from different suppliers or using different principles of operation (orthogonal design).

3.4.8 In the field of reliability engineering the term orthogonal design indicates that a completely different method has been used to provide redundancy from that used as the primary method. Orthogonality in design can reduce the risk of common mode failures in redundant systems compared to systems using identical redundant elements.

3.4.9 DP class rules require orthogonality in measurement methods used for position references. A minimum of three position references are required for DP class 2 and DP class 3. Two of these three should be based on different measurement principles.

3.4.10 It is good practice to have orthogonality in sensors such as gyros, anemometers and MRUs. Different measurement principles (orthogonality) offers the greatest advantages but where this is not practical a diversity of manufacturers can be desirable.

3.4.11 Differentiation can reduce the risk of common mode failures. Differentiation can be achieved on redundant position reference systems operating on the same principle by combining one of the position references with position information from an inertial navigation system to create Inertial Aided Navigation (IAN). (e.g. Inertial Aided DGNSS or Inertial Aided Acoustic Systems). IAN changes the characteristics of how the reference behaves and minimizes the probability of both (IAN and non-IAN) systems being rejected. IAN can also be known as INS (Inertial Navigation Systems).

3.4.12 **Fault tolerance:** Single fault tolerance is to be achieved by design. Fault tolerance can be achieved through clear segregation of equipment into well-defined redundant equipment groups or by the use of protective functions. Taking the latter approach has the potential to significantly increase the burden required to periodically prove the fault tolerance of the DP systems with consequential exposure to non-productive time.

3.4.13 **Fault resistance:** Components and systems can be designed in such a way that they are less likely to fail in the application for which they are being used. They should be suitable for the temperatures, vibration, humidity and saliferous atmosphere in which they operate. Improving the reliability of equipment reduces reliance on the protective functions and performance attributes of the other redundant equipment groups. These protective functions and performance attributes have the potential to become disabled / affected by hidden failures.

3.4.14 **Fault ride-through:** Ride-through is the property of a system or component that allows it to remain in operation or recover its function naturally during and after the period when protective functions are operating to isolate potential fault propagation paths (or discrimination failures). The severe voltage excursions associated with the operation of overcurrent protection is a very typical example of a condition which requires ride through capability.

3.5 MTS COMBINED ICONOGRAPHY

3.5.1 MTS has combined the elements and vocabulary discussed above are combined into a common iconographic representation for ease of communication. See Figure **3-6** below.

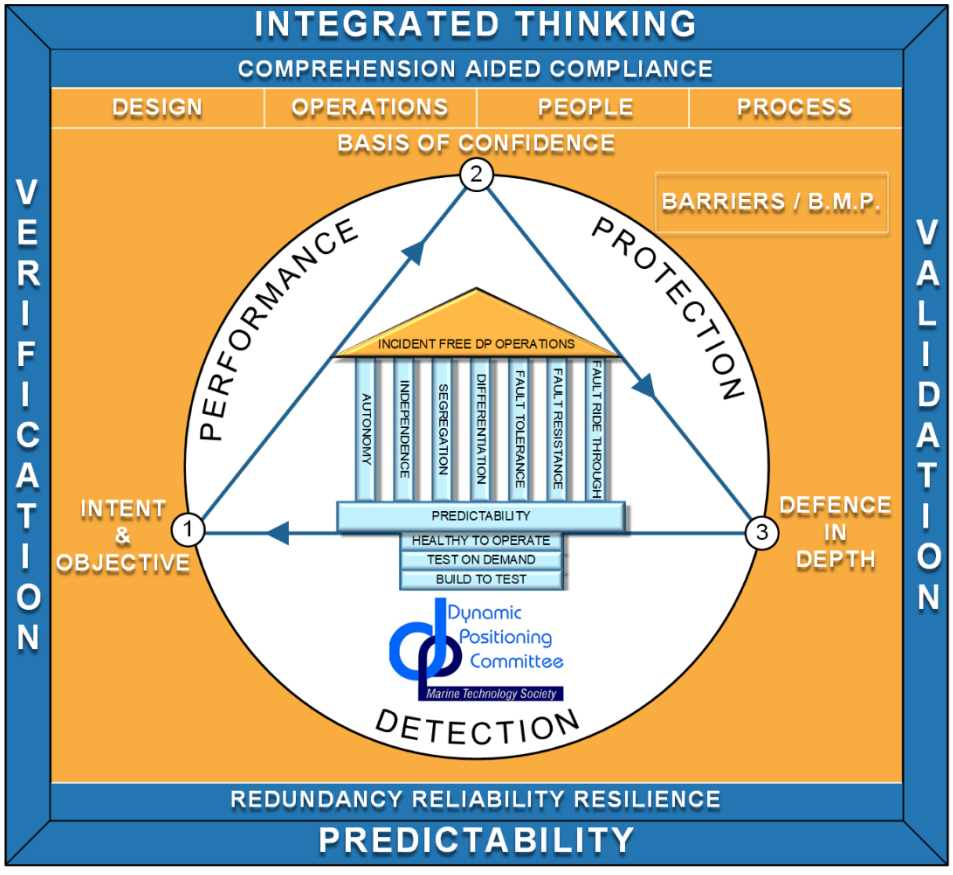


Figure 3-6 **MTS Iconography**

3.6 VERIFICATION AND VALIDATION

3.6.1 Overview of verification and validation

Verification and validation testing should be based on sound engineering principles and comprehensive analysis of the system. Effectiveness of the analysis is dependent on the transparency of information including functional data and impacts of interfaces and influences with other systems.

Where there is a lack of transparency it is essential to document observations, follow through on anomalies and incorporate experiences and lessons learnt during testing and operations into test programs. It should thus be recognized that legacy test methodology may need to be refreshed periodically.

3.6.2 Organizations carrying out verification and validation

There are several entitles that are involved in carrying out Verification and Validation (V&V). Although there may be overlap, there are significant divergences in the objectives intended to be achieved by such V&V activities.

The principles of integrated thinking may not be embedded in the processes of the diverse entities carrying out V&V activities. The vessel technical operator and the ultimate risk owner may be the entitles most invested in driving and reaping the benefits of integrated thinking and application of effective V&V to achieve predictable outcomes.

Note: *Notwithstanding the above paragraph it should be acknowledged that the ship builder is usually the system integrator and may be contractually obligated to deliver in this role. Input from the vessel technical operator must be facilitated as this input may incorporate lifecycle objectives. (example – choice of equipment driven by taking into consideration impacts of inspection, repair and maintenance over the vessel's intended lifecycle – critical and non-critical redundancy driven by operational up-time objectives).*

Table 3-1 below summarizes the different stakeholders and their focus areas as pertinent to the V&V process.

Note: It is acknowledged that the observations summarized in the table below may not apply to all stakeholders. Efforts to generalize these statements should be avoided by evaluation of V&V capability should be on a case by case basis.

Table 3-1 Stakeholder Verification and Validation Responsibilities

Entity	Focus of V&V	Remarks **(Based on incidents experienced in industry)**
Classification societies	Compliance with class rule: in some cases, to issue DPVAD on behalf of flag State in accordance with IMO MSC 1580 and FSVAD document in accordance with IMO MSC 645.	Divergences between class societies in requirements, interpretation and approval by field surveyors introduces lack of consistency. Lack of focus on industrial mission issues. Type approval is typically at equipment level and does not address influences and interfaces sufficiently

Entity	Focus of V&V	Remarks **(Based on incidents experienced in industry)**
Coastal states when engaged exhibit similar levels of engagement as flag state or marginally more.	Usually delegate responsibility to class	As above. Lack of evidence that engagement with stake holders exists and / or is effective
OEMs (DP equipment, Shipyards, Integrators)	Limited by scope dictated contractually, increased focus on systems thinking, systems engineering approach is needed. Should adopt a more holistic approach to verification of end effect (Generators and Thrusters) leading to loss of position and heading.	Contractual agreements don't cover life cycle aspects. Accountability drive by contractual scope. OEM V&V activities typically associated with type approval. (Equipment level does not address interfaces and influences).
Independent 3rd party verifier	Dictated by scope and influenced by expectations of client and technical skills	Significant variability in skill levels. Market driven. Deliverables perceived to be focused on audit, compliance considerations / ticket-to-trade requirement.
Vessel Technical Operator	Base compliance with rules and meeting minimum expectations set by end user client (typically audit focus).	Wide variability in demonstration of diligence. Influenced by end user's diligence and expectations.
End user charterers	As above in most cases. Additional enhanced requirements influenced by incidents experienced in own organization	Wide variability in demonstration of diligence. Influenced by company's HSSE control framework requirements. Integrated thinking not leveraged to full potential.

3.6.3 The focus on effective verification and validation in this document attempts to address some of the identified observations summarized in the table above. This document, by design, has the potential to drive consistency if all stakeholders are held accountable for adherence to the guidance.

3.6.4 **Performance, Protection & Detection**

The role of these essential attributes of a fault tolerant system based on redundancy has been discussed above. Proving the efficacy of protection systems is an important part of the verification and validation process.

3.6.5 **Dependencies**

Dependencies is the term used to describe the relationship of one component or system to another. Dependencies between redundant equipment groups may cause them to be vulnerable to a common cause of failure. Dependencies may take many different forms. Establishing the dependencies between redundant DP equipment groups and their effects upon failure is an important part of the verification and validation process.

Minimizing the number of dependencies between items of main machinery (engines and thrusters) helps to reduce the impact of failures. In particular, it is not good practice to design systems where the failure of relatively inexpensive components and / or low reliability components can lead to the loss of several generators and thrusters even if the effect does not exceed the worst-case failure design intent. Onset of such failures tend to result in avoidable non-productive time.

- **Principles of minimalism as applied to DP** – Minimalism as relevant to DP is defined as the focus on "elegance in simplicity" in system design. It is the attribute that is achieved by incorporating elements of autonomy, independence and segregation to derive the end objective of predictable outcomes including minimizing the loss of functionality. Examples of application of the principal of minimalism are vessels designed to the LIFE concept (Low Impact Failure Effect), Bespoke Generator Protection etc.

  Complexity invariably creates challenges with achieving transparency and increases the burden on the verification and validation process. Where complexity or sophistication is required it may be achieved by a combination of numerous and varied simple systems. Lack of transparency and the increased burden may come in the way of achieving the objective of proving the fault tolerance of the DP system.

  System design should acknowledge that verification and validation processes are an integral part of establishing the basis of confidence. Failure to establish the basis of confidence due to inadequate or added burden of effective verification and validation may result in lost opportunities to leverage the functionality designed into the systems. Typically, such challenges are experienced with complex integrated systems.

  A pragmatic approach to enable effective verification and validation could be to design simpler systems or improve the effectiveness of verification and validation such that it is capable of proving the fault tolerance of more complex systems. It is emphasized that it is not the intent to imply that simple systems are crude. Elegance and simplicity should address all relevant aspects of design, operations, people and process and enable effective verification and validation in a manner that delivers the full functionality for utilization and provides a basis for confidence. Simplicity does not exclude sophisticated (verified and validated) systems.

  Embedding the principles of autonomy, independence and segregation by design achieves the above objectives whilst alleviating the burden of developing a comprehensive FMEA, proving trials and annual trials throughout the vessel's lifecycle and reduces exposure to non-productive time.

  The approaches outlined above are achieved by the application of the principles of minimalism to DP system design.

- **Influences and external interfaces:** The boundaries of the DP system are typically defined by the hardware installation of DP related equipment. However, there will be interfaces between DP related and non-DP-related equipment (typically industrial mission equipment). Such interfaces may provide a propagation path that allows faults in the industrial mission related equipment or safety systems to adversely affect the operations of more than one redundant DP equipment group with the potential for loss of position and/or heading. Internal and external influence may also have the potential to defeat the redundancy design intent. Such influences may be categorized as internal and external common cause or common mode failures. The effects of Influences and external interfaces and their failures should be thoroughly assessed during the FMEA process.

  Note: Please refer to 'MTS TECHOP (D-01 - Rev1 - Jan21) ADDRESSING C^3EI^2 TO ELIMINATE SINGLE POINT FAILURES'.

3.7 TERMINOLOGY

3.7.1 The key themes of Design, Operations, People and Process features to different degrees in all activities related to the management of station keeping risk:

- **Design**: The term 'design' refers to all aspects of DP system design and the interfaces between DP related equipment and industrial mission related equipment, including human machine interface. Guidance on 'design' intends to offer information on good practice in the development, verification and validation of a DP redundancy concept. Guidance on this subject may also deal with failure modes and their effects in specific systems and subsystems such as power generation, power distribution and power management. Design related items are described using concepts and terminology such as the seven pillars, the three pegs and performance, protection and detection.
- **Operations:** The term 'operations' is used to cover all operations essential to undertake the industrial mission using DP as a means of station keeping. The industrial mission will influence the management of stations keeping risk. The choice of DP as a means of station keeping requires the influences of the industrial mission on DP to be managed.
- **People:** The term 'people' is used to describe all aspects of managing station keeping risk associated with the interaction of the DPO and DP system as well as the influences of the other crew members such as the engineers, instrument technicians, personnel associated with the industrial mission and other members of the vessel technical operations teams. The interface between the DPO and DP system, and to a large extent, relevant maintenance personnel (DP focused) is normally well understood but this may not be true for other personnel whose interfaces' may influence outcomes. The term 'people', as used in this, context is intended to encompass all personnel with the potential to influence the delivery of incident free DP operations.
- **Unwarranted human intervention:** Unwarranted human intervention is a term that describes issues arising from avoidable human interaction with equipment. Examples of such interventions include altering user configurable settings in a misguided attempt to address a perceived issue while at the same time inadvertently creating another defect in the systems. Other examples include carrying out intrusive maintenance on equipment in order to survey its condition in such a way that there is a high risk of degrading the reliability of the equipment in the process of dismantling it for survey or restoring it for use. This is particularly true of mechanical and electro mechanical systems which are vulnerable to maintenance induced failure.

  DP incidents have been experienced where a conscious decision has been made to rely on operator intervention to prevent escalation in lieu of limiting escalation by design. Reliance on operator intervention introduces potential for unpredictability and can be a weak barrier.
- **Cognitive burden:** The term 'cognitive burden' refers to the extent to which a human operator may be 'loaded' by decision making tasks (especially under stress) and by the effects of other computationally intensive tasks. Reliance on cognitive ability of the operator to intervene effectively to prevent escalation of an event has limited potential for success. Examples include, expecting the DPO or engineers to diagnose problems from a large number of alarms and indications, particularly when many of those alarms are not directly related to the fault condition itself but rather the consequence of failures elsewhere in the DP system. One way of alleviating the cognitive burden is to provide information absorbable in an intuitive manner rather than reams of data (Examples, dashboards linked with pointers to impacted equipment and actions)

- **Maloperation:** The term maloperation is used to describe an inadvertent act by anyone onboard the DP vessel. DP system design seeks to eliminate opportunities for a single inadvertent act to create a loss of position. Examples include acts such as inadvertently taking the DP control system out of auto-position mode or accidentally operating the 'all vessel shut down' function on a DP MODU.
- **Configuration errors:** The fault tolerance and post failure DP capability of some DP system designs can be highly configuration dependent. Failing to configure the DP system correctly can defeat the redundancy design intent leading to loss of position and / or heading when a single failure occurs.

  Equipment taken out of service for inspection, repair and maintenance can / may impact fault tolerance and post failure DP capability. Processes should be in place to address such changes in fault tolerance and post failure DP capability including rationalization of operational limits and criteria.
- **Process:** The term 'process' refers to the procedures and operations guidelines that stakeholders use as 'control-of-work' to progress the industrial mission and manage station keeping risk. It also refers to processes that vessel technical operators use to manage the safe operations of their vessels and supplement the processes of vessels hired in from subcontractors. Examples of processes are Hazards and Effects Management Practices (HEMP), permit to work, return to work authorization (post incident event), vessel specific familiarization, contingency plans, emergency response, training and drills.

4 DP VESSEL DESIGN PHILOSOPHY

4.1 RESPONSIBILITIES

4.1.1 This document is intended to be a design philosophy guide. However, it is important to note that the process of the overseeing and implementing a DP vessel design concept involves many stakeholders. Consequently, it should be recognized that the 'contracting philosophy', employed at each level of design and the various disciplines involved, directly affects both the design and execution of the design.

4.1.2 Whether the contract is turnkey "design and build" or the owner presents a fully developed and reviewed design complete with owner furnished equipment to the shipyard, the fact remains that oversight of the process, as a whole, is a key factor in the success of the design.

4.1.3 Regardless of the contracting philosophy, the key disciplines and stakeholders in the process remain the same. The responsibilities of each stakeholder for a given project should be clearly defined by contract, communicated to, and understood by all parties involved in the design and execution of the design. The following list attempts to provide a high-level description of the scope of design responsibilities for the various stakeholders; it does not address financial responsibilities:

1. **Senior Management:** The owner's senior management is responsible for the project charter, which should clearly define the mission parameters for the design. The charter should include the basis of design. Strict guidelines should be incorporated for management of change to mitigate scope creep.
2. **Project Team:** The owners project team will vary depending on the type of contract, however there are common skill sets required on the team including project management, engineering and administration. While each contract will differ, it is important to state that it is the responsibility of the owner to adequately staff the project in order to diligently oversee the entire design process as well as the implementation of the design.
3. **Naval Architects / Designers:** Naval architects and designers are responsible for the conceptual design. The naval architect does not provide detailed engineering or systems designs. In general, the naval architect provides hull form drawings, scantlings, conceptual general arrangement drawings, and reports such as weight estimates, hull friction, stability, etc. The Naval architects drawing must be translated by others into detailed production design drawings.
4. **Flag State:** The flag state administers the rules adopted by legislation for the flag state. In general, these rules are mainly Health, Safety and Environment and manning related. Flag state rules will normally enforce international conventions such as IMO, SOLAS and Marpol. While some flag states have extensive design codes in place, it is not uncommon for flag state rules to defer to one of the class society's codes for design criteria.
5. **Class Society:** Class societies establish design codes, review and certify adherence to the codes during design, review the vessel while it is being built and tested, and ultimately certify that the completed vessel complies with their rules. Class societies do not have any governmental authority other than that which may be granted by a flag state. They developed first as a method of providing insurers with technical reviews of vessels to determine whether a vessel was safe and fit for the purpose it was designed for.

6. **Shipyard:** While there are many forms of shipyard contracts and many levels of ability within shipyards throughout the world, it must be noted that the shipyard generally either does or subcontracts the detailed design. With the exception of a complete design and build contract, the shipyard works from a conceptual design by others. The shipyard must interpret the design from the naval architects, various systems designers and vendors, produce detailed designs across disciplines, then fabricate and assemble the hull and systems per the design. Ultimately, the design must be tested as a completed system per the basis of design.

7. **Integrator:** Regardless of the contracting philosophy, the equipment specified by the design must be integrated into a system. It should be noted that when the term "Dynamic Positioning System" is used it refers to the fully integrated vessel systems. There are numerous disciplines, vendors, flag state requirements, class society requirements and design basis requirements that must be integrated into a fully functional, 'fit for purpose' system. The integration process must be closely monitored from the basis of design through to the delivery of the vessel. Design/system reviews at identified points with participation by relevant stake holders could facilitate the integration process.

4.2 RELIABILITY OF STATION KEEPING

4.2.1 Reliability and redundancy should not be considered as synonymous. DP class rules have redundancy requirements stipulated to achieve fault tolerant systems and meet the objective of not having a single failure leading to a loss of position. They often do not address the ability of the vessel to continue its industrial mission.

4.2.2 For the purposes of this document the properties of redundancy and single fault tolerance are considered to be synonymous. It is acknowledged that this interpretation is not universal.

1. Often, redundancy is interpreted as having two items of equipment required to perform a function with no consideration given to ensuring that the redundant unit can take over from the failed unit without unacceptable interruption of the function.

2. Similarly, there may be no consideration of how to prevent a fault in one redundant element affecting the operation of others.

3. The above factors should be taken into consideration during design and avoided by incorporation into specifications.

4. The terms 'redundancy' and 'single fault tolerance' are used interchangeably throughout this document.

4.2.3 DP vessels should have a sufficient level of station keeping reliability. Reliability is a product of the quality of the equipment and suppliers selected, the competence of the engineers who design and build the DP vessel and the competence of the crew and management who maintain and operate it.

4.2.4 Redundancy does not in itself guarantee a sufficient level of reliability leading to overall availability. It can contribute to availability if the redundant elements themselves are sufficiently reliable. DP rules and guidelines do not specify a level of reliability. When mentioned it is in the context of the consequences of loss of position.

4.2.5 The vessel‘s availability to work can be related to the probability of losing fault tolerance. The vessel’s industrial mission should determine what overall level of reliability should be attained to achieve the required vessel availability. Higher vessel availability can be achieved by the application of non-critical redundancy and attention to reliability. A robust design can provide high reliability and availability and this should be the primary objective of any design process. Vessel build specifications that make reference to Class rules alone without explicitly addressing Industrial mission requirements and robust design may not achieve the above goal.

- This goal may not be achieved if the only objective is compliance with class rules.
- Requirements for single fault tolerance must be satisfied in any design to comply with the rules.
- This guidance document only deals with design.

The guidance provided in this document is intended to assist with delivering a robust design capable of:

1. Preventing loss of position.
2. Preventing loss of redundancy.

This is expected to result in a vessel that meets class requirements and delivers the desired availability to carry out its industrial mission.

4.3 DP EQUIPMENT CLASS

4.3.1 IMO Marine Safety Committee Circulars for DP are:

- MSC.1/645 ’Guidelines for Vessels with Dynamic Positioning Systems’, 1994.
- MSC.1/1580 ’Guidelines for Vessels and Units with Dynamic Positioning Systems’, 2017.

4.3.2 These guidelines are intended to provide an international standard for dynamic positioning systems. They define three DP equipment classes which are intended to provide different levels of station keeping reliability which can be matched to the consequences of loss of position. The three equipment classes are defined by the effect of failure and the nature of the failures which must be considered.

4.3.3 IMO MSC 645 does not address the industrial mission of the vessel. Its successor, IMO MSC 1580 does make reference to mission specific requirements and the need for decision support tools. Operational requirements in IMO MSC 1580 are applicable to existing vessels built before and after 9th June 2017.

4.3.4 The equipment class of the vessel required for a particular operation should be agreed between the owner(s) of the vessel and their respective customer based on a risk analysis of a loss of position. Some Coastal States imposes minimum DP Equipment Class requirements for activities carried out within their domain.

4.4 DP EQUIPMENT CLASS 1

4.4.1 Loss of position may occur in the event of a single failure.

4.5 DP EQUIPMENT CLASS 2

4.5.1 **IMO MSC 1580:** 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.

4.5.2 **IMO MSC 645:** Loss of position is not to occur in the event of a single fault in any active component or system. Normally static components will not be considered to fail where adequate protection from damage is demonstrated and reliability is to the satisfaction of the administration. Single failure criteria include:

1. Any active component or system (generators, thrusters, switchboards remote controlled valves, etc.).
2. Any normally static component (cables, pipes, manual valves, etc.) which is not properly documented with respect to protection.

4.6 DP EQUIPMENT CLASS 3

4.6.1 **IMO MSC 1580 and 645:** A single failure includes:

1. Items listed for class 2, and any normally static component are assumed to fail.
2. All components in any watertight compartment, from fire or flooding.
3. All components in any one fire subdivision from fire or flooding.

4.7 CLASSIFICATION SOCIETY DP NOTATION

4.7.1 Each of the main classification societies produces its own DP rules which align to different degrees with the requirements of IMO MSC 645 & IMO MSC 1580.

4.7.2 Classification society rules are generally updated once or twice a twice a year and are not applied retrospectively.

Table 4-1 Class IMO Equivalent Notation

Classification	IMO Equipment Class 1	IMO Equipment Class 2	IMO Equipment Class 3
DNVGL	DYNPOS-AUT DPS(1)	DYNPOS(AUTR) DPS(2)	DYNPOS(AUTRO) DPS(3)
ABS	DPS-1	DPS-2	DPS-3
LRS	DP(AM)	DP(AA)	DP(AAA)
BV	DYNAPOS AM/AT	DYNAPOS AM/AT R	DYNAPOS AM/AT RS

4.7.3 This document only considers requirements for Equipment Class 2 and Equipment Class 3. Several classification societies offer additional notations which address other issues such as the use of standby redundancy.

4.8 FUNCTIONAL REQUIREMENTS

4.8.1 In order to meet the single failure criteria, it will normally be necessary to provide:

1. For equipment class 2 - redundancy of all active components.
2. For equipment class 3 - redundancy of all components and physical separation of redundant components.

4.9 TIME TO TERMINATE

4.9.1 DP rules and guidelines require only that DP vessels be able to maintain station following a single failure for long enough to safely terminate the work in progress.

4.9.2 Different industrial activities have different termination times, and this may influence the design of the DP system and choice of operating configuration. For example, in certain drilling activities the drilling rig can disconnect fairly rapidly and move off station in a controlled manner. In other activities a much longer time to terminate is required. Diving support, pipe laying, umbilical-lay and heavy lift activities may have longer time restrictions in some cases.

4.9.3 Industrial missions that inherently require longer duration time to terminate should consider designs that limit loss of thrust, post failure. Fuel service tank capacity thermal capacity of cooling systems or provision of HVAC are factors that could influence achieving the desired duration necessary for time to terminate.

The designs of DP systems reliant on limited stored energy sources (e.g. hybrid power, flywheel) should take into consideration time-to-terminate as this could have significant influence on the design, capacity and interfaces (DP system level).

4.10 MITIGATION OF FAILURES

4.10.1 DP rules and guidelines generally require that equipment intended to provide redundancy is available immediately and with a minimum of operator intervention. Classification societies interpret this differently and some DP notations require that the vessel must be able to hold position with the main machinery that remains operational following the worst case failure. Others accept that standby machinery may be brought online automatically. The requirement for all redundant machinery to be ‘active redundancy’ was sometimes relaxed in the case of cooling systems. This was reasonable if the time taken for temperatures to reach critical levels was long. As interpretation of rule requirements changes over time it is important to clarify such issues at the redundancy concept development stage to avoid delay and rework at a later date.

4.10.2 Operator intervention can be considered as part of the failure mitigation process. In a limited number of cases operator intervention may be accepted provided there is sufficient time for the operator to act before the failure effects escalate to unacceptable levels and there are clear alarms and indication to identify the fault. ‘Drive off’ is an example of a failure effect where operator intervention is likely to be required. Unambiguous instruction and procedures should be developed for all cases where operator intervention is part of the failure mitigation. Training and drills should also form part of the confidence building measures designed to ensure the failure can be safely mitigated by operator intervention.

4.11 REDUNDANCY CONCEPT AND WORST-CASE FAILURE DESIGN INTENT

4.11.1 The worst-case failure design intent describes the minimum amount of propulsion and control equipment remaining operational following the worst-case failure. The worst-case failure design intent is used as the basis of design. Single fault tolerance is to be achieved by the provision of redundant systems. Adequate holding capability is to be achieved by provision of adequate remaining power and thrust.

4.11.2 The redundancy concept is the means by which the worst case failure design intent is achieved and should be documented as part of the preliminary design process. This is highlighted and emphasized as it determines the ability of the vessel to undertake critical activities associated with its Industrial Mission in the desired range of environmental parameters.

4.11.3 The redundancy concept and post failure DP capability should take into account the long term loss of a major item of machinery such as a generator or thruster. This is not a requirement but will aid in system availability and operational uptime for a wider range of environmental conditions. It adds flexibility in maintenance and improved efficiency. It should also be possible to account for long term unavailability in the consequence analysis.

4.11.4 Design should precede ordering of capital equipment. Long lead times for equipment such as engines or thrusters may preclude this. Features and design attributes of such pre-purchased items may influence design development and needs to be accounted for in the development of the redundancy concept.

Some classification societies have a requirement for a vessel specific design philosophy document. It should be recognized that such a document will of necessity be a high-level document. It is acknowledged more detailed information will be contained in other documentation produced during the build cycle. The value of this document can be realized when it is produced in the early and initial phases of a project (finalization of the concept and preceding commitments of purchase of capital equipment). Such a document should be leveraged as a means to align the needs of the industrial mission, vessel owner's objectives, the yard's delivery obligations and achieve a common understanding amongst diverse stakeholders including key vendors and assurance providers in addition to meeting class requirements.

4.12 AVAILABILITY AND POST FAILURE DP CAPABILITY

4.12.1 System availability and post failure capability strongly influences the ability of the vessel to undertake its industrial mission in a range of environmental conditions. This influences operational uptime.

4.12.2 The Worst Case Failure Design Intent (WCFDI) is the basis of DP vessel design. The Worst Case Failure is the failure that has the greatest effect on station keeping capability. A successful DP vessel design is one where the WCF achieved is less than or equal to the WCFDI. The WCF is used in the DP control system online consequence analyser.

4.12.3 The philosophy espoused within this document strives to limit loss of thrust capacity post worst case failure. In the discussion that follows, redundancy depends on systems being available in both number and capacity to produce the required post worst case failure DP capability.

4.12.4 The redundancy concept can have a very significant impact on DP vessel design and there are several variations on how to provide a fault tolerant system. In general terms the redundancy concept is based on power and propulsion systems that are independent in respect of single point failures. That is to say no defined single point failure in one independent system will disrupt the operation of the other. Independent systems can be designed to provide full or partial redundancy.

4.12.5 An independent system is said to provide full redundancy if it can develop the necessary surge, sway and yaw forces required to maintain position and heading in the defined post worst case failure environmental conditions.

4.12.6 An independent system is said to provide partial redundancy if it can only provide the necessary surge, sway and yaw forces in combination with another independent system. For example, all independent systems may be able to provide equal surge, sway and yaw forces but more than one independent system is required to produce the level of thrust required by the defined post worst case failure DP capability. The redundancy concept must ensure that suitable combinations of systems are available following any defined failure. Alternatively, one independent system may develop alongships thrust and the other athwartships thrust, thus redundancy is required in each axis.

4.12.7 The simplest diesel electric redundancy concepts have two fully redundant power and propulsion systems each capable of maintaining position and heading if the other fails. More complex designs make use of multiple systems each providing partial redundancy such that the vessel can maintain position with all combinations of independent systems that survive any defined failure. For example, a vessel with three systems can hold position with any two of the three systems available.

4.12.8 An advantage of redundancy concepts based on multiple independent systems, each providing partial redundancy, is that provided each system can develop surge, sway and yaw forces and has all necessary services required to support DP it is possible to consider these systems as providing full redundancy in reduced environmental conditions. Thus, a DP system with three independent power and propulsion systems can still be considered fault tolerant if only two of the three systems are available and may be able to continue DP operations in this degraded condition if environmental conditions allow. However, it is important to establish this as a design objective as it is possible to create redundancy concepts based on partially redundant system which do not remain fully redundant with reduced capacity when one system has failed.

4.12.9 The use of multiple independent systems offers other advantages. A vessel with four independent systems can in theory remain fault tolerant up to 75% power compared to one with only two systems which can only operate up to 50% power. Thus, the design based on multiple independent systems can have smaller machinery for the same post failure DP capability or use the same machinery and have a greater DP capability.

4.12.10 The redundancy concept has a strong influence on machinery sizing. Design should ensure adequate margins to accommodate increased demand for power and thrust associated with development of the detailed design.

4.12.11 A basic redundancy concept and WCFDI should be developed as a precursor to design and before orders are placed for long lead items (e.g. engines and thrusters to ensure the correct ratings are ordered.) Designers and naval architects will have established the amount of thrust required. The equipment required to provide the stipulated uptime in the expected range of operating conditions will determine the required post worst case failure DP capability. The redundancy concept will determine how that post failure DP capability is provided by establishing the number of generators and thrusters available after worst case failure. This is likely to be an iterative process influenced to some extent by the equipment that can be purchased in the expected development and construction timescale. See also Section 4.11.4.

4.13 EXTERNAL FACTORS

4.13.1 When considering the type of failures that can occur it is normal to consider the vessel and its DP related equipment. Influences external to the vessel can also initiate failures in the vessel's power plant and control systems. Typical external influences that must be considered include:

1. Uncommon environmental effects:
    a. Sudden squalls.
    b. Winter storms.
    c. Hurricanes.
    d. Typhoons.
    e. Micro-bursts.
    f. Waterspouts.
    g. Solitons.
2. Seawater - fouling - aeration – contamination.
3. Combustion air – contamination.
4. Ventilation – contamination.
5. Fuel - contamination - microbial – water.
6. Position reference signal path (Sea and Sky).
7. Lightning.

4.14 KEY ELEMENTS OF DP SYSTEM PERFORMANCE

4.14.1 There are two key elements in DP performance:

1. Holding capability.
2. Reliability.

4.14.2 **Station keeping capability:** Is the ability of the vessel to maintain position and heading in defined environmental conditions.

4.14.3 **Component reliability:** As used in this document is the choice of individual elements of equipment or software for prolonging Mean Time Between Failure (MTBF).

4.14.4 Redundancy is provided to give the required level of reliability and comply with classification society requirements for fault tolerance. Holding capability gives the expected uptime in the intended area of operation. Redundancy applied to ensure there is no loss of position following a single fault is defined as critical redundancy. Additional equipment intended to ensure the vessel remains fault tolerant following a single failure is defined as non-critical redundancy.

4.15 KEY ELEMENTS OF REDUNDANT SYSTEMS

4.15.1 There are three key elements in any redundancy concept:

1. Performance.
2. Protection.
3. Detection.

4.15.2 **Performance:** Holding capacity is fundamental to the design process. Appropriate engineering studies establish the amount of installed thrust and power generation for the environmental ranges the vessel is designed to operate in.

4.15.3 When establishing thrust requirements for ship shaped hulls, designs should not be overly reliant on keeping the bow into the weather as the design basis. This has proven inadequate in many cases, as heading often cannot be changed fast enough to follow changes in wind direction. The design should account for operations that might require a non-optimal heading including a beam environment. Experience has shown that DP MODUs, designed to cope with 70 knots of wind on the beam (zero waves or current) in an intact condition, have proved to have adequate capability to undertake operations in most environments. This is a good rough check.

4.15.4 At system and component level all equipment must be capable of its rated performance to ensure fault tolerance.

4.15.5 **Protection:** Fault tolerant systems based on redundancy require protective functions to prevent faults in one redundant system being coupled to others by way of common connections or equipment. The design should ensure all necessary protective functions are provided. Operator intervention should not be considered a protective function.

4.15.6 Protective functions exist in many different systems including DP control, automation and power generation. The drivers for applying protection may be compliance with Class Rules, safety, equipment protection or in support of the redundancy concept. Addition of a protective function should not conflict with DP redundancy. Where conflicts exist, a solution should be developed to satisfy all requirements.

4.15.7 **Detection:** Equipment intended to provide redundancy must be available in both number and capacity. The design must include means to detect reduction in capability or unavailability. Redundant components should be immediately available and with such capacity that DP operations can be continued for long enough to safely terminate the work in progress.

4.16 COMMUNICATING AND SUPPORTING THE REDUNDANCY CONCEPT

4.16.1 Once the preliminary redundancy concept has been developed it is important that it be communicated to all stakeholders and understood. The vessel specific design philosophy document could be leveraged to serve this purpose. As a minimum the stakeholders should include:

1. Shipyard.
2. Classification societies.

3. DP control system provider.
4. Automation system provider.
5. Power system provider.
6. Propulsion system provider.
7. Integrators if applicable.
8. FMEA contractor.
9. Vessel owner's site team.
10. Crew.
11. Charterer if applicable.

4.16.2 Interface issues between various vendors should be carefully managed. Responsibility for this may lie with the shipyard or owner's team depending on the nature of the contract. Responsibility should be clearly defined, identified and made visible.

4.16.3 It is important to concurrently develop vessel specific Inspection, Repair and Maintenance (IRM) procedures, operating procedures, guidelines and reference materials such as DP Operations Manuals to develop and support the redundancy concept. Supporting documentation may include Activity / Well Specific Operating Guidelines (A/WSOG) and Thruster and Generator Operating Strategy (TAGOS).

4.17 CONNECTIONS BETWEEN REDUNDANT SYSTEMS

4.17.1 Experience suggests that common connections between systems intended to provide redundancy create the paths by which a fault in one redundant system may affect another independent system. Some connection points are unavoidable such as remote-control systems and those introduced to achieve additional objectives (example – reduction of emissions, hybridization etc.) and may be beneficial to the design. Where common points exist between redundant systems, risk assessments on impacts of failure propagation should be carried out, documented in the FMEA, verified and validated through appropriate testing and adequately mitigated.

4.17.2 Comprehensive analysis should be carried out and identified in the FMEA where common points and / or cross connections are identified. Validation testing should be based on the engineering basis (comprehensives analysis). The burden of a such activities (including skill levels) should not be underestimated.

4.18 MULTIPLE POWER PLANT CONFIGURATIONS

4.18.1 Diesel electric plant design should incorporate configuration flexibility to cope with equipment unavailability. (e.g. failures or equipment taken down for maintenance) However, it is important that the effect of such reconfigurations are understood as some may not be redundant. Major configurations should be identified and analyzed in the vessel's DP system FMEA to prove the DP system remains redundant. Fault tolerance of configurations should be made visible and understood by the crew. Where there is configuration flexibility in the design, the Critical Activity Mode (CAM) should be clearly defined in addition to other Task Appropriate Modes (TAM) for use on DP with any additional risks made visible. For example, some task appropriate modes may rely more heavily on protective functions than others.

4.18.2 It may not be practical to consider every possible variation particularly in vessels that have complex power distributions systems and some classification societies state that the vessel is only considered to comply with their requirements for the DP notation when operated in one of the configurations analyzed in the approved FMEA. Vessels with complex power distribution systems should consider the most likely configurations that the vessel will be operated in and have them analyzed in the FMEA. If there is a need to operate in a configuration that is not addressed in the FMEA, it may be necessary to supplement the FMEA with additional analysis and tests to confirm the level of redundancy provided by the intended configuration. This will be required if verification of class compliance is required.

4.19 CRITICAL AND NON CRITICAL REDUNDANCY

4.19.1 Class rules require DP systems to be redundant with the primary objective of achieving no loss of position. However, redundancy in itself does not guarantee a particular level of reliability. Loss of fault tolerance could cause operational issues impacting the industrial mission of the vessel. Where aspects of the design are identified as being of lower reliability or there is a need to ensure higher availability it may be beneficial to provide redundancy over and above that required to meet class requirements.

1. Critical redundancy is defined as equipment required to ensure the vessel is single fault tolerant. To remove such equipment would either remove the DP system's fault tolerance entirely or reduce its post failure DP capability.
2. Non critical redundancy is equipment intended to provide greater availability.

4.19.2 If redundant elements are highly reliable, there is no need for non-critical redundancy but it can be usefully applied to allow maintenance or in cases where it is uneconomical or impractical to increase the reliability further.

4.20 COST EFFECTIVE RISK REDUCTION

4.20.1 When the redundancy concept is developed there will be a number of failures that have a severity equal to the worst-case failure design intent (WCFDI). Design should focus on minimizing the number of failures equal to the WCFDI. These failures should be reviewed to determine whether a cost-effective improvement can be made. When considering cost benefit analysis, it is the lifecycle cost that should be considered including the penalties for non-availability. For example, the worst case failure design intent for a particular vessel accepts that three out of six generators may be lost as the result of a single failure. The design is such that this failure effect may occur because of a main switchboard bus bar failure or because a 24Vdc power supply fails. Given the relative probabilities of failure it may be cost effective to provide a second 24Vdc power supply or possibly one for each generator. This would reduce the severity of the failure effect associated with the 24Vdc supply system.

4.21 ENHANCING CLASS MINIMUM STANDARD

4.21.1 Classification society rules are generally intended to provide a minimum technical standard. The Industrial mission and desire to achieve greater availability may influence vessel owners to exceed the minimum requirements and improve reliability, operability and maintainability. Vessel owners should be aware that any such improvements to the DP system need to be expressly agreed in the shipyard contract for the vessel. The default position for shipyards is to meet class requirements. Where the owner wishes to apply a different worst case failure design intent to some aspect of the redundancy concept over and above that required by class this needs to be agreed to and reflected in the contract. If the shipyard contract only requires the design to meet class requirements the additional features may not be provided. For example, the redundancy concept for a DP class 3 vessel may accept that that three of six generators are be lost because of an engine room fire but the owner wishes to limit the effects of technical failures to loss of a single engine or thruster. Class 2 DP rules allow all generators to be located in a single space. Many vessel owners prefer to have two or more engine rooms. Such arrangements limit the risk from crank case explosions and engine room fires and other risks such as flying debris.

4.21.2 A fully automatic blackout recovery system is not a class requirement. Main class rules and SOLAS have requirements for some degree of automatic restart of electric power systems but for a DP vessel it may be unwise to rely on this to ensure a full blackout recovery system is provided. A fully automatic black out recovery system can be supplied by all the major marine automation providers and should be specified by vessel owners. Modern blackout recovery systems can typically restore thrust in less than one minute from blackout. DYNPOS(ER) and ABS-EHS have higher requirements for automatic blackout recovery compared to traditional DP notations.

4.21.3 The classification society may limit its plan approval process to proving compliance with the worst-case failure arising from application of the failure criteria defined in the rules appropriate to the DP notation being sought (e.g. fire or flooding). The FMEA and proving trials should cover the redundancy concept and worst-case failure design intent at all levels in addition to addressing class requirements. The contract with the shipyard should expressly stipulate this. Sometimes, the choice of the FMEA vendor is selected by the owner or charterer according to their preference. Class will accept an FMEA commissioned or carried out by the shipyard.

4.22 INFLUENCE OF THE VESSEL'S INDUSTRIAL MISSION

4.22.1 Dynamic positioning is provided to allow the vessel to carry out its industrial function such as drilling, pipe laying, or heavy lifting. In diesel electric designs based on the power station concept, the electric power systems supply all power for propulsion, hotel, auxiliary systems and the consumers associated with the vessel's industrial mission. There may be competing requirements for power between station keeping and the industrial function. This needs to be defined and carefully managed to ensure the propulsion system has access to the power it needs to prevent loss of position in the range of environmental conditions the vessel is operating in. The requirements of the industrial consumers may dictate or favour a particular power plant configuration. Such configurations should not conflict with the redundancy concept or compromise the industrial mission.

4.22.2 Rules for DP notations are intended to ensure a satisfactory level of station keeping integrity. They do not specifically address the vessel's industrial mission so it is important when specifying the DP system to ensure that it has all the appropriate features and functions required to carry out its mission effectively. For example, number and type of position reference systems should be appropriate to the type of work to be carried out. In the case of multi-purpose DP vessels, design should consider systems appropriate to all types of work that may be required of a vessel.

4.23 REGULATORY REQUIREMENTS

4.23.1 Although IMO MSCs 645 and 1580 are intended to provide an international standard, compliance with this standard or rules for DP notations do not guarantee compliance with other regulatory requirements imposed by flag and coastal states. For example, requirements related to environmental legislation such as emission control may be difficult to reconcile with requirements for active redundancy contained in DP rules (DYNPOS ER differs from traditional DP notations in this respect). Operating large diesel engines at low load levels is inefficient and may not achieve the gas temperature required for exhaust gas scrubbers to work efficiently. Asymmetric thruster loading of independent power systems may assist to some extent. Thruster bias can similarly be used to increase load levels which consumes more fuel. It is a challenge to reconcile a scheme that requires burning more fuel with an environmentally conscious policy.

4.23.2 A single generator / single thruster - worst case failure design intent allows the power plant to be much more heavily loaded than the class minimum of a two way split. This is of benefit in the efficient operation of pollution control equipment. A larger number of smaller generators can assist in addressing this issue. If the power consumers related to the vessel's industrial mission are large these can be used in such a way that the power plant is operated efficiently provided there are effective means to shed load when power is required for station keeping either as a result of deteriorating weather or partial power plant failure.

5 LIFE CONCEPT (SINGLE THRUSTER SINGLE GENERATOR WCFDI)

5.1 INTENT & OBJECTIVE

5.1.1 The intent of the LIFE concept is to reduce the effect of more probable power and control system failure modes to loss of a single generator or single thruster. In general terms, the only failure modes that should cause effects exceeding these are:

- Fire.
- Flooding.
- Failures acting directly on the bus bars of the HV switchboard.

Note:

- *If desired these failure modes can be accommodated within LIFE Concept designs - If they are not, then there may be a difference between the WCFDI defined for class and the WCFDI defined for LIFE and therefore the associated post failure DP capabilities.*
- *There must be a documented basis for managing the residual risk by means other than power plant segregation.*
- *Some classification societies have DP notations that are very close to LIFE concept in the philosophy they apply. (Example - ABS EHS notation and DNVGL DYNPOS(E) DYNPOS(ER) notation).*

5.1.2 It is possible to reduce the risk of experiencing these residual failure modes by means other than further segregation of the power plant (which tends to be costly and of limited value if taken to extremes). These failure modes are better addressed by focus on preventative measures than creating systems which are 'theoretically' capable of surviving them.

5.1.3 In many DP class 3 designs, these failure modes cause effects equalling the original (Pre-LIFE upgrade) worst case failure designs intent but experience of these infrequent failure modes suggests the worst-case failure design intent could be exceeded anyway, thus, the need to focus on 'prevention' to address these modes of failure in a practical and effective way.

5.1.4 Experience with vessels operating on DP with the minimum class requirement power systems configured as a common power system is that this will introduce the possibility of experiencing failure effects exceeding the worst case failure design intent. Unless the vessels are fitted with the protective functions and features which form the core of the LIFE concepts, it is common for total blackout or loss of all thrusters to occur even for relatively probable failure modes. This occurs because the level of verification and validation applied to these stock designs is relatively superficial and the DP system is not fully fault tolerant. Elements of the LIFE concept may be incorporated in enhanced DP notations.

5.2 KEY OBJECTIVES IN LIFE & RETROFIT LIFE APPLICATIONS INCLUDE:

- Enhancing Post Failure Capability to 83% or better (For a monohull – 6 generator, 6 thruster equipped vessel) - Excluding items listed in 5.1.1.
- Improved Basis of Confidence by improving reliability and limiting loss of critical equipment impacting redundancy.
- Lowering Green House Gas Emissions and Fuel Consumptions.
- Reducing Maintenance Costs.

- Improved resilience and fault ride through capability (Achievable by implementation of hybrid power for station keeping).

5.2.1 Application of the LIFE Concept includes the verification and validation requirements to enable operation of the power plant in a closed bus / ring configuration for Critical Activity Mode (CAM Operations). Decision to operate in such configurations may require alignment between the Operator and the Owner.

5.2.2 Enhanced verification and validation capability can be achieved by the pursuit of the following philosophies / objectives utilizing a systems thinking / systems engineering approach.

- Built to Test (BTT).
- Test on Demand Capability.
- Healthy to Operate.

Note: *Many MODUs currently operates in an open bus configuration due to a failure to prove equivalent integrity of the power plant in a closed bus / ring configuration.*

Consequences of operating in such configurations can be:

- *Running increased number of Diesel Engines.*
- *Increased Green House Gas (GHG) emissions.*
- *Increased fuel consumption.*
- *Higher maintenance cost.*
- *Higher potential for changes in status to yellow necessitating suspension of drilling operations (potential for increased Non-Productive Time (NPT).*
- *Lower power plant stability.*
- *Lack of resilience.*

5.2.3 Application of LIFE Concept principles leads to highly autonomous system designs which are elegant in their simplicity. These highly autonomous designs lend themselves to being retrofitted to existing DP MODUs. With proper planning and execution, such retrofits can be accomplished by minimizing the time the MODUs need to be taken out of service (days rather than weeks! – is possible with effective planning and preparation).

5.3 LIFE CONCEPT FUNDAMENTALS

5.3.1 DP redundancy concepts in stock / standard DP vessel designs may not be optimized to make best utilization of the capability of the installed machinery. There tend to be a relatively large number of high probability and reasonably foreseeable failures with effects equal to the worst-case failure design intent which is acceptable but undesirable. The worst-case failure design intent is often loss of 50% (or 33% in better designs) of the installed power plant capacity. As the worst-case failure design intent defines the DP vessel's working environmental envelope, the exposure to non-productive time is significant and the power plant may need to be operated in configurations that are inefficient and thus detrimental to the machinery, fuel consumption and greenhouse gas emissions.

Note: *WCFDI based on a typical two or three redundancy group vessel.*

5.3.2 it is possible to effectively and predictably mitigate the higher probability failure modes and therefore, improve the vessel's post failure DP capability, operability and availability by reducing the impacts of failures. This is achieved by applying the concepts of autonomy independence and segregations to the DP redundancy concept and the (protective function upon which it depends). The pragmatic use of non-critical redundancy plays an important part. Note that the decision to consciously exclude the potential for fire, flooding and bus bar failure when applying the LIFE concept is not in alignment with the requirements of DP Class 3 notations and IMO DP Equipment class 3 failure criteria.

5.4 RETROFITTABLE LIFE

5.4.1 It is recognized that a retrofit, may not be able to achieve the full functionality of a purpose-built LIFE concept design in a cost-effective manner. However, the autonomous and modular nature of the systems that were developed / implemented to achieve the LIFE objectives lend themselves to being effective in a retrofit situation. Short comings / gaps from a purpose-built design, if any, have minimal effect on achieving the desired functionality. Such short comings, usually in the verification / validation space, can be effectively addressed by alternate means albeit with a little more burden / additional infrastructure. Such infrastructure is part of the retrofit design.

5.5 CORE ELEMENTS OF LIFE & RETROFITTABLE LIFE

5.5.1 The practical application of the LIFE concept embodying the Seven Pillars (Autonomy, independence, segregation differentiation, fault resistance, fault tolerance and fault ride-through) produces robust autonomous system designs with effective protective functions.

5.5.2 Key elements which emerge from this process are:

- Generator autonomy.
- Protection against power plant common mode failures (fuel & excitation control etc.).
- Thruster autonomy and protection.
- Cascade waveform injection testing and datalogger ecosystem.
- Independent performance validation.
- Thruster hybrid power (optional).
- Details of these core elements are discussed in the sections that follow.

5.6 ADDRESSING COMMON MODE POWER PLANT FAILURES

5.6.1 An extremely high level of predictability to common power plant failures is required to ensure the worst-case failure is loss of a single generator compared to loss of a complete bus or loss of the entire power plant with a conventional system. Generator protection includes protection against:

- Fuel control faults.
- Voltage control faults.
- Over current and overload faults (kW or kVAR).
- Short circuits.
- Load or generator induced instability.
- Hidden failures.

5.6.2 The protection must be autonomous to remove all generator interdependencies so that when a generator is connected to the main bus it operates predictably with a high level of reliability without any required connections other than its main power connection to the bus.

5.6.3 The dedicated generator protection should include a high-level diagnostic tool with built in oscillography to assist in the rapid analysis and resolution of faults after a generator, load or distribution failure.

5.6.4 Power systems equipped with such dedicated, specialist generator protection, (operated in a closed bus/ring configuration) are capable of undertaking industrial missions with significantly reduced fuel costs, lower emissions, higher reliability and predictability while providing equivalent integrity to those power plants operated in an open bus configuration.

5.7 THRUSTER AUTONOMY AND PROTECTION

5.7.1 Thruster systems can be developed or modified to provide autonomous thruster operation, monitoring and protection. Reliance on a centralized control system is removed (No dependencies). The thruster operates and recovers from power generation and distribution faults without the intervention of a centralized control system. Such autonomy and independence provide both, a high level of resilience to faults as well as a rapid and predictable recovery from faults when they occur.

5.7.2 In a retrofit design, control topology changes are made to ensure that the thruster is as autonomous as possible. However, it is likely that power system topology cannot be modified cost effectively. Additional effort often has to be applied to retrofit designs to ensure that autonomous control and operation is achieved.

5.8 SECONDARY INJECTION OF THREE-PHASE WAVEFORMS

5.8.1 Secondary current and voltage waveform injection is an alternate form of testing provided as part of the design or retrofit process to achieve the Built to Test, Test on Demand and Healthy to Operate design principles / objectives. Waveform injection testing leverages the features of modern-day digital control and protection devices. Embedded control and data analytics can establish deviation from an established model of healthy operation as well as determine if existing healthy status has become ‘stale’ and requires actions to be refreshed. Continuous monitoring of normal operation is compared against stored models as well as a statistical model established from operation. Additionally, further comparisons are made through multiple signal sources and when conditions allow or are warranted by situations, further testing is done through embedded ‘Built to Test’ / ‘Test on Demand’ functionality.

5.8.2 This type of integrated embedded design approach is typically not available in standard industrial switchboard and thruster designs and must be specified as part of the upgrade or newbuild project. Such systems provide a high level of confidence in the health of the system, continuously, and while it is in operation. Relying on real time indicators such ‘healthy to operate’ status to provide a high ‘basis of confidence’ is a significantly different approach to traditional designs that are usually built to demonstrate compliance with (regulatory driven) periodic testing and inspection requirements.

5.9 INDEPENDENT PERFORMANCE VALIDATION (IPV)

5.9.1 IPV is a protection concept designed to be added to any mission critical function / system to independently monitor performance, health and any deviation from an established normal / healthy model. The system is independent of the elements that are being monitored. In the event that IPV detects abnormal operation it can provide a configurable tiered level of response from notification to a supervisory system capable of isolation / shutdown of the function. This independent device provides protection in redundant and non-redundant systems, where failure of a common element can have adverse impact on the remainder of the plant, potentially affecting other functions cascading to a complete failure of the mission critical function / system.

5.9.2 In addition to a healthy status, output from IPV can be collected and analyzed against a community of other similar functions as well as combined with other data to provide value added data analytics and further insight into the operation of the plant and comparison to other plants carrying out similar missions.

5.10 THRUSTER HYBRID POWER AS PART OF LIFE CONCEPT

5.10.1 Energy Storage in the form of batteries or other devices may be applied at different points in the power systems (See Figure 5-1). Although it is possible to create acceptable designs using a variety of design concepts there are advantages in providing the thrusters with their own dedicated stored energy systems (See Figure 5-2). This concept provides an additional layer of defense against loss of power to a thruster function through built in energy storage supplied directly to the thruster prime mover and critical auxiliaries.

5.10.2 In the event of a partial failure (complete bus) or complete failure of the infrastructure required to support and provide power to the thrusters, the thruster hybrid power system is able to be isolate the thruster from its main power supply and continues to provide power to the thruster prime mover and critical auxiliaries. This makes the thruster completely autonomous for a finite amount of time. The amount of time is dependent on the power required and amount of energy storage that is in the system. The duration of this autonomous capacity and therefore the amount of energy storage required is determined by the operating profile of the asset and the time required to safely suspend operations plus a design safety margin.

5.10.3 While the infrastructure that provides power to thrusters is made to be as robust and reliable as possible and the redundancy concept is designed to prevent loss of all thrusters, there are failure modes that have resulted in loss of power to all thrusters on a vessel. These failure modes include external influences (e.g. environment (i.e. gas), spurious triggering of ESD, human error, etc.)

5.10.4 In essence, this system provides time when it is needed most. This time can be the difference between a failure cascading to a catastrophic failure and a favourable recovery from a critical failure.

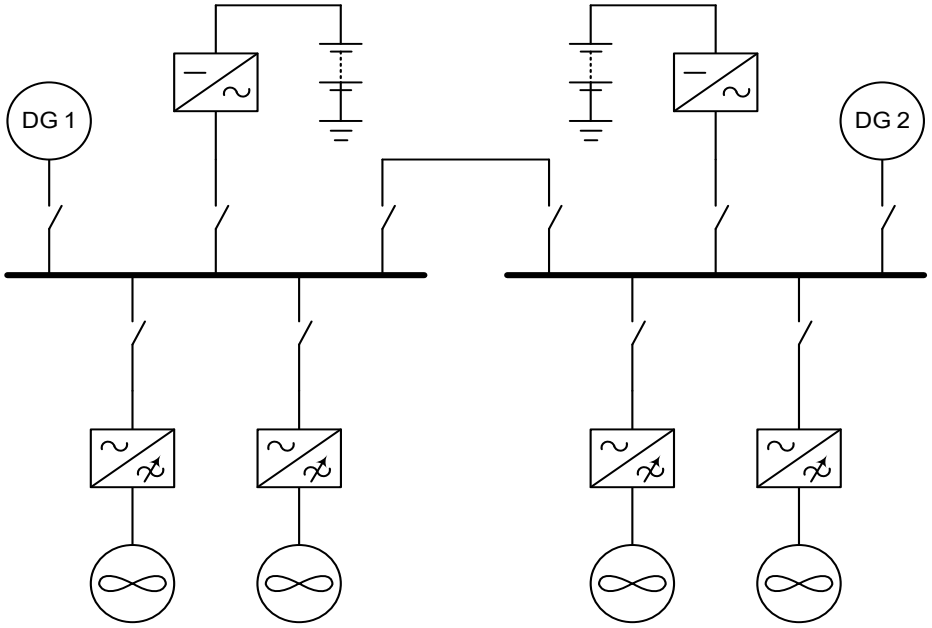


Figure 5-1 Example of Battery on Board Design (BOB)

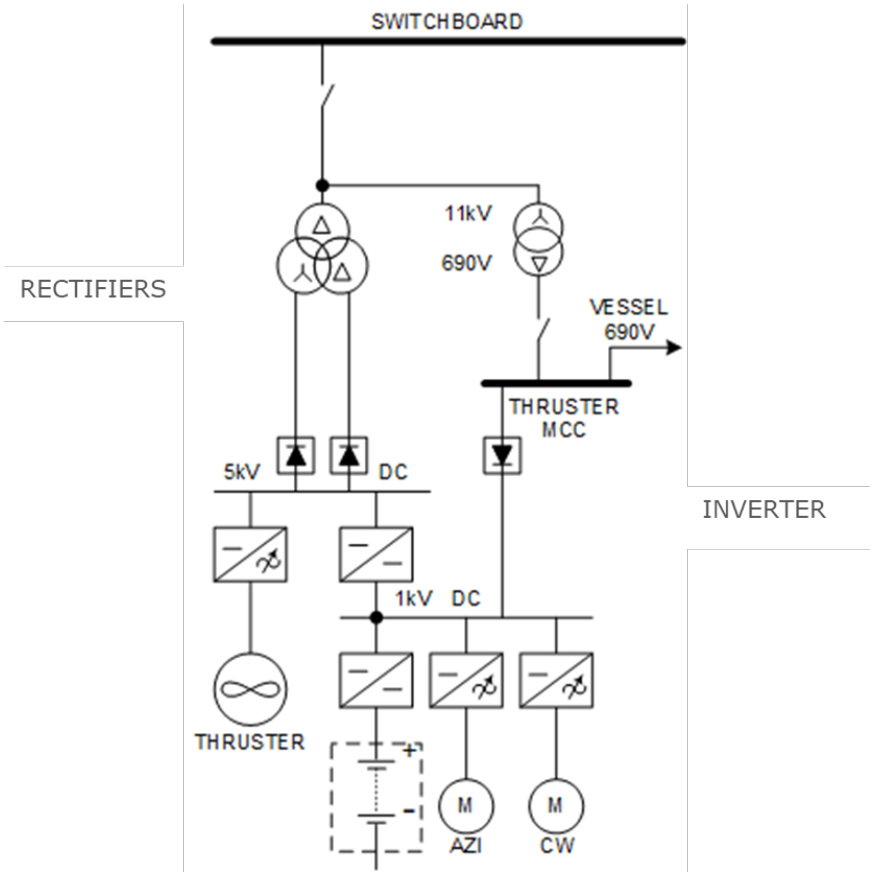


Figure 5-2 Example of Battery on Thruster Design (BOT)

5.11 VERIFICATION AND VALIDATION OF LIFE CONCEPT DESIGNS

5.11.1 A high-speed data logging eco-system with built in test equipment makes the initial and period verification and validation of LIFE concept designs much easier, more efficient and much more effective than traditional verification and validation processes. Key points include:

- A Systems Engineering approach is applied and documented (including but not limited to FMEA and Proving Trials).
- Supporting studies are commissioned as required to prove any assumptions upon which the FMEA depends for its conclusions of single fault tolerance.
- Any dependencies with other parts of the DP system (that are introduced to provide advantages) must be clearly identified and fail to a safe condition.
- Analysis should be comprehensive and accompanied by a robust verification and validation program.

Notes:

Analysis is deemed to be comprehensive when it covers all aspects of design and intended functionality.

The conclusions arrived at from the analysis must be transparent.

The basis of the conclusion and transparency are clearly articulated and independently verifiable.

Analysis and conclusions 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 benign, aggressive and hidden failure modes. The failure mode identification should incorporate 'build to test' and 'built in test capability' requirements.

Benign failure modes are often characterized by failure to some inactive state. For example, cessation of a function, failure to zero speed or power. Failure to logic low.

An aggressive failure mode is one where the item fails in an active way e.g. to full speed or power or to logic high.

A hidden failure mode is one which may cause an unacceptable failure effect if a second fault occurs when the hidden failure is present. Means to reveal such hidden failures should be part of the design and may include alarms, diagnostics and test procedures.

FAT, CAT and SAT should incorporate elements of testing to prove performance, protection and detection and predicable failure effects in addition to proving functionality.

6 CAPABILITY

6.1 INITIAL DESIGN PROCESS

6.1.1 It should be recognized that Classification Rules or Regulations do not specify the station keeping capability of DP vessels.

6.1.2 The first step in the design process is to establish the desired capability and is typically stipulated by the owner. Achieving the required capability is an iterative process during design and should be carried out to establish the amount of thrust and power to be installed.

6.1.3 The following should be taken into consideration:

1. Industrial Mission of the vessel.
2. Objectives to be achieved (Operational uptime, limiting loss of post failure thrust capability).
3. Environmental parameters under which the Industrial mission is to be undertaken.
4. Transit capability desired.
5. Limitations imposed by:
    - Hull form (impacts on wind and current drag coefficients, thruster to thruster and thruster to hull interaction).
    - Environment (current inflow and impact on thrust).

6.1.4 A robust iterative process as described above should result in well-designed vessel with matched power plant (station keeping and industrial mission requirements being met) capable of accomplishing its industrial mission.

6.1.5 The Holding Capability of a vessel is depicted in capability plots. IMCA M 140 addresses specification for capability plots.

6.1.6 A facility to create online capability plots can typically be provided by DP equipment manufacturers. This is a desirable feature and should be specified.

6.2 CAPABILITY PLOTS

6.2.1 The station keeping capability of a DP vessel is not covered by any rules or regulations. It is typically determined or specified by the owner of the vessel. The capability, however, must be demonstrated by submittals to the classification body. Upon approval, the capability documentation will become a part of the vessel's operating manual and describes the limits of operation of the vessel in the intact and ‘post worst-case failure’ condition.

6.2.2 The station keeping capability of the DP vessel is typically presented as a set of polar plots indicating the performance of the vessel under certain environmental and, in some cases, operational conditions. The environmental conditions include the forces due to wind, current and waves. Capability plots should take into account changes in the wind or drag coefficients caused by execution of industrial functions. e.g. pipe tension, heavy lift drag, hawser tension, etc.

6.2.3 A capability plot is an analytical presentation of the vessel's performance during station keeping operations while exposed to external forces - environmental forces such as wind, current, and waves - as well as external force generated by industrial mission of the vessel. Static capability plots do not indicate the excursions of the vessel. They represent analysis of the equilibrium of the steady-state forces and moments of the vessel and establish the static holding capabilities. A dynamic time-domain simulation is not required by the classification societies.

6.2.4 If an alternate centre of rotation (other than centre of gravity / centre of vessel) is contemplated as a means to undertake the industrial mission, capability plots should be developed for this condition for both intact and post worst case failure scenarios.

6.3 ENVIRONMENTAL FORCES

6.3.1 The plots should be generated for environmental events controlling the limits of DP operations that are likely to occur at the anticipated sites of operation. Maximum predicted combinations of current and wind speed with associated wave height and period should be considered.

6.3.2 The classification societies require that the plots should be generated assuming that the environmental forces are imposed on the vessel collinearly and concurrently.

6.3.3 It may be necessary to generate capability plots that consider other combinations of wave and wind direction specific to the area of operation.

6.4 THRUSTERS

6.4.1 The thrusters generate the counter forces necessary to establish the force equilibrium. A realistic assessment of the actual thruster net forces acting on the vessel is a prerequisite for accurate polar plots.

6.4.2 The following should be considered when assessing actual thruster net forces:

1. The basic thruster performance data should be based on sound hydrodynamic principles, not on marketing considerations.
2. The thruster data used for generating capability plots at different current inflow velocities should be based on performance curves for that inflow velocity. Using bollard pull data which is usually based at zero inflow velocity leads to inaccuracies.
3. The potential impact of current inflow on thrusters that are not aligned with inflow should be considered.
4. The thruster performance data provided is usually for open water conditions. Thruster data used for station keeping calculations should account for thruster to hull interaction losses. The magnitude of the losses is a function of the hull shape, thruster location, degree of tilt of the propeller or nozzle axis, etc.
5. ‘Barred zones’ prevent thrust in defined sectors. These zones can be created in the DP control system software to address issues associated with thruster wash for azimuthing thrusters. Such barred zones may result in reduced capability. Typically, the arc of this sector is small and the associated losses are a few percent of the nominal thrust.
6. 100% thruster power in DP is not always the actual 100% power due to scaling the thruster in DP within a linear range. Some drives are tuned 0-80% or similar leaving less power available in DP.
7. The thruster power used for generating capability plots should be based on the actual maximum power achievable in DP control.

6.5 CAPABILITY PLOTS FOR INTACT AND FAILURE CASES

6.5.1 Capability plots should be developed for multiple cases based on the specific vessel configuration. The following cases are offered as an example.

1. Intact - All thrusters are available.
2. Failure mode 1 - One thruster not available (selecting the worst case).
3. Failure mode 2 - Two thrusters not available (selecting the worst case).
4. Failure mode 3 - Worst Case Failure Design Intent.

6.5.2 Other thruster configurations may be investigated if warranted.

6.5.3 Capability plots should consider the influence of the power plant,(including limitations if any) and power available to the thrusters not just rated capacity.

6.6 PRESENTATION OF CAPABILITY PLOTS

6.6.1 Capability plots should be easy to understand, comprehensive and informative.

6.6.2 Several types of static plots are common in the industry. Dynamic plots are also available and useful when knowledge of the maximum excursion is important. This section addresses static plots.

6.7 BASIC PLOTS

6.7.1 This is the most common type of plot. It presents the maximum (only) capability of the vessel under certain environmental conditions and intact/failure modes and could be used during the preliminary design phase.

6.7.2 Typically, one environmental criterion (e.g., current velocity) is selected for the plot, together with intact or failure mode data. The resulting plot indicates the maximum station keeping capability of the vessel for the remaining environmental forces (e.g., wind and associated waves for a given, predetermined relationship between wind velocity and waves) over an environmental force incident angle of 0-360 degrees. These types of plots are valid only for the assumed relationship between wind velocity and wave data and consequently apply only for one particular operational region.

6.7.3 These plots typically do not consider the influence of the power plant. It is recommended that an iterative process be carried out to validate the basic capability plots once the power plant design is available. The validity of these plots depends upon the accuracy of the power plant data which is in turn dependent on knowledge of the capacity and efficiency of all components of the power plant and thruster drives.

6.8 COMPREHENSIVE PLOTS

6.8.1 These types of plots allow an individual input of wind, current and wave data (in magnitude and direction) and display the power required for the thrusters over 360 degree heading angle of the vessel. These plots allow the selection of optimum heading angles and indicate the exact power levels for the thrusters which is a valuable tool for the optimized operation of the vessel. The validity of these plots depends upon the accuracy of the power plant data which is in turn dependent on knowledge of the efficiency of all components of the power plant and thruster drives.

7 MODELLING

7.1 SCOPE OF MODELLING

7.1.1 Modelling as referenced in this section addresses pertinent topics related to design in the following areas:

1. Naval Architecture.
2. Power and Safety Systems.
3. Operability Parameters.

7.2 NAVAL ARCHITECTURE

7.2.1 Modelling in Naval Architecture can be accomplished in the following three ways:

1. Modelling by example (prior example - build like before).
2. Analytical modelling.
3. Hull form modelling.

7.3 MODELING BY EXAMPLE

7.3.1 Prior example is the simplest modelling technique. In this method an existing design with validated performance characteristics is used. Prior example could be effective when replication allows cost and schedule benefits without compromising the performance of the industrial mission.

7.3.2 Designing by prior example may preclude opportunities for improvement. When opportunities for improvement are pursued as an objective, it should be accompanied by a robust MOC process. It is important to consider the impact in differences between applications and avoid replicating any inherent weaknesses in the design.

7.4 ANALYTICAL MODELING

7.4.1 Use of analytical modelling, early in design, facilitates delivery of a robust vessel. Advances in computing technology have resulted in effective tools capable of aiding design decisions (e.g. Computational Fluid Dynamics (CFD), optimization of tilt of azimuthing thrusters)

7.4.2 Analytical modelling could be used as a technique to aid in establishing preliminary thrust requirements for further iterations in the design cycle. (Station keeping capability)

7.5 HULL FORM MODELING

7.5.1 Hull form modelling for DP vessel design is suggested when:

1. Validation of analytical modelling data is warranted.
2. Novel hull forms or prototypes are being considered.

7.5.2 Hull form modelling is accomplished at:

1. Test Basins.
2. Wind tunnels (to establish wind and current drag coefficients).

7.5.3 Hull form modelling for non-prototype / non-novel vessels, as the primary means of establishing station keeping performance, delivers limited value due to cost, scaling factors, and availability of alternate means of establishing equivalent data.

7.5.4 Information availability on station keeping performance is usually the driver to initiate hull form modelling. This information can be established by analytical modelling.

7.6 POWER AND SAFETY SYSTEMS

7.6.1 **Power systems:** Advances in computing technology have facilitated the ability to accurately model power plants:

1. Stability.
2. Harmonics.
3. Resonance.
4. Protection coordination.
5. Short circuit withstand capability.
6. Load analysis.

7.6.2 Adopting these techniques in the design phase enables delivery of a fault tolerant/fault resistant system capable of meeting station keeping requirements and the industrial mission of the vessel.

7.6.3 **Safety systems:** Advances in computing technology have facilitated the ability to use modelling as an effective technique to:

1. Analyse Major Events (e.g. gas dispersion studies).
2. Safety Integrity Levels (SIL) (Establishing and analysing Cause and Effects Matrix for ESD systems, ability to carry out “what if analysis”).

Modelling techniques mentioned above provide design support and can be carried into operations by facilitating decision support.

7.7 OPERABILITY PARAMETERS

7.7.1 The ability of the vessel to carry out its industrial mission is dependent on the respective vessel motions in addition to its station keeping capability. The optimum heading for reducing thrust for station keeping may not be the optimum heading to be within the limits for motions to carry out the industrial mission. Modelling to establish RAOs (Response Amplitude Operators), during the iterative design process for determining thrust requirements, aids in decisions such as evaluating the benefits of additional thrust versus potential mission uptime.

7.8 PRIOR EXAMPLE

7.8.1 Prior example is the cleanest form of modelling. It is effective when performance expectations are met and relies on replication in the following areas:

1. Vessel hull form.
2. Range of environmental conditions.
3. Industrial mission.

7.8.2 It offers the following advantages:

1. Costs for engineering and design are far less.
2. There is high probability that it will work and perform to expectations.
3. Reduced construction time if replication is extended to the yard and project team.

7.8.3 Care should be taken to avoid replicating mistakes.

7.8.4 There are many issues that can make use of a prior example inappropriate. For example, a change of mission, deeper water, mixing of drilling and construction functions and most of all advancing technology.

7.9 ANALYTICAL MODELING

7.9.1 Analytical modelling is an effective tool to aid design.

7.9.2 There are well established techniques and equations that allow calculation of wind drag, wave drift force and current drag on a vessel from all directions. Guidance on calculation is provided in API RP 2 SK and can be used to calculate the thrust requirements for a DP vessel. These values are used as the starting point for DP control system tuning. Final values are established as the result of the tuning effort.

7.9.3 The ability to carry out numerical analysis has been enhanced by the use of modern computers. Numerical analysis can be used to model dispersion of thruster wakes and losses from all forms of the Coanda effect. Such modelling has aided in the optimization of the tilt down angle for thrusters to minimize loss of thrust.

7.10 PHYSICAL HULL FORM MODELING

7.10.1 Test basins were the only established form of physical hull form modelling until the advent of wind tunnels. After accounting for scale and viscosity, testing of a small model of a large hull in a wind tunnel can yield comparable results to test basin.

7.10.2 Test basins are generally used to establish:

1. Expected vessel motions in different sea states including green water impacts.
2. Expected speed in different sea states.

7.10.3 Test basins have been used to validate DP station keeping capability. The intent was to measure how ‘tightly’ the vessel is able to hold position on DP using a particular DP control system. While this is a question asked by those new to DP, the results (test basin and full scale test) have shown that most DP control systems can maintain position to within a meter in calm weather and a few meters in rough weather. That is up to the point where the available thrust is exceeded when the vessel will drift at a rate proportional to the exceedance of the weather against the available thrust.

7.11 POWER SYSTEMS

7.11.1 Mathematical models of power systems should include:

1. Transient stability - The ability of generators to remain in synchronism following power system transients.
2. Power system voltage ride through capability following the worst case transients due to faults such as short circuit and generator loss of excitation.
3. Harmonics and resonance - To confirm levels of power system harmonics remain within acceptable values.
4. Protection coordination - The ability of a protection scheme to isolate a fault at source.
5. Load analysis - To confirm all power sources are capable of supplying the expected load.
6. Short circuit withstand and breaking capacity of switchboards and switchgear.

7.11.2 It should be noted that power system studies for main-class notations do not necessarily cover the full range of failure modes that may be experienced from a ‘continuity of supply perspective’ (safety focus only).

7.11.3 The faults listed below are some examples that may not be addressed from the perspective of maintaining continuity of electrical supply for DP:

1. Over voltage, under voltage.
2. Over frequency, under frequency.
3. Earth fault.

7.11.4 Requirements for main-class, if any, are focused on protecting personnel and equipment and may not address the needs of the industrial mission.

7.11.5 Addressing the full range of power plant failure modes in appropriate studies during the design phase aids delivery of a fault tolerant / fault resistant system capable of meeting the station keeping needs and the industrial mission of the vessel.

7.12 OPERABILITY PARAMETERS

7.12.1 The ability of the vessel to carry out its industrial mission is dependent on vessel motions in addition to its station keeping capability. The optimum heading for reducing thrust for station keeping may not be the optimum heading to restrict vessel motions to the maximum allowed for the Industrial mission. Modelling to establish RAOs during the iterative design process of determining thrust requirements, aids in decisions evaluating benefits of additional thrust to increase potential mission uptime.

7.12.2 Umbilical lay vessels experience similar issues. In this case the governing factor is restrictions on vessel heading rather than vessel motions. There might be the need to maintain required pipe tension following the worst case failure. Such industrial mission requirements may be enhanced by modelling modes such as follow target mode to provide predictability during DP operations.

8 MANAGEMENT OF CHANGE IN DESIGN (MOC)

8.1 REQUIREMENTS FOR MOC

8.1.1 A robust Management of Change Process should be established at the concept phase, implemented systematically and followed diligently throughout the Project life cycle. The MOC process should be in place prior to finalizing the redundancy concept for the vessel. Any changes to the redundancy concept should be subjected to the MOC process.

8.1.2 Integrity of the MOC process should be maintained, communicated and used effectively. All stakeholders should have ownership in the process. Rationalization of changes by specific disciplines should be avoided as changes may impact other disciplines.

8.1.3 Any changes to the redundancy concept should be subjected to the MOC process.

8.1.4 Changes to the redundancy concept are relatively rare but when they occur they can have a broad effect on vessel design. For example:

1. Changes to the vessel industrial mission.
2. Changes to the desired post failure capability of the vessel that changes the redundancy split say from a two way split to a four way split (to reduce the impact of the worst case failure).

8.1.5 MOC should identify all the design changes required so that the vessel's revised design will comply with the new redundancy concept.

8.1.6 Changes in the design that violate the redundancy concept are more common. Diligent application of the MOC process could aid in avoiding such violations.

8.1.7 Configuration changes to DP control systems and other equipment with software (e.g. automatic power management systems) are particular examples of failure to apply the. MOC process.

8.2 MOC EXAMPLES

1. Vessel moves to a new work location where a different setup is required for the acoustic position references to accommodate SIMOPS with several vessels (Wide band). Failure to control the change in working location under the MOC process could result in degraded position reference status in that location.
2. A drilling vessel was originally equipped with two DGNSS. Modifications were made to add several more DGNSS without understanding the consequence of relying so heavily on the DGNSS as a reference to the detriment of the hydro acoustic references.
3. To solve an unrelated reliability problem, a thruster drive manufacture adds an under-voltage trip to a thruster variable speed drive without fully understanding the consequences for the redundancy concept. This modification removed the drive's voltage dip ride through capability leading to multiple loss of thrusters when short circuit fault occurred in the power distribution system.
4. An ESD system was fitted to a MODU without a systems engineering approach resulting in a design which introduced single point failures. A blackout occurred when the ESD system failed.
5. Operational impact of working in shallower water depth not understood and appropriate barriers (equipment and procedures) not implemented.

9 THRUSTERS

9.1 PRINCIPLES

9.1.1 Thrusters as referenced in this section means propulsion to achieve:

1. Transit.
2. Station keeping using dynamic positioning.

9.1.2 Designers of DP vessel propulsion systems should incorporate the following principles in design:

1. Robustness.
2. Reliability.
3. Simplicity.
4. Redundancy.
5. Efficiency.
6. Maintainability (routine and intrusive IRM).
7. World Wide Operations (temperature ranges, ice).

9.2 PROPULSION CHOICES

9.2.1 Propulsion system choices are mainly threefold:

1. Azimuthing propulsors & cycloidal.
2. Fixed direction propulsors.
3. Vessels using a combination of fixed and azimuthing propulsors.

9.2.2 When choosing propulsors during the design phase, the following should be taken into account:

1. Reliability.
2. Service intervals.
3. The industrial mission (station keeping versus transit requirements).
4. Desired hydrodynamic aspects.
5. Number of thrusters with respect to post failure thrust capability and ability to exercise control in surge, sway and yaw axis.
6. Location and geometric arrangement.
7. Installation and maintainability methodology over life cycle of vessel - Service access (keel haul, dry dock, retractable).
8. Influence of the hull form.
9. Drive system.
10. Hybrid power.
11. Control of thrust.
12. Regulatory requirements for dry docking of vessels with tail shafts.
13. Draught restrictions.

9.2.3 The impact on the Industrial mission and the stated objectives due to a loss / reduction of thrust following a failure event should be recognized and carried through all phases of the design cycle. Particular attention should be given to:

1. Seals.
2. Auxiliary systems (principles of independence to be followed).
3. Ease of maintenance.
4. Specification and testing of key components (e.g. gears).
5. Impacts of vibration.
6. Introduction of vulnerabilities to thrusters not in use during transit.
7. Life extension of components and thruster.

9.2.4 Incorporating non-critical redundancy into identified elements of the propulsion systems could aid in mission uptime. Robust FMEA / FMECA techniques can aid in identifying such key elements.

9.2.5 There has been a noticeable reduction in failure rates of thrusters since the introduction of variable frequency drives (VFDs) with fixed pitch propellers. VFDs facilitate fast phase back capability, a key feature to prevent power plant instability.

9.2.6 Adding energy storage (typically batteries) directly at the thrusters can provide propulsion capability during a power plant blackout even if the power distribution system is damaged or otherwise unavailable. This should be considered as an alternative or supplement to adding electronic generators and energy storage to the main bus.

9.3 DESIGN BASIS CRITERIA

9.3.1 A DP vessel is subjected to environmental forces such as wind, waves, and current. In order to maintain a certain position, these forces have to be counteracted by the vessel's propulsors.

9.3.2 The dynamically positioned vessel has to be able to provide the forces required to execute manoeuvres in surge, sway, and yaw. The total forces must be controllable in magnitude from zero to full power, and in direction through 360 degrees.

9.3.3 A variety of propulsor options are available to generate thrust for station keeping.

9.3.4 The propulsion system of a typical DP vessel has to be developed to comply with the following mission requirements:

1. Transit over extensive distances.
2. Optimum speed (typically 12 -14 knots for ship-shaped vessels and 5 - 7 knots for semisubmersibles).
3. Station keeping for extended time periods.

9.3.5 The following **design basis criteria** should be applied by the designers of the propulsion system:

1. Robustness.
2. Reliability.
3. Simplicity.
4. Redundancy.
5. Efficiency.
6. Maintainability of systems without outside support or dry docking.

9.4 PROPULSION CONCEPTS

1. Azimuthing propulsors.
2. Fixed direction propulsors.
3. Hybrid concepts utilizing a combination of azimuth thrusters and fixed-direction thrusters.

9.4.1 The characteristics of propulsors are outlined in the table below.

Table 9-1 Propulsor Characteristics

TYPE	APPLICATION	ADVANTAGES	DISADVANTAGES
Propulsors with fixed direction of thrust			
In-Line Conventional propulsion systems	Used widely for transit as well as station keeping (providing thrust in longitudinal direction) on ship shaped DP vessels (OSV's, diving support vessels, pipe-laying vessels, older generation of drill vessels)	Simple, reliable, robust and proven system. Very low maintenance, highly efficient for DP when equipped with ducted propellers	Requires reverse gear or CP propeller to change direction from AHEAD to ASTERN. Additional thrusters needed for transverse thrust forward and aft. Efficiency reduced in reverse operations
Transverse Tunnel Thrusters	Installed in the bow and/or stern of vessels to provide transverse thrust and forces for yaw manoeuvres	Simple installation inside a transverse tunnel in the hull. Well protected; hydrodynamically smooth uniform operation; long life	Mediocre performance (depending on length of the tunnel, tunnel exit/entrance configuration). For fixed pitch propellers, reversing of the sense of rotation is required to change the direction thrust. No access for maintenance. Removal/installation requires drydocking in most cases; may lose thrust during heavy motions of the

TYPE	APPLICATION	ADVANTAGES	DISADVANTAGES
Ducted transverse thrusters	Installed below the hull, forward and aft to provide transverse thrust; mostly installed in retractable containers. Bi directional ducts and propellers generate equal amounts of thrust in both transverse directions. Many successful installations on first generation DP drill vessels	High performance in both directions. Simple and robust design. Access for maintenance after retracting the assembly	For fixed pitch propellers, reversing of the sense of rotation is required to change the direction of the thrust.
Propulsors with directional control of thrust			
Azimuth thrusters including Azipods	Most popular thrusters applied for transit as well as station keeping for DP MODUs (Mono hull and column stabilized) Typically installed under the bottom of the hull thus increasing the draft of the vessel, Smaller ship shaped DP vessel (OSV's etc.) uses azimuth thrusters installed in the skeg of the vessel (above the base line). Installation forward requires retractable azimuth thrusters to minimize draft during transit	Reliable proven designs, High performance. Bottom mounted thrusters are accessible for maintenance after underwater removal, No drydocking required for maintenance. Containerized azimuth thrusters:- This thruster is installed in a watertight container which encloses the drive motor and the auxiliary systems. The entire container is retractable to a position above the waterline at which servicing the thruster is feasible. This is the optimum installation for DP application if achievable.	Underwater installation and removal complicated and time consuming. Requires support vessels in many cases. Retractable azimuth thrusters (without containers) are mechanically complex, expensive, require a high degree of maintenance. Access typically only during dry-docking. Custom dock preparations necessary

TYPE	APPLICATION	ADVANTAGES	DISADVANTAGES
Voith Schneider propellers (VSP)	A very special type of propulsor applicable for DP operations. It is a cycloidal propeller operating on a vertical axis.	The VSP is an ideal propulsor for DP combining the propeller characteristic of a controllable pitch propeller combined with control of the direction of thrust through 360 degrees. Allows step less control of thrust in magnitude and direction. Can be supplied with active anti-roll system. (This might introduce commonality and use on DP should be subject to the same verification and validation processes as the rest of the DP system)	The mechanical complexity, high costs, and maintenance of a large diameter seal limit the application to low draft vessels and usually for specialized applications.

9.5 LOCATION AND GEOMETRICAL ARRANGEMENT OF THE PROPULSORS

9.5.1 The layout of the thrusters should be such that effective thrust can be generated in surge, sway and yaw in both intact and post worst case failure conditions. Effective thrust capability is dependent on the lever arms. This should be taken into consideration during the design phase. Location of thrusters should be optimized and is dependent on the hull geometry.

9.5.2 For a monohull, the most onerous criteria for the assessment of the DP capability of a vessel are its performance when exposed to environmental forces from the beam direction. A vessel which excels in this condition typically performs well in any other situation. Care should be exercised when assessing DP capability of a vessel where a portion of the thrust is required to carry out the industrial mission (for example thrust to overcome bottom tension on a S-Lay pipe lay vessel.

9.5.3 For effective counter forces against wind, the size (capability) of the thrusters should be approximately proportional to the windage area at the area of installation. In other words, a vessel with a high superstructure forward requires the installation of adequately sized thrusters forward. Failure to follow this basic design philosophy introduces the potential to lose station in conditions where the wind velocity and direction is shifting rapidly (numerous instances of occurrence in the Gulf of Mexico).

9.6 THRUSTER-THRUSTER INTERACTION

9.6.1 In order to minimize negative effects caused by thrusters interacting hydro-dynamically with each other, the distance between thrusters should be maximized to the extent feasible.

9.7 THRUSTER- HULL INTERACTION

9.7.1 The operation of a thruster in the vicinity of a body such as the vessel's hull may result in interaction effects resulting in a reduction of effective thrust. The tilting of the nozzle or (better) of the propeller axis several (optimum approximately 7 to 8 degrees) reduces the interaction losses noticeably. In addition, this also reduces the thruster-thruster interaction losses.

9.8 HYDROPHONE INTERACTION

9.8.1 For DP vessels equipped with acoustic equipment installed under the hull, an interference of the thruster wake (jet) and the hydrophones should be avoided.

9.9 MINIMUM NUMBER OF THRUSTERS

9.9.1 The number of thrusters should be determined by:

1. The ability to develop forces in surge, sway and yaw post worst case failure.
2. Classification society requirements for redundancy post worst case failure.
3. The desired post failure DP capability for the industrial mission.
4. Maintenance considerations - maintaining redundancy for both intact and post worst case failure conditions when a thruster is taken out of service for IRM. For example, a scenario where a vessel with a four-thruster configuration where power distribution is such that two of them come off each switchboard. When one thruster is required to be taken out of service - post worst case failure capability is reduced to one thruster and vessel may not be able to maintain station.

9.10 THRUSTER HANDLING REQUIREMENTS OVER LIFECYCLE

9.10.1 The choice of handling options should be made during the design phase taking into account the industrial mission over the lifecycle of the vessel. A variety of handling options are available:

1. For below hull azimuthing thrusters, the underwater mountable and removal feature should be considered if dictated by the industrial mission. Handling aids should be designed for the range of environmental conditions contemplated for this activity.
2. Thrusters installed in capsules which are retractable inside the hull allow access for minor repairs, e.g. service to the propeller shaft seals.
3. Access to non-retractable thrusters may require dry docking the vessel or provision of special arrangements to facilitate intrusive maintenance (for example habitats) or special docking arrangements to allow lowering of the thrusters inside the dock.

9.11 BASIC THRUSTER HYDRODYNAMIC ASPECTS

9.11.1 Thruster design requirements for DP operations may conflict with those of transit:

1. Thrusters for station keeping are normally designed to operate in zero or low velocity inflow conditions. Optimizing the thruster design for this condition leads to a thruster with a large propeller diameter turning at a relatively low rpm. Thrusters exclusively applied for station keeping should be designed with these features.
2. Thrusters for transit are normally designed to operate at high inflow velocities leading to propellers with smaller diameters turning at higher rpm.
3. For applications which require the thrusters to provide thrust for station keeping and for transit operations (e.g. DP drill vessels, DP OSVs), the thrusters should be designed for the best compromise between the two operating scenarios.

9.12 THRUSTER DRIVE SYSTEMS

9.12.1 Thruster drive systems can be:

1. Electric motors - AC induction, synchronous, DC (less frequently used).
2. Hydraulic motors.
3. Direct drive by diesel engine.

9.12.2 Electric motor driven thrusters are most common in DP service. Thrusters that are driven directly by diesel engines are common in logistics vessels. Some vessels are outfitted with thrusters powered by hydraulic motors.

9.12.3 Most modern day electric motors for thrusters are powered by AC variable speed drives. The characteristics of these drives are a good match to the characteristic of a propeller. The drive system is capable of delivering a constant maximum power over a certain rpm range of the motor (approximately + 10 to 15% of the base rpm). This feature is similar to the field weakening feature of older DC/SCR controlled systems; however, it utilizes simpler components (i.e. motors) and operates at higher efficiencies.

9.12.4 A thruster drive system for a DP semisubmersible, for instance, can be designed to deliver maximum power to the thruster over the entire operating range of the vessel. In this case, the thruster propeller pitch is selected for bollard pull. By increasing the rpm (by field weakening), full power is available even at a transit speed of 5 to 7 knots.

9.12.5 For a typical DP monohull vessel, the operating range is too large to utilize the field weakening effectively. The propeller pitch has to be optimized between bollard pull and transit to deliver an effective thruster.

9.12.6 Thrusters (or in-line main propellers) with fixed pitch propellers driven directly or through a reduction or reverse/reduction gear by Diesel engines are not able to control the lower part of the engine rpm below the engine's minimum idling rpm, which is approximately 40% of the rate rpm. Operating the diesel engine in this range with the clutch leads to high wear of the clutch and is not desirable. Where thrusters are driven by diesel engines, control of thrust in magnitude and direction (ahead/astern) is best achieved by a controllable pith propeller (see also below: Control of Thrust).

9.13 CONTROL OF THRUST

9.13.1 Thrusters in DP service must provide controllable thrust from zero load to full load in stepless increments. This can be achieved through control of the propeller pitch or the speed of the propeller.

9.13.2 Controllable pitch (CP) propellers: Before the introduction of devices allowing the control of the rpm of electric motors, this was the predominant method of thrust control. The complexity of the mechanical pitch control and its inaccessibility for service caused many failures of these systems in the past.

9.13.3 Thrusters of fixed pitch design, driven by electric motors controlled by variable speed drives are more common. This approach has increased the mechanical reliability of thruster systems.

9.13.4 The exception is thrusters (including in-line main propulsion systems) which are driven by diesel engines. The characteristic of the diesel engine and its inability to control the rpm over the full operating range generally excludes a direct (or geared) drive of a thruster with a fixed pitch propeller. CP propellers and slipping clutches have been used for lower power applications.

9.14 THRUSTER VARIABLE SPEED DRIVES

9.14.1 **General:** The voltage source Pulse Width Modulation (PWM) convertor is the most common type of variable speed drive installed for DP propulsion systems and is used with asynchronous (induction) motors. Induction motors are highly reliable. This type of drive is able to convert power at fixed voltage and frequency to power at variable voltage and frequency using power electronic switches. This type of drive may have a rectifier front end or an active front end.

9.14.2 Load Commutated Invertors (LCI) drives are also available. These are current source convertors and are used with synchronous motors for higher power applications.

9.14.3 DC drives for propulsors are typically based on fully controlled rectifiers driving shunt excited motors. DC drives are relatively inexpensive and are still used in some propulsion applications for this reason. It can be difficult to make DC drives fully fault tolerant as they are prone to commutation failure associated with power system transients. The dc motor has reliability issues and more onerous maintenance requirements than ac motors.

9.14.4 **Reliability:** Variable speed drives have adequate reliability but several failures in the lifetime of a vessel can be expected. Modular design allows rapid repair if a stock of critical spares is maintained. Reliability may be influenced by environmental conditions. Elevated temperatures and salt-laden atmospheres reduce reliability and consideration should be given to installing the drives in a clean air-conditioned compartment.

9.14.5 **Failure modes:** Modern variable speed drives generally fail to zero speed. It may be necessary to make special arrangement to test the failure modes of internal control loops due to perceived risk of damage. For this reason, it may be advantageous to conduct such testing at FAT when technical expertise is available to support the testing. DC drives may fail to zero speed or full speed in some designs. Failure to full speed (significantly increased thrust) is generally not accepted in DP rules and guidelines and should be addressed appropriately in the design.

9.14.6 **Water cooling:** Many modern drives use water-cooling to conduct away significant amounts of unwanted heat from power electronic devices. Rupture of water cooling systems within the drive cabinet can develop into a short circuit fault on the main power system which may have failure effects of greater severity than loss of the drive itself. Design should carefully consider the robustness and failure modes of the cooling water system. Hose terminations may need careful attention. It may be beneficial to monitor cooling water system flow. Some variable speed drives use high purity de-ionized water. The cooling water system will typically contain instrumentation intended to confirm the purity of the cooling water. The control systems for these cooling water skids may carry out various checks on restoration of power which may delay starting of the thruster. These features should be considered when developing blackout recovery functions.

9.14.7 **Obsolescence:** Design should consider obsolescence of power electronic technology. This issue should be discussed with the variable speed drive manufacturer.

9.14.8 **Field weakening:** This is a feature that allows the thruster motor to run 10 to 15% over base speed for certain applications. It may be useful in transit applications and should be discussed with the thruster and variable speed drive manufactures at the design stage.

9.14.9 **Ride through capability:** This is an essential feature in any variable speed drive to prevent unwanted tripping of the drive on power systems transients. Vessels intending to operate the power plant as a common power system should be able to confirm the ride through capability of their drives by testing.

9.14.10 Extended ride through capability can be provided by fitting energy storage (typically batteries) to the DC link of the variable speed drive, typically by way of a DC to DC convertor for voltage matching / control purposes. Energy storage can be applied to the thrusters in other ways too. Energy storage may be arranged to supply power for auxiliaries and steering. This is easier in designs with highly autonomous thrusters.

9.14.11 Failure to achieve sufficient ride through capability can result in the loss of all thrusters leading to loss of position. Parameterization can have significant influence on a variety of drive functions and care should be taken not to defeat the ride through capability by inappropriate selection of parameters or other settings. It is important to consider auxiliary systems such as cooling water and hydraulic pumps as these also require ride through capability. In some cases, it may be possible to achieve this by automatic restart if this method is accepted by the classification society rules for the DP notation being applied for.

9.14.12 **Thruster starting sequence:** The thruster blackout recovery sequence should be carefully designed to optimize starting time reliability. There may be a number of permissive, interlocks and safety shutdowns which can be configured. However, it is important that these are active only when necessary. For example, it may not be necessary to make cooling water flow a start permissive as the drive will later shut down on over temperature if the pumps fail to start. A large number of permissives may reduce the reliability and extend the recovery sequence. In a blackout recovery situation, auxiliary systems may become available at different times depending on the operation of the blackout recovery function. If the drive control system delays starting until auxiliaries become available, the time taken to make the thruster ready for DP can be excessively long or the starting sequence may fail.

9.14.13 **Regeneration:** Some propulsion systems are designed to regenerate significant quantities of power back to the power system during braking manoeuvres. Design should ensure this regenerated power can be handled safely without risk of tripping generators on protective functions. Propulsion systems based on torque control typically do not produce regenerated power. Consideration can also be given to using dynamic braking resistors rather than regeneration as a means of dissipating energy from the propeller. The effect of inflow on starting should be considered. During blackout recovery thruster propellers may be turning due to inflow. Drives without regeneration capability may experience starting problems if the drive is not capable of starting with the propeller turning in forwards or reverse rotation. If one or more thrusters fail to start then blackout recovery may be compromised. Most drives are capable of starting on-the-fly but the issue of starting with inflow should be clarified with the manufacturer.

9.14.14 **Drive operating quadrants:** Selection of operating quadrants depends on the choice of propulsor. Most modern azimuthing thrusters have single quadrant drives which do not reverse direction and do not intentionally regenerate power to the bus. Control issues associated with low levels of environment are generally resolved by using thruster bias. There may be other applications where regeneration and / or the ability to reverse thrust direction without azimuthing are desirable and these should be considered in the design and discussed with the drive and thruster manufacturers. It is important to note that some thrusters are not rated mechanically for significant amounts of reverse thrust.

9.14.15 **Speed and torque control:** Most modern variable speed drives operate on the torque control principle using a mathematical model of the motor. However, speed control and torque control may still be options for the DP control loop and the advantages of each should be discussed with the DP control system manufacturer. Some DP control systems switch from Torque (Force) control to Speed control at low RPM. Careful design of the switching function is required to ensure a bump-less changeover.

9.14.16 **Auxiliary systems:** Auxiliaries such as cooling water pumps and fans should be powered from same source as drive main power. Pre-charging and pre-magnetizing power may be required before the main breaker is closed. The design should carefully consider the need to provide these power sources during normal operation and for blackout recovery. Control power should be provided from a UPS. The main input to the UPS should be from the thruster auxiliary system power supply. A backup power supply to the UPS input should be arranged from the emergency switchboard.

9.14.17 **Protection settings:** Variable speed drives typically have a large number of protective functions designed to protect the drive from damage. Design should carefully review these protective functions to confirm that they do not defeat the redundancy concept or reduce drive availability to unacceptable levels. It should be noted that some drives require local reset following activation of protective functions. This can significantly increase the time required to restart a thruster and design should consider providing a remote reset function.

9.14.18 **Fast phase back:** This feature is provided in most modern variable speed drive systems. It allows the thruster to shed load rapidly in response to falling bus frequency which indicates that the generators are in overload. The phase back function attempts to maintain an acceptable bus frequency during overload conditions. This method of load shedding has several advantages:

1. **Independence:** Each drive makes the decision to shed its load independently of the others reducing the risk of control system failure leading to the loss of more than one thruster.
2. **Continuity:** This function allows time for the power system to recover by connecting standby generators. Phase back is reduced as the power plant recovers.
3. **Integrity:** By basing the phase back function on frequency rather than power the integrity of the load shedding function is not dependent on an assumed generator capacity. Thus, the system will act in response to failures that cause the generators to lose power such as fuel or combustion air problems.
4. **Maximum capacity:** Systems based on maintaining acceptable bus frequency provide access to whatever power is available from the plant even if generators are only capable of reduced capacity.
5. **Load acceptance:** The phase back system can compensate for poor load acceptance in modern medium speed diesel engines. This may be required if the step loads associated with power system faults are greater than the load acceptance rating of the engines.

9.15 MAINTAINABILITY AND MAINTENANCE OF THRUSTERS

9.15.1 The consequences of unavailability of thrusters can be extreme. Design should facilitate uptime, availability and ease of maintenance. The principles of non-critical redundancy, detection, protection, and ergonomics should be incorporated in the design to facilitate maintenance and achieve availability and uptime.

9.15.2 Thrusters should be designed for DP service. The consequences of equipment failure can be significant. For example, in the case of a DP drilling vessel, the financial losses caused by taking the vessel out of service to repair a leaking propeller shaft seal may easily exceed the value of the thruster.

1. The lubrication system should be equipped with a seawater indicator/alarm for early detection of leaks.
2. The lubrication system should allow retrieving samples of the lube oil from the lowest point of the gear housing.
3. Facilities should be provided which allow the lube oil to be changed easily while the vessel is at operating draught.
4. Auxiliary systems in the thruster room should be installed with easy access for service and exchange in mind.

5. As far as feasible, support systems (azimuth drives, lubrication systems, etc.) should be installed with redundant key components. If redundancy of the components is impractical, design should incorporate easy interchangeability as a feature (for example, hose connections instead of hard piping for hydraulic components). Provisions should be made for an adequate inventory of spares.

9.15.3 Experience has shown that occasional intrusion of seawater through the propeller shaft seal into the gear housing is unavoidable. An external filtration or purification system should be provided to remove seawater contamination from the lubrication oil for each thruster. Examples of filtration systems include lube oil purifiers and coalescing type filter arrangements.

9.15.4 A condition monitoring system should be considered for continuous surveillance of the condition of power train.

9.16 TESTING OF THRUSTERS

9.16.1 The thrusters should be subjected to thorough testing during the various states of manufacturing. Confirming thrust performance objectively after installation on the vessel is a challenge. Contractual stipulations should take this into consideration.

9.16.2 Estimation of thrust from a fixed pitch propeller is feasible by comparison of measurement of shaft speed with performance data.

9.16.3 Estimation of thrust from a controllable pitch propeller by measurement of pitch is difficult as it depends on the alignment of mechanical components in the hub.

9.16.4 The following are examples of thruster related equipment to be tested:

9.16.5 **Testing of the right-angle gear tooth contact:** This test is important for the assurance of the correct installation and adjustment of the gears. It also indicates errors in gear cutting or machining of the gear housing.

The test should be carried out by applying full, rated torque to the pinion shaft and providing a retarding force to the propeller shaft. The optimum indication for the contact tooth condition is achieved after one revolution of the propeller shaft. More revolutions may corrupt the contact patterns, and less than one full revolution may leave several potential errors undetected.

It is highly recommended to apply the (maximum) propeller thrust to the propeller shaft during this test. This creates a realistic simulation of the actual working conditions of the thrusters.

9.16.6 **Functional component and subsystem testing of propeller shaft seals:** The consequences of a propeller shaft seal leak and the efforts and cost (direct and consequential) involved in servicing or replacing the seal are high. A factory bench test is recommended for large thrusters, particularly those equipped with mechanical type radial seals.

9.16.7 **Hydraulic systems for azimuth power, control and gear lubrication:** These systems should be tested for appropriate function and connection.

9.16.8 **Gear housing:** The gear housing should be air-pressure tested for tightness after final assembly.

9.17 VIBRATION MEASUREMENTS

9.17.1 The base vibration signature will assist in future troubleshooting and failure analyses. After completion of the sea trials, a base vibration measurement should be taken several locations on top of the thruster inside the thruster room. The results should be recorded and the location of the measurements should be marked for future repetition of the test and comparison of the results.

9.18 OPERATION OF THE THRUSTERS

9.18.1 **Number of thrusters in operation:** During station keeping operations, the highest overall efficiency for fixed-pitch propellers is achieved by running all thrusters.

9.18.2 **Propeller "windmilling":** The design of a right-angle gear thruster should consider the potential adverse effects of windmilling:

For example, a drilling vessel with six thrusters is intended to undertake an extended transit one of the thrusters is unavailable. The vessel will be propelled by the remaining five thrusters and is expected to move at twelve knots. The failed thruster would be exposed to twelve knots inflow velocity, causing the propeller to windmill. This generates thrust in the opposite direction to the normal operating thrust. The mechanical design of the power train must be designed for this condition to prevent damage to bearings and gears. Addressing windmilling by braking the (high-speed, low-torque) pinion shaft is detrimental. It could cause the engagement of one pinion gear tooth with two gear wheel teeth. The turbulent action of the inflowing water to the propeller would cause a continuous rattling of the gear teeth and may lead to a failure.

9.18.3 Depending on the type of electric drive system, the windmilling action of the motor may generate current. The electric drive arrangement should be able to cope with this.

9.19 MECHANICAL DESIGN OF THE RIGHT-ANGLE GEAR THRUSTERS

9.19.1 **General:** The majority of electric thrusters are of the mechanical, right-angle gear box design. A few electric-direct drive thrusters are in DP service (podded thrusters).

Gear design factors, and the calculated life of the bearings should be key elements for the evaluation of the quality of thrusters. Gear design factors include:

1. Safety factor against pitting.
2. Safety factor against tooth breakage.
3. Safety factor against scuffing.

9.19.2 A further gear design factor is the application factor which is a function of the (input) drive system (either reciprocal action such as Diesel engines, or uniform action such as electric motors), and the (output) operational condition, i.e. the condition in which the thruster is operating (e.g. smooth water or heavy turbulence - probability of exposure to the turbulent wake of another thruster in the vicinity).

9.19.3 Guidance for the selection of these factors is given in DIN Standard 3991, and Klingenberg Standard KN 3030. The rules of the classification societies typically reflect these standards.

9.19.4 The gears should be designed and rated to transmit the specified torque for unlimited life.

9.19.5 The minimum calculated L-10 life of the bearings should be specified as 30,000 hours. The L-10 life is defined in ISO 281:2000, ‘Standard for calculation of bearing ratings and life’. L-10 indicates the life that 90% of a large sample of identical bearings should achieve.

9.20 PROPELLER SHAFT SEALS

9.20.1 Propeller shaft seals are the weak point of the thruster design. It is said the failures of these seals have caused more downtime in the offshore industry than any other single component. It is of utmost importance that the seals including their support systems are selected for quality and proven performance and independent of cost considerations.

9.20.2 Axial (mechanical-type) seals as well as radial (lip-type) seals are used for large thrusters. The selection of seal type depends on factors such as draught of the vessel, the quality of the water in which the thruster is operating, and personal preferences based on experience. For water contaminated with sand and silt, the mechanical seal is suggested due to the higher hardness of the seal surfaces.

9.20.3 Debris and fishing line contribute to seal failure. Design should incorporate mitigating measures such as streamlining the housing contour, attaching rope cutters to the propeller hub to protect seals from such exposure. The propeller-shafting-housing intersection should be designed to prevent debris and fishing line from entering the vicinity of the shaft seals. The rope guards should be designed for an extreme low clearance. A net protection ring with U-shaped cross-section may be attached to the forward end of the propeller hub.

9.21 THRUSTER PROPELLERS

The propeller material should be nickel-aluminium bronze for strength and ease of repair. Propellers should be manufactured, tested and balanced in accordance with International Standard ISO 484/1-1981 (E) Class I.

9.22 THRUSTER SELECTION CRITERIA

9.22.1 The following are examples of criteria that should be evaluated to assess thruster quality and performance as an aid to selection during the design phase.

1. Power to thrust ratio.
2. Maintainability.
3. L-10 life of the bearings.
4. Compliance with the specification and owner requirements.
5. Gear design factors such as:
    a. Safety factor against pitting.
    b. Safety factor against tooth breakage.
    c. Safety factor against scuffing.
    d. Application factor.

9.23 LIFE EXTENSION OF THRUSTERS

9.23.1 The following step should be considered to aid life extension of thrusters:

1. Protection of the gear housing with state-of-the-art epoxy compounds.
2. Installation of cathodic anodes at the outside of the thruster housing and at the nozzle.
3. Coating the inside of the nozzle shell plating with a corrosion-preventive compound. Design should incorporate features to facilitate renewal of the coating.
4. The nozzle should be equipped with openings for draining and filling.

9.24 SPECIAL APPLICATIONS

9.24.1 Certain vessels industrial mission is taking them into frontier areas where DP is being contemplated as a means of station keeping (e.g. Arctic Exploration).

9.24.2 Thruster designs will need to take into account specific requirements for operating in these environments (e.g. clogging of nozzles, ice loads and impacts on gears and appurtenances).

9.25 THRUSTER VERIFICATION

9.25.1 Baseline measurements should be documented when vessels are commissioned in service. Such measurements include:

1. Pitch limits
2. Stroke
3. Centre or zero thrust.
4. Power consumption (kW and A)
5. Rate of ramp
6. Rate of turn
7. Vibration.

9.25.2 Periodic verification activities should be carried out, documented and monitored for early anomaly / divergence detection.

10 MARINE SYSTEMS

10.1 DESIGN OF MARINE SYSTEMS

10.1.1 The design of Marine systems supporting DP should follow the redundancy concept and WCFDI. Design of such systems should reflect the Industrial Mission and the objectives to be achieved. The benefits of incorporating design features of independence, segregation, critical redundancy, non-critical redundancy and monitoring beyond Class Requirements should be assessed. These enhanced features should result in vessel that meets the objectives of its industrial mission and achieve the desired Class Notation.

10.1.2 Marine Systems as addressed in this section include:

1. Fuel oil system.
2. Seawater cooling systems.
3. Fresh water-cooling systems.
4. Compressed air.
5. Lubricating oil systems.
6. HVAC and ventilation.
7. Remote controlled valves.
8. Water tight integrity /Subdivision Integrity.
9. Pipe work.

10.2 FUEL OIL

10.2.1 Fuel Oil systems should be designed to provide one per engine room or minimum of two for DP Class 2 and 3.

10.2.2 There should be sufficient redundancy in the fuel transfer system to allow each engine room access to the vessel's entire fuel capacity following any single failure.

10.2.3 Actuators for Quick Close Valves should be installed on a per engine basis - any remote-control system should fail safe in respect of position keeping.

10.2.4 Water content monitoring with remote alarms should be installed.

10.2.5 In addition to Class rule stipulated level monitoring, fuel level monitoring appropriate to the Industrial mission should be considered.

10.2.6 Fuel filter arrangements should be designed to facilitate changes without taking equipment out of service.

10.2.7 The design of the fuel system should facilitate isolation of services between station keeping and industrial functions if applicable.

10.2.8 Height of the day tanks for fuel should be designed to avoid dependence on emergency generator for black out/black start.

10.2.9 Co-location of auxiliary systems supporting fuel systems should be avoided. Where segregation is chosen as a design principle, it should follow the redundancy concept.

10.3 SEAWATER COOLING

10.3.1 The design should incorporate redundancy in sea chests and pumps in line with the redundancy concept and follow the WCFDI.

10.3.2 The design should facilitate isolation of services between station keeping and industrial functions if applicable.

10.3.3 Each engine room should have a sea water cooling system with one duty and one standby pump (interchangeable assignment). A high and a low sea chest will be provided, and either can be selected. No single failure of an active component in the seawater system should lead to a loss position.

10.3.4 Two sea strainers will be fitted for each engine room seawater system with differential pressure alarms to identify the onset of severe fouling and it will be possible to remove one of the two sea strainers for cleaning with the seawater cooling system in operations.

10.3.5 Means to select the offline sea suction remotely should be provided.

10.3.6 Thruster seawater cooling system should follow the redundancy concept with one duty and one standby pump (interchangeable). One low and one high sea suction should be provided with two sea strainers and isolation valves to allow the thruster(s) to continue to operate while one strainer is being cleaned.

10.3.7 Engine room sea water cooling systems could be incorporated into the thruster seawater systems provided the redundancy concept is not contravened.

10.3.8 An effective anti-bio fouling system should be installed to ensure the seawater cooling systems retain their efficiency between maintenance periods.

10.3.9 Temperature, flow and pressure monitoring (local and remote) should be an integral part of the design of sea water cooling systems.

10.4 FW COOLING

10.4.1 Freshwater cooling systems supporting station keeping equipment, per consumer, should be independent to the maximum extent feasible. Where independence is not part of the design philosophy, failures of the freshwater cooling system should not result in failure effects exceeding the WCFDI.

10.4.2 FW cooling systems for engines should consider use of engine driven freshwater pumps. Dual pumps should be provided in a duty / standby arrangement to improve availability.

10.4.3 Water makers should not introduce commonality in redundant FW circuits.

10.4.4 Flow and pressure monitoring (local and remote) should be an integral part of the design of freshwater cooling systems.

10.4.5 Fail safe condition for valves in FW system should fail as is.

10.4.6 Fail safe condition for automatic temperature control valves should be fail open.

10.5 COMPRESSED AIR

10.5.1 Compressed air is used for:

1. Starting air.
2. Control air.
3. General service.

10.5.2 Compressed air for starting engines should be independent to the maximum extent feasible. Where independence is not part of the design philosophy, failure of the system should not result in a failure mode worse than the WCFDI.

10.5.3 The above philosophy should be applied to general service air when used to support station keeping equipment.

10.5.4 Compressed air systems for DP related and non-DP related functions should be independent. Compressed air systems for DP related functions should follow the redundancy concept.

10.5.5 Control air and starting air may be taken from the same source provided any pressure drops associated with starting air do not affect the control function.

10.5.6 Where starting air is used for other purposes means should be provided to ensure the starting capacity required by class is protected against depletion.

10.5.7 Starting air system should be designed to allow simultaneously cranking, starting and connection of all diesel generators.

10.5.8 Control air for the thrusters may be derived from the associated engine room supply or locally. Loss of air supply to the thrusters should be alarmed and should have no effect on thruster operation.

10.5.9 Devices such as oil mist detectors should not have common mode failures such as common air supplies or crank case breathers.

10.5.10 Pressure monitoring (local and remote) should be an integral part of the design of compressed air systems.

10.6 LUBRICATING OIL SYSTEMS

10.6.1 Lube oil systems for engines should be associated with one engine only.

10.6.2 Facilities for storage, changing and disposing of oil may be on a per engine room basis but suitable interlocks should be provided to prevent inadvertent cross connections between engines which could lead to one engine sump being emptied and the other overfilled.

10.7 HVAC AND VENTILATION

10.7.1 Ventilation and HVAC for spaces containing equipment essential to DP should be designed to comply with the redundancy concept and failure should not have an effect exceeding the worst case failure design intent.

10.7.2 Consideration should be given to the use of temperature alarms for temperature critical spaces where cooling is essential to the correct operation of equipment, a backup temperature control system should be provided.

10.8 REMOTE CONTROLLED VALVES (DP RELATED)

10.8.1 All remotely controlled valves should fail in a manner that supports the redundancy concept. In general, this will require double acting remote controlled valves which fail ‘as set’ unless required otherwise by Class.

10.8.2 Where any conflict arises between the requirements of Class and the redundancy concept a solution is to be developed to satisfy both requirements.

10.8.3 Consideration should be given to the need for remotely controlled valves for DP related equipment to operate reliably in challenging environments. The effects of technical failures, fire and flooding should be considered. Hydraulically operated valves may offer advantages in some failure scenarios.

10.8.4 Monitoring of valve position of remote controlled valves should be based on feedback not command.

10.9 WATER TIGHT INTEGRITY/SUBDIVISION INTEGRITY

10.9.1 Design should incorporate features that will maintain watertight integrity/subdivision integrity of spaces containing DP critical equipment and be able to cope with inadvertent acts compromising integrity. Remote monitoring capability of such spaces is suggested.

10.9.2 Particular attentions should be directed towards hull penetrations associated with DP equipment. (e.g. hydro-acoustic transducers).

10.10 PIPEWORK

10.10.1 Failure of pipework associated with redundant elements passing through the same high risk area without adequate protection from mechanical damage and fire should not result in a failure worse than WCFDI.

10.10.2 Cross over valves where fitted between independent systems, to facilitate maintenance, should be provided with local and remote monitoring to indicate open/closed status.

Table 10-1 MTS Design for Auxiliary Services - Basis for Action, Cost Beneficial Risk Reduction

Systems	Independence	Separation	Monitoring	CR	NCR	CMF/CCF	X-OVER	IRM
Fuel supply	✓	✓	✓				✓	
Fuel Storage		✓	✓			✓	✓	✓
SW Cooling			✓		✓		✓	✓
FW Cooling	✓	✓			✓			
Starting air		✓	✓	✓			✓	
Control air	✓	✓	✓		✓			
Lubricating Systems	✓	✓						
HVAC and Ventilation		✓	✓	✓				
Remote Controlled valves		✓		✓				

Definitions	
Independence	Provide auxiliary service in a manner that makes thrusters and generators independent.
Separation	Provide auxiliary service in a manner that supports redundancy & minimizes commonality – WCFDI.
Monitoring	Provide monitoring to reveal loss of redundancy and common mode / cause failures.
CR	Critical redundancy is sufficient i.e. supports WCFDI.
NCR	Add non critical redundancy to improve reliability over that required for WCFDI.
CMF/CCF	Pay special attention to common mode and common cause failures for internal and external sources.
X-Over	Add normally closed crossovers for ease of maintenance.
IRM	Pay special attention to maintenance requirements and develop specific procedures.

11 POWER GENERATION

11.1 ATTRIBUTES OF A ROBUST REDUNDANCY CONCEPT

11.1.1 DP class notation dictates the redundancy requirements. A robust redundancy concept has the following attributes:

1. Fully fault tolerant in relation to the defined failure criteria.
2. Main machinery is independent to the maximum extent feasible.
3. Redundant systems are clearly defined and well separated.
4. The division of systems into redundant groups is maintained at all levels, systems and auxiliary systems throughout the design.
5. Low impact worst case failure effect.
6. Minimum number of failures leading to the worst-case failure effect.

11.1.2 A robust redundancy concept should be rigorously applied to the design of the power generation system.

11.1.3 The design of the power generation system should take into account:

1. The industrial mission of the vessel.
2. Power required to maintain station and perform the industrial mission in the desired range of environment.
3. The need to work efficiently in all required power plant configurations.
4. Power required to maintain station in the defined environmental limits in:
   - Intact condition.
   - and post worst case failure.
5. The need for a robust blackout recovery system as a risk reduction measure
6. The role of electrical energy storage in reducing the criticality of dependence on protective functions when applied to the thrusters (in closed busties configurations).
7. Any restrictions imposed by a particular choice of main machinery.

11.1.4 The key power system attributes that need to be considered during the design phase are:

1. Power, voltage, current, frequency and operating power factor (for ac systems).
2. Short circuit withstand capability.
3. Protection philosophy.
4. Power management.
5. Phase back of large consumers.
6. Regeneration from large consumers.
7. Starting of large consumers.
8. Load acceptance and rejection.
9. Load balance.
10. Voltage transient ride through.
11. Stability.

12. Efficiency.
13. Harmonic distortion.
14. Electromagnetic compatibility.
15. Maintenance requirements.
16. Environmental and pollution requirements.
17. Power delivery and capacity of stored energy systems.

11.1.5 The design effort should incorporate the necessary analysis and studies required to deliver a robust power plant, delivering effective capacity to undertake its industrial mission in the stipulated environmental conditions.

11.1.6 It should be recognized that Class Rules addressing the above attributes are minimum requirements for vessels and do not consider the industrial mission the vessel will be undertaking. The design philosophy should integrate the requirements of the Class Rules and the Industrial mission. This will translate into a more comprehensive design effort resulting in a more effective vessel.

11.1.7 Power generation design should deliver:

1. Flexibility (Optimize the number of generators in favour of flexibility for example six smaller generators rather than four larger ones).
2. Maximum independence and separation.
3. High availability.
4. Fault tolerance and fault resistance.
5. Resilience and ride through capability
6. Continuity of supply of power.
7. Maximize post failure capacity.
8. Optimized Black Start requirements (minimize recovery time).

11.1.8 Design should consider the significance of the power plant in relation to the industrial mission of the vessel. Most modern DP vessels of medium to large size have a diesel electric power plant based on the power station concept. The power station concept is based on a centralized power generating and distribution system which provides power for all vessel power requirements including propulsion, industrial loads, auxiliary systems and hotel services.

11.1.9 Generators and thrusters are connected to two or more main switchboards to create independent power systems which are capable of maintaining position and heading in the event that one of the power systems fails.

11.1.10 The design of the power plant should be based on a redundancy concept achieving the objectives of the vessel specific DP design philosophy. The redundancy concept describes the way in which each of the independent power systems supplies power for engine room services, thrusters and thruster auxiliary systems. The separation between these independent power systems is often referred to as the ‘split’ in the redundancy concept. A vessel with two power systems is described as having a ‘two-way’ split. A vessel with three independent power systems is described as having a ‘three-way’ split.

11.1.11 In good redundancy concepts, the split between the power systems is clearly defined and there are few cross connections between systems. Where cross connections are unavoidable, they should be easily identifiable. In these types of redundancy concepts, failures within each independent power system should only affect thrusters and generators in one of the power systems.

11.1.12 In poorly defined redundancy concepts, the boundaries between each power system are more difficult to identify and there may be a larger number of shared components or connections. Vessels with this type of redundancy concept are susceptible to failures that could exceed Worst Case Failure Design Intent (WCFDI). Even if WCFDI is not exceeded, failure in one power system may affect generators and/or thrusters in the other power system and different combination of thrusters may be lost. Multiple failure permutations exist in such systems.

11.2 POWER SYSTEM ATTRIBUTES AND STUDIES

11.2.1 **General:** Alternating current power systems must operate within limits for voltage, current and frequency. Control systems on the generator continuously adjust the fuel admission and excitation levels to ensure each generator is running at the correct voltage and frequency and is carrying its proper share of the active and reactive power.

To maintain system stability:

1. The load on each generator must be the same and within the generator's rating. Asymmetric load sharing may be applied for maintenance purposes provided all necessary protective functions are in place to ensure system stability in this control mode.
2. Generator current must remain within rating to prevent the generator being tripped on over current.
3. When load is applied to the generators the application rate must be within the generator's load acceptance rating.
4. The worst-case load rejection must not cause the generators to trip on over speed or over frequency.

System stability may be assisted by phase back of larger consumers if the step load is caused by sudden loss of generating capacity exceeding the load acceptance.

11.2.2 **Harmonic distortion:** Modern power electronic convertors used for thrusters drives and other applications create harmonic distortion of the power frequency waveform.

Levels of harmonic distortion must be maintained within set limits to reduce the risk of equipment malfunction.

All these conditions must be met in both the intact case and after a fault has occurred.

Harmonic distortion of power frequency waveforms can be caused by:

1. Incorrect design of power systems.
2. Failures in variable frequency drives.
3. Failure of harmonic filters.
4. Loss of harmonic cancellation.

Harmonics can also be related to commutation notches from large rectifiers and contribute to overheating of service transformers.

High levels of harmonic distortion can have undesirable effects including failure of generator synchronizers, failure of control systems, noisy operation, overheating of machines and failure of ballasts in fluorescent lighting.

Harmonics are often a problem in large diesel electric power plants.

Measures such as phase shifting transformers, active front end rectifiers, and phase shifting transformers are used to reduce harmonic distortion to acceptable levels.

Harmonic filters can be unreliable. There have been well documented failures on DP vessels leading to severe short circuit faults and associated voltage dips and consequences.

Harmonic studies should be carried out to determine the worst-case levels of harmonics in the intact condition and following the worst case failure of any harmonic reduction measures.

The system should be designed such that post failure levels of harmonics remain within acceptable levels or the power plant should be designed to operate at higher harmonic levels without malfunction.

Levels of harmonic distortion should be continuously monitored by the vessel management system and unacceptable levels should initiate an alarm.

Vessels that operate with the main switchboard busties open should only experience harmonics related to failure on one power system. However, some power systems use phase shifting transformers with a different vector group on each side of the main busties to achieve additional harmonic cancellation. It is important that the harmonics remain within acceptable levels when the busties are opened and this harmonic cancellation effect is removed.

Some types of diesel electric power systems use phase shifting transformer between two bus sections to create a phase shift between the two power system voltage waveforms. When one power systems fail the 12-pulse rectifiers revert to 6-pulse operation. It is important to confirm that operation can continue for as long as required with the higher levels of distortion. Systems using this method should be designed for continuous operation in all defined bus configurations.

Guidance on acceptable levels of harmonic distortion is available from a number of sources including IEC 533. Protection relays and monitoring units are available to provide alarms or initiate actions on defined levels of harmonic distortion.

11.2.3 **Load balance:** The load balance indicates the load on the generators for various operations. It is important that the load balance acknowledges requirements for the DP system to have active redundancy i.e. ability maintain position with the machinery that remains available following the worst case failure. It is important that the load balance reflects the configurations that will be used for DP including CAM and TAM.

When the power plant is configured as a common power system all generators can feed all loads. There may be significant currents across the busties if loads are not equally divided up amongst the main switchboards.

It is important to balance DP loads and those associated with the vessel's industrial mission.

Failure to do this can create a design which cannot operate effectively with the busties open because one power system reaches capacity before the other preventing thrusters being utilized effectively.

Note: *load balances are also required for other DP related energy sources such as UPS, transformers and DC power supplies.*

11.2.4 **Voltage transient ride through:** Voltage transient ride through describes the ability of electrical consumers to continue in operation following a significant voltage excursion. Voltage transients can be caused by short circuit faults, voltage regulator faults and excessive regeneration from drives.

Many consumers such as variable speed drives and motors are supplied through electromagnetic contactors that are susceptible to voltage dips associated with clearing a fault elsewhere in the power system.

Unless all DP related consumers have the necessary voltage transient ride-through capability there is a risk of loss of all thrusters or blackout in DP vessels operating with a common power system. Typical issues related to voltage transients include:

1. VFDs DC link trips on over/ under voltage.
2. Insufficient under voltage release delay on feeders - For example service transformer feeders.
3. Drop out in contactors for pumps and fans.

Some designs incorporate energy storage systems connected to the DC link of the thruster drives utilized to extend ride through capability.

11.2.5 **Voltage transient testing:** Live short circuit and earth fault testing is an established method of proving the voltage transient ride through capability of HV power plants. Test results should be used to validate a power plant model to allow simulations of conditions beyond that which can be achieved by practical test methods.

Careful development and planning is required to ensure such tests can be conducted safely with minimum exposure to people and risk of equipment damage. This type of testing has been carried out successfully on DP vessels with appropriate analysis, planning and execution. Such testing has revealed vulnerabilities and identified opportunities for improvement. Addressing any vulnerabilities and opportunities for improvement aids in delivering a robust power plant.

Such analysis and testing is recommended for DP class 3 vessels even if the power plant is operating with the main busties open especially if cable routes or collocation of non DP related equipment create a common point. A voltage transient could be experienced by all redundant power systems because of the effects of fire or flood damage to electrical equipment and cables.

Note: *Sufficient time should be allocated to carry out the required analytical modelling to enable execution of this test safely.*

11.2.6 **Mitigation for effects of voltage transients:** The effects of voltage transients can be mitigated by:

1. The provision of UPSs for control power.
2. Suitable under voltage delay on circuit breaker opening.

3. Ride through power supplies on drives.
4. Kinetic buffering of thrusters.
5. Local energy storage systems (batteries or super/ultra-capacitors)
6. Automatic restart of auxiliary services.
7. DC coils for MCC contactors.

11.2.7 **Resonance:** This is a condition which occurs when there is sufficient inductive and capacitive reactance in a power system to create a resonant frequency at or near one of the naturally occurring harmonic frequencies of the system.

Such an effect can cause a severe over voltage leading to equipment failure and blackout.

Resonance can occur if there are large capacitors on the system for filtering purposes etc.

The harmonic study can also be used to check for resonance.

11.2.8 **Transient stability:** Parallel generators are held in synchronism by the synchronizing torque developed from the bus voltage at the generator's terminals.

During a severe short circuit fault the terminal voltage may drop close to zero causing generators to lose synchronism with each other.

Similar conditions may occur because of the crash synchronization of a generator, or two power systems. Inadvertent connection of a stopped generator may also cause severe disruption.

In marine power systems the generators are usually so closely coupled that the plant re-stabilizes when the short circuit has been cleared by the protection. A study should be performed to confirm this.

11.2.9 **Spinning reserve:** In discussion of marine diesel electric systems the term 'spinning reserve' is used to describe the difference between the system load and the online generating capacity. It does not include the capacity of standby generators.

It is good practice to maintain sufficient spinning reserve to cope with the worst case loss of power generating capacity without resorting to thruster phase back.

It may be impractical to carry sufficient spinning reserve to allow industrial consumers to continue without disruption and it may be acceptable to use load shedding functions to make power available for the thrusters. This method of power plant operation can only be considered as contributing to redundancy and included in the consequence analysis if the load shedding function is sufficiently reliable.

Studies should confirm the levels of spinning reserve required to provide active redundancy. Load dependent starting should be programmed to ensure such margins are preserved under all operating conditions.

Some designs deliver such functionality of 'spinning reserve' that is made available near instantaneously from Energy Storage Systems connected to the main bus, thrusters or in other locations.

11.2.10 **Short circuit withstand:** This is the property of electrical equipment that indicates that it is able to withstand the mechanical forces created by a short circuit fault.

The short circuit current increases with the number of generators or service transformers operating in parallel.

In low voltage power plant designs the maximum prospective short circuit current is sometimes greater than the withstand capability of the main switchboards. The power management system may be programmed to subdivide the power system to reduce the fault current available when the number of generators becomes too great.

In other designs service transformers are prevented from operating in parallel by system of interlocks. Device such as Is limiters (a type of fuse) can also be used to overcome such difficulties.

Whatever method might be employed to overcome the problems of high short circuit currents it is important that these are considered in relation to the redundancy concept and worst case failure design intent.

Classification societies require that short circuit calculations are carried out to ensure the prospective short circuit current does not exceed the rating of electrical equipment specified.

Note: *Energy Storage connected to the DC link of thruster drives does not typically contribute to the short circuit current on the main bus (when fitted downstream of the rectifier front end). This may make locating stored energy at the thrusters an attractive solution for retrofit / upgrade.*

11.2.11 **Protection relay coordination:** Modern DP vessels intending to operate a diesel electric power plant as a common power system require a very sophisticated and comprehensive range of protection relays to prevent faults in one redundant power system affecting the operation and stability of others.

The type and settings of the protective functions must be carefully coordinated to ensure there are no conflicts and that faults are isolated as close as possible the source of the fault.

It is essential that protection relay coordination studies consider the need for protection to support the redundancy concept, industrial mission requirements, personnel safety and equipment protection.

11.3 GENERATORS

11.3.1 **Engines:** Generators for diesel electric power plants in medium and large sized DP vessels are usually powered by medium speed diesel engines. These engines are often highly turbocharged and have a number of features that can influence the DP redundancy concept. Features vary from engine to engine and from one manufacture to another even for engines of the same size and rating. It is important to understand any restriction imposed by these features. Engine attributes that should be considered in the design include:

1. Load acceptance.
2. Load rejection.
3. Starting time.
4. Load up time and emergency loading ramp.
5. Time on hot standby.
6. Minimum load and part load ratings.
7. Black start requirements.

11.3.2 **Load acceptance and rejection:** Load acceptance and rejection ratings define the step loading that can be applied to the diesel engine without unacceptable loss of cyclic regularity (frequency for a generator).

In modern medium speed diesels this figure varies with the load at the time the step is applied and is often worst at mid load. Figures of around 25% are not unusual in some engine types.

Care must be taken to ensure that failures in the power generation system which cause loss of multiple generators do not impose a greater step load than specified. Tests confirm that blackout can occur if this figure is exceeded.

In some designs it may be impractical to ensure this step loading cannot be exceeded.

- It is established practice to relieve any fall in frequency using frequency based phase back of large power electronic drives such as those for thrusters or drilling. A temporary reduction in the power consumption of these devices can rapidly relieve the load on the generator allowing it to maintain frequency and develop the required power.
- Stored energy system can also be used to support generator load acceptations. Super capacitors and batteries can provide assistance to prevent unacceptable fall in system frequency.

If these methods of preventing cascade failure of generators is envisaged as part of a redundancy concept it is important to ensure that the frequency phase back function in the drives is fast acting, stable, effective and proven at sea trials. Similarly, the method by which the peak shaving function of the stored energy system operates is reliable.

11.3.3 **Starting time:** Large engines may have restrictions on starting which extend their connection time. Some engines require slow turning after sitting stationary on cold or hot standby for an extended period. These pre-starting activities can extend connections times to the order of several minutes which is generally too long for DP requirements.

A connection time of 30s or less can usually be achieved but may require certain engine management functions to be incorporated in the power management system to ensure optimal engine readiness.

It is essential that starting time requirements are understood and agreed with the shipyard, engine manufacturer and power management system vendors. Interfaces and integration should be effectively managed.

11.3.4 **Load up time and blackout recovery loading ramp:** The engine manufacturer may impose restrictions on the rate at which load may be applied during normal operating conditions. Care must be taken to ensure that this load up ramp is suitable for the requirements of the DP controls system. The DP control system manufacturer may apply ramps in software to ensure the engines are not loaded up too quickly. A faster load up ramp may be agreed for blackout recovery - if this is the case then it will be necessary to provide the control options to utilize this in the power management systems.

Note: In the case of blackout recovery, the first generator to connect has to accept the load presented to it on reconnection of the distribution system. Significant hotel loads could contribute to this load. Design should consider this scenario and address appropriately. For example, a service transformer that supports engine and thruster auxiliary systems as well as hotel services.

11.3.5 **Time on hot standby:** Some engines have limitations on how long they can remain on hot standby before they have to execute slow turn functions on start up.

Automation system manufactures may have standard functions designed to relieve this problem by starting the engines periodically and rotating them through a period of operation. Design should consider features of the engine and ability of the automation system to effectively address such features.

11.3.6 **Minimum load and part load ratings:** There may be restrictions of the minimum load at which a large engine can be operated. Low load running may result in build-up of soot and other combustion products which reduce engine efficiency to the point where it cannot deliver rated load on demand.

Many power management and automation system providers have standard functions for engine conditioning but it is necessary to make sure that such requirements are included in the specification for the automation system.

In some type of load sharing systems the engine conditioning or 'base load' function may have to be provided by other means if the PMS does not perform the load sharing function. For example, digital governors may have an asymmetric load sharing function built in.

11.3.7 **Black Start Requirements:** Different types and sizes of engine have different requirements for black starting depending on how much time has passed since the engine was running or in hot stand by.

Some engine manufacturers stipulate that the engine must not be started without pre-lubrication. Others will allow starting without pre-lubrication for a defined time after pre-lubrication.

If pre-lubrication must be provided, consideration can be given to using air driven pre-lube pumps from the starting air supply. This is preferable to using the emergency generator.

Some engines may be very difficult to start if the jacket water temperature drops below a certain point. This is not usually an issue for blackout recovery if the engines have been running or the jacket water heaters are normally on during standby.

If the power plant cannot be recovered in a short time it may be advantageous to have alternative supplies for the jacket water heaters and pre-lube pumps from the emergency switchboard. This feature could be useful during the commissioning phase.

11.3.8 **Generators:** Generators for diesel electric power plant are typically salient pole brushless self-exciting synchronous machines running at 720rpm or 900rpm, 60Hz. A range of voltages are available from around 440V to 13.8kV; 690V, 6.6kV and 11kV are the most commonly found ratings. Generators are available in a large range of power ratings. On medium and large DP vessels generator sizes typically range from around 2MVA to 10MVA and are normally installed in groups of 4, 6 or 8 depending on the size and type of DP vessel. Many smaller diesel-electric vessels use high speed Caterpillar generators (1800 rpm).

11.3.9 Note in this context the word 'generator' refers to the electric part of the generating set.

The impact of the following services on the redundancy concept needs careful consideration when choosing a generator.

1. Excitation system.
2. Lubrication system.

3. Cooling system.
4. Facilities for alarms, monitoring and protection.
5. Neutral earthing.

Excitation support: Several types of excitation system are available for synchronous alternators and not all are suitable for use in marine diesel electric plants. Class requires that alternators are capable of delivering sufficient fault current to operate over current protection effectively during fault conditions and this may require the alternator to be provided with excitation support. The permanent magnet generator is the preferred method of providing this function. It has the advantage that it can also be used as an independent source of generator control power once the generator is up and running.

11.3.10 **Neutral Earthing (Grounding)** Main HV power distribution systems are normally unearthed but have a means of earth reference such as high resistance earth. LV power distribution is normally not earthed.

11.3.11 The size of the prospective earth fault current determines whether it is acceptable to have alarm and indication of earth faults only or whether they must be automatically isolated by tripping the faulty circuit.

High resistance earthing is normal on larger high voltage power distribution system. Class rules on cable insulation have changed and some classification societies allow the cable line to earth insulation to be rated for less than the line to line voltage which is the voltage experienced by the insulation following a ground fault. Adopting this approach requires that the earth fault protection operate almost immediately to relieve the stress on the cable insulation and this may not be compatible with the redundancy concept.

The HV cable earth insulation should be rated for the line to line voltage regardless of the method of earthing or fault isolation. This has negligible cost impact if specified upfront and is part of the bid spec.

Distribution systems may be earthed by neutral earthing transformers at the main switchboards or by neutral earthing resistors at the generator star points.

Earthing at the main switchboards provides a more consistent earth fault current unaffected by the number of generators connected. This is better for protection purposes.

11.3.12 **Generator control power:** It is good practice to make each generator independent in terms of control power. This can be done quite effectively when the alternator has a permanent magnet generator.

Providing control power battery systems for groups of generators inline with split in the redundancy concept is usually satisfactory for control purpose during starting and connection. Design should facilitate independence from the common battery supply once the alternator has excited.

11.4 FUEL CONTROL

11.4.1 **Load sharing:** In a diesel electric power system the engine governor controls frequency and load sharing. There have been a number of DP incidents attributed to governor faults.

Modern digital governors have advanced to the point where external trimming of load is not usually required. Operating parallel generators in uncorrected speed droop introduces the fewest common points and fewest failure modes of all the load sharing techniques.

Other examples of load sharing methods include:

1. Isochronous load sharing using analogue or digital load sharing lines.
2. Pseudo isochronous using external trimming of governor by the PMS (compensated droop).

The above two methods introduce additional failure modes which if not adequately militated against can result in blackout or loss of position incidents.

11.4.2 **Governor types and failure modes:** Governors can be forward or reverse acting. Reverse acting governors fail to full fuel which can be catastrophic for a DP power system.

Most modern DP vessels use digital forward acting governors for fuel control. These have proved to be a better choice in most applications.

The integral backup mechanical governor offered as an option by governor manufactures is of limited benefit to the DP redundancy concept. Such devices can introduce additional failure modes.

11.5 EXCITATION CONTROL

11.5.1 **The Automatic Voltage Regulator** (AVR) is used to maintain system voltage and reactive power sharing. It may also be involved in ensuring sufficient fault current is delivered for effective relay coordination.

AVRs that are operated in uncorrected voltage droop introduce the fewest common connections and failure modes for redundant systems. Design should take this into consideration.

External trimming of the AVR introduces additional failure modes and seldom offers benefits.

A few reactive power sharing schemes use sharing lines sometimes referred to as a cross current loop. These lines introduce further complexity in the control scheme and additional failure modes and are generally unnecessary in modern designs.

Most modern DP vessels use digital automatic voltage regulators.

11.6 SWITCHGEAR

11.6.1 **Switchboards:** Metal enclosed switchgear is normally specified for high voltage applications. Circuit breakers and contactors are used to connect generators and other loads. For 11kV and 6.6kV systems these can be vacuum circuit breakers or SF_6 type or may be air circuit breakers at lower voltages.

Switchboards should be arranged for full remote-manual and automatic control and be provided with all necessary alarms, controls and indications to allow local manual control of the power plant.

Switchgear can be arranged to fail 'as set' on loss of control power. This has advantages for DP redundancy provided there are other means of disconnecting circuits if required such as mechanical opening controls.

Note: Classification societies normally accept switchboards on the basis of type approval provided the prospective short circuit fault current is well within the rating of the switchboard.

If the calculation suggests it is close to the rating, full scale short circuit testing at a test facility may be required. This could have a significant cost and time impact. The cost effectiveness of specifying a switchboard with a higher rating should be evaluated.

Some classification societies require switch boards to have an arc proof rating for HV applications.

11.6.2 **Busties:** It is good practice to have a bustie circuit breaker at each end of a tie line connecting two switchboards, even if classification society rules only require one. For example, as permitted in DP Class 2.

This is particularly important for safety reasons if the switchboards are located in separate switchboard rooms. There have been serious accidents associated with single bustie designs due to improper and ineffective isolation procedures.

Some classification societies enforce the requirements for two busties if the switchboards are in different compartments under main class rules or by interpretation of SOLAS.

11.7 POWER SYSTEM PROTECTION

11.7.1 **General:** Protection schemes for power systems are intended to protect life and limit damage to equipment. DP Class 2 and DP Class 3 vessels depend upon continuity of supply to essential consumers such as thrusters and auxiliary systems.

The protection scheme should be designed to ensure that faults are isolated at source and that failure effects do not exceed the worst case failure design intent.

Over current protection is the primary protection function and is intended to prevent overheating caused by high currents in cables and windings which may result in fire.

In diesel electric power plants for marine applications the main protection elements are:

1. Generator protection.
2. Bus bar protection.
3. Feeder protection.

Generator protection limits the effects of internal faults in the generator, to protect it from the effects of power system faults and protect the power system from the effects of generator faults.

Bus bar protection is intended to protect the switchboard against faults on the switchboard itself.

Feeder protection is designed to disconnect faulty circuits from the switchboard.

All protective functions are potential hidden failures which may defeat the redundancy concept by removing fault tolerance.

Critical protective equipment should be tested periodically, and equipment settings confirmed to match the approved protection and coordination study, to have a high degree of confidence that they will operate on demand.

Protective functions should be provided in such a way that spurious operation of the tripping functions should not produce a failure effect exceeding the worst case failure design intent.

11.7.2 **Arc detection:** Arc detection by optical means or by pressure wave detection has becomes a popular method of bus bar protection for high voltage marine power systems.

Arc detection offers advantage of very fast isolation of the fault. It does not depend on detecting the fault current. It does not require coordination with other protection as it positively identifies the location of the fault. It may be supplemented by over current protection to cover the possibility of a short circuit occurring without an accompanying arc.

11.7.3 **Over current detection:** This is the most basic form of protection and is applied at all levels in the power distribution systems for short circuit and over load protection.

Over current can be detected by current transformers, fuses, magnetic over current or bi-metal strips with heating coils. At the main power distribution levels ‘protection-class’ current transformers are used to provide digital relays with a signal representing the line current. Various current versus time curves are used to produce the required degree of coordination with other over current protection upstream and downstream.

Note: Protection class CTs may not provide the degree of accuracy required for instrument applications.

11.7.4 **Differential protection:** Differential protection is a form of over current protection based on summing the currents entering and leaving a node such as a switchboard, busbar or a generator winding.

Current transformers are used to monitor the current entering and leaving the zone to be protected. Provided there is no fault path within the zone the currents will sum to zero.

If a fault occurs this will no longer be true and a difference signal will be generated operating the over current trip on the circuit breaker.

Differential protection can be used to create zones around individual bus sections in a multi-split redundancy concept connected as a ring. With this arrangement only the faulty bus section is tripped and all other bus sections remain connected. This has advantages if some of the bus sections do not have a generator connected.

Differential protection schemes can have problems with high levels of through-fault current. That is current passing through a healthy zone on its way to a fault in some other zone. There have been problems with healthy zones tripping causing failure effects exceeding WCFDI. It is for this reason that some designers favour arc protection for this application.

The effectiveness of differential protection for bus bar applications is difficult to establish conclusively without conducting short circuit testing.

Differential protection is almost universally applied for the protection of generator windings on machines above about 1.5MVA.

11.7.5 **Directional over current protection:** Directional over current protection is sometimes applied for bus-bar protection. It is less expensive than differential, due to the reduced number of current transformers required to define a protection zone. Directional over current generally cannot be used with ring configurations as it depends on blocking the upstream circuit breaker from tripping.

11.7.6 **Earth fault protection:** The size of the power distribution system and the maximum prospective earth fault current influences the type of earth fault protection specified for marine system.

Low voltage marine power systems are often designed as un-intentionally earthed systems where the power system has no direct connection or reference to earth (vessel's hull). On these systems, earth faults are typically indicated by earth fault lamps or meters connected from each line to earth.

Intentional earth impedance should be considered in the case of high voltage systems. High resistance earthing of various types is generally employed.

All power systems are referenced to earth by way of the distributed capacitance of cables and windings. A significant earth fault current can flow even in unintentionally earthed HV systems.

The intentional earth impedance adds to the system charging current when an earth fault occurs and should be sized to provide an earth fault current three times that which would flow as a result of the capacitive charging current. This provides well defined current paths for protection purposes.

Earth fault protection for the main power system is sometimes based solely on time grading. The relay in the earthing resistor or earthing transformers for each bus will detect an earth fault at any point in the plant not isolated by a transformer.

Earth fault protection in the feeders is used to isolate a fault in a consumer. If the earth fault persists after the tripping time of the feeder the fault is assumed to be in the generators or on the busbars itself. At this point the protection driven from the neutral earthing transformers will trip the main busties to limit the earth fault to one bus or the other. Whichever neutral earthing transformer continues to detect an earth fault will then trip all generators connected to that bus. Losing a whole bus due to an earth fault in one generator is unnecessarily severe. Design should consider adding restricted earth fault protection to the generators.

11.7.7 **Over under voltage:** This protection element is often a class requirement. It assists in preventing equipment damage but does not contribute to redundancy concept directly.

There should be other protective functions to prevent the power plant reaching the point at which this protection operates. Over / under voltage protection is not selective and blackout is the likely outcome.

To prevent blackout in common power systems (closed bus), design should provide other protective functions which detect the onset of the voltage excursion and divide the common power system into independent power systems or isolate the sources of the fault before healthy generators are tripped (for example a faulty generator).

Operating the power system as two or more independent power system (busties open) provides protection against this fault.

11.7.8 **Over under frequency:** Under frequency can be caused by system overload and there must be means of preventing the power plant reaching this condition. Such functions are normally found in the DP control system, power management system, thruster drives and other large drives. Over frequency can be caused by a governor failing to the full fuel condition. This will cause a severe load sharing imbalance which can drive up the bus frequency to the point where several healthy generators trip on over frequency or reverse power. The failure scenarios are similar to those for over and under voltage as described above.

11.7.9 **Reverse power:** This protective function is applied to prevent a diesel generator that has lost power from becoming an unacceptable burden on other generators operating in parallel. If a generator with a fuel supply problem sheds the load it is carrying it will be motored by other generators. The power required to motor the faulty generator adds to the load on the healthy generators.

Although the reverse power trip is a useful function, it makes healthy generators vulnerable to being forced to trip on reverse power if a faulty generator takes all the load. In this failure scenario the healthy generators all trip on reverse power and the faulty set trips on some other protective function leading to blackout.

Vessels operating their power plant as a common power system should have a means to detect the onset of a generator fault which could have this effect and either subdivide the power plant into independent power systems or trip the generator that is creating the problem.

Operating the power plant as two or more independent power systems (busties open) provides protection against this type of failure.

11.7.10 **Field failure:** This protective function is designed to prevent a generator with field failure (under excitation) becoming an unacceptable reactive power drain on other generators. However, a generator may also fail due to over excitation. If this happens it may push the operating point of healthy generators into the tripping zone of their field failure protection leading to cascade failure and blackout.

Vessels operating their power plant as a common power system should have a means to detect the onset of a generator fault which could have this effect and either subdivide the power plant into independent power systems or trip the generator that is creating the problem.

Operating the power plant as two or more independent power systems (busties open) provides protection against this type of failure.

11.7.11 **Negative phase sequence protection:** Three phase synchronous generators can only tolerate a limited degree of imbalance in their line currents. Large single phase loads, faulty motors or broken conductors may cause a large imbalance which sets up a backwards rotating field in the generator causing overheating.

Negative Phase Sequence protection is used to trip any generator which has a line current imbalance larger than a defined percentage of the full load current. This protection function is not selective and there is a possibility that all online generators may trip in response to a large negative sequence fault.

Vessels operating their power plant as a common power system should have a means to either subdivide the power plant into independent power systems or trip the circuit (feeder, bus section or generator) that is creating the problem.

Operating the power plant as two or more independent power systems (busties open) provides protection against this type of failure.

11.7.12 **Bespoke Generator Protection:** A number of electrical system vendors now offer some form of bespoke generator protection.

This protection is intended to protect the power plant from blackouts caused by the common mode, common cause failures discussed above. It is able to detect the types of failures that standard generator protection relays cannot and trip a faulty generator before it can force other healthy sets to trip.

Any DP Class 2 or DP Class 3 vessels intending to operate their power plant as a common power system should be fitted with an appropriate and effective form of Generator Protection that addresses all potential common cause failures in power plant operating with their busties closed. Note for DP class 2, some classification societies may accept a combination of the protective functions that address a specific list of failure modes considered to be the most probable even though the list is not comprehensive. .

Generator Protection can be provided by systems that are:

1. Independent.
2. Centralized.

Designs based on independence provide each generator with its own dedicated protection function that is able to determine whether that generator is healthy or not. This type of system has another level of protection. If the generator protection function in the faulty set is unable to trip itself, the generator protection in the healthy sets will all act to divide the common power system.

Designs based on centralized control usually function on the basis of comparison and voting. In this design a centralized control system attempts to identify which generator is faulty by comparing the operating points of several online generators and using a voting function to determine which generator to trip.

Independent systems are generally considered to be more robust than centralized systems using comparison / voting techniques.

11.8 SYNCHRONIZATION

11.8.1 **Generator synchronization:** Synchronization is the process of matching the voltage, frequency and phase of an incoming generator so that it connects smoothly to the power system at minimal load. Voltage matching is not usually necessary in marine power systems but frequency and phase must be tightly controlled.

The synchronizing process is normally controlled by an automatic synchronizer which takes over control of the generator's governor during the synchronizing process and adjust the speed of the generator to bring phase and frequency within defined limits. The relative speed of the incoming machine is set to ensure it takes a slight positive load on connection. When this has been achieved the synchronizer closes the generator circuit breaker and relinquishes control of the governor which then loads up the generator.

Connecting a generator out of sync can cause very severe power systems transients and these have been known to cause blackout in some cases.

Some marine power systems are robust enough to withstand a 'crash synchronization'. This can be demonstrated by mathematical modelling of the generator and bus bar currents which prove the generators will pull into synchronism before the transient current reaches the tripping point of over current protection.

Modelling of crash synchronization should be carried out for any DP Class 2 or DP Class 3 vessel intending to operate with the power plant configured as a common power system. Modelling may not be necessary if the FMEA can demonstrate that crash synchronization cannot occur because of a single failure. This can be difficult to prove in typical marine power systems.

In the case of vessels operating the power plant as two or more independent power systems, the effects of a crash synchronization are limited to one redundant power system.

Synchronizers may have problems connecting standby generators if the load on the power system is changing rapidly. Incidents of this type have occurred in the past. Such issues have been overcome by initiating a brief thruster command freeze during the synchronizing process.

Potential for failure to synchronize is common to power systems that are operated in both open and closed bus configurations. This scenario can be mitigated by ensuring sufficient spinning reserve and effective load shedding functions in each independent power system.

11.8.2 **Bus synchronization:** Bus synchronization is the process of connecting two independent power systems together. In this process the automatic bus synchronizers will raise or lower the speed of all generators on one bus to match the phase and frequency of the power system to which the incoming bus is to be connected. Failure scenarios are similar to those discussed under generator synchronization.

11.8.3 **Note:** *Designs have been developed that require no cross connections to achieve bus to bus synchronizing or dead bus detection. Such designs remove potential fault propagation path associated with VT signals and status contacts etc. crossing the boundaries between redundant equipment groups intended to be independent and fail safe.*

A suitable opportunity should be chosen to carry out bus to bus synchronizing to limit the consequences should a failure occur. Hybrid power dedicated to the thrusters can help reduces the criticality of such events.

11.8.4 **Manual synchronization:** Classification societies require that there be an alternative means of connecting generators if the automatic synchronizers fail. A synchroscope with check sync function to supervise the manual closing command is the normal method of meeting this requirement.

The risks associated with manual synchronizing are not significantly different to those associated with automatic synchronization provided there is a check synchronizer.

11.8.5 **Breakout and inadvertent energization:** Inadvertent connection of a stopped generator may occur through maloperation, or a generator circuit breaker control system fault. This type of fault can also cause severe power systems transients with the potential for blackout. A running generator may also suffer a severe mechanical fault which may cause it to break synchronism and pole-slip.

Some marine power systems are robust enough to withstand this type of fault. Mathematical modelling of the protection response should be carried out to prove this for any DP Class 2 or DP Class 3 vessels intending to operate with the power plant configured as a common power system.

In the case of vessels operating with two or more independent power systems the failure effects should be limited to one power system.

11.9 INTERLOCKS

11.9.1 **General:** Dangerous power plant configurations should be prevented by design. Design should identify vulnerable configurations and effective mitigations should be implemented. Interlocks are a common mitigation.

All interlocks are potential hidden failures in much the same way as protection systems are. Critical interlocks should be tested non-destructively and periodically to confirm their effectiveness.

In power distribution systems with several voltage distribution levels it is important to carefully define the protection interlocking strategy to prevent faults on upper levels being back-fed by way of the lower levels and service transformers.

Classification societies may require that all interlocking is hardwired although it may be backed up by software equivalents in the VMS or PMS.

Hardwired interlocking that crosses the boundaries between systems intended to provide redundancy requires careful attention particularly in DP class 3 when it can provide a path for fault propagation.

Interlocks to prevent non redundant configurations which may compromise the redundancy concept by removing its fault tolerance are not a class requirement. These issues are usually dealt with by suitable checklists, consequence analysers and criticality analysers of various degrees of sophistication. Design should consider interlocks for preventing non redundant configurations to minimize vulnerabilities to human error or misinterpretation.

11.9.2 **Shore power:** Shore power connection points may be interlocked with the service transformers which supply the switchboard for hotel and auxiliary services.

The practice of inter tripping the service transformers if the presence of shore power is detected may introduce failure modes leading to loss of all thrusters or blackout if the interlocking / inter tripping fails or operates spuriously.

This failure effect cannot be avoided by changes in power plant configuration (open / closed bus) and should be designed out.

11.9.3 **Short term paralleling and auto transfer:** Short term paralleling is the process by which a bustie between two switchboards may be closed for long enough to change oversupply from one service transformer to another.

The process may be automated to the point that the operator indicates to the VMS that it should change the supply arrangement and the process will be carried out without further operator intervention.

The design of such systems requires careful scrutiny to ensure they cannot disconnect both sources of supply, if the short term paralleling system has a hidden failure.

Such transfers, if needed, should be carried out during non-critical DP operations whenever possible.

Some low voltage power distribution systems are designed to transfer a switchboard or consumer to another source of supply on loss of the normal supply.

Such systems should be designed in such a way that the transfer does not operate if the switchboard or consumer itself is faulty.

11.9.4 **Back feeding:** This term is used to describe the practice of back feeding the low voltage distribution level from the emergency generator. This can be a useful feature for maintenance purposes when the vessel is in dock and the main power plant is not operating.

Interlocks and intertrips associated with this arrangement need careful scrutiny to ensure the redundancy concept is not defeated, if they fail or operate spuriously.

Classification societies normally require that use of the emergency generator for non-emergency purposes is kept to a minimum and that the protection systems for back feeding are arranged to ensure continued operation of the emergency switchboard if there is a fault in a back-fed consumer.

Design should provide clear indication of emergency generator / switchboard status on the PMS power mimic to reduce the risk of putting to sea with the emergency switchboard in harbour mode.

11.10 DC POWER GENERATION AND DISTRIBUTION SYSTEMS

11.10.1 At one time dc power and dc drives were the de-facto choice for speed control. Early dc power systems had motors and generators that relied upon commutators and brush gear for their operation. These mechanical parts were vulnerable to failure and wear and required more frequent maintenance. The development of power electronic convertors has made it possible to develop dc power systems that use robust alternating current generators and motors. Typically, power is generated in alternating current form and immediately rectified to direct current at the generator's terminals. It is then distributed as dc to other power electronic convertors (inverters) which turn it back to alternating current a variable frequency to allow speed control of asynchronous motors.

DC power generation systems have been popular in small and medium sized DP vessels. It is in theory possible to develop designs for the largest DP vessels. Even in large alternating current designs, direct current plays an increasingly important role in distribution systems for thrusters and industrial mission equipment.

11.10.2 Direct current systems differ from their AC counterparts in areas such as:

- Protection and switchgear.
- Load sharing.
- Engine speed control.
- Voltage control.
- Generator connection and disconnection.
- Electronic busties (ultra-fast fault clearance).

11.10.3 **Protection and switchgear:** Unlike ac power, there are no natural current zeros to assist in interrupting arcs. More use may be made of fuses in high power applications and electronic circuit breakers or bus links may be used in preference to mechanical circuit breakers. Electronic circuit breakers typically use power transistors to interrupt fault currents rapidly.

Fault currents may be reduced and extinguished more quickly than ac systems because the generator excitation may be controlled to reduce it and the initial high current phase of the fault is provided by capacitor banks and not by the generator.

11.10.4 **Engine speed control:** Engines may run at variable speed as their output is rectified. This has advantages in reducing wear and losses at low power as the engine can be operated at lower speed compared to a synchronous ac generator which is typically run at constant speed regardless of load.

11.10.5 **Load sharing:** Load sharing can be achieved by the voltage regulators.

11.10.6 **Voltage control:** This is typically achieved by the AVRs. Voltage control of energy storage systems may also require consideration in hybrid power system designs.

11.10.7 **Generator connection and disconnection:** Synchronization is no longer required in the same way as it is ac systems because there is no need to match generator and bus waveforms in frequency and phase.

11.10.8 **Power for auxiliary systems may be distributed using alternating current.** Large inverters may provide fixed frequency and voltage ac power to distribution systems for use by constant speed motors used in pumps and fans.

11.10.9 **Redundancy concept:** Although the means by which power is generated, distributed and consumed is different to ac systems there is essentially no significant difference in the way the DP system's redundancy concept is designed and analyzed. The same requirements to identify fault propagation paths, created by common points between redundancy groups, hidden failures and barriers to acts of maloperations apply. DC power systems may make it easier to accommodate energy storage in the form of batteries or super capacitors.

11.11 VARIABLE VOLTAGE AND FREQUENCY ALTERNATING CURRENT POWER SYSTEMS

11.11.1 Power systems can be designed to operate with both variable voltage and variable frequency. Such designs have some of the advantages of direct current systems in so far as its possible to reduce the engine speed at lower power levels allowing additional energy savings. There is fundamentally no difference in the way such systems should be analyzed to determine their worst-case single failure effect.

11.12 PROTECTION AGAINST THE EFFECTS OF FIRE AND FLOODING

11.12.1 Classification society rules for DP Class 3 differ from each other and from IMO MSC645 / 1580. Some classification societies require a higher standard of fire and flood separation than others.

11.12.2 **Physical separation of equipment:** The central tenet of DP Class 3 is that equipment intended to provide redundancy must be physically separated to protect against the effects of fire and flooding. Redundant equipment should be separated by A60 rated bulkheads or equivalent fire protection to A60 requirements.

Common points in the redundancy concept are created by co-location of equipment and cable routes. For DP class 3 there should be no co-location of DP related equipment.

It is not usual for industrial consumers to be fed from more than one redundant power system and effectively create a common point whether the busties are open or closed.

Where this type of design exists, it is necessary to prove beyond reasonable doubt that the effects of fire and flooding at the common point cannot adversely affect the operation of all redundant power systems to which they are connected.

If many circuits from more than one power system enter a common space to provide auxiliary services for some part of the industrial function of the vessel there is a risk that fire and flood damage may create simultaneous or sequential faults which may divide the fault current available or extend the voltage dip applied to each power system.

This possibility should be considered in the protection relay coordination study and discussed in the DP system FMEA.

This issue can be avoided by supplying LV consumers from local Motor Control Centres rather than from main LV switchboards. This reduces the number of parallel cables runs into a single compartment. Thus, if the discrimination fails, the failure effect should be limited to loss of the MCC.

Supplying DP related and non-DP related equipment from switchboards and MCCs supplied by separate service transformers largely negates the issues of extended voltage dips caused by sequential faults.

It is recommended that dual power supplies to the same space from redundant power systems be avoided if possible. If dual supplies are required, but only one feed is required at a time, then consideration should be given to carrying out the switching function at the main switchboards so that both cables are not live at the same time.

11.12.3 **Fire subdivisions:** All equipment intended to provide redundancy should be separated by bulkheads and decks of A60 rating or by two A0 bulkheads /decks with a low fire risk compartment in-between.

Watertight doors in A60 bulkheads need not be A60 rated but should have a melting point not less than 950°C. Combustible materials should not be located closer than 450mm from the door.

11.12.4 **Watertight subdivisions:** Equipment intended to provide redundancy should be contained within separate watertight and A60 compartments below the damaged waterline. As a minimum, the arrangement of watertight compartments should reflect the split in the redundancy concept and support the worst-case failure design intent.

Consideration should be given to locating each thruster in its own watertight compartment. This is required by at least one classification society.

Watertight separation should be considered above the waterline when there is a risk of leakage from large bore pipe work, tanks or other sources.

11.12.5 **Cable and pipe routes:** Cable and pipe routes for equipment intended to provide redundancy should be physically separated by bulkheads of A60 rating. Where this is not possible cables may be run together in a single A60 rated duct where the only fire risk is from the cables themselves. This method should not be used in high fire risk areas such as engine rooms.

Means are to be provided to ensure the temperature of cables within ducts is maintained at or below the rating of the cable when operating at full power.

On open decks, cables in pipes that are separately routed are acceptable.

12 HYBRID POWER

12.1 APPLICATIONS OF STORED ENERGY FOR PROPULSION AND IM EQUIPMENT

12.1.1 Stored energy systems in the form of uninterruptable power supplies, based on batteries and power electronic convertors, have long been used to supply control power to sensitive consumers. Such devices are essential when there is a possibility of more than one redundant DP equipment group being exposed to a power system disturbance. They also allow controllers to remain active during blackout recovery speeding up the recovery process. Advances in battery and convertor technology have allowed this concept to be extended to very large power consumers for propulsion and industrial mission applications.

12.1.2 The term 'Hybrid Power' is used to describe a power system with a mix of energy sources. In the case of DP vessels with hybrid power, the term is most commonly used to indicate that the electrical power generation system can be powered from a combination of diesel generators and power electronic convertors supplied from stored energy sources such as batteries. The term can however be applied to other combinations of energy sources. Classification society rules guide the way in which hybrid power can contribute to redundancy based on the time to terminate the DP operation. The 'time-to-terminate' is a key factor in dimensioning the energy storage system. Emphasis is placed on clear and unambiguous indication to the operator that the plant is using stored energy and the remaining time available on stored energy. This is an area of focus for some classification societies.

Note: *The application of the focus on time to terminate is driven by the interpretation of the IMO guidelines (IMO MSC 645 & 1580)* and does not take into consideration acceptable position excursions appropriate to the industrial mission.

12.1.3 Stored energy sources find a number of applications in a marine power system including:

- **Fuel saving and emissions reduction** - Providing short term 'spinning reserve' allows the power system to be operate with fewer generators at higher load. In this case the stored energy and conversion systems provide short term power in the event of failure of a diesel generator or an increase in load until another generating set connects to replace it.
- **Peak shaving** – The performance of diesel generators can be optimized by operating them at a high and constant load. Stored energy facilities can be used to supply cyclical peak power demands by charging during periods of low demand and discharging to the power distribution systems during periods of high demand. The type of loads that can be supplied in this way depends upon the periodicity with which they draw and regenerate power from and to the vessel's power distribution system.
- **Fault ride-through capability –** Stored energy systems can provide power to consumers during a power system upset associated with clearing a fault. This is possible when the stored energy facility is connected to the power consumers themselves and not connected directly to the main power distribution system. (Example thrusters, cranes, drawworks). A correctly designed and configured hybrid power system can significantly reduce the criticality of protection system used to provide fault tolerance in power supplies operating with closed busties. The effect of such a design is to 'decouple' the thrusters from the generators in terms of the failure modes and effects at least for the endurance of the batteries.

- **Dynamic support for high inertia loads -** Loads with very high inertia can cause the power system frequency to fall to unacceptable levels during periods of high acceleration. Traditional methods of addressing this issue required the connection of several, or all, generators. This is a very inefficient way of addressing peak demands for power. Stored energy systems can be used to supplement the poor load acceptance of diesel generators thus reducing the number of generators that must be running at light load (example, large active-heave drawworks).
- **In-port and shore power charging facilities** - Vessels that make frequent port calls can benefit from shore power not only to supply their power needs while loading or discharging cargo but also to charge battery banks to reduce reliance on the main diesel generators in port. When shore power is of limited capacity or not available, stored energy and conversion systems can be used to supplement the capability of a much smaller harbour generating set. If the vessel's load profile in-port is such that there are infrequent, shorter term, demands for high power levels (example cargo pumps) it may be possible to dimension the stored energy system to provide the higher short-term power demand and recharge from the small harbour set or limited shore supply.
- **Providing power to operate drawworks during a blackout:** The ability to space out and hang off the drill string during a total blackout is essential to ensure the reliable operation of the EDS system on a DP MODU. Power for this may be provided by dedicated energy storage facilities for the drilling power system.
- **Increasing the time to reach the red watch circle in a drift off condition.** In practice, the action that a driller would take on receiving confirmation that the thrusters were operating on battery power is little different from the action taken on a conventional drilling power system during a blackout. However, the added advantage that hybrid power provides is that the time taken to reach the red watch circle can be extended allowing greater margins before the EDS must be operated and additional time to recover the power plant and / or safely suspend ongoing operations. Stored energy may also be used to move some non-shearables away from the shear rams using the drawworks.

12.1.4 The nature of the industrial mission that the DP vessel performs will determine the extent to which it is possible to benefit from the applications discussed above.

12.2 TYPES OF ENERGY STORAGE SYSTEMS

12.2.1 There are currently two forms of electrical energy storage systems in mainstream use in marine power systems:

- Super / Ultra capacitors.
- Batteries (Various chemistries are in use but predominantly Lithium based).

12.2.2 Super capacitors typically have a lower energy density and higher discharge rates than batteries but are capable of many more charge and discharge cycles without significant degradation. Batteries on the other hand require more careful management to ensure they are not used in a manner that significantly shortens their life-time. The performance gap between super capacitors and batteries has closed to some degree in recent years. Capacitors also have certain limitations to be observed.

12.3 INTEGRATING STORED ENERGY

12.3.1 Many hybrid power schemes treat the stored energy and conversion systems as ‘static’ or ‘solid-state’ generators connected to the main power distribution system (or sometimes on the LV power distribution). This may be the easiest approach for retrofits and allows the energy to be distributed to anywhere it is needed (but it may also be more difficult to ensure it goes where it is most needed). Other designs provide local energy storage at the thrusters and drawworks. This arrangement has significant advantages including:

- The power can be reserved for use by critical consumers and not depleted by others.
- When the energy storage and conversion equipment is located downstream of the rectifiers that feed those consumers, it cannot feed a distribution side fault and thus there is no change in the fault characteristics of the power plant. Coordination studies and short circuit test results remain valid. This may be beneficial for upgrades and conversions.
- The distributed nature of the battery installation means the concentration of flammable or explosive materials in any one space is reduced.
- The thrusters do not stop during blackout and blackout recovery (but may operate at reduced power). This reduces the criticality of the dependence on correct functioning of protective functions that are intended to prevent blackout. All such protective functions are potential hidden failures, so this arrangement provides another barrier to immediate loss of position even if the protection systems have failed to deal with the cause of the blackout correctly.
- If properly designed for operation in emergency conditions, hybrid power offers the possibility of DP MODUs retaining some propulsion capability with the engines shutdown which may be beneficial in the case of a hydrocarbon gas release.
- Connecting the batteries at the thrusters rather than to the bus-bars may require batteries to be installed at more locations with consequential infrastructure requirements.

12.4 CONSIDERATIONS

12.4.1 There are a number of design and operational issues to be considered when implementing a hybrid power solution.

- **Battery safety**: There are a variety of battery chemistries. Some are associated with greater fire and toxicity risk than others. Batteries are a potential fire risk but are also at risk from fire. It is for these reasons that there are restrictions on battery location and requirements to protect batteries from fire. Cooling, ventilation and fire suppression measures are other facilities to be considered.
- **Time to terminate**: Propulsion capability on battery power and time taken to terminate the DP operation safely influences whether the stored energy system can count towards redundancy and post failure DP capability. Part of the work in dimensioning a hybrid power system is to identify the time to terminate the intended DP operation and estimate the power and energy required from the batteries. If the batteries can be dimensioned to provide power for long enough to safely terminate the work in progress, then they can be considered to contribute to redundancy and post failure DP capability.
- **Time Line**: When dimensioning the battery banks the following should be take into consideration:

- The classifications societies generally do not validate that the time line provided to them is sufficient to allow the stated operation to be terminated, only that the installed hybrid system has the capacity to provide the stated endurance in the defined conditions.
- Means and time to detect that propulsion is being supplied from batteries (time on DP is now limited by battery endurance).
- Time to take action and communicate the need to terminate the operation.
- Time to terminate the operation.
- The possibility that the environment may increase during the time it takes to terminate the operation.
- The propulsion capability required in the intact and post worst case failure conditions.

- If the batteries cannot be dimensioned to achieve this requirement, they can still be used for peak shaving provided the 'spinning reserve' required for DP redundancy is supplied by the diesel generators.

Note: *Provided the batteries are dimensioned to allow the work in progress to be terminated it is possible to rely on the connection of standby machinery and blackout recovery to prevent further position loss position and potentially prevent having to terminate the operation. This is based on the time on DP available from the batteries being sufficient to wait for a successful standby start before taking the decision to commence termination of the operation (in case the standby start was not successful).*

12.5 SINGLE GENERATOR OPERATIONS

12.5.1 Objective of operating the power plant with a single generator connected is now a possibility with hybrid power installations. Some vessels have obtained class approval to operate in this configuration.

12.5.2 When designing hybrid DP power plant for single generator operations (with hybrid sources operating in parallel) there are some additional considerations.

- The possibility that a power distribution system fault will have to be cleared by the static generator alone. That is to say, the static generator may have to provide fault current to operate the over current protection for the bustie if operating in closed bus configuration.
  i. What impact will this have on protection coordination?
  ii. Will there be a need to alter the protection coordination dynamically depending on the configuration and combination of rotating and static generators?
- Reliance on the cognitive and intervention skills of the operator.

12.6 POWER, ENERGY AND BATTERY MANAGEMENT SYSTEMS

12.6.1 **PMS** - Diesel electric vessels traditionally have Power Management Systems (PMS) designed to ensure there are always sufficient generators online to cope with increasing power demand and also to cope with the worst-case loss of generators (spinning reserve). In such systems it was always assumed that there was sufficient stored energy, in the form of fuel oil, to allow operations to be terminated when required.

12.6.2 **EMS** - In the case of hybrid power installations, the static generators are considered to be akin to diesel generators with very small service tanks. Thus, it becomes important to ensure that these 'service tanks' are full. This is particularly important if they are to be used for other activities like 'peak shaving' in addition to a role as 'spinning reserve'. In hybrid power systems the power management system must also manage the stored energy, not just the power. PMS which manages the energy are called Energy Management Systems (EMS). This is done in recognition of this additional functionality.

12.6.3 **BMS** – Batteries require their own dedicated management systems. Battery banks are made of modules which are, in turn, constructed from many such smaller cells. Battery Management Systems (BMS) must perform several functions including:

- Protecting the batteries from over charging. Lithium cells are particularly sensitive to overcharging and failing to manage this aspect correctly has severe consequences including thermal run-away, off gassing of flammables and explosion.
- Balancing the charge in each module, and in some designs, balancing the energy in each cell.
- The BMS will typically monitor the 'state of charge' and 'state of health' of the battery bank. Battery banks are typically dimensioned to allow for decrease in capacity with age and duty cycle.

12.7 BATTERY SAFETY

12.7.1 Battery safety is a subject in its own right and a considerable part of the verification and validation effort is focused on ensuring the battery banks do not significantly increase the risk of fire and explosion. However, it is also worth noting that there are many other fire and explosion risks associated with diesel electric power plant that are currently accepted. The requirements for ventilation and fixed firefighting are influenced by the amount of gas that can be evolved from a battery bank. Restrictions of location within the vessel's hull also apply in recognition of the increased fire risk to the batteries from other sources of ignition. All vessel stakeholders should align on the verification and validation processes required to achieve the basis of confidence in the energy storage systems so as to ensure expectations are met. This may require additional verification and validation over and above that required by class as a minimum standard.

Fire and explosion risk is considered in two ways:

- **Internal** - **The risk of off-gassing from within the battery bank** – The amount of gas evolved can be reduced if the design limits the effects of internal faults to a single cell. A cell may short circuit, It the adjacent cells do not fail because of this short circuit and the heat from the faulty cell does not drive the adjacent cells into thermal run-away then it can generally be accepted that the contents of one cell is defined as the total amount of explosive / toxic gas that can be released. The BMS must also prevent the whole battery bank being exposed to an over voltage / overcharging.
- **External** – It has to be assumed that the entire battery banks could be subject to thermal run-away and off-gassing if it is consumed by an external fire source. Verification and validation activities attempt to assess the likelihood of this event based on the fire risks in the compartment in which the battery bank is located. Firefighting systems may contribute to a lowering of the risk. Flooding or water ingress may also be a credible threat.

13 POWER DISTRIBUTION

13.1 DISTRIBUTION PHILOSOPHY

13.1.1 The design philosophy for the power distribution should:

1. Support the worst-case failure design intent.
2. Be fully fault tolerant in respect of the defined failure criteria.
3. Follow the divisions in the redundancy concept which define redundant systems.
4. Maintain independence and separation.
5. Closely associate the power source of auxiliary systems for engines and thrusters with their respective main feeders.
6. Ensure the electrical protection scheme supports the redundancy concept.
7. Provide sufficient flexibility without compromising redundancy.

13.1.2 Failure modes in the power distribution should be minimized. Some of the common areas for vulnerabilities to be avoided are:

1. Single busties circuit breakers in DP Class 2 systems - Most classification societies accept a single switchboard being divided in two using a single bustie breaker. This introduces the possibility of a crash sync leading to a blackout in case the single bustie breaker spuriously closes tying both bus bar sections. Consideration should be given to installing two bustie breakers.

   Note: *Some classification societies require two circuit breakers between any two bus sections intended to provide redundancy when the vessel operates with closed busties.*
2. Dependence on emergency switchboard / generator.
3. Voltage dips associated with short circuit faults.
4. Vulnerability to earth faults in deck equipment on DP distributions.
5. Poor regulation in service transformers.
6. Poor separation of DP and non-DP related power consumers.
7. Control lines for interlocks, intertrips and protective functions which cross the divisions in the redundancy concept without adequate protection or selectivity.
8. Poor design of auto changeovers, backup supplies and common connections which can transfer faults.
9. Common backup supplies which span the divisions in the redundancy concept.
10. Co-location of services (DP and/or non DP related) fed from power systems intended to be redundant creates a common point under DP Class 3 failure criteria.
11. In DP Class 3 a common point is created by cable routes supplying non DP essential services where the route includes cables from power systems intended to be redundant.
12. Providing duty standby supplies for auxiliary systems confined to one redundant machinery group from power systems intended to provide redundancy.

13.2 MAIN POWER DISTRIBUTION

13.2.1 The main power distribution level in a diesel electric plant includes the switchboards to which the generators and thruster are directly connected. Power is typically generated at voltages of 690V, 6.6kV and 11kV depending on the size of the power plant. High voltage power generation is chosen because it reduces the required fault withstand rating of the switchboards and reduces the amount of copper required in cables to transmit the same amount of power. Most modern thruster drives operate at lower voltages so it is not uncommon for almost every consumer on an 11kV main power distribution level to be a service or drive transformer. At low voltages consumers may be connected directly to main.

13.2.2 The main power distribution should be arranged to reflect the split in the redundancy concept. Physical separation should be provided for DP Class 3 vessels.

13.2.3 Some classification societies still permit a single bustie between switchboards for DP Class 2. One bustie circuit breaker in each switchboard is the recommended arrangement. Some designs utilize a single bus coupler between two bus sections in the same switchboard. This arrangement is acceptable. The design should provide for two busties between separate switchboards, particularly if the switchboards are in different compartments. Also refer to 13.1.2.

13.3 AUXILIARY SYSTEM DISTRIBUTION

13.3.1 Design philosophy should strive to provide independence of main machinery such as generators and thrusters to the maximum extent feasible.

13.3.2 The distribution voltage for auxiliary systems is typically 480V. On vessels with 690V main generation level it is common to find larger motors supplied directly at 690V.

13.3.3 The split in the auxiliary power system should follow the split in the main power distribution system to match the worst-case failure design intent. Switchboards for non DP essential services such as accommodation power and other hotel services need not be supplied with the same split or have only limited redundancy provided such arrangements do not compromise the industrial mission.

13.3.4 The auxiliary power distribution level is normally supplied from the main power distribution level by way of transformers. These service transformers should have an earthed screen between primary and secondary sides to reduce the risk of an over voltage failure on the secondary side caused by an internal fault.

13.3.5 The auxiliary power system provides all power for the pumps, fans and compressors used in the engine rooms, thruster rooms and other machinery spaces such as pump rooms.

13.3.6 Design should strive to closely associate supplies for auxiliary systems for engine and thrusters with the main feeder or incomers for those thrusters and generators.

13.3.7 In some applications, it is possible to feed auxiliaries from the high voltage incomer for a thruster by way of a dedicated step down transformer. This significantly improves the independence of the thruster drive. The rational for this arrangement is that if there is no main power, the auxiliary power is not required. It may also offer advantages in terms of reduced cabling for LV distribution.

13.3.8 Exceptions to the above philosophy that may need to be considered in design are:

1. Pre-charging circuits.
2. Cooling water pumps.
3. HVAC and ventilation.

13.3.9 Functions delivered by 1 and 2 are sometimes a perquisite for closing the main HV breaker to a variable speed drive.

13.3.10 HVAC and ventilation may be required for the comfort of engineers while the drive is shut down for maintenance. Consideration should be given to providing a normal supply from the drive auxiliary distribution and a backup supply from the main power systems. Control power UPSs for the drive and other thruster control systems should also be supplied in this manner.

13.3.11 The emergency switchboard is normally fed from the auxiliary power level. It is useful to have more than one feed to the emergency switchboard for flexibility. Difference in failure effects, if any, due to dual feed should be fully understood and documented in the FMEA.

13.3.12 Protection for auxiliary consumers usually consists of:

1. Short circuit.
2. Over load.
3. Earth fault - may be alarm only.
4. Under voltage - with suitable delay where required.

13.4 EMERGENCY POWER DISTRIBUTION

13.4.1 Dependence on the emergency switchboard for DP operations should be avoided.

13.4.2 The emergency switchboard may have several useful functions in a DP vessel in addition to its intended emergency role. Design should facilitate operation of the vessel with the emergency power system completely unavailable.

13.4.3 The emergency switchboard may provide the shore power connection point and be able to back feed the auxiliary power system in harbour mode.

13.4.4 The emergency switchboard should not be required for blackout recovery but may be utilized for longer term black start functions.

13.4.5 Every UPS and battery system should have a main power supply from an auxiliary system switchboard appropriate to the split in the redundancy concept and a backup supply from the emergency switchboard.

13.4.6 All changeovers should have sufficient interlocks and protection to prevent them transferring a fault from one supply to the other.

13.4.7 Failure of backup supply from the emergency switchboard to over voltage should also be considered. This should not be able to affect multiple consumers with backup supplies.

13.4.8 In DP Class 3 designs it may be more appropriate to carry out the switching functions at the switchboards such that only one supply is energized at a time. This prevents voltage dips occurring because of fire or flood damage at the common point created by the compartment.

13.4.9 In addition to all the emergency consumers and lighting required by SOLAS the emergency switchboard may also provide emergency power for certain functions associated with the industrial mission. This may require the emergency generator to be much larger than that found on merchant vessels. Emergency generators of 1MW or 2MW rating are not unusual.

13.5 RATING AND ROUTING OF CABLES

13.5.1 **Rating:** Classification society rules provide extensive guidance on the cable properties and ratings. In summary, cables should be rated for the line current and voltage they will carry, and the following should be considered:

1. Bend radius restrictions may be an issue particularly in HV designs.
2. Ambient temperature is a design consideration.
3. Cables must be de-rated if more than a certain number are grouped together due to the reduction in cooling effect when cables are bundled together.
4. Cable restraints to cable trays must be strong enough to withstand the mechanical forces created by short circuits.
5. Three core and single core power cables may be used as appropriate but single core cables require non-ferrous gland plates to avoid overheating created by eddy currents.
6. Cables for power and control functions should be installed with due regard to electromagnetic compatibility (physical separation requirements).
7. Voltage drop is to be considered.
8. Cables are to be marine approved types and at least flameproof.

13.5.2 Some classification societies may allow cables to be rated for a line to earth voltage lower than that experienced if design provides for automatic disconnection on detection of earth fault. To facilitate alignment with the redundancy concept, it is recommended that cables for DP vessels are rated for the full line to earth voltage that the insulation will experience under earth fault conditions.

13.5.3 **Routing:** In DP Class 2 vessels, physically separate routes should be provided for cables to equipment intended to provide redundancy. The cables should be protected from mechanical damage. Cables for redundant systems should not be run together through high risk areas. Control cables for dual networks should be separated and protected from damage.

13.5.4 For DP class 3 vessels the same stipulations above apply but the separation between redundant cable routes should be of A60 rating. Two A0 bulkheads with a low risk compartment in-between are also acceptable. Where a common cable route is unavoidable, cables may be run in a single A60 rated duct provided the only fire risk within the duct is associated with the cables themselves.

13.5.5 Cable transits should not compromise the A60 rating of fire subdivisions. Cable transits should have properties equivalent to the subdivision that they are being used in and be able to withstand the maximum water pressure likely to be experienced.

13.6 SUPPLIES FOR DUTY STANDBY PUMPS

13.6.1 Duty and standby pumps should be provided to improve the availability of the system in the event of pump failure and not to maintain operation if one of the auxiliary switchboards fails. Therefore, the supplies for duty and standby pumps should come from the same side of the power distribution system in a manner that supports the worst case failure design intent. It may be advantages to provide power from different distribution boards for additional security and convenience.

13.6.2 The above philosophy is applicable when the auxiliary system to which the pumps belong serves only one redundant machinery group.

13.6.3 There are some class societies which accept designs in which the auxiliary system serves more than one redundant machinery group provided it has at least two pumps. In this case the pumps should be supplied from redundant power sources (opposite sides of the power system).

13.6.4 Shared auxiliary systems introduce commonality and are not recommended. Such a design may be accepted in the case of seawater cooling systems with appropriate and effective alarm and monitoring facilities.

13.7 TRANSFERABLE GENERATORS AND DUAL FED THRUSTERS

13.7.1 **Class requirements:** Carefully engineered transferable generators and thrusters are accepted by some classification societies. Designs that consider transferable generators and thrusters should be fault tolerant, fault resistant and follow a systems engineering approach.

13.7.2 Transferable or dual fed consumers are treated differently by different classification societies. In some DP notations thrusters of this type can be considered to contribute to redundancy as follows:

1. Thruster with changeover power supply which does not stop when the power supply is changed over.
2. Thruster which draws power continuously from two redundant supplies.

Note: The design of transferable generators and thrusters must accommodate the need for the provision of auxiliary services (example – cooling water pumps and control power) to be supplied from both redundancy groups.

13.7.3 Care must be taken to ensure that faults cannot be transferred from one redundant power systems to the other because of faults in one system or in the dual fed consumer itself.

13.7.4 In the case of DP Class 3 vessels, the effects of fire and flood at the common point should be considered and designed such that there is no adverse reaction on either power system.

13.7.5 Some DP class notations discourage transferable thrusters and generators and may not accept such features as contributing to redundancy. They may be provided to improve post failure DP capability after a fault provided requirements to prevent transfer of fault and hidden failures are adhered to.

13.7.6 **Transfer of fault and hidden failures:** In general terms, the fewer common points there are between redundant systems the less likely it is that a fault will be transferred from one redundant system to the other. Dual supplies may introduce risk of a hidden failure if one supply fails.

13.7.7 If it is possible to achieve the desired post failure DP capability without transferable or dual fed elements, then this should be done. If this is not possible or there are clear benefits to providing such features, then all necessary measures to prevent transfer of fault and reveal hidden failures should be in place.

13.7.8 Designs that incorporate transferable generators and thrusters should document comprehensive analysis in the FMEA. Results of verification and validation testing should be documented in accordance with the supporting engineering studies and comprehensive analysis.

Note: *The scope and depth of the analysis and testing required for transferable thrusters and generators is typically equivalent to that required for closed-bus power systems. (End users may require validation testing beyond what is accepted by classification society).*

13.8 OPEN AND CLOSED BUSTIES

13.8.1 Bustie circuit breakers should be fully independent and each should have the necessary protective functions to ensure that switchboards intended to provide redundancy can be separated.

13.8.2 In some designs only one bustie (Master) has control and protection and the other bustie is a slave. Such arrangements should be avoided.

13.8.3 The above are particularly important in DP Class 3 vessels where class rules require consideration of damage by fire or flooding.

13.8.4 DP power plant can usually be operated as a common power system or as two or more independent power systems.

13.8.5 It may be possible to make a common power system fully fault tolerant in respect of single failure criteria for DP Class 2 and DP Class 3. However, in such designs fault tolerance depends on a very comprehensive range of protective functions and on many items of equipment being able to perform to capacity.

13.8.6 Operating the power plant as two or more independent power systems reduces dependence on protective functions and vulnerability to hidden failures. It does not remove all common points between redundant systems. The potential to lose one part of the system is higher but the potential to lose the complete system is reduced.

13.8.7 The security of station keeping with independent power systems still depends on redundant equipment being capable of its rated capacity and there may be greater demand for one power system to maintain position and heading in this configuration. Thus, there may also be more frequent demand for systems to operate at high load. These issues should be carefully considered when determining the critical activity mode of operation (CAMO). Designs that reduce the impact of the worst-case failure beyond that required by class improve availability to carry out the industrial mission. For example, designs that reduce impact to loss of 33% capability against 50% (See also LIFE concept).

13.8.8 It is important to understand that the integrity of station keeping ability of independent and common bus configurations depends on having all systems and equipment fully functional and available. Equipment intended to provide redundancy and fault tolerance should be periodically tested and maintained to ensure the required level of performance and to reveal hidden failures.

13.8.9 The use of distributed stored energy sources (typically batteries) can significantly reduce the criticality of protection by providing another barrier to prevent or limited the speed of loss of position giving time for blackout recovery or connection of standby redundancy.

13.9 PRE-MAGNETIZATION TRANSFORMERS

13.9.1 Pre-magnetization transformers can be usefully employed to reduce the inrush current transient associated with starting larger service transformers. This has advantages in blackout recovery as it allows loads to be connected as soon as the first generator becomes available with reduced risk of blacking out again when the first transformer is closed on to the bus.

13.9.2 Premagnetisation may also enable protection levels to be set at more effective levels.

13.10 DC CONTROL POWER SUPPLIES & BATTERY SYSTEMS

13.10.1 DC control power and battery charger systems should as a minimum be provided in line with the spit in the overall redundancy concept. Design should consider addition of non-critical redundancy to improve availability. For example, a second battery supply to allow battery maintenance.

13.10.2 The output of DC systems supplying equipment intended to provide redundancy should not be cross connected. Crossovers for maintenance should not be provided in DP Class 3 vessels if this can lead to transfer of fault by fire or flooding. Control supplies should have a normal supply from the appropriate part of the power distribution system in a manner that supports the redundancy concept and a backup power supply from the emergency power distribution systems. The risk of transfer of fault and hidden failures should be reduced to a minimum.

13.10.3 Control supplies for thrusters and generators should be provided in a manner that makes each thruster or generator as independent as possible.

13.10.4 Control systems for sensitive circuits should not be shared with heavy consumers such as circuit breaker spring winders. Operation of multiple spring winders may cause control systems to malfunction.

14 POWER & VESSEL MANAGEMENT

14.1 KEY PRINCIPLES OF POWER AND VESSEL MANAGEMENT

14.1.1 The key principles to be taken into account when designing management systems for power and vessel systems are:

1. Topology.
2. Autonomy.
3. Detection.
4. Simplification.

14.2 FAILURE EFFECTS OF POWER MANAGEMENT SYSTEMS

14.2.1 It is accepted that power management systems can fail and that single failures can lead to loss of functionality and remote control.

14.2.2 Design should ensure that the effects of failures are benign. Benign effects have been achieved by adopting a ‘fail safe’ philosophy. The ‘fail safe’ condition may be context sensitive but is typically ‘fail as set’ for PMS functions. Machinery should continue to operate without interruption.

14.2.3 Total failure of the power management system should not produce failure effects exceeding the worst-case failure design intent.

14.2.4 Failure of the PMS should not inhibit local manual control.

14.2.5 Protective functions provided by the PMS should be tested periodically to prevent those becoming hidden failures which could compound another failure.

14.2.6 Some class Societies require two independent power management systems in order to ensure that the remaining system can maintain sufficient power to hold position after failure of the other power management system.

14.3 TOPOLOGY

14.3.1 The choice of topology between distributed and centralized systems should take into consideration.

1. Industrial mission of the vessel.
2. Size of the vessel (Number of I/Os).
3. Separation of control, monitoring and protection functions.
4. Separation of redundant machinery groups.
5. Independence of main machinery.
6. Failure effects.
7. Class notation being sought.

14.3.2 Failure effects of distributed control systems tend to be less severe than centralized control systems.

14.3.3 Control systems can fail in either a benign way (absence of performance) or an active way (potential cascading effect). The assumption that control systems fail in a benign way can be misleading and should be avoided. The fail-safe condition for each application may be context sensitive (operation in progress) and should be clearly defined with the reasons thereof. Vulnerabilities in control systems can be minimized by addressing this in a design that facilitates simplification, detection and autonomy.

14.3.4 The temptation to use the vessel / power management system to solve unforeseen problems in the redundancy concept late in the commissioning phase should be avoided. If unavoidable, such resolutions should be treated with caution and accompanied with the appropriate MOC, and additional verification to ensure that further vulnerabilities are not added.

14.3.5 Field I/O should be assigned to field stations in line with the overall division of the DP system into redundant machinery groups. Field stations should be provided in such a way as to make main machinery such as generators and thrusters as independent as possible. Links between field station in different redundant groups should be kept to a minimum and any such links should have well defined error handling arrangements and fail to the safest state possible. The ‘safe state’ must be considered with respect to the industrial mission of the vessel.

14.3.6 In modern power management systems, there is a tendency to utilize the same hardware and software for control, monitoring and for protection functions for reasons of convenience. This is contrary to established engineering practice and should be avoided. When unavoidable, there should be separate power supplies, processors, software and I/O interfaces for protective functions.

14.3.7 The key factors that need to be considered in Power Management systems:

1. Redundancy.
2. Remote / local control.
3. Auto / manual.
4. Load sharing (if applicable).
5. Blackout prevention - heavy consumer control, load limitation and reduction.
6. Blackout recovery.
7. Industrial mission and industrial power consumers.
8. Power available calculation.
9. Power priority.
10. Starting standby gen sets - maintenance of spinning reserve, load dependent and alarm start functions.

14.3.8 While designing Power and Vessel Management Systems particular care is to be exercised in:

1. Automation.
2. Analysis Capability.
3. Data loggers.
4. Redundancy and criticality analysers.

14.3.9 The Owner should approve, and specify, that all control systems be supplied with Instrument Loop Diagrams as per Instrument Society of America Standard ISA-5.4-1991, or equivalent international standard (i.e. IEC, DIN, etc.)

14.4 AUTOMATION

14.4.1 Automation of key equipment systems can allow a predictable response to disturbances and provide rapid restoration of operation of those systems.

14.4.2 Automation associated with the power and vessel management systems must follow the redundancy concept and the WCFDI for the vessel. A distributed system minimizes the risk of failures exceeding the WCFDI.

14.4.3 Load Sharing: It should be recognized that any method of load sharing has the potential to cause power plant instability. Design should consider a method that minimizes risk of a blackout and ensure that independent protection is provided to address all possible failure modes of the load sharing system.

14.5 BLACKOUT PREVENTION

14.5.1 A distinction is to be made between a blackout and brownout and the consequences thereof.

14.5.2 An efficient design should result in minimizing the potential for a black out accepting that a brown out may be a consequence.

14.5.3 Brownouts have the potential to impact the industrial mission and may impact station keeping depending on the environment. A blackout not only compromises the industrial mission but also the station keeping ability.

14.5.4 Effective blackout prevention depends upon:

1. Recognition of immediate potential for a blackout.
2. Immediate Increase of online generating capacity.
3. Stabilize consumption while increasing capacity.
4. Security of blackout detection.
5. Temporarily transferring load to energy storage systems if fitted.

14.6 INDUSTRIAL MISSION

14.6.1 The Industrial mission may dictate assigning the same power priority to some industrial consumers as those required for station keeping. The identification of such industrial mission consumers should be analyzed, rationalized and appropriately addressed in the Power Management System.

14.7 BLACKOUT RECOVERY

14.7.1 Fully automatic blackout recovery of the power plant to pre blackout conditions is not a requirement for the traditional DP class notation but should be considered in the design as an essential risk reduction measure (it is a requirement of DYNPOS ER).

14.7.2 Key factors to be taken into consideration while designing blackout recovery systems are:

1. Speed of recovery.
2. Minimize potential for false initiation of blackout recovery.
3. Reduce risk of recurrence of blackout on or during recovery.
4. Automatic return (e.g. enabling) of thrusters to DP.
5. Independence from the Emergency Switchboard.
6. Role of stored energy system in hybrid power plant designs.

14.8 ANALYSIS

14.8.1 Power and Vessel Management systems should have capabilities to facilitate analysis. (predictive as well as post event). Post event analysis is typically facilitated by the use of data loggers. Predictive analysis may be accomplished by Redundancy Criticality Analysis (RCA). See also Cascade Waveform Testing.

14.8.2 Data loggers:

1. A data logger can be invaluable for post incident investigations, because of its ability to demonstrate the sequence of events, identify the initiating event and root cause. However, to be able to accomplish this, the data logger must have certain characteristics, relating to the number of data channels, selection of data that is to be recorded, time resolution and time stamping of data, and data resolution.
2. A data logger should facilitate trend monitoring.
3. Data logger files should be in a format that supports efficient plotting of data.
4. Guidance on desirable features for data loggers is given in Section 17.21.

14.8.3 Redundancy and Criticality Analysers (RCA):

1. A properly configured RCA can help with configuration of complex systems by drawing attention to non-redundant configurations where WCF can be exceeded.
2. RCA should align with the WCFDI, redundancy concept, and results of FMEA and proving trials.

14.9 TOPOLOGY OF VESSEL AND POWER MANAGEMENT SYSTEMS

14.9.1 Vessel and power management systems can be of the centralized type or distributed type. In centralized control all field sensors and actuators are connected to a centralized control unit which may have a redundant processor operating in a Master-Slave arrangement.

14.9.2 In distributed systems field sensor and actuators are brought to local field stations. Field stations should be provided in a manner that supports independence of main machinery and provides separation between systems intended to provide redundancy. Power supplies for field stations should be from UPS distributions which are arranged in a manner that supports independence and the redundancy concept.

14.9.3 The failure effects of distributed control systems are generally less severe than failure of centralized control.

14.9.4 Control systems should fail to the safest condition. For DP this is generally continued operation of the equipment in its last ordered state (fail as set). The failsafe condition for each application should be decided on a case by case basis and documented.

14.9.5 It is important to understand that control systems can fail in more than one way. A control input or output may fail in a benign way or it may fail in an active way. The failure effects of the two different modes may be very different. For example, if a generator speed control output fails to zero it will generally only affect the operation of that one generator and other generators will pick up the short fall associated with loss of the faulty set. If the speed control output fails to maximum the generators may force all generators operating in parallel to trip on over frequency or reverse power and blackout may occur.

14.10 REDUNDANCY REQUIREMENTS FOR POWER AND VESSEL MANAGEMENT SYSTEMS

14.10.1 Most power management systems provide protective functions. These should be tested periodically to have a high degree of confidence that they will operate on demand.

14.10.2 Design of power management systems should ensure that failure effects do not exceed the worst-case failure design intent. Furthermore, design should endeavour to minimize the number of failures which have effects equal to the worst-case failure effect.

14.10.3 Design should follow the principles of independence and redundancy to the extent feasible. For the purpose of this section, independence means that failure of a PMS function or hardware should not result in the loss of more than one generator or thruster.

14.10.4 Redundancy requirements for PMS systems:

1. At least two PMS operator's stations.
2. Field stations for generators, thrusters, safety systems and switchboards should have dual processors.
3. Field stations for generators, thrusters, safety systems and switchboards should have dual power supplies.
4. There should be one field station for each bus section in the main power generation. Failures should leave switchgear configured as set and not cause a change of state.
5. There should be one field station for each thruster and generator.
6. Failures of generator field stations should leave the generator running as set.
7. Field stations for auxiliary systems should be provided in line with the divisions in the redundancy concept. I/O from an auxiliary system's field station for control of DP related pumps and valves should not cross the divisions in the redundancy concept.
8. Field stations and I/O for vessel safety systems should be provided in line with the divisions in the redundancy concept.
9. In field stations for engine control and safety systems control, the safety functions should reside in different hardware (processors and I/O modules).

14.10.5 It is accepted that I/O interfaces to items of main machinery are not redundant.

14.10.6 Care should be taken when assigning I/O and fail-safe settings on data acquisition cards within field stations. There have been several cases where power management systems have used faulty generator circuit breaker status (frozen) to attempt load sharing on generator that was no longer connected. The result was a severe reduction in bus frequency followed by phase back of all thrusters and loss of position.

14.10.7 In order to enable transparency in PMS/VMS configurations, control systems should be supplied with Instrument Loop Diagrams as per Instrument Society of America Standard ISA-5.4-1991, or equivalent international standard (i.e. IEC, DIN, etc.)

In the absence of Loop diagrams, wiring diagrams offer limited value in operational phase of the vessel.

14.11 POWER AVAILABLE CALCULATION / MEASUREMENT

14.11.1 Power management systems must be designed to accurately control the power plant in any defined configuration.

Note: *Classification society rules may influence the way in which the capacity and power delivery of stored energy systems is integrated into power available calculations. A fuel gauge or 'time on batteries' at present thrust levels may be required for display to the DPO and for use by the consequence analyser. IMO MSC/Circ. 1580, section 3.2.7 states, "Alternative energy storage (e.g. batteries and fly-wheels) may be used as sources of power to thrusters as long as all relevant redundancy, independency and separation requirements for the relevant notation are complied with. For equipment classes 2 and 3, the available energy from such sources may be included in the consequence analysis function required in paragraph 3.4.2.4 when reliable energy measurements can be provided for the calculations."*

14.11.2 The power management system is one of the systems that create a common point between redundant power system even when the busties are open and the power plant is operating as two or more independent power systems. Hidden failures related to incorrect calculation of available power in one power system can defeat the redundancy concept by limiting the power available for station keeping in the event that one redundant power system fails.

14.11.3 Note that if the power management system is designed to intervene to prevent blackout by reducing thrust it is important that the PMS advises the DP control system that the reduction in thrust is due to its intervention. Thus, the DP control system does not associate any loss of position with external forces. This is equally true of other systems with such functionality. For example, phaseback functions in thruster drives which operate on detection of low power system frequency.

14.11.4 Note that loss of generating capacity due to tripping of generators will be apparent to the DP control system but loss of generating capacity for other reasons such as fuel starvation or contamination of combustion air will not be apparent because the DP control system assumes generators are capable of rated power.

14.11.5 The DP control system is continuously calculating the power available to the thrusters and should not order more thrust than there is generating capacity to support. It is the task of the DPOs / engineers backed up by the power management systems to ensure that sufficient generating capacity is made available to the DP control system for present and expected thrust demand. This is normally done by ensuring there is adequate spinning reserve and standby sets are ready for load dependent starting. This will replenish spinning reserve as it is used up by increasing environmental loading.

14.11.6 Consideration is being given to designs where the DP control system will be allowed to order as much thrust as it feels is necessary but autonomous functions in the power plant will limit what is actually produced by the thruster based on power plant loading. Means to advise the DP system that an external system is limiting thrust already exist in many DP control system designs. The DP system is advised of this thrust reduction by an external system so that it can apply the thruster allocation logic in the most efficient manner so as to prioritize heading control. The reason to remove the self-imposed limit in the DP control system is to remove a potential common mode failure associated with miscalculation of the available power. Such designs would eliminate many of the concerns discussed in the sections that follow.

14.11.7 Station keeping is vulnerable to errors in the 'power available' calculation. Software errors are less common but faults in power transducers and status contacts can have significant consequences. If the power available figure is too low then the DP system may not be able to order the thrust it requires to maintain position. If the power available figure is too high the DP system may order more thrust than the generators can provide leading to overloading.

14.11.8 Power available is calculated by subtracting the measured power being delivered by each generator from the assumed generating capacity calculated by adding the ratings of the online generators. The power available figure will be in error if the generators are not capable of delivering rated power on demand. Generator performance should be proven periodically.

14.11.9 Designs should provide means for recognition and alarming of erroneous values and inhibiting execution actions as a result of such values. For example, kW transducers may fail to some erroneous value which maybe higher or lower than the actual figure. They may also fail to an invalid state, an invalid state is easier for the power management to recognize and raise an alarm. A general principle that may be applied for execution functions in a PMS / VMS is that it is safer to take no action than take the wrong action.

14.11.10 Status contacts are used to indicate status of equipment to the power management system. These contacts are used in the PMS as follows:

1. Status contacts in generators indicate to the PMS that it should include the rating of that generator in the sum of the online generating capacity.
2. Bustie status contacts indicate that another switchboard is able to contribute power or take it from another.

14.11.11 Status contacts may fail such that they provide false indication of generator and busties status.

14.11.12 In the case of generator status, a fault may indicate that there is one generator more or less than is actually connected. The virtual loss of a generator should be no worse than losing a real generator and the error may provoke the PMS to connect an additional generator under the rules for load dependent starting.

14.11.13 Provided the spinning reserve is greater than the rating of the lost generator the PMS should not activate any load shedding functions. If the PMS indicates that there are more generators connected than is actually the case there is a risk that load dependent start and load shedding functions may not operate to maintain spinning reserve or prevent overloading.

14.11.14 This risk can be mitigated by connecting additional generators manually provided there are sufficient checks in the PMS to identify the issue and notify the DPO that there is an error.

14.11.15 It is important that the power management system software has appropriate bounds on measurements from generators to prevent a single hardware failure creating an error greater than the rating of one generator. For example, a kW transducer input should not be able to indicate that a generator is providing more power than a generator can physically deliver. Additional confidence in measurements can be gained by cross checking parameters from different transducers. For example:

1. It is possible to cross check active power (kW) using a signal from a reactive power transducer (kVAr) and the product of current and voltage transducer signals to provide a kVA value.
2. It is possible to cross check circuit breaker status by noting whether current is flowing through the circuit breaker.

14.11.16 In the case of circuit breaker status contacts, it is good practice to have one normally open contact and one normally closed contact that change state together. An indication of both contacts being in the same state should initiate an alarm. This alarm will be initiated when the circuit breaker changes state or when a line break is detected on closed contact. It is acknowledged that line break on an open contact will not be detected until there is a change of state. Design should provide line monitoring to facilitate immediate alarm initiation for line break.

14.11.17 All practical measures should be taken to ensure that errors in the power available calculation are detected. The following features may be used to increase confidence in the calculation.

1. Provide error checking of circuit breaker status contacts by duplication and line monitoring.
2. Cross check power measurements using information from other transducers.
3. Cross check status measurements against circuit breaker current.
4. Line monitor all transducers.
5. Confirm the accuracy of transducers periodically.
6. Ensure there are unambiguous alarms and indications to warn the DPO that the power available calculation may be in error.

Maintaining adequate spinning reserve provides a means to reduce the effects of erroneous calculations.

14.11.18 In the case of vessels that have the ability to operate with the power plant configured as two or more independent power systems, separate power management calculation should be performed for each power system. In the case of a distributed control system all the hardware and software should also be separate.

14.11.19 The design of centralized control systems should exercise additional care to ensure calculations for independent power systems are truly independent.

14.12 REMOTE CONTROL

14.12.1 Automatic and remote manual control are functions normally provided by automation systems like PMS and VMS. The degree of automation is a matter for owner preference, as is the degree of remote manual control. Power management systems normally control all generator circuit breakers. Failure of the power management system should not cause spurious opening of generator circuit breakers leading to cascade failure and blackout or loss of position if load shedding intervenes.

14.12.2 Similarly, remote control facilities for thruster and service transformer circuit breaker should not cause spurious tripping. Such failures could cause multiple thrusters and/or generators to be lost.

14.12.3 Decentralizing the control interface to the power plant in such a way that matches the split in the redundancy concept provides a high degree of protection against the effects of hardware failures exceeding the worst-case failure design intent. Consideration should be given to further distribution of the interface by providing one field station for each item of main machinery such as a generator or thrusters.

14.12.4 Failure of remote-control systems should not inhibit local / manual control.

14.13 LOAD SHARING

14.13.1 **General:** Generators operating in parallel in a common power system must share load in proportion to their rating so that the full capacity of the power plant can be reached without any one generator overloading first. Failure to ensure balanced load sharing can result in one generator becoming overloaded leading to cascade failure and blackout or limiting the amount of power to less than the capacity of the power system.

All methods of load sharing have the potential to cause power plant instability if they fail but some methods introduce greater commonality and therefore greater risk than others. Design should strive to reduce commonality.

There are various methods of load sharing and the main ones are discussed in the sections that follow.

14.13.2 **Load sharing by compensated droop:** Mechanical governors used in early marine diesel electric plant were operated in uncorrected speed droop mode. These mechanical governors were less accurate than their modern digital counterparts and relatively large differences in the load carried by each generator could develop due to wear and other factors. Power management systems were used to trim out the difference to restore load sharing and correct the frequency across the entire load range. PMS control of the governors is effected by way of 'raise' and 'lower' contacts which drive the governor speed set point up and down to balance the load and maintained frequency. These contacts are a relic from the days when mechanical governors were controlled by 'speeder motors' as the remote control interface and are susceptible to failure modes.

Most modern governors still provide this interface facility. These contacts have been known to stick in either the raise or lower position causing the generator to shed load or take more load with the potential to destabilize the entire power plant if operated as a common power system.

This type of load sharing system also takes no account of the fact that a generator may have a problem which is temporarily reducing its capacity to deliver power. The PMS may continue to increase the governor set point to force the generator to carry more load. A typical example is a stuck intake valve or a fuel system blockage. If these faults subsequently clear, the capacity of the generator is driven to the PMS set point, which may be at maximum, leading to severe load sharing imbalance, excessive bus frequency and possible blackout.

Power management systems that trim governors are susceptible to the above faults and should have means to mitigate the consequences.

14.13.3 **Load sharing by isochronous load sharing systems:** The advent of electronic governors driving electro mechanical actuators for fuel control allowed the development of isochronous load sharing using analogue or digital load sharing lines. In this method of load sharing the governors operate in constant speed mode rather than speed droop. In constant speed mode the generators do not naturally share load and slight differences in speed set-point caused by measurement and control errors leads to one generator taking the entire system load.

In constant speed mode, information on the load being carried by each generator is passed to all other generators to make them share load equally. If the load sharing lines fail, a severe load sharing imbalance will develop and blackout may follow. Most manufacturers of these types of system offer redundant load sharing lines or functions which transfer control to uncorrected drop mode on detection of load sharing line failures. Although these methods address many of the deficiencies, they are not sufficient in themselves to remove all failure modes that could result in blackout. Design should provide additional protective functions. Some vendors have developed protective functions that can be implemented on isochronous load sharing systems.

Note: A common error in the design of these systems is to omit contacts that follow the status of the main bus ties allowing each system to operate as an independent power system.

14.13.4 **Load sharing by fixed speed droop:** The advent of accurate digital governors has allowed a return to the use of uncorrected speed droop mode without the disadvantages inherent in the old mechanical and hydraulic governors. Accurate load sharing can now be obtained with minimal speed droop using these types of governor. This arrangement has the fewest number of failure modes and does not rely on the power management system for trimming nor does it depend on protective functions to transfer operating mode to speed droop. There are governor failure modes that can destabilize the power plant and protective functions are required to subdivide the common power systems or trip the faulty generators to prevent blackout. Vessels which are not at risk from this type of failure by virtue of operating their power plant as two or more independent power systems can still benefit from protective functions which reduce the risk of losing more than one generator on the same power system. Loss of multiple generators on one independent system is an undesirable failure effect even if the integrity of the other systems is maintained as it may impact the industrial mission. Some vendors have developed protective functions that can be implemented on power systems operating in uncorrected speed droop.

Note: Failure to full fuel is always an undesirable failure mode but it should only succeed in causing a blackout of a common power system if the system load is less than the rating of the faulty generator. The adoption of variable speed thruster drives makes this condition more likely and very large vessels can DP in benign conditions at very low load. Thruster bias can be used to increase the systems load as mitigation. It is difficult to reconcile burning large amounts of fuel as a protective function with an environmentally conscious policy.

Thruster bias, as a method of protection, may be defeated by load shedding systems that act on the overload of a single generator. It should be noted that the ratio of generator rating to system load increases with subdivision of the power system. The risk of partial blackout is increased by designs operating as multiple subdivided power systems. The risk of partial blackout may be acceptable in preference over the consequence of a full blackout. To mitigate against partial and full blackouts, protective functions associated with governors and AVRs are recommended for open and closed bus power system configurations.

It is reiterated that integrity and success of open bus power system operation is dependent upon the engines performing to their rated capacity. Maintenance objectives should be geared to achieving this.

14.14 BLACKOUT PREVENTION

14.14.1 **Power priority:** In diesel electric power plants there may be a need to prioritize power to the most important consumers. The thrusters and the auxiliary systems that service them are usually the most important consumers and if there is a need to shed load to prevent blackout these are the last to be affected.

Consumers associated with the industrial mission are normally the first to be shed unless integrity of power supply is to be maintained for safety reasons or to prevent potential escalation. Example power to drawworks designed for active heave compensation (additional information on active heave compensation is provided below). Designs should strive to ensure adequate power margins are available to supply station keeping and safety critical industrial consumers.

It may also be possible to identify a large amount of non-essential load associated with heating, HVAC and ventilation that could be shed first if problems occur.

Stored energy systems that can provide short term power from large battery banks are likely to play and increasingly important role in blackout prevention.

14.14.2 **Active heave compensation:** All systems and industrial processes should be designed to fail safe on loss of power as it must be accepted that supply breakers, transformers or generators can trip at any time. Design should explore opportunities to provide sufficient power to bring safety critical industrial consumers to a safe condition in the event of a shortage of power, by temporarily diverting power from the thrusters. This diversion should not result in a position excursion that exceeds defined limits. If the position excursion exceeds these limits, priority for power should be returned to the thrusters.

In very large DP vessels such as drillships it may be possible to make use of the large inertia of the vessel to buy time to bring industrial processes such as active heave compensation to a safe condition in a controlled manner.

The use of these power priority functions should be a last resort. Design should make every effort and provide protective functions to ensure the plant is unlikely to reach a condition where it becomes necessary to divert power from station keeping. Such functions should be designed to be fault tolerant, fault resistant and follow a systems engineering approach. There should be a high level of confidence that thruster power priority will not be permanently lost and power will revert to the thrusters on demand. Measures to establish this confidence should span all activities from the design phase through to testing.

14.14.3 **Blackout recovery:** Full automatic blackout recovery of the power plant to pre-blackout conditions (or better) is not a requirement of DP class notation. It should be considered as an essential risk reduction measure and fitted to DP vessels where warranted. The energy storage systems that form part of hybrid power systems can maintain prolusion during blackout if they are connected to the thrusters and not only to the main bus.

There are elements of SOLAS and main class rules that require a degree of automatic restart of electric power systems. It may be unwise rely solely on these requirements to ensure the vessel has a competent blackout recovery system. Design should provide for a blackout recovery system that is commensurate with its industrial mission.

14.14.4 **Blackout detection:** It is important that the methods used to detect blackout are reliable and that they do not operate spuriously particularly if the first action of the blackout recovery system is to open all the generator circuit breakers before proceeding to reconnect them.

Design should facilitate use of several methods to confirm there has been a blackout including blackout relays, voltage and frequency transducers. However, the diversity provided by this multiple detection scheme can be negated if all detection methods connect to one bus VT.

It is good practice to provide suitable delays to prevent a voltage dip initiating a blackout recovery sequence. Even in power systems with adequate voltage dip ride through it is acknowledged that voltage dips may result in the loss of some auxiliary systems. In such circumstances, it may be desirable for the power management system to restart them. This task should be assigned to a different function from the main blackout recovery function.

The preferred method to reduce the consequences of spurious blackout recovery is to limit the actions of the power management system to starting of consumers and rely on individual protection functions within generators and consumers to disconnect any transformers, faulty circuits and unwanted loads prior to restart.

There have been known and published vulnerabilities experienced in designs that ‘clear the board’ as a precursor to blackout recovery. Such designs need the highest level of blackout detection reliability.

14.14.5 **Automatic return of thrusters to DP:** Modern protective functions have advanced to the point where automatic restart and selection of thrusters into DP following a blackout is recommended. This aids in arresting vessel motion with minimum operator intervention. Some designs will halt automatic reselection of thrusters once vessel motion has been stopped.

14.14.6 **Independence from emergency switchboard:** Blackout recovery should not depend on the emergency switchboard or the emergency generator.

Blackout recovery should be possible with the emergency switchboard and emergency generator unavailable at least for a reasonable period of time. It is acknowledged that beyond a reasonable amount of time blackout recovery may need to depend on the emergency switchboard and generator to provide needed auxiliary systems.

14.14.7 **Testing blackout recovery:** When testing automatic blackout recovery systems, it is important to trip the last generator not just shut it down or E-Stop it. This is a more realistic test as most diesel electric vessels blackout with the generators still running but not connected. The test protocol should be appropriately defined taking into consideration the characteristics of the power system. For example, it may be necessary to prevent the tripped generator immediately reconnecting depending on what type of simulated fault was used to trip it. It may be possible to push the lock-out button or simply hold down the CB open button.

Some blackout recovery systems have failed to operate when tested in under realistic failure scenarios even though they have worked perfectly in scenarios where the last engine was emergency stopped or manually shut down. Ideally, blackout recovery should be tested in the following scenarios.

1. Recover from all engines stopped.
2. Recovery from engines running but generator circuit breakers tripped.

Independence of the blackout recovery system from the emergency generator or switchboard should be established by testing and documented to prove the design (Starting of the emergency generator to be inhibited).

Tests should be conducted to validate full and partial blackout recovery on power plants operating in open and closed bus configurations.

14.15 DATA LOGGERS

14.15.1 Data loggers are an extremely useful tool for fault finding and for understanding events leading to DP incidents. Data loggers for DP control and PMS/VMS should be provided. Data logging functions in modern protection relays are also useful.

14.15.2 Means to ensure the alignment of time and date stamps applied by all data loggers on the vessel should be provided. Using a time signal from a DGNSS is one way to achieve this.

14.15.3 Design should ensure that all data logging functions are powered from a UPS or other battery sources so that they will continue to operate during a blackout.

14.15.4 Data loggers for PMS and VMS should be configurable such that the tags to be recorded can be selected efficiently. Design should consider the most appropriate tags to be recorded.

14.15.5 Guidance on desirable features for data loggers is given in Section 17.21.

14.15.6 Data loggers play an important role in the ‘Build to test’, ‘Test on demand’ and ‘Health to Operate’ strategy which can be adopted into DP vessel design concepts. The “Stairway to DP Heaven” strategy is an integral part of the LIFE concept.

14.15.7 Care needs to be taken not create fault propagations paths when adding data acquisition and data logging facilities. These installations should be subject to the same design considerations as other parts of the DP system. Maintaining the split in the redundancy concept all the way back to the server / data logger may be an effective strategy. Even at this point, each redundant group should have a separate interface.

14.16 REDUNDANCY AND CRITICALITY ANALYZERS

14.16.1 RCA is a useful tool whose primary objective is to limit the potential for configuration errors and defeating the redundancy concept. It can be integrated into the vessel's automation systems. If properly implemented they can supplement bridge and engine room checklists. A well specified and performed DP system FMEA should contain all the information necessary to develop an effective RCA. RCA is particularly helpful on vessels with complex multi-way splits with many options for cross connection.

14.16.2 These tools are available from a limited number of suppliers.

15 NETWORKS AND SERIAL LINES

15.1 NETWORK DESIGN

15.1.1 Network design has evolved to Ethernet based solutions and use of communication switches rather than hubs. Configuration of network architecture and equipment is a key element of providing the necessary level of fault tolerance.

Note: *There are a few designs (older DP vessels still in service) which have used Factory Interface Protocol or similar field bus designs.*

15.1.2 Networks, may be comprised of:

1. Two independent full duplex data highways.
2. Remote Control Unit (RCU) / processor / Programmable Logic Controller (PLC).
3. Network switches.
4. Source of power.
5. Human machine Interface.

15.1.3 A network topology with a proven track record and demonstrable history of reliability is recommended. The physical star, logical bus network is one such example.

Note:

1. *In some cases, a ring network topology has been used. There have been instances of network related incidences where such a topology has been attributed as a vulnerability. In some instances, remedial measures have included a redundant ring topology network.*
2. *There have been instances where networks have been used to provide HMI or other interfaces. Some designs have introduced a common point in otherwise redundant systems. The vulnerability of introducing a common point has been justified on the basis that no control elements are prevalent in transmitted data. However, Incidents have occurred resulting in failure effects that have exceeded the worst-case failure design intent which belies such justifications. Architecture that results in common points should be avoided if possible or if unavoidable should be effectively mitigated by protective functions. Such protective functions should be verified and validated by testing.*

15.1.4 Network design has evolved to Ethernet based designs and use of switches and is typically within the scope of supply of the DP control system vendor. In some projects the VMS network may be provided by an automation system vendor who is not the DP control system provider.

15.1.5 Design should facilitate monitoring of the status of the network by the DPO. The alarm terminology used for network alarms should be designed to be readily interpreted and avoid misinterpretation.

15.1.6 The range of protective functions that are active with a network should be understood and proven periodically by testing.

15.1.7 Certain types of ring topology network use a dedicated switch to redirect the transmission path in the event that on part of the ring is broken. Periodic testing should help to increase confidence that protective functions operate correctly and alarms provide warnings of network degradation.

15.2 TESTING

15.2.1 **Ethernet:** Comprehensive tests of the network storm protection should be carried out during FAT, FMEA proving trials and periodically (Annual DP trials) to ensure that such an event cannot fail both networks or stop the IJS from working at the point where it connects to the thrusters. The requirements for such tests to be repeated periodically is to confirm the protection remains effective. Software updates or hardware changes would be reason to consider repeating the network storm and throughput tests.

Note: *There have been instances of incidents where the full effects of a network storm were not experienced until several minutes after the event was initiated. The effects exceeded the worst-case failure design intent. The duration of the test is important, and lessons learned from testing should be incorporated in test methodologies. Testing methods should consider the need to demonstrate that the outcome is immune to variability in the duration of the event being simulated (long enough to confirm that the steady state condition has been observed).*

15.2.2 **Serial Links:** Serial interfaces should be tested to show they do not cause a common mode failure. Typical tests should prove that faulty serial interface cannot slow down a controller to a point where more critical controller functions are affected. Wire break tests are not sufficient to prove this and tests to prove immunity to jabber type faults, truncation of a message, frozen message, etc. should be carried out. This will require specialized equipment.

15.3 MONITORING

15.3.1 Means of monitoring the performance and redundancy of the networks along with useful alarms should be available to the DP Operator. Monitoring of lost messages, collisions and loading should be available.

15.3.2 A mimic should be provided to show the health of network connections, power supplies and processors throughout the network. This should positively identify any faulty section or component.

15.4 DP ALERT SYSTEM

15.4.1 Networks should not be the sole source of communicating DP alerts.

15.5 TOPOGRAPHY

15.5.1 Generally, ‘dual star’ topology has given a long history of satisfactory performance on DP vessels. This is not to say there have been no incidents related to failures in this topology but measures to address them may be more mature. Network switches should be included (rather than hubs) so that any faulty network node cannot ‘hang up’ both networks. Note that managed switches learn the network topology on power up. Cycling the power to a switch may cause it to lose this knowledge and return to the status of a hub until such time as it relearns the connections.

15.6 INDEPENDENT JOYSTICK AND MANUAL CONTROLS

15.6.1 These should not use the same networks as used by the DP system to transmit its thruster command to the thrusters etc. However even if a separate transmission path is used there may still be shared components at the local thruster control systems. From this perspective it is very important that network storm protection is effective to prevent the thruster control systems being disabled by the storm thereby disabling the IJS.

15.7 CABLING

15.7.1 Networks should use fibre optics when they leave a compartment. This has advantages for DP Class 3 designs and reduces concerns associated with interference and lengthy cable runs. Consideration should be given to running spare fibres.

15.7.2 Cable runs for redundant networks should be installed in separated cable routes to provide protection from fire and mechanical damage to both networks.

15.8 COMPATIBILITY

15.8.1 There may be compatibility issues between data serial communication systems used by different equipment suppliers. For example, an engine supplier may use a different protocol or standard from the vessel automation system provider. Integration issues can be resolved if the engine manufacturer provides their communications interface for testing by the automation system provider. FAT may be a useful opportunity to do this but it needs to be specified in the contracts.

15.9 INDUSTRIAL NETWORKS

15.9.1 Offshore industrial network systems are subject to environmental factors and other design requirements not normally included in the design of an office network.

15.9.2 Design of networks for DP should provide:

1. Required speed and capacity and bandwidth.
2. Predictable response across the full range of traffic conditions.
3. Reliability in a harsh environment.
4. Minimum downtime.
5. Ease of maintenance and repair.

15.9.3 **Required speed and capacity:** The speed of the network and the number of field stations should be matched to the type and number of I/O channels used.

15.9.4 **Predictability:** The system must have some degree of determinism. As systems operate in a real time environment any failure or alarm must be reported and acted on quickly enough to prevent any knock-on effect further affecting the system. The network topology plays a part in this determinism. Token ring networks and star/bus networks operating in full duplex can be considered deterministic. Predictability also means that the performance of the network should be satisfactory across the full range of traffic conditions. Attempts to use data communications to implement protective functions requiring a rapid and predictable response may fail if high data rates delay the arrival of information on which the protective function must act.

15.9.5 **Reliability in a harsh environment:** Offshore environmental factors including, vibration, heat, salt-laden atmosphere, electrical noise, etc. must be taken into account when designing the network system.

15.9.6 **Minimum downtime:** If a network is unavailable, some systems or devices may stop communicating. At a minimum this will mean redundancy is compromised. The network system should have been in service long enough for any inherent design flaws to come to the fore or to have been stress tested to ensure mean time between failures is acceptable.

15.9.7 **Ease of maintenance/repair:** A well designed system should have built-in diagnostics that enable the electrical or instrument technicians to quickly pinpoint where system failures have occurred. Most vendors now provide some type of net status page or mimic on the HMI to assist fault finding. Where possible, modules should be designed to allow them to be swapped out either without switching off the rest of the network, or by isolating just the faulty section.

15.9.8 Other issues which may influence the choice of a particular network are compliance with relevant standards, scalability and ease of use.

16 UNINTERRUPTIBLE POWER SUPPLIES

16.1 PURPOSE

16.1.1 The purpose of a UPS in a DP system is to provide:-

1. Stable, clean power.
3. Continuity of power during main power system outage.
4. Power system transient ride through capabilities.

16.1.2 Design of UPS systems follow either a centralized topology or distributed topology. Centralized topology lends itself to a robust system but introduces commonality while a distributed system potentially could be less robust but minimizes commonality. Commonality potentially increases the amount of equipment lost as a consequence of failure.

16.1.3 The design of UPS systems, their power sources and distribution should:

1. Accomplish robustness.
2. Follow the Redundancy Concept.
3. Not introduce additional vulnerabilities.

16.2 TOPOLOGY

16.2.1 Design of UPS systems follow either a centralized topology or distributed topology. Centralized topology lends itself to a robust system but introduces commonality while a distributed system potentially could be less robust but minimizes commonality. Commonality potentially increases the amount of equipment lost as a consequence of failure. Distribution of UPS power from centralized sources may be particularly challenging in DP Class 3 designs but some compromise between a large number of small UPSs and fewer larger UPSs (supporting the overall split in the redundancy concept) should be achievable.

16.2.2 The redundancy concept should not be dependent on battery endurance. UPSs should be provided in a manner which supports the WCFDI and matches the divisions in the redundancy concept. (Minimum two UPSs for DP Class 2 two-way split and minimum three UPSs for DP Class 3 two-way split plus backup DP control system).

Note: *The temptation to solely comply with the minimum class requirements and not align the UPS installation and distribution with the divisions in the redundancy concept may result in undesired and unwarranted cross connections between redundancy groups which could negatively impact achievable post failure capability. This is specifically the case where the number of redundancy groups exceeds two.*

16.2.3 UPSs should have their normal power supply aligned to the same side of the redundancy concept as the equipment they supply.

16.2.4 The UPS battery endurance should only be considered as providing time to transfer control to other control equipment in an orderly manner. The DP system will typically not be fully fault tolerant once one of the UPSs has failed. It may be possible to recover operation by switching to the bypass depending on the nature of the UPS fault but fault tolerance may still be compromised.

16.2.5 Failure of a UPS output should not lead to failure effects exceeding the worst case failure design intent. Input power supplies for DP related UPS's should be split in line with the redundancy concept. Where a group of UPSs share a common input power supply, loss of that power supply (switchboard) should not lead to failure effects exceeding the worst case failure design intent when all UPS batteries in that group are exhausted. Classification society requirements for UPS battery endurance are typically 30 minutes. Consideration should be given to extending the endurance if required by the industrial mission. Where UPS's are provided with a normal and back up supply, the normal power supply should be from the appropriate part of the main power systems. The backup supply should be from the emergency switchboard when this does not compromise the redundancy concept.

16.2.6 Design should acknowledge the reluctance to test UPS systems and incorporate means to establish conditions of the batteries. Testing of UPS systems should include testing under load conditions.

16.3 RECOVERY FROM ESD

16.3.1 Designers should be aware that some UPSs will not start from battery supply alone. This type of UPSs is unsuitable for DP vessels especially, those vessels with Emergency Shut Down (ESD) systems which disconnect the battery on ESD 0 (total shutdown). The UPS will not restart when the battery is reconnected and therefore there will be no control power available to restart the power plant. It may be possible to overcome this by arranging for backup supplies from the emergency generator, but this approach makes recovery from ESD 0 dependent on the emergency generator starting. Dependence on the emergency generator for DP operations is to be avoided.

16.3.2 There is significant variation in the quality of batteries available for UPSs and the price difference is often related to the life expectancy of the batteries supplied with a unit. A cheaper UPS may appear attractive, but the cost of ownership may be greater if the batteries have to be changed more frequently. Careful consideration should be given to the choice of control system UPSs in the vessel's specification.

16.3.3 There are several types of UPS.

1. The 'online' type, also known as the 'double conversion' type is the recommended UPS type for control systems onboard vessels.
2. Line interactive types may exhibit a small output voltage glitch as they transfer from line power to battery power. This glitch is usually too brief to affect the operation of controls systems with DC power supplies but may be detected by protective functions on variable speed drives as an indication that the control supply is failing. The drive may shut down in response leading to loss of thrust.

16.3.4 UPS designs having a function called Phase Tracking are not suitable for vessel applications. These UPSs attempt to track the mains power frequency waveform for synchronization purposes and are used in land based applications.

16.3.5 Some types of UPS are unable to charge their batteries from the poor quality power supplies found on some DP vessels due to high levels of harmonic content and poor voltage and frequency stability. Thus, their batteries may be discharged when called upon to provide power in a blackout.

16.3.6 The practice of supplying all UPSs and DC battery systems only from the emergency switchboard should be avoided. Such functionality may be provided as an additional feature to facilitate black-start should the batteries be depleted. Failure of the emergency switchboard such as a faulty circuit breaker or service transformer fault can limit the vessel's time on DP to the battery endurance, after which the vessel may be completely without power.

Note: *There is a perception that a supply from the emergency switchboard is a SOLAS requirement. It should be recognized that while this functionality should be provided, there is nothing in the rules precluding the provision of supplies from the appropriate redundancy group.*

16.3.7 The emergency switchboard may be usefully employed as a backup supply to UPSs to allow batteries to be charged when the main power system is not available. There should be means to isolate potential fault propagation pathways if it compromised the redundancy concept. Automatic and manual transfer to the backup supply is possible.

Note: *Standing alarms generated by isolation to align with the redundancy concept (if any) should be designed out.*

16.3.8 There should be a remote indication that the UPS is connected to its normal supply. In the case of automatic transfer to the backup supply, the changeover should be carefully designed to prevent a faulty UPS transferring and affecting main and emergency supplies.

16.3.9 UPSs should be provided with comprehensive alarm and monitoring facilities. As a minimum there should be alarms to indicate.

1. UPS on batteries.
2. UPS in bypass.
3. Battery disconnected.
4. Mains power present.

16.3.10 UPS output should not cross the boundaries between redundant equipment groups. This is particularly important in DP Class 3 designs.

16.3.11 Discrimination is a property of electrical protection schemes. Full discrimination is achieved if a fault is isolated at source under defined power distribution system configurations. Discrimination may be achieved by varying the current and/or the time at which protection devices in the fault current path operate. Typically, the highest current or longest delay is applied to the protection devices nearest the power source To achieve full discrimination in over current protection the power source must be able to supply the required level of fault current for a time exceeding the longest delay. Some types of UPS may not be able to deliver sufficient fault current to clear faults selectively. Ideally UPS distribution should stay within the redundant machinery and control system group and not be used to power equipment in other redundant machinery groups. Adopting this design approach prevents voltage dips, over voltages and other faults transferring from one redundant system to the other. UPSs for DP controls systems should be able to clear faults selectively. Care should be taken to confirm a UPS has all the necessary attributes required by the redundancy concept.

16.3.12 Some classification societies require UPS battery charging to cease on loss of ventilation. Care should be taken not to create a common cause failure associated with ventilation design including its power supply. Suitable alarms should be provided to indicate that charging of the battery has been stopped. This common cause failure can be avoided by using sealed batteries not requiring ventilation.

16.3.13 The practice of switching UPS outputs to allow various loads to be supplied by any UPS may allow failure effects to exceed the worst case failure design intent.

16.3.14 DP system FMEAs should not consider a UPS to be an infallible supply. Analysis should consider UPSs to fail like any other power distribution system. UPSs can fail causing:

1. Over and under voltage.
2. Over and under frequency.
3. Short circuit.
4. Earth fault.
5. Open circuit.
6. Phase failure (on three phase UPSs).

17 DP CONTROL SYSTEMS

17.1 DESIGN FACTORS TO BE CONSIDERED

17.1.1 DP Control systems, due to their maturity, tend to receive less attention and scrutiny during the design phase. It should be recognized that lack of attention in the design phase can introduce vulnerabilities that can impact the Industrial mission of the vessel. Certification of DP Control Systems by Classification Society is a requirement of obtaining a Class Notation.

17.1.2 Enhanced redundancy over the minimum requirements for Class Notation in Control Systems may be desired to increase operational uptime while executing the vessel's industrial mission.

Note: *Example of the above is a triple redundant controller system being limited by the provision of two power supplies. However, if three power supplies are provided, the full benefit of the redundancy can be realised.*

17.1.3 Ergonomics in the DP control system and HMI play a key role and should be focused upon in the design phase.

17.1.4 Factors that need to be considered in selection of DP control systems are:

1. Reliability and potential service life of components, subsystems and systems.
2. Availability.
3. Stability.
4. Topology.
5. HMI.
6. Mathematical modelling (Optimal control theory).
7. Sensor handling.
8. Appropriate modes for its industrial mission.
9. Power limiting.
10. Independent simulation capability for use as a trainer.
11. Consequence analysis aligned with WCFDI.
12. Independent joystick system.
13. Alarms and alarm management.
14. Alarms and display printers.
15. Data logging.
16. Source of power.
17. Remote diagnostic capability.
18. Potential service life and obsolescence.

17.2 INDEPENDENCE OF 'INDEPENDENT' JOYSTICK AND MANUAL CONTROLS

17.2.1 The independent joystick and manual controls should be truly independent of the DPCS with direct connection to the thrusters control electronics or thruster outstation/process station. IJS and Manual Controls should not send thruster commands over the same networks as the DPCS.

17.3 SENSOR HANDLING

17.3.1 The design of the sensor processing should:

1. Be robust enough to reject rogue measurements.
2. Not follow jumps.
3. Reject seemingly perfect measurements.
4. Include a median check on each sensor set as long as there are three available.

Note: Design of the DPCS should permit monitoring of the sensor weighting to ensure that no one system or set of systems is 'skewing" the weighting.

17.4 NEW OR RETROFITTED SENSORS

17.4.1 New or retrofitted position references are sometimes interfaced into DP through inputs designed for other position references because the DP control system has not been designed to accept them. Examples of this are pseudo Artemis or pseudo acoustics. This practice is not recommended unless the design is subject to a fault tolerant, fault resistant systems engineering approach.

17.4.2 Consideration should be given to providing additional sensor inputs to prevent using inputs not intended for the application.

17.5 TRIPLE REDUNDANCY

17.5.1 Some vessel owners choose to specify triple redundant DP control systems even on vessels with a DP Class 2 notation. This is good practice and is encouraged. While this can often apply to the operator stations and control processors, such systems do not always have triple power supplies. The design of triple redundant DP control systems should provide three power supplies. This reduces commonality between the control systems by removing the need to provide each controller with multiple supplies.

17.6 DPCS INPUT/OUTPUT WORSE CASE FAILURE

17.6.1 DPCS interfaces to the thrusters and power generation should preferably be through a digital interface with suitably distributed outstations/process stations. There should be one process station for each thruster. Where the DPCS has an analogue interface to the thrusters, the input / output cards in the main DPCS should be provided in a manner that supports the divisions in the redundancy concepts and the worst case failure design intent.

17.7 SUITABLE MODES AND FEATURES

17.7.1 Suitable DP modes and features required for the vessel to undertake its current and possible future industrial missions should be included. Examples are heavy lift mode, target follow, external force compensation, fast current update, shuttle tanker modes, weather vane, bow only, firefighting, use of GPS only, etc. Suitable modes and features for various DP applications are given in the MTS DP operational guidelines. Additional notes on certain modes and features are given below.

17.7.2 **Heavy lift mode:** This is a feature that is used to address potential instability caused by the stiffness imparted to the DP control systems during set down of the load (tonnes per meter offset). Note that the stiffness is related to the weight of the lift and the geometry of the lift height etc. Instability is not only related to mass but also to the vertical height from the end of the upper end of the lifting device to the load touch down point. The smaller the distance the greater the stiffness. For example, a relatively small load on an A frame with a shorter vertical height could result in destabilizing stiffness. There are known instances of A frames being damaged due to side loads imparted by instability. Vessels whose industrial mission includes lifting should evaluate the need to have heavy lift mode.

17.7.3 **Shuttle tanker mode:** This is a feature provided on DP tankers designed to offload product from offshore floating installations, typically turret moored FPSOs. This mode is implemented to take advantage of weather-vaning capability of the FPSO and facilitate the industrial mission of the shuttle tanker without the need to provide it with a large transverse thrust capability. Shuttle tankers by design are provided with adequate thrust in the surge axis. Shuttle tanker mode optimizes thrust requirements on the shuttle tanker by allowing some freedom for misalignment with the FPSO.

17.7.4 **Fast current update:** This may be required for applications where the heading needs to be changed quickly e.g. mono hull MODUs or the direction of the current forces changes quickly. This needs to be used with caution as the natural time constant of the DP loop in systems with model control is about 15 to 20 minutes. This time lag has been acceptable in most situations as a vessel responds slowly and the sea current typically changes slowly (wind compensation is feed forward). Fast current update decreases the time taken to 'learn' about a new situation. It should be recognized that any improper use of fast current update can cause instability and other problems. This feature should not be used to compensate for lack of external force compensation mode.

17.7.5 **Fire-fighting:** DP vessels outfitted with fire-fighting capability as part of its industrial mission should address effects on DP control of forces related to azimuth, elevation and flow of fire nozzle water. If these are not compensated for directly the DP will consider them as an environmental force. Sudden loss of forces associated with water flow can cause a loss of position incident if inadequately compensated for by design.

17.7.6 **Target follow mode:** This is a feature that facilitates automatic change of position set-points to follow movements of another floating body. Examples of industrial mission which could benefit by this mode are:

1. ROV tracking inspection work to automatically follow the ROV.
2. Positioning alongside a floating object susceptible to movement such as a TLP, Spar, MODU etc.

   Note: *Trials should be carried out prior to using Follow Target mode for operations described in (2) above. This mode requires the use of both absolute and relative position references. But "out of sync" measurements may be experienced in this mode and prevent its use. In such circumstances, positioning can be accomplished by using only redundant relative position reference sensors and conventional set-point auto DP mode.*

3. Functionality of the conventional follow target mode may need to be enhanced for industrial missions where relative positioning is required off targets which exhibit dynamic movements such as free weather-vaning FPSOs. Such functionality may require the provision of additional sensors and sub-modes. The burden of the development of detailed procedures and additional training requirements should not be underestimated.

17.7.7 **External Force Compensation:** When pipelaying, pulling in SCRs, hook-up of mooring lines etc. horizontal forces are exerted on the vessel. Vessels undertaking industrial missions where such forces can be experienced should be equipped with means for external force compensation. Reliance on the DP control system treating such forces as 'learned' environment has and resulted in loss of position incidents with significant consequences.

17.7.8 The input of forces values for external force compensation can be manual or instrumented. Systems designed to provide and accept input from instruments should be subjected to a robust fault tolerant and fault resistant systems engineering approach. Sensible limits should be applied to these inputs to avoid the DP control system responding to erroneous values.

17.7.9 **Weather Vane** (**bow only):** Monohull vessels with a predominantly aft super structure will naturally head into the wind like a weather vane. Similarly, they will tend to head into the current especially where there are high currents. It may be useful to the DP vessel to take advantage of these two effects when permissible by the industrial mission. Vessels that naturally weather vane as described above can be held on position and heading with a single bow azimuth thruster over the set point. This can be a mitigating feature in designs where the number of thrusters is limited and permits the vessel to bring itself to a safe condition post failure.

This feature has been used on semi-submersible hull forms with a four thruster configuration. This mode allows the vessel to weather vane around one thruster.

17.7.10 **Track follow:** There are two types of track follow called Slow and Fast:

1. Slow Track Follow is used where fore/aft, port/stbd and heading are all controlled to keep the vessel on track or a fixed offset from it. This is typically used for pipe laying, SCR installation etc.
2. Fast Track Follow is used where the vessel heading is steered back towards the track. The heading change applied is broadly proportional to the port/stbd offset from the track. This is typically used for cable laying, seismic streamers, etc.

17.7.11 **Axis priority select:** DP control systems are designed by default to give priority to controlling heading when there is insufficient thrust. This is appropriate for monohulls. Such vessels have the potential to lose position more rapidly if thrust is not prioritized to control heading.

17.7.12 Some industrial missions may require priority in another axis. This should be specified during design, for example, vessels intending to operate beam on to a platform as a default.

17.7.13 **GPS only operation:** Nearly all DP vessels use GPS with some form of differential correction to enhance the accuracy of the raw GPS position calculation. However, raw GPS may be sufficient for use where the industrial mission does not require precision position accuracy.

17.8 EXTERNAL INTERFACES

17.8.1 Sometimes a vessel's industrial mission requires the DPCS to be interfaced to other equipment that can affect the positioning of the vessel such as pipe tensioners, hawser tension, draught sensors or fire monitors. If external interfaces of this nature are required then a careful system engineering approach should be implemented. This should consider redundancy and failure modes. In addition to error checking functions provided by redundancy, the acceptable signal ranges should be carefully bounded/limited to be within a realistic range.

17.9 POWER SYSTEM INTERFACE

17.9.1 Erroneous power limitation may occur if the DP control system is unable to calculate the available power correctly. Power calculation depends on the integrity of power transducer signals and circuit breaker position status indication. There is a history of DP incidents related to errors in signals used to determine available power.

17.9.2 DPCS may be designed to ensure that demand for thrust does not exceed the online capacity of the power plant. Information on available power should be accurate. Inaccurate information may cause the DPCS to limit thrust at too low or too high a power level with the potential for loss of position or blackout.

Note:

1. Caution should be exercised if there is the potential for the DPCS to reduce the demand for thrust solely based on sensor-based indications of online capacity of the power plant. (Vulnerability to erroneous sensor input).
2. The DPCS should be able to command the thrust necessary to maintain or achieve the desired position independent of its interpretation of the state of the power plant (including hybrid systems) provided overload conditions are handled by other means and this condition is made known to the DPCS.

17.9.3 The failure modes and effects of these power signals to the DPCS should be considered and design should facilitate monitoring and alarm of these signals and appropriate response. For example, rejection of erroneous circuit breaker status.

17.9.4 For analogue signals, the use of 4-20mA loop monitoring provides some protection against an incorrect signal. This can be supplemented by application of suitable out-of-range checks. Logical checks can be used to facilitate error handling. Examples of logical checks are:

1. Comparing power and circuit breaker status to increase confidence in the measurement. For example, the DP control system should indicate that it has low confidence in a power signal from a generator that indicates it is delivering power with its circuit breaker open.
2. Power flow through a tie line that indicates one bus tie closed and the other open is likely to be anomalous.
3. Confidence in critical breaker status can be improved by comparing signals from a normally open and a normally closed auxiliary contact. The DP control system should indicate low confidence in the power available calculation if signals from both auxiliary contacts are ever the same logic value.
4. Some DP control systems compare the power delivered by the generators with the power consumed by the loads. Low confidence should be alarmed if the two measurements differ by a defined amount. Thrust limiting functions which require an accurate power available value should be disabled by this alarm.
5. State of health, and state of charge information may be required for hybrid power systems using electrical energy storage systems.

17.10 INPUT PARAMETERS (OPERATOR INPUTS AND EXTERNAL INTERFACES) –

17.10.1 A sensible boundary check should be applied in software for every parameter that can be input to the DP by the operator or by external interfaces. The DP control system should reject any attempt to enter a value that is wildly incorrect and notify the operator that the entry is invalid. (e.g. Use of null fields for invalid position strings)

17.11 DP MANUAL CHANGE OVER SWITCH/CIRCUITS

17.11.1 The DP mode selection switch allows control of the thrusters to be changed from DP to manual or independent joystick. This is a critical item that requires a detailed systems engineering approach considering design and failure modes. Responsibility for this item should be placed with a supplier capable of applying the systems engineering approach and carrying out the integration. DPCS suppliers generally have this experience.

17.12 ON BOARD TRAINER/SIMULATOR

17.12.1 Most DPCS have limited features allowing DPCS functions to be simulated when it is not in control of the thrusters. If extensive simulation capability (range of features and time) is required for operator training, an independent on board operator training simulator should be considered. This can be useful when there is limited opportunity for actual hands on time for a new operator (e.g. DP MODU), or different scenarios are required to be checked off line – e.g. weather forecast, effect of equipment being off line, practice specific manoeuvres or track follow. An instructor station should be considered when the simulator is expected to be used to provide onboard training.

17.13 DP ARRANGEMENT

17.13.1 The DP control position should be designed to ensure:

1. View of work area.
2. Orientation of controls and displays are in line with the operator's orientation with respect to the vessel.
3. Night vision and minimum glare.
4. CCTV of important work areas.
5. Manual thruster control and independent joystick should be within reach of the operator. Thruster emergency stops should be within arm's reach.
6. Essential communication should be within arm's reach of the operator.
7. The information and controls on important displays should be readily visible without the need for the operator to move from his normal station. Examples include DGNSS, position reference sensors, radar etc.
8. DP control position design should facilitate distractions to be kept to a minimum.

17.14 DP ONLINE CAPABILITY ASSESSMENT AND DRIFT OFF CALCULATOR

17.14.1 DP online capability assessment is a useful feature and should be provided.

17.14.2 The models used in these for wind and current should be updated to be in line with the models as tuned and adjusted on sea trials.

17.14.3 The online capability plots should be validated even if only subjective validation is possible. An example of subjective validation is to compare the vessel's maximum transverse speed in very light wind conditions against capability plots generated for zero wind and an equivalent current equal to the maximum speed. The test should be carried out by moving the vessel transversely in port and starboard directions to minimize inaccuracies.

17.14.4 Generating capability plots for zero current allows the mathematical model to be subjectively validated by the following method. Orient the vessel beam on to any reasonable steady wind with no current and scale up the thruster demands to 100% by a square law. The resulting wind speed is then compared with the beam wind speed predicted for 100% thrust by the online capability plot. For example, a vessel that can hold 25 knots of wind at about 25% thrust should be able to hold 50 knots (2 times the wind) at 100% thrust (4 times the thrust). It is acknowledged that these tests are subjective but can reveal errors of an unacceptable order of magnitude.

17.14.5 Whenever possible, these tests should be repeated with the thrusters and power plant configured as they would be following the worst case failure design intent.

17.14.6 A drift off calculator can be provided as a sub set of online capability plots. Industrial mission that could benefit from this feature should specify it.

17.15 CONSEQUENCE ANALYSIS

17.15.1 This feature is required by class. It is intended to advise the DP operator that there will be insufficient thrust or power available should a single failure occur. Class does not specify what that single failure should be. The worst case failure should be used for this purpose. The consequence analysis should warn if there will be either insufficient thrust or power available to stay on station.

17.15.2 Desirable Features include:

1. Should consider worst case failure.
2. Should consider availability of standby generators.
3. Should consider the ability to shed load.
4. Should consider configuration errors in all parts of the power plant.
5. Should consider unavailability of equipment (for example thruster down maintenance).
6. Should consider time / thrust available from energy storage systems where such are considered to contribute to DP redundancy.

17.15.3 The sampling or filtering of the consequence analysis should be such that a useful warning can be given in sufficient time but without initiating numerous nuisance alarms which will bring the credibility of any warnings into doubt.

17.16 SINGLE STERN THRUSTER VESSELS

17.16.1 Capability and Consequence Analysis do not adequately address vessels that have a single stern thruster and use rudders to produce transverse thrust at the stern. The worst case failures of such systems typically leave a bow thruster, single prop and rudder in DP. For the rudder to produce transverse thrust at the stern a certain minimum ahead environment is required. The vessel's ability to have post failure capability is dependent on the vessel's orientation with respect to the environment and may impose limitations in ability to carry out its industrial mission.

17.16.2 Power distribution from shaft generators used to supply equipment supporting DP operations should follow the redundancy concept and failure should not exceed the worst case failure design intent. Reduction gears, if any, should be designed facilitate declutching of the main propeller without clutching out the shaft generator and vice versa. This facilitates emergency stopping of a failed main propeller without introducing the WCF.

17.16.3 Attempts to use assignable thrusters to address vulnerabilities in single stern thruster vessels have resulted in blackout in designs that have not considered the potential for transfer of fault. For example, by transferring the effects of a faulty stern thruster or by inadequate motor starting capacity in the surviving power system.

17.17 THRUSTER ALLOCATION – BARRED ZONES AND THRUSTER BIAS

17.17.1 Barred Zones are used to prevent thruster wash in certain directions. They are used to avoid thruster to thruster interaction, interference with hull mounted acoustic transducers, ROV launch area, etc. Care must be taken to test these thoroughly as incidents have occurred when a barred zone has been active even not required. For example, when barring is active for an adjacent thruster even when it is stopped and barring is no longer required. In such cases the barred thruster is unable to produce thrust in the direction of the stopped thruster and position is lost.

17.17.2 DP Control system thruster allocation logic on vessels with azimuthing thrusters often have a ‘thruster bias’ feature. This feature allows thrusters to be run against each other.

1. In light conditions, Thruster bias is used to prevent excessive azimuthing causing undue wear and tear.
2. Thruster bias is sometimes used to provide a base load intended to protect the power plant from blackout. The failure scenario involves a diesel generator governor taking the engine to full load and the remaining diesels tripping on reverse power.
3. This however is not without potential problems as in an incident where a governor failed and the base load of the bias was sufficient to avoid a black out. The operator however saw the faulty generator at full load and manually reduced the bias to try and lessen its load, this then tripped the healthy remaining generators on reverse power and the unhealthy one on overload which blacked the vessel out.
4. This method of protection also requires that the healthy generators are able to accept the step load which occurs when the faulty generator trips.
5. Thruster bias can be shed manually or automatically. Shedding bias automatically can cause a position excursion to the surprise of the operator. Position loss can also occur in the case of systems that only have manual selection / de-selection of bias. Forgetting to remove the bias as the weather increases has resulted in loss of position incidents.
6. Some DP control systems shed thruster bias automatically on:
    a. Thruster alarm conditions.
    b. Detection of insufficient thrust.
    c. Insufficient power or insufficient thrust.
7. Designs that shed bias on insufficient power should be considered for vessels with critical power consumers required by the industrial mission. For example, DP drilling vessels with active heave compensation.

17.18 CALCULATED CURRENT

17.18.1 Some DP control systems provide a figure for estimated sea current. The current is estimated by subtracting the overall force on the vessel (learnt) from forces derived from wind measurements applied to a wind force model of the vessel. The remaining force is assumed to be sea current and a speed and direction is estimated. This estimate is prone to inaccuracies as it also includes wave drift forces and thruster interactions to hull and other thrusters etc. It is also affected by thruster inaccuracies. Clear guidance should be provided highlighting that calculated current may not be representative of actual sea current. Operational decisions should not be based on calculated current.

17.19 AUTOMATIC DP ALERT / DISCONNECT

17.19.1 The DP Red Alert should not be the only initiator for an emergency disconnect. This is particularly important if the DP Red Alert is triggered by the watch circles set in the DP control system. Multiple means of communication between DPO and driller should be provided to enable confirmation.

17.19.2 Automatic disconnection is to be generally avoided. It has been used in shallow water riser based drilling as a means to address lack of effective operator intervention. Design of such systems, if considered, should be fault tolerant, fault resistant and subject to a robust systems engineering approach. Automatic disconnect must account for leaving the well safe regardless of the well construction operation in progress.

17.20 OTHER INPUTS

17.20.1 Other systems concerned with the vessel's industrial mission may be interfaced with the DP control system. Examples are:

1. Lower riser angles.
2. Upper riser angles.
3. Tensioners stroke.
4. Stack heading.
5. Pipelay tensioners.
6. Hawser tension.

17.20.2 Such interfaces could be used for information, monitoring and alarms. However, when used for control the design must be fault tolerant, fault resistance and subjected to a robust systems engineering approach.

17.21 DP DATA LOGGER

17.21.1 A data logger recording DP control system performance can be invaluable for incident investigation.

17.21.2 The purpose of the data logger is to capture information used by the control system in order to conduct analysis. As such it is required to capture:

1. Computed variables.
2. Parameters.
3. Operator key strokes.
4. Input / output tags.

17.21.3 The users must be able to query and display all alarm and event data on the data logger.

17.21.4 The data logger should be fully functional before commencing sea trials.

17.21.5 If there are limitations on the number of channels that can be logged then design should consider which channels will be most useful in analysing a DP incident.

17.21.6 The process of selecting channels to be logged should be efficient.

17.21.7 The following features should be considered:

1. Data retention requirements:
   a. Absolute capacity before transferring to long term storage media.
   b. Redundant data storage.
2. Time series graphs - live data (near real time) and historical data, multiple tags can be plotted.
3. Ability to export data to spreadsheets as comma separated values.
4. User friendly operation.
5. Ease with which the 'playback' period can be selected.
6. Conform to a recognized data logging standard.

17.21.8 The following should be considered in relation to the data logger hardware:

1. Data loggers should be supplied from a UPS.
2. Dual power supplies.
3. Manufacturer's support for at least 5 years.
4. Ability to accept time reference from GPS if tags are not already time-stamped.
5. Optical media read and write.
6. Packaging - rack mount or work station.
7. Remote access and security.

17.22 REMOTE ACCESS DIAGNOSTICS

17.22.1 Many system suppliers, for example DPCS and thrusters drives, offer a service that can allow remote diagnostics providing the vessel has sufficient communication infrastructure to support it. Generally, these are contracted with the supplier and require advance set up. They can be very valuable when operating in regions that are remote or that have immigration restrictions (such as time to obtain visas, etc.) because remote diagnostics can respond more quickly than a physical service engineer.

17.22.2 Firewall and security are an issue. Some systems can allow remote control as well as remote diagnostics so care needs to be exercised in granting and disabling access.

17.23 JOYSTICK SENSITIVITY

17.23.1 DP and IJS joysticks can command large amounts of thrust over a very small lever range. Joysticks are usually provided with two settings:

1. A 'fine control' setting is provided to improve the sensitivity of control when manoeuvring.
2. A 'full control' setting is used when high power is required.

17.23.2 Design should consider default selection to 'full control' setting when control is transferred from DP mode to joystick. There have been known incidents where the operator has transferred to joystick control to pull away from a platform as an emergency measure but failed to realize that the joystick was still in 'fine control' setting.

18 SENSORS

18.1 DESIGN PRINCIPLES

18.1.1 Sensors as referenced in this section include:

1. Position reference sensors.
2. Sensors used for environmental monitoring including weather radar and Doppler current profilers.
3. Vessel Motion Sensors.
4. Draught sensors.

18.1.2 During Design the following should be taken into account:

1. Suitability.
2. Differentiation.
3. Diversity.
4. Independence.
5. Location / installation.
6. Maintainability

18.1.3 The industrial mission of the vessel will dictate the setting of the objectives to be achieved and the degree of focus on each of the above elements as it pertains to position reference sensors.

18.2 SUITABLE POSITION REFERENCE SENSORS

18.2.1 The DP vessel should be equipped with suitable Position Reference Systems (PRS) to meet operational requirements and in accordance with the vessel's DP class notation. Choice of position reference systems should consider the manner of deployment and the expected performance in a range of operational conditions.

18.2.2 Design should consider exceeding the minimum sensor requirements stipulated by Class rules in order to maximize operational uptime and achieve industrial mission objectives.

18.2.3 Suitable PRS required for the vessel to complete its current and possible future missions should be considered and included in the specification. In some cases, it may be appropriate to provide an interface for future addition of a PRS.

18.2.4 Redundancy in relative position reference sensors should be considered when the DP vessel will be required to operate in close proximity to a floating facility and there is potential for shadowing of DGNSS.

18.2.5 Position reference systems are either absolute or relative systems. An absolute system gives vessel geographical position. A relative system gives vessel position in relation to a reference point (e.g. TLP or Spar). A relative system can be used as an absolute system if installed on a point that is a fixed geographical position (e.g. platform). An acoustic absolute system can be used as a relative system if suitably attached to a floating asset.

Table 18-1 Most Common Position Reference Systems In Use

Absolute	Relative
DGNSS (DGPS and GLONASS)	Artemis
Acoustic (USBL, LUSBL, LBL)	Laser / Imaging (Fanbeam, CyScan, SpotTrack)
Taut Wire See Note	Radar / Imaging (RADius, RadaScan, SceneScan)
Inertial (INS) in combination with DGNSS or acoustic	DARPS
	Gangway

18.2.6 **Caution:** Position reference systems should be based on different principles. Any number of DGNSS systems may be installed but it is not recommended to use more than two at any time in DPCS in conjunction with other position references. Using more than two may result in skewed weighting in favour of multiple satellite systems. This exposes the DP control system to common mode failures associated with DGNSS such as constellation jumps.

18.2.7 It can be argued that taut wire and acoustic position reference systems are relative position reference systems. For purposes of this document, absolute indicates that this position reference sensor is independent of another fixed or floating offshore structure.

18.2.8 It is recommended that, wherever possible, multiple acoustic systems are completely separated and independent in all respects. This may be multiple transponder arrays or a single array with sufficient redundancy to accommodate transponder failure. It is acknowledged that a degree of commonality is introduced by the water column and the local noise environment around the vessel.

18.2.9 Consideration should be given to having a diversity of suppliers for GNSS systems with differential correction systems that have diversity.

1. Having more than two DGNSS systems selected to DPCS should not be considered as adding to active redundancy.
2. The impact of high latitudes on DGNSS performance should be considered if relevant.
3. Careful consideration needs to be given to the sighing of GPS antennas with respect to obtaining a minimum 2m separation from other antennas and/or emitters. Location of antennas should achieve minimum blockage or shadowing and sited in a manner to achieve protection against loss due to lightning strikes.

18.2.10 Guidance on suitable PRSs for various DP applications is given in the MTS DP Operational Guidelines, DNV-RP-E307 DYNAMIC POSITIONING SYSTEMS OPERATIONS GUIDANCE and MTS TECHOP (D-09 - Rev1 - Jan21) PRS AND DPCS HANDLING OF PRS.

18.2.11 **Decision support sensors:** Doppler weather radar, Doppler current profilers, riser stroke position (DP MODUs), Acoustic Doppler Current Profilers (ADCP) are examples of sensors used for decision support to aid DP operations. They are not interfaced with the DPCS.

18.3 SENSOR LOCATION

18.3.1 Location is an important aspect of sensor design and the following should be considered:

1. Human Machine Interface (Relationship to DP operator station).
2. Cooling and access to electronics.
3. Antennas and transmitters etc.

18.3.2 Correct choice of GNSS antenna location is essential for reasons of satellite visibility and avoiding problems with interference. RFI is becoming one of the most common causes of degraded or lost GNSS signals.

18.3.3 Careful consideration needs to be given to the location of the wind sensors. Masking by structures and the effects of downdraft from helicopter operations can cause erroneous readings. Design should consider effects of masking by structures and mitigation provided by installation of additional wind sensors.

18.3.4 Hull mounted hydrophones, transducers used by acoustic position reference systems benefit from installations in locations that have a low noise environment and close to vessel centre. Access for maintenance and retracting and lowering the deployment stems is also a consideration. For ship shaped MODU, heavy weather will produce noise and aeration of water in the vicinity of the moonpool. Also, MODU may discharge mud and cuttings that can disturb the acoustic environment. Approaching and departing boats may add noise and their prop wash may disturb the acoustic environment.

18.4 SUITABLE MOTION, HEADING AND ENVIRONMENTAL SENSORS

18.4.1 Some PRS systems are dependent on correction of their measurements for roll and pitch noise. Sensors providing such measurements should not become a common point of failure. Examples of PRS systems that may share correction data are DGNSS, laser system, taut wire and acoustics. Three MRUs/VRUs with suitable error handing can aid in mitigating errors but PRS requiring correction should be able to use different MRUs in a manner that provides diversity of correction source and does not create a single point failure.

Attention is drawn to IMO MSC/Circ 645 & 1580 where three MRU/VRUs are stipulated when vessel positioning is fully dependent on correct MRU/VRU signals.

18.4.2 Design of position reference systems should consider the following attributes.

1. **Suitability:** This should be assessed on the basis of repeatability, accuracy, resolution, update rate, latency, geometry (e.g. range, HDOP, constellation) and availability.
2. **Differentiation:** The details of the design of the position reference systems are sufficiently different to change the performance characteristics and minimize common mode failures. Differentiation includes source of signals, signal path and receiver location, for example:
    a. DGNSS and inertial aided DGNSS.
    b. Acoustics and inertial aided acoustics.
3. **Diversity:** Diversity in measurement principles and manufacturer is recommended to the extent practical. The objective is to minimize common mode failures (both hardware and software) Note: Diversity in manufacturers of redundant acoustic systems offers limited benefits.

18.4.3 **Diversity:** Where systems using the same principle are involved, e.g. 3 wind sensors, consideration should be given to having a diversity of manufacturers to avoid potential common mode failures to all three. For example, ultrasonic wind sensors can all fail in heavy rain or lightning, it is therefore prudent to have one wind sensor from a different manufacturer and working on different principles.

18.4.4 Similarly, it is prudent to have one of the three gyro compasses from a different manufacturer to minimize potential for common mode failures.

18.4.5 This applies equally to sensors such as gyro compasses, VRUs and wind sensors.

18.4.6 **Differentiation:** Inertial aided position references can:

1. Overcome the update rate limitations of speed of sound in water.
2. Minimize the consequences of erroneous or missing measurements.
3. Enhance the rate of valid data provided to the DP control system.

18.4.7 Inertial Aided Navigation (IAN) can create differentiation and prevent the potential for vulnerabilities due to skewing.

18.5 ISSUES TO BE CONSIDERED IN DESIGN OF SENSOR SYSTEMS

18.5.1 **Gyros:** Given the impact on heading/ position keeping it is recommended that vessels with an equivalent DP Class 2 notation are provided with three gyro compasses, irrespective of the requirements of the applicable Classification Society DP rules. It should be noted that some classification societies, including ABS and DNV already require three gyro compasses for a DP class 2 notation.

Gyro compasses are normally fitted with a correction facility which inputs the vessel's latitude and speed. The effects of incorrect latitude or, more importantly, speed could result in a significant error in output heading. It is therefore important to ensure that latitude and speed corrections are applied. Some systems use automatic input from GPS for these corrections. This is not recommended since there are a number of system errors that can result in undesired heading changes. It is therefore recommended to use manual input of latitude and speed when in DP.

The impact of high latitudes on gyro performance should be considered if relevant.

18.5.2 **Wind sensors:** Wind sensors are known to suffer common mode failures, such as icing in higher latitudes, lightning, heavy rain and birds. All types of wind sensors are vulnerable, including ultrasonic types.

18.5.3 **Bounding of values:** DP vessels are frequently fitted with sensor systems other than heading, motion and wind, which have a potential to affect the DP system and station keeping should there be an erroneous or invalid input from them. These include draught sensors, pipe lay tension sensors and fire monitors, where an erroneous or invalid input could result in extreme values resulting in a large position excursion (drive off). There should be means to prevent erroneous values being accepted by the DPCS. If automatic inputs are used, the design of the interface should be fault tolerant, fault resistant and follow a systems engineering approach. There should be means to input values manually. Suitable configuration and commissioning should provide means of ensuring that erroneous values are prevented.

18.5.4 **Sharing of sensor data:** The practice of connecting survey suites to DP control systems is not recommended. Where it is unavoidable, effective isolation between the systems is to be provided. DPOs should have ultimate control over the input. All necessary precautions should be taken to ensure that the vessel's station keeping is not affected and should be addressed in the FMEA.

Guidance is provided on the proper use of shared sensors between DP and survey systems in IMCA S010, Rev 1, 'Guidelines for the shared use of sensors for DP and survey operations'.

18.5.5 **Taut wire:** Taut wire systems are known to suffer inaccuracies at water depths over 350m, especially in high current areas. Design should not consider Taut Wires as one of the three position references required by class if operations are contemplated in water depths over 350m.

18.5.6 **Software:** NMEA message formats should be used for sensor interface. A compatible data transmission rate (Baud rate) is required as the DPCS may only be able to accept one particular transmission rate. It is important that software, parameters and values used by position reference systems are compatible with the software and acceptance criteria used by the DP control system and that this is verified by analysis and testing.

18.5.7 **Isolation:** Consideration should be given to properly isolating DPCS sensors from external devices that share the data such as gyro switching units, gyro repeaters, satellite communications systems, radars, ECDIS etc.

18.5.8 **Logging:** Position references should have the means to log sensor data, internal variables and operator input.

18.6 REGIONAL REQUIREMENTS FOR DP DRILLING UNITS

18.6.1 Owners/ operators of DP drilling units should consider adopting the following standards for hydroacoustic and satellite systems for deepwater DP drilling operations. The adoption of these standards should enable the DP drilling unit to operate anywhere in the world.

18.6.2 Deepwater DP drilling hydro acoustic systems:

1. A minimum of two independent acoustic systems each one with internal redundancy as to transponders/ beacons and transducers/ hydrophones capable of operating in maximum specified water depths with such a configuration that allows a minimum accuracy of 0.5% of water depth in 95% of measurements. Each acoustic system should have redundancy in the input of sensors (gyros and VRUs) and each transducer/ hydrophone should have redundancy in electrical supply.
2. Acoustic systems operating in a master/ slave relationship or hot standby should be avoided. They should simultaneously supply the DP controllers as totally independent position reference systems. The allocation of weight or deselection of a faulty position reference system should be performed automatically by the DP controllers without DPO intervention.
3. The unit (i.e. DP drillship or DP semi) should have a number of transponders/ beacons sufficient to constitute submarine arrays capable of operating in the maximum water depth, including redundancy on the bottom for the configuration of each operational mode and the backups on the surface. Further, transponders should have an acoustic release function.

4. Where ABOP controls systems are used the acoustic position reference systems should have as an additional function the primary actuation of the ABOP through the acoustic system hull transducers. The BOP specific portable acoustic unit should be used only in certain circumstances, such as failure of the primary system or abandonment of the platform.

18.6.3 **Cautionary Note:** Where acoustic BOP systems are required, there is potential for interference by the use of equipment provided by multiple acoustic vendors.

18.6.4 Consideration should be given to using USBL as a top down means of calibrating LBL systems. This will often optimize calibration times as well as improve accuracy.

18.6.5 **Satellite Based Systems:**

1. Two independent satellite positioning systems should be in operation, each with minimum accuracy of three meters. The primary receivers should have GPS dual frequency (L1/L2) in addition to one GLONASS receiver. Each system should have double redundancy in the differential signal reception system as follows; two different satellite systems, for example, Inmarsat and Spot Beam and two different radio systems with distinct frequencies and redundant transmitter stations with range covering the whole operational scenario of the unit (i.e. DP drillship or DP semi), for example, IALA, MF and UHF.

2. Note:

   Spot beam and Inmarsat both may be transmitted via Inmarsat satellites. Designs should provide for two separate satellite correction data links. It is acceptable to receive both links via L-band omni directional antennas or combined GNSS-L- Band antennas. Reception of such correction data links via Inmarsat communications does not provide enhanced reliability or redundancy.

   Availability of the local radio system infrastructure varies by region.

   IALA station errors have been experienced due to poor geodetic coordination.

3. Each satellite positioning system should have redundancy in the input of sensors (gyros and VRUs), if used.

4. Antennae (both primary GPS and differential) should be situated in different places on the unit spaced apart in order to guarantee redundancy and minimize shadow sectors.

5. The satellite systems should provide the DP controllers with positioning reference information simultaneously and independently.

19 EXTERNAL INTERFACES

19.1 SYSTEMS ENGINEERING APPROACH

19.1.1 The vessels industrial mission may require the DPCS to be interfaced with non-station keeping related equipment (For example, pipe tensioners, riser tensioner stroke, draught sensors or fire monitors). Design of such interfaces should follow a system engineering approach and may result in a degree of complexity that was not initially envisaged. Examples of systems engineering approaches are FMEA and consequence analysis.

19.1.2 Interfaces into the DPCS providing input (automatic and manual) data should be 'bound' or 'limited' (e.g. range of permissible data) to minimize the consequences of erroneous data or input.

19.1.3 The vessels sensors may require to be interfaced with non-station keeping related equipment (For example, RADAR, GMDSS, Survey systems). Design of such interfaces should follow a system engineering approach and may result in a degree of complexity that was not initially envisaged.

19.2 TESTING

19.2.1 Where interfaces with the DPCS are provided, failure modes are to be tested to ensure no hidden failure modes and confirm that failure modes, if any, do not exceed the WCFDI. Interfaces should be designed to avoid data overload of the respective control system's communication processor.

20 SAFETY SYSTEMS

20.1 SAFETY SYSTEM DESIGN WHICH MAY AFFECT DP

20.1.1 Vessels safety systems as referenced in this document comprise of:

1. F & G systems.
2. Fixed firefighting systems.
3. ESD systems.
4. QCVs (Quick Closing Valves).

20.1.2 The redundancy concept for station keeping is to be followed through to these systems to ensure that actions or failures initiated by these systems do not cause consequences that exceed the WCFDI. The actions initiated by these systems should be scaled to the detected threat level.

20.2 ARRANGEMENT OF MACHINERY SPACES

20.2.1 DP equipment class 2 allows for redundant machinery to be located in a common space. This can make it difficult to fight fires or deal with other emergency situations without compromising station keeping. Whilst not a class requirement for DP class 2 notation, fire protection over and above that required by main class rules may be considered in high risk areas such as engine rooms when warranted by the industrial mission (e.g. engine rooms divided) Owners may, at their discretion, opt for a DP Class 3 redundancy concept with full separation and protection against the effects of fire and flooding. Any additional fire and flood protection applied to DP Class 2 designs should be along the lines of the overall split in the DP redundancy concept.

20.3 FIRE & GAS

20.3.1 Fire and gas systems may be passive or active. Active systems may initiate actions in direct response to a detected threat. Passive systems initiate an alarm to indicate the nature and location of the threat.

20.3.2 Fire & Gas and ESD systems typically make use of a Cause and Effects matrix. This matrix should support the DP redundancy concept in so far as the threat areas are divided up along the lines of the redundant machinery groups so that it is possible to control lower level threats and still maintain position and heading. System architecture at the physical and logical level should be aligned with the redundancy concept. Design should achieve immunity against common mode failures (including spurious activation) that could defeat the DP worst case failure design intent.

20.3.3 Modern systems may be distributed monitoring and control systems which are an extension of the overall vessel management system.

20.3.4 The integrity of these systems should be established by a system engineering approach (e.g. SIL, FMEA).

20.3.5 The effects of loss of engine room ventilation on station keeping is to be specifically addressed in the DP FMEA.

20.3.6 Consideration should be given to providing more than one means of closing engine room fire dampers. Dampers are usually closed by stored mechanical or pneumatic energy.

20.3.7 Fire dampers for engine rooms should fail as set or to the open position. Dampers for other spaces should fail to the safest condition or as prescribed by class rules.

20.3.8 The benefits of ducting combustion air from out with the engine room directly to the engines should be taken into consideration as this provides flexibility to address fire and gas threats. Physical separation of combustion air intakes to the extent feasible is recommended.

20.3.9 Where actions are automatically initiated on the detection of a threat condition great care must be exercised to ensure there are no other conditions that can inadvertently trigger that action. For example, some fire and gas systems will shut down an engine room and transfer load to a redundant engine room on detection of a confirmed fire. False indication of fire from smoke on deck or cement dust from tank cleaning etc. may trigger the 'confirmed fire' response. If the dust is drawing into both engine rooms, there is a risk that both may shut down leading to loss of position.

20.3.10 Where the F&G systems is able to take executive action that can affect station keeping choosing a systems architecture that follow the overall split in the DP redundancy concept may offer the most secure defense against spurious operation leading to a loss of position.

20.4 FIXED FIREFIGHTING SYSTEMS

20.4.1 Fixed firefighting systems may include CO_2 or other fire suppressant agents such as water mist. These systems should be arranged in a manner that supports the overall divisions in the DP redundancy concept. That is to say it should be possible to release the fire suppressant in a manner that only affects one redundant machinery group.

20.4.2 Fixed firefighting systems may incorporate engine stops and ventilation shutdown into their remote and local controls. These must be designed such that no single failure can exceed the WCFDI but still allow fires in spaces associated with one redundant machinery group to be tackled without affecting any other.

20.5 ESD

20.5.1 Drilling rigs and certain other DP vessels are required to have an Emergency Shutdown System commonly referred to as ESD. The IMO MODU code requires this function and the classification societies have various rules in relation to the design of ESD systems. The main ESD control station is usually on the bridge or some other important location.

20.5.2 The highest shutdown level usually called 'ESD Level 0' initiates a total shut down of the drilling rig including propulsion and support facilities. ESD 0 buttons are sometimes required at helideck, lifeboat stations and other locations but experience shows that these facilities only serve to reduce the reliability of the DP system and should be avoided . IMO MODU Code requires a total shutdown that is available somewhere. It is acceptable to have multiple levels or cascading levels that are activated prior to the ultimate total shutdown.

20.5.3 ABS MODU Rules 4-3-5/7.1 states, "ESD Stations that can enable a total unit shutdown should not be located in locations which are unmanned under normal operations except in the backup DP Control Station, if applicable and provided. Where ESD stations are provided at the lifeboat stations or other unmanned locations, the total unit ESD (complete shutdown) is to be protected from unauthorized personnel or not available at these unmanned locations."

20.5.4 Digital and analog I/O for the ESD push buttons and for shutdown functions should be divided up amongst I/O units in a manner that support the overall division of the redundancy concept into redundant machinery groups such that false activation of any button, control output of group of pushbuttons or outputs associated with one remote I/O unit or other control interface can cause loss of no more than one redundant machinery group.

20.5.5 An ESD system design with a multilevel approach is an alternative design where several buttons have to be pushed in sequence to achieve the total shutdown and such buttons are located in controlled areas such as the bridge or OIM's office. Some designs have a feature which arms the ESD 0 function from the control room so that remote ESD 0 buttons only become active in a genuine emergency.

20.5.6 No single technical failure of the ESD circuit should initiate an ESD 0. The DP system FMEA should carefully consider the provision of all ESD buttons and question the need for ESD 0 at remote locations in relation to the risk of loss of position. Risks associated with technical faults and inadvertent operation should be considered.

20.5.7 Direct acting ESD 0 buttons should be avoided. 'Direct acting' means active all the time with no provision for override from a controlled location.

20.5.8 Warning signs and local keys have not proved to be effective and adequate mitigation of the risk of inadvertent operations.

20.5.9 ESD disables Blackout recovery capability in the PMS. It is imperative that detailed and well-rehearsed vessel specific procedures are developed and implemented for post ESD recovery measures.

20.5.10 As an ESD system is able to take executive action that can affect station keeping, choosing a system architecture that follows the overall split in the DP redundancy concept may offer the most secure defense against spurious operation leading to a loss of position. Maintaining clear separation and independence between redundancy groups should be established and proven by testing which simulates all shutdown signals going active from the control systems for that entire redundancy group to confirm nothing has been inadvertently crossed over to another DP redundancy group.

20.6 FUEL QUICK CLOSING VALVES

20.6.1 These valves are provided to allow rapid isolation of fuel supplies in emergency situations. The valves should be provided in line with classification society requirements and in a manner that allows fuel to be isolated to only one redundant machinery group without affecting the operation of any others.

20.6.2 Valves should typically fail as set on loss of control signal and actuator power and be protected against inadvertent operation both locally and at the remote control position.

20.6.3 Great care must be taken not to introduce unacceptable failures by providing common control systems for valves in systems intended to provide redundancy. The effects of fire and flooding on the pneumatic, hydraulic and electrical control circuit should be considered, particularly in DP class 3 applications.

21 ERGONOMICS

21.1 OPERATOR INTERVENTION

21.1.1 It is acknowledged that technical faults are triggers that sometimes require operator intervention to prevent escalation. Addressing ergonomics and decision support in the design enables effective operator intervention.

21.2 HUMAN SYSTEMS INTEGRATION

21.2.1 Human Systems Integration (HSI)[1] is the application of knowledge of human behaviour and limitations to the design of systems. The objective in this application is to reduce the risk of DP incidents by developing the human machine interface to support and optimize human performance and response to developing conditions so as to limit escalation.

21.2.2 HSI is a vast subject and not all fields of HSI can be appropriately addressed in the design of a DP vessel as other design and regulatory requirements may influence development. HSI is not entirely under the control of the vessel owner but failing to consider all aspects of HSI to the extent possible precludes opportunities to decrease the likelihood of human error and DP incidents.

21.2.3 All the major classification societies have guidance on ergonomics and various notations which apply to the design of DP vessels. These can be implemented by applying for the appropriate notations.

21.2.4 In DP vessel projects there are opportunities to influence HSI issues particularly in the layout of DP control system consoles and the presentation of information on mimic screens.

21.2.5 Factory Acceptance Tests for the DP control system, power and vessel management systems provide useful opportunities to comment on HSI issues.

21.3 HSI DESIGN OBJECTIVES[2]

21.3.1 Key objectives for HSI in DP system design are a reduction in the frequency of DP incidents through:

1. Enhancement of human performance.
2. Manpower optimization.
3. Training requirement reduction.
4. Enhancement of safety and survivability.
5. Improvement in quality of life.

21.4 CLASS RULES AND GUIDELINES

21.4.1 There are two significant HSI issues related to the design of fault tolerant systems based on redundancy which appear in existing DP rules and guidelines:

1. Acts of maloperation.
2. Configuration errors.

21.4.2 Implementing HSI in the design phase provides opportunities to address the above issues.

21.4.3 IMO MSC 1580, IMO MSC 645 and some classification society's rules for DP notations have requirements that no inadvertent act should lead to a loss of position. IMO MSC 1580/645 states:

'For equipment classes 2 and 3, a single inadvertent act should be considered as a single fault if such an act is reasonably probable.'

21.4.4 **Maloperation:** An act of maloperation is any act which can immediately lead to a loss of position. The design of a DP system should already have addressed all the technical single point failures. For example:

1. There should be no single electrical supply that could be turned off that can lead to a loss of position.
2. The exemption of pipe work failure and manual valves from some aspects of DP Class 2 design means that there may be fuel and cooling water system valves that could be inadvertently closed which could lead to a critical situation.

Maloperation can be controlled by suitable interlocks, barriers and methods for controlling access to systems vulnerable to maloperation.

Software interfaces can be programmed with means to confirm intentions such as controlling critical operations using several key strokes. (A typical example is the double push - pushbuttons used to select and deselect thrusters. These offer some protection from dropped objects or carelessly placed materials.)

21.4.5 **Configuration errors:** A configuration error is an act which removes the DP system's fault tolerance. It may not lead immediately to a loss of position but can compound the effect of a single failure which occurs later on.

Configuration errors can be controlled by procedures and checklists. Configuration errors can be controlled by design using more sophisticated means such as redundancy and criticality analysers available in vessel management systems.

21.5 CULTURAL EXPECTATIONS[3]

21.5.1 Humans learn how to interact with their surroundings from their cultural experience. DP vessels by nature of their mission are required to be designed, built and operated for multi-national and multi-cultural stakeholders.

21.6 PRACTICAL IMPLEMENTATION

21.6.1 It is beneficial to assign specific responsibility for HSI in a vessel project team.

21.6.2 The colours used to indicate the operational status of machinery should be uniform across all control systems and equipment. For example, if the colour red is used to indicate machinery is stopped on the DP control system then it should also indicate 'stopped' on the power management system, the vessel management system and the illuminated indicators fitted to switchboards.

21.6.3 The conventions used for switch operation should be treated similarly. If operating a switch in the 'up' direction turns equipment on and 'down' turns the equipment off, then the same conventions should be used throughout the overall design.

21.6.4 Emergency stops for thrusters should be located within easy reach of the DPO at the main DP control station.

21.6.5 Emergency stops for thrusters should be laid out in a logical manner which reflects the position of the thruster in the vessel's hull.

21.6.6 The arrangement and layout of the main DP control station should follow the logic and orientation of the visual field if applicable. For example, directional controls such as levers, joysticks etc. should be aligned such that pushing the lever aft moves the vessel aft.

21.6.7 Communications should be located within easy reach of the DPO at the main DP control station.

21.6.8 Anti-glare screens for bridge windows allow DPOs to see operator station screens more easily.

Reference 1 and 2- "Adapted with permission, from F 1337 10 Standard Practice for Human System Integration Program Requirements for Ships and Marine Systems, Equipment and Facilities, copyright ASTM International, 100 Barr Harbor Drive, West Conshohocken, PA 19428."

Reference 3 "Adapted with permission, from F 1166 07 Standard Practice for Human Engineering Design for Marine Systems, Equipment and Facilities, copyright ASTM International, 100 Barr Harbor Drive, West Conshohocken, PA 19428."

22 ALARM MANAGEMENT

22.1 THE NEED FOR ALARM MANAGEMENT

22.1.1 The design of an effective alarm management system should achieve timely response without imposing unwarranted demands on cognitive ability. A well-designed alarm management system is one which provides clear indication of problems and identification of affected equipment without inundating the operator with extraneous information. Examples of extraneous information are:

1. Alarms from the failure of items of equipment within the main item that has failed if they are only a consequence of the initial failure.
2. Alarms associated with intentional configuration changes or intentional stopping of equipment.

22.1.2 An effective Alarm Management System should be incorporated into the design. Alarm management enables three fundamental functions:

1. Notification.
2. Intervention.
3. Post incident analysis.

22.1.3 Poorly designed alarm management systems do not facilitate effective operator intervention. An effective design should facilitate:

1. Instant awareness of criticality and consequence.
2. Interpretation leading to effective response.
3. Focus and avoidance of alarm ‘fatigue’.

22.2 ALARM MANAGEMENT

22.2.1 There is some evidence (ref IMCA 181) that the escalation of many DP incidents could have been arrested by operator intervention.

Note: *The above should not be construed as justifying poor designs with reliance on operator intervention to prevent failures equal to or exceeding the worst-case failure design intent. Vulnerabilities if any should be designed out to the maximum extent practical.*

22.2.2 Sometimes operator intervention is offered as an acceptable barrier to prevent single point failures exceeding the worst-case failure design intent. For this to be effective:

1. The operator must have readily interpretable and meaningful alarms.
2. Not be overwhelmed by a large number of alarms.
3. Relevant alarms enabling operator intervention should be easily distinguished.
4. Ample time to take action before the effect escalate to a critical condition.

22.2.3 The alarms provided, especially by the DPCS and VMS, often do not aid the operator in an emergency as they are presented with numerous alarms many of which are difficult to interpret. Furthermore, alarm logs are not generally as helpful as might be expected for the investigation of an incident. Design should consider an effective alarm management strategy.

22.2.4 Even though the DPCS is often seen as an ‘off the shelf‘ commodity, attention to alarms and signal limits is still required on an individual project basis to ensure they are appropriate and the alarm messages are readily interpretable.

22.2.5 The alarms should be clearly documented, explained and reviewed. Examples of illogical and inadequate alarms include:

1. Half a radian gyro check.
2. Negative draft reading accepted.
3. 200 T tension reading accepted.
4. Wind sensor failure to zero volts accepted as a valid wind direction.

22.3 STAGES IN THE DEVELOPMENT OF AN ALARM MANAGEMENT STRATEGY

22.3.1 The DPCS and VMS supplier(s) should validate effective alarm management principles as identified by reference to ISA 18.2. Examples as below:

1. **Alarm Philosophy:** Is this documented for the alarm system giving the objectives and work processes to meet them. Major contents should include alarm definition, roles and responsibilities, alarm prioritization basis, performance monitoring, management of change, and training.
2. **Identification:** Are work processes in place that determine which alarms are necessary. All modern control systems have comprehensive built-in alarm capability; often having more than a dozen types of alarms available for many measurements. Alarm choices should be made explicitly, not by general rules.
3. **Rationalization:** What process is there for ensuring an alarm meets the requirements set forth in the alarm philosophy. This should include activities such as alarm type and set point determination, prioritization, advanced method applicability, classification, and documentation.
4. **Detailed Design:** How are new alarms created that meet the requirements determined in the rationalization.
5. **Implementation:** How are the alarms brought into operational status, involving commissioning, testing, and training?
6. **Operation:** The alarm is functional.
7. **Maintenance:** The alarm is non-functional, due to either test or repair activities. (Do not equate this life-cycle stage with the maintenance department or function.)
8. **Monitoring and Assessment:** How is the alarm system's performance monitored and reported against the philosophy goals. Several analyses are recommended, including a non-mandatory table of metrics.
9. **Management of Change:** Do changes to the alarm system follow a defined process.
10. **Audit:** Are periodic reviews conducted to maintain and evaluate the alarm system and related work processes.

22.4 FACTORS TO SUPPORT DESIGN

22.4.1 The following is offered as guidance to support design and specification of alarm management systems.

22.4.2 **Alarm Priorities:** Alarms should be automatically organized and presented to the user in prioritized form. Prioritization should be accomplished using a maximum of three levels.

A message priority system should be established so that a more critical message should override the presentation of any message with a lower priority.

Priority can be conveyed with either visual or auditory coding methods. Prioritization should be based on a combination of:

1. Relative severity of the consequences of not responding to the condition or situation.
2. Time required for the operator/maintainer to act.
3. The tasks required of the operator to respond to the alarm.

22.4.3 **Alarm Integration:** In the event of a complete system failure, a single summary alarm (for example, “Diesel Generator Set B Failure”) should indicate the failure rather than requiring personnel to integrate the information presented by numerous component level alarms (for example, “Low Bus Voltage,” “Stator Trouble,” or “Lube Oil Pressure Low”).

22.4.4 **Master Silence Control:** If a master silence control is provided it should only silence active audible signals. It should not block audible signals at the onset of subsequent alarms. The master silence control should not affect the visual portion of the alarm.

22.4.5 **Subsequent Alarms:** Each subsequent alarm onset should activate visual and audible signals such as a flashing visual indicator and audible alerting signal. This should occur regardless of the condition of any other active alarms (for example, acknowledged, not acknowledged, cleared, active, or reset). If a single alarm has multiple inputs, any new alarm condition should reactivate that alarm.

22.4.6 **Repetitive Alarms/Controls:** Repetitively appearing groups of alarms should have the same arrangement and relative location on different panels and consoles. Placement of all alarm controls (for example, silence, acknowledge, reset, clear) that appear in more than one location should be consistent between panels and consoles.

22.4.7 **Alarm Test:** For control consoles or panels, a means should be provided to test the flashing and auditory signals associated with alarms without disrupting the normal operation of the alarm system.

22.4.8 **Temporary Disconnection of Alarms:** Alarm circuits may be temporarily disabled or left ON (for example, for maintenance) if such action is coordinated with appropriate personnel (for example, operations centres, the bridge engine control room) and is clearly indicated at all locations where such information may be required. These locations include the specific piece of equipment, the local control panel or console, the central control room, and work permits control centre. Permanent alarms (for example, fixed lights or tiles, as opposed to computer-driven displays) should be provided with a means to indicate their status (for example, by tag out or sticker indicating that the alarm is disabled).

22.5 NAVIGATION BRIDGE ALARMS

22.5.1 Alarms on the navigation bridge should be limited to those that are critical to the safety of the vessel or maritime structure. Visual alarms and indicators should not interfere with night vision.

22.5.2 Alarms on the bridge that are displayed in mimic arrangements on a panel (for example, fire doors, smoke alarm locations) should be designed so that the mimic lines are visible both in day and night lighting conditions.

22.5.3 Alarm panels located on the bridge should be arranged and located so the individual alarmed items are located.

22.6 TIME AND DATE STAMPS

22.6.1 Time and date stamping should be coordinated and uniform across all control systems. A GPS output may be interfaced for this purpose provided it introduces no common cause / mode failures.

23 COMMUNICATIONS

23.1 DESIGN CONSIDERATIONS

23.1.1 Communications as referenced in this document incorporates visual and audible means of communication.

23.1.2 Communication is a key management tool during execution. This should be incorporated in the design phase. The following should be taken into account:

1. Identification of locations where DP related communication is essential.
2. Means of communication (audible and visual).
3. Layered topology for audible and verbal communications.
4. Methods of transmission.
5. Independence of power supply.
6. Visual Communication to follow systematic processes that tie in with the DP Procedures and responses.

23.2 IDENTIFICATION OF LOCATIONS WHERE DP RELATED COMMUNICATION IS ESSENTIAL

23.2.1 A system of lights and audible alarms should be provided in key locations, manually activated from, and repeated in, the DP control room. The lights should be:

1. Steady green light to indicate vessel under automatic DP control, normal operational status and confirming the alert status system functional.
2. Flashing or steady yellow light to indicate degraded DP control.
3. Flashing or steady red light to indicate DP emergency.
4. Further guidance on suggested locations of the DP alert panels for various DP applications is given in IMCA M103.

23.2.2 An advisory status should also be included which indicates a discrepancy in the Critical Activity Mode set up. Advisory status typically initiates a risk assessment with appropriate mitigating measures in place prior to continuing operations. Advisory status may be verbally communicated if no visual means is available. Use of the colour blue for the advisory condition, if it has not been used for any other purpose, allows the DP alert status to align with established procedures for WSOG and ASOG.

23.2.3 Where an alert system is not easily included the means of clear communication of yellow or red status should be agreed before commencement of operations. For example, a DPO may inform the deck crew of an OSV of the DP alert status by a pre-agreed sequence of blasts on the fog horn.

23.3 MEANS OF COMMUNICATION (AUDIBLE AND VISUAL)

23.3.1 Means of communication can be audible and visual. Design should take into consideration established procedures and protocols and align with the operational parameters. Conflict should be avoided. For example, use of visual means of DP communication that duplicates or conflicts with the non DP related alarms.

23.3.2 Hands free means of communication should be used wherever the person using the comms is likely to need his hands free in the event of an emergency.

23.4 LAYERED TOPOLOGY FOR AUDIBLE AND VERBAL COMMUNICATIONS

23.4.1 Design should incorporate layered topology for audible and visual communications as a means to provide redundancy. For example, audible communication can be achieved by radios, telephone, talk-back systems.

23.5 REDUNDANCY

23.5.1 Redundant means of communication should be provided between the key work areas depending on the vessels industrial mission. Design should facilitate the integrity of power supply for at least one means of communication following the worst case failure.

23.5.2 If two means of communication are installed for the same purpose, they should be powered from two independent sources.

23.5.3 The DP network should not be the only means to communicate the DP Alert status.

23.5.4 The DP alert system should not be powered from a source associated with the DP system.

23.6 INDEPENDENCE OF POWER SUPPLY

23.6.1 It is recommended that the vessel's PA /GA and DP alert are powered by batteries or UPS independent of the DP control system if not otherwise mandated by Class Rules.

24 INSPECTION REPAIR AND MAINTAINABILITY

24.1 INFLUENCE OF MAINTENANCE ISSUES ON REDUNDANCY CONCEPTS

24.1.1 Design philosophy and redundancy concept should take into account Inspection Repair and Maintenance over the life cycle of the vessel. Equipment related to station keeping should be identified as Safety Critical Elements (SCE) and addressed in the Planned Maintenance System accordingly.

24.1.2 The following IRM factors need to be considered during the design phase:

1. Impact on post failure capability due to non-availability of equipment as a result of planned or unplanned maintenance.
2. Optimum sizing of equipment to enhance post failure capability.
3. Copackaging / colocation of redundant equipment limiting accessibility to IRM.
4. Non-intrusive means to facilitate testing.

24.2 IMPACT ON POST FAILURE CAPABILITY DUE PLANNED MAINTENANCE OR REPAIR

24.2.1 Design philosophy and redundancy concept should take into account Inspection Repair and Maintainability (IRM) over the life cycle of the vessel. Equipment related to station keeping should be identified as Safety Critical Equipment (SCE) and addressed in the Planned Maintenance System (PMS) accordingly.

24.2.2 When a specific task of the industrial mission dictates that the vessel is required to operate in the Critical Activity Mode of Operation (CAMO), equipment unavailability due to planned maintenance is to be avoided if the redundancy concept will be defeated.

24.2.3 Unplanned non availability of equipment should trigger a risk assessment of ongoing and upcoming operations. The consequences of further failures should be assessed and appropriate mitigating measures implemented. This activity should be part of the contingency planning prior to commencing execution.

24.2.4 Redundancy (fault tolerance) can be compromised if equipment is taken out of service for repair. Operational personnel may incorrectly consider redundant equipment to be ‘installed spares’ rather than required equipment.

24.3 OPTIMUM SIZING OF EQUIPMENT TO ENHANCE POST FAILURE CAPABILITY

24.3.1 During the design phase, the impact of non-availability of equipment due to planned or unplanned maintenance on redundancy is to be carefully considered in conjunction with the nature of the industrial mission being undertaken. This may influence optimum sizing (number and capacity) and additional redundancy with the objective of delivering greater post failure capability which provides higher availability to carry out the industrial mission.

24.3.2 Design should consider a redundancy concept which can remain fully fault tolerant after a single failure with reduced post failure capability. A typical example is a three way split providing two-out-of-three redundancy in the intact condition which reverts to a two-way split with reduced post failure capability if one of the redundant systems becomes unavailable.

24.3.3 Design should consider the impact of the worst-case failure. The impact on post failure DP capability can be reduced by subdivision of the power plant into several independent power systems. However, reliability reduces with complexity and the greater the number of independent systems, the more likely it is that one or more will be unavailable in a given time period. Therefore, there is a balance to be achieved between:

1. Limiting the impact of the worst-case failure to enhance post failure capability.

2. Optimizing equipment utilization.
3. Providing fault tolerance in the form of redundancy.
4. Creating a vessel that is adequately reliable in the intact condition.

24.4 CO-PACKAGING / CO-LOCATION OF REDUNDANT EQUIPMENT LIMITING ACCESSIBILITY TO IRM

24.4.1 The design should consider Mean Time to Repair (MTTR), by accounting for ability to remove large components from the hull, e.g. thruster motors or generators.

24.4.2 Design should avoid co-packaging of redundant equipment such that safe access for repair of a failed item in one system is limited by the presence of the other redundant system that must remain in service.

24.4.3 Design that facilitates ride through capability or “pause and restore” for transient faults to achieve a fault tolerant or fault resistant system for station keeping is encouraged. Adopting this philosophy for equipment related to the industrial mission without a clear and documented understanding of the consequences is to be avoided.

24.5 MEANS TO FACILITATE MAINTENANCE AND TESTING

24.5.1 **Maintenance of Redundancy:** This is the process of identifying functions and features on which redundancy depends and including them in planned maintenance. This process is described in IMCA M190, ‘Guidance for Developing and Conducting Annual DP Trials Programmes for DP Vessels’.

24.5.2 Annual trials and periodic FMEA proving trials as required by class are to be conducted. Appropriate pre-planning of these trials and guidance is to be provided as part of the vessel documentation. Issues identified in the FMEA as requiring periodic testing should be embedded in the PMS and highlighted as pertaining to safety critical elements.

24.5.3 Design should take into account the need for periodic testing and facilitate appropriate means to do so without creating vulnerability to damage due to frequent testing. (e.g. including knife contacts or switches to allow wire break testing to be carried out).

24.5.4 The following should be considered when assessing overall system availability during design phase and tested where feasible:

1. Provision of additional heat exchangers to allow cleaning.
2. The provision of additional pumps to allow maintenance.
3. The provision of bypass facilities.
4. Provision of dual filters with changeovers where feasible.
5. Asymmetric load sharing - potential means to enable maintenance without disabling redundancy concept.
6. Endurance testing (frequency as determined appropriate) under expected and realistic load conditions.
6. Doubling up on low reliability items such as control power supplies, without introducing unacceptable risk for failure propagation between redundant equipment violating the WCFDI.

24.5.5 Protective devices are to be identified as safety critical elements in the IRM. Protective device settings of all station keeping critical equipment should be confirmed periodically with the settings approved by Class. Changes to the settings are to be avoided without an MOC and engineering review by appropriate technical authorities.

24.5.6 Battery powered equipment such as UPS units should have the capability to monitor actual battery performance during endurance testing and to provide information on remaining operational time of the equipment. UPS units should be the double conversion type.

24.5.7 **Capacity testing:** Fault tolerance relies upon all redundant elements being capable of their rated capacity. Capacity testing should be carried out periodically to prove the required capacity is available. For example:

1. Thrusters.
2. Generators.
3. Cooling systems.

24.5.8 Endurance Testing:- It should be recognized that Class requires endurance testing. Such testing is carried out to validate stability of the system over a period of time.

21.5.9 Acoustic reference systems use a number of stem designs to deploy and retrieve the hull transducers. When deployed for extended periods, marine growth and corrosion can make it very difficult to raise the stems. Occasional exercising of equipment, by raising and lowering of stems, and closing and opening of the associated gate valve will improve service life.

25 COMMISSIONING AND TESTING

25.1 THE INFLUENCE OF COMMISSIONING AND TESTING

25.1.1 The design of the DP system has a significant impact on the commissioning and pre commissioning. A philosophy that incorporates facilities to carry out efficient testing by design is likely to deliver a vessel with fewer hidden failures (e.g. testing of protective functions). Addressing testing and commissioning at the preliminary stages of design, (i.e. development of the redundancy concept), enables optimization of the time required for commissioning and proving trials.

25.1.2 Equipment that is largely self-contained lends itself to fewer integration interfaces and is less likely to introduce issues at the pre commissioning and commissioning phases.

25.1.3 A uniform labelling/numbering system should be incorporated in the design phase and systematically followed through in all aspects of the project. This should be clearly communicated to all stakeholders (e.g. design house, yard, vendors, FMEA providers and operational manual generators).

25.1.4 There are five distinct phases in the project cycle as it pertains to this section:

1. Factory Acceptance Test (FAT).
2. Mechanical “completion” (when equipment is installed, cabled and cables rung out).
3. Pre commissioning (Pre-commissioning should be done with the equipment set up in the defined operational configurations and must include loop testing).
4. Commissioning (Commissioning of equipment should be validated following tuning and tested under load and stability established. It should be recognized that accurate tuning is a precursor to effective commissioning. Time required to accomplish tuning is not to be underestimated).
5. Testing (The activity encompassing testing of the fully integrated system with the objective of proving that the performance meets specifications and that tuning is consistently effective across a representative range of conditions). Testing also includes proving the FMEA to demonstrate the following:
    a. The redundancy concept.
    b. Effectiveness of protective functions
    c. Stability of the system under the full range of load/operational conditions
    d. Monitoring functions
    e. Degraded and failure conditions.

The above should be sequential activities.

25.1.5 FAT is an important phase of testing and should be carried out with the necessary diligence and participation of required stakeholders (i.e. FMEA providers, Project and Operational personnel deemed necessary) This is of particular significance for equipment that has the potential to be damaged if tested during proving trials and that would have schedule impact (e.g. internal control loops for thruster variable speed drives), and on equipment whose design does not lend itself to field testing. (e.g. MRUs - no means to check calibration). It is acknowledged that the quality of the FAT tests from an FMEA perspective will depend on the degree of progress and access to detailed information to perform an FMEA analysis of the equipment being Factory Acceptance tested.

25.1.6 When feasible the FAT should include all Inputs and Outputs, particularly interfaces with other systems, simulated and measured to meet the full range of expected operating criteria.

25.1.7 Vessels with complex designs requiring extensive integration should consider the need for a full scale integration test.

25.1.8 A robust pre commissioning and commissioning process is fundamental to the execution philosophy and should be integral to the project from concept. Three legs that contribute to a robust pre-commissioning and commissioning process are:

1. Documentation.
2. Verification.
3. Clearly defined Performance Acceptance Criteria.

25.1.9 The responsible party for designing the commissioning and testing process should be clearly identified and made visible to all stakeholders. The party responsible for integration should be specifically included in the list of stakeholders.

25.1.10 It is highlighted that Class participation in the testing and commissioning process may be limited to those elements required by Class rules. Testing geared towards the station keeping elements supporting the Industrial mission and not covered by Class rules needs to be addressed specifically in the shipyard contract and in the FMEA. Performance and acceptance criteria should be clearly established.

25.2 TESTING

25.2.1 Implementation and testing of the redundancy concept is a team effort. The team is comprised of:

1. Designers.
2. Builders.
3. Vendors (propulsion, prime mover, DP control system, control system).
4. Commissioning teams.
5. QA teams.
6. Classification society.
7. FMEA provider.

25.2.2 Each of these stakeholders has a significant role in ensuring that the vessel meets the redundancy concept and has the ability to perform its industrial mission. Issues are to be addressed as they are identified, and resolution communicated to all stakeholders. Deferring resolution until the FMEA proving trials precludes opportunities to mitigate issues earlier and more effectively.

25.2.3 Testing at individual systems level must be followed by testing as an integrated system:

1. Testing as an integrated system must be on a “no touch basis” (e.g. commissioning engineer laptop not connected unless specifically required for the test or changes being made during testing, tuning).
2. Tuning must be completed before formal acceptance testing is commenced.
3. Test plans should be communicated to all stakeholders with ample time for review and comments, such that they can be incorporated into the final testing plan.
4. All settings for protective functions should be confirmed against the class approved values.
5. Acceptance criteria should be clearly defined. Methods for determining scope of retesting following modifications during testing should be defined and agreed to by relevant stakeholders.

25.2.4 **Equipment systems:** Equipment that is largely self-contained and that had a Factory Acceptance Test or a Manufacturer's certificate of conformity may need less commissioning than other systems e.g. a motion reference unit or a UPS:

1. Verification of power source and label of such.
2. Verification of data connections and label of such.
3. Verification of label of the system itself, with respect to any vessel wide system of labelling, colour coding that is used in the vessel piping.
    a. Verify installed vessel specific configuration settings are correct, e.g. lever arm, configuration. Relevant sensors for positioning should be surveyed, example antenna locations, hydrophone locations (X, Y and Z axis).
    b. Verify physical installation meets the equipment manufacturers' specification, e.g. precision of alignment.
7. Equipment that requires extensive integration with other systems or significant amounts of configuration or application software that is written on site will need testing at commissioning and acceptance phases. The dependencies on other systems and the level of detailed testing is greater than that normally performed at FAT.

25.3 FAT TESTING

25.3.1 Factory Acceptance tests may be the first opportunity to check equipment and control system functionality against the functional design specifications and the vessel's specification. There can be considerable variation in the scope of testing and demonstration carried out at FATs. There may be an opportunity to carry out integration testing as part of the FAT if several systems can be connected for an integration test however it is acknowledged that this may be difficult to achieve unless specifically planned for in the contract for the vessel. Integration testing is effective when one main vendor has responsibility for integration. It may take considerable effort on the part of the equipment vendor to create realistic conditions at FAT but the use of advanced simulators to exercise control systems in the absence of the actual equipment to be controlled can provide advantages but must be planned for well in advance.

25.3.2 It is acknowledged that practical limitations may be experienced in executing testing in the suggested sequential manner. When as a matter of expedience, non-sequential testing has been accepted, the impacts on FMEA testing should be considered. Some level of retesting may be required to achieve the desired level of confidence in the test results.

25.4 HARDWARE IN THE LOOP TESTING

25.4.1 Hardware-in-the-loop testing addresses software issues not considered by traditional FMEAs and proving trials. An advanced simulator takes the place of the actual vessel and can be used to test the response of the DP control system to failures and other conditions. HIL testing can also be applied to a range of other control systems including power management systems. A HIL notation is available for DP and other control systems. HIL testing is a carried out at several stages including FAT, dockside and sea trials. The full cooperation of the equipment vendor is required.

25.5 FMEA TESTING

25.5.1 A vessel should operate in a configuration which has been analyzed and proven in its approved DP system FMEA. Compliance expectations from the regulators on this requirement are increasing.

For example, DP system FMEAs for diesel electric vessels should consider open bus and closed bus operation if these are intended to be fault tolerant design configurations.

25.5.2 A failure modes and effects analysis is a classification society requirement for DP class 2 and DP class 3 vessels. The quality of DP system FMEAs varies enormously. It is not unusual for shipyards to retain responsibility within their scope for providing a DP FMEA. A poor DP FMEA precludes opportunities to address vulnerabilities. Since much of the risk resulting from a poor DP FMEA resides with the vessel owner, and vulnerabilities continue into operations, it is strongly recommended that owners specify robust DP FMEA requirements and include them in the shipyard contract. Guidance on DP FMEAs is available from a number of sources including IMCA M247 (based on erstwhile M04/04), 'Guidance to Identify DP System Components and their Failure Modes', IMCA M166, 'Guidance on Failure Modes and Effects Analysis (FMEA)', and DNVGL 'Recommended Practice for FMEA of Redundant Systems', RP D102. An example specification is also provided in the Appendix of these MTS guidelines.

25.5.3 An FMEA is an excellent tool for raising awareness of concerns regarding the design of a DP system. Addressing these concerns to closure may require a significant contribution from designers. Supplemental studies may be required to address issues raised by the FMEA.

25.5.4 Where closed bus operation of the power plant is contemplated, the following studies should be performed:

1. The effects of crash synchronization of a generator.
2. Severe mechanical fault leading to loss of synchronism.
3. The effects of severe voltage transients on power system stability.
4. The effects of failures on levels of harmonic distortion - particularly in vessels employing various forms of filtering and harmonic cancellation.

25.5.5 The consequence of having a severe DP incident if the redundancy concept fails to deal adequately with what are relatively common faults carries a very significant risk. Vessel's intending to operate their diesel electric power plants as a common power system should consider carrying out live short circuit and earth fault testing at the main power distribution level and simulation of severe over/under voltage and over/under frequency faults to prove the robustness of the power plant and its protection scheme for this mode of operation.

25.5.6 Note: *This type of testing should not be undertaken lightly. Such tests should only be carried out if the vessel has been designed and built to be tested with dedicated protective functions to deal with each type of fault. Engineering studies including mathematical modelling has been carried out to demonstrate that the stresses experienced by the power plant are well within its capabilities to contain the energy levels involved. Suitable risk assessments, procedures and plans to carry out such testing should be developed by a competent body and put in place prior to commencing the tests.*

25.6 SCOPE OF FMEA PROVING TRIALS (E.G. BLACK OUT RECOVERY, AUTOMATION TESTING)

25.6.1 The purpose of a DP FMEA proving trials is to prove that the analysis is correct and that failure effects are as predicted by the FMEA. However, it also confirms that all the functions and features upon which the fault tolerance of the DP systems depends are functional in so far as it is practical to do so. It is a common misunderstanding that FMEA proving trials should consist only of failure tests. Some tests which appear to be function tests are there to prove the effectiveness of protective functions upon which the redundancy concept depends. This is particularly true of power management system functions such as thruster phase back which must be tested under realistic conditions with the vessel operating on full auto DP even though they may have been tested at commissioning with the vessel at anchor for example. Power management system tests carried out on load banks may not replicate the power system conditions created by the operation of large variable speed thruster drives and transducers may respond differently under such conditions. A limited retest of PMS functions on DP provides additional confidence.

25.6.2 For example - Modern medium speed diesels may have insufficient load acceptance to cope with the worst-case step loads that may be experienced following power plant failures when continuity of supply depends entirely on the correct operation of fast load shedding functions such as frequency-based thruster and/or drilling phase back. Thus, it is important that such systems be thoroughly tested under realistic conditions.

25.6.3 FMEA tests fall into four categories under the headings:

1. **Performance:** Performance tests are intended to prove that equipment and systems are capable of their rated capacity. These tests are carried out to prove that each redundant machinery group is capable of maintaining position and heading independently in the case of ‘full’ redundancy. In the case of partial redundancy, it is carried out to prove that it can maintain position and heading in combination with other independent systems.
2. **Protection:** Protection tests are designed to prove the effectiveness of the range of protective functions upon which the redundancy concept depends. In particular those functions which prevent failure in one redundant system affecting the operation of others.
3. **Detection:** Detection tests are designed to prove alarms and indications intended to prevent the redundancy concept being defeated by hidden failures.
4. **Information:** Information tests may be necessary to provide information on the operational and failure modes of equipment or systems required to complete the FMEA. In some cases, this may be the only practical way to obtain the required information.

25.6.4 Sea trials time is expensive and there can be significant pressure to optimize DP FMEA proving trials programs. Optimization based on commercial considerations should not result in inadequate testing. FMEA proving trials on large complex vessels may be carried out in several stages typically:

1. Alongside.
2. On DP - shallow water.
3. On DP - deep water.

Note: It is important to stress that systems should be fully commissioned prior to any testing. Some vessels may go on sea trials and require retests. This is often due to numerous commissioning changes made to equipment post testing on the sea trials.

25.6.5 In the 'alongside' phase of the program the vessel will not be on DP and the thrusters will not be operating. The range of testing that can be carried out is fairly limited but it may be possible to perform around 10% of the trials in this configuration without compromising the integrity of the test results. In this phase all vessel systems related to DP should have been commissioned and no significant changes should be made after the test has been carried out. In particular there should be no significant changes to the system under test. Tests carried out in this phase should be restricted to those tests where there is a high degree of confidence that the test result will not change if carried out on full auto DP. As examples, typical tests that can be carried out are:

1. Testing of non-critical redundancy such as standby pump changeovers.
2. Testing of UPS battery endurance provided the load is representative.
3. Testing of engine alarms and shutdowns provided the VMS is fully commissioned.

25.6.6 In the 'on DP - shallow water' phase all DP related systems should be fully commissioned, tested and tuned but some of the position reference systems may not be available (or available with reduced accuracy) due the depth of water. Hydro-acoustic systems are typical of the type of reference that may not be available. However, it is acceptable to carry out tests that do not require all the position references to be available.

25.6.7 In the 'On DP - deepwater' phase, tests requiring the full range of position reference systems to be available should be carried out including any power distribution failures intended to prove that sufficient position references remain available after failure.

25.6.8 It is useful to provide some justification for each test by stating its purpose and objective. This may help the shipyard and classification society surveyor understand the importance of each test to proving the redundancy concept.

25.6.9 The scope of the FMEA proving trials may be significantly influenced by the owner's specification for the FMEA. Testing of features such as automatic blackout recovery and the redundancy concept may be precluded if proof of compliance with classification society rules is the only stipulation.

25.7 OVERLAP WITH OTHER TESTING

25.7.1 The FMEA proving trial may contain several tests which are closely related to tests in the DP control system manufacturer's Customer Acceptance Test. To save time, the FMEA proving trials team should witness and record the results of the CAT in the FMEA proving trials as this provides a complete and integrated record of the tests carried out to prove the redundancy concept. The FMEA team will also view and judge the test results from the redundancy concept perspective. The CAT can be supplemented with any additional tests which may be required by the FMEA.

25.7.2 Other stakeholders may also have test programs and it is useful to integrate these as far as practical.

25.8 TESTING AND ANALYZING ALL CONFIGURATIONS

25.8.1 It is important that the FMEA proving trial verifies the redundancy concept in all operational configurations. It is expected that all possible operating configurations have been analyzed in the FMEA. It may be unreasonable to carry out every test in every configuration but there will be a number of tests which are influenced by the configuration. These tests should be identified and repeated in each defined configuration.

25.9 RETESTING FOLLOWING MODIFICATIONS DURING PROVING TRIALS

25.9.1 It is frequently the case that the FMEA proving trials reveals some fault or deficiency in the redundancy concept which requires rectification and retesting. It may be unreasonable to require a complete retest in such cases but methods should be established for determining the extent of any retesting.

25.10 DEVIATIONS FROM TRIALS PROCEDURES OR FAILURE TO MEET PRE-REQUISITES FOR TESTING

25.10.1 During the conduct of the FMEA proving trial it may become apparent that the original prerequisites cannot be met because some piece of equipment such as a generator or thruster is unavailable due to a fault. In such circumstances all stakeholders should agree the extent to which the FMEA proving trials may continue with the vessel in the degraded condition and which tests may need to be repeated or carried out when the faulty equipment becomes available.

25.11 CATEGORIZATION OF FMEA & FMEA PROVING TRIALS FINDINGS

25.11.1 It is important to have a transparent and well understood scheme for the categorization of FMEA proving trials findings as the responsibility for rectification of faults or non-compliances may carry a significant time and cost penalty.

25.11.2 In general terms it is only necessary to have one category of finding that is a 'Non-compliance' with the acceptance criteria defined in the FMEA'. However, it may also be useful to define two other categories of finding which identify cost effective opportunities for improvement of the design which the vessel owner may consider. In the case of new buildings, the builder will usually be responsible for the rectification of issues assigned Category A. The vessel owner may then choose to address findings of category B or C.

25.11.3 It may be useful to relate the findings category to the severity of the failure effects as follows:

Category A The failure effects exceed the worst case failure design intent or some aspect of the design is non-compliant with the *….Insert Classification Society…* rules for notation *…Insert DP Notation…* Improvement is recommended.

Category B The failure effects equal the worst case failure design intent. The design complies with the *….Insert Classification Society…* rules for notation *Insert DP notation…* but should be reviewed to determine whether a cost effective improvement can be made.

Category C Observations, comments and suggestions associated with DP safety and reliability, which *…Insert Owner…* may consider.

25.11.4 Findings arising from trials results may include references to other issues such as non-compliance with DP rules and faulty equipment and not just unacceptable trials results. Detailed guidance on how to assign a category to FMEA proving trials findings is given in Table 25-1.

Table 25-1 Guidance on Assigning FMEA Desktop and Proving Trials Findings

Category A	Category B	Category C
Test result > WCFDI.	Test results = WCFDI but there is a clear opportunity for improvement.	Test result is < WCFDI but there is an issue related to DP industry good practice.
Any test resulting in loss of position or heading excursion as defined in the specification.		
Any non-compliance with class DP rules.		
Any non-compliance with guidelines referenced in the specification for the FMEA.		
Any non-compliance with main class rules that impact the redundancy concept.		
Any non-compliance with owner's specification in relation to the redundancy concept.		
Pre-existing fault - Any fault found during trials that disables the redundancy concept such that WCFDI would be exceeded should another fault occur. e.g. faulty protection or auto changeover	Test results reveal that equipment providing non critical redundancy is faulty for example a third 24Vdc supply is faulty but only two are required to satisfy the redundancy concept.	
Any test result which reveals that that the vessel may not be capable of its defined post failure DP capability e.g. generator or thruster not capable of rated power or thrust. Protection system that causes thrust reduction at too low a level. Faulty cooling system not able to provide full cooling such that temperatures do not stabilize.	Any test result that indicates that process load such as drilling, pipe lay, crane etc. may be phased back too early.	
Any faulty alarm required to initiate operator intervention on which the redundancy concept depends, e.g. SW low pressure alarm.		
Any missing or faulty alarm required to reveal a hidden failure where periodic testing is not a credible alternative.	Any missing or faulty alarm required to reveal a hidden failure where periodic testing is a credible alternative – recommendation can be made to install or repair the alarm or add a test procedure to routine maintenance or DP checklists.	
Testing reveals that some aspect of the 'as built' status of the vessel deviates so significantly from the design on which the FMEA and trials were based that there can be no confidence that the tests are applicable. Further analysis and testing are necessary.	If modification or repairs are required as a result of the trials findings which do not significantly affect the redundancy concept, a recommendation should be made to revise the FMEA and retest the affected area.	
Any incomplete tests considered to be essential to proving the redundancy concept and therefore allowing the compliance statement to be made.	Any incomplete tests considered to provide useful information.	

25.12 ACCEPTANCE OF OTHER TESTS RESULTS IN LIEU OF FMEA TESTING

25.12.1 It may be possible to accept test results for other testing such as that carried out during the commissioning phase in lieu of some FMEA testing. The range of tests that can be accepted is usually fairly limited because the vessel and the DP system are in a fairly incomplete state. For example, endurance load testing of generators is acceptable.

25.13 RESPONSIBLE PERSON IN OWNER'S PROJECT TEAM FOR THE FMEA

25.13.1 It can be of great benefit to have a person responsible for dealing with FMEA issues on the owner's project team and/or shipyard site team. This individual will be able to better understand FMEA issues as they arise and represent the vessel owner's interests at review meetings etc.

25.14 DYNAMIC AND STATIC FULL LOAD AND LOAD ACCEPTANCE

25.14.1 Testing, implementing and proving the redundancy concept is a team effort and FMEA testing is only a small part of what is required to ensure the DP system is reliable and fully fault tolerant. Performance testing is an important part of proving the integrity of the DP redundancy concept. The following performance tests should be carried out:

1. Generator full load test.
2. Thruster full load test.
3. Thruster load up ramp test speed / pitch.
4. Thruster rotation test direction at full load / pitch reversal.
5. Generator load rejection and acceptance testing - with the assistance of phase back functions if required.
6. Dynamic load sharing stability in droop and other applicable load sharing modes.

These tests should be carried out as part of the FMEA proving trials.

25.14.2 **Cooling systems:** An endurance test should be conducted to prove that common cooling systems are capable of supporting the operation of redundant machinery groups (associated with the WCFDI) at full load. Unlike the individual thruster or generator full load tests these may require groups of generators and thruster to be operated at full load. This requirement may apply to freshwater cooling, seawater cooling and HVAC depending on the design.

25.15 EQUIPMENT SUBSYSTEM FMEA AND TESTING

25.15.1 It is not uncommon for equipment vendors to supply FMEAs for their scope of supply. These can vary significantly in quality but the best examples do provide very useful information for inclusion in the overall vessel FMEA. Some classification societies require the DP control system manufactures and PMS manufacturers to supply an FMEA. If FMEAs for other system are required they should be included in the vessel's specification and contract with the shipyard. Such FMEAs should be accompanied by a test program.

Note: *The scope and content of the equipment vendor FMEAs should enable the comprehensive analysis required of the vessel's DP FMEA by providing the substantiating information required to support verification and validation of the redundancy concept including clear and unambiguous identification of the fail-safe condition.*

25.16 CLOSING OUT FMEA FINDINGS

25.16.1 A permanent record of all FMEA findings should be retained throughout the life of the vessel along with details of how the issues were addressed. All changes to a DP system other than like-for-like replacement of equipment should be notified to the appropriate classification society and included in a revision of the DP system FMEA. Guidance on FMEAs can be found in IMCA M166.

25.16.2 Vessel owners should understand the procedures for raising and closing FMEA findings. Various procedures are used but it is generally considered poor practice to remove entries from the FMEA findings register after closure. The vessel owner should review all close-outs to confirm they are satisfactory. The classification society may be used as the arbiter in cases of disagreement between the shipyard and FMEA provider in such cases the finding may be closed with the entry 'Finding not accepted by client' therefore it is important to review all findings not just the open issues. Where the FMEA provider is in agreement with the close out the entry should state 'closed by FMEA provider', In cases where the FMEA scope exceeds classification society requirements any difference of opinion regarding compliance with the owner's specification may have to be settled by contractual negotiations between the shipyard and the ship owner.

25.16.3 The vessel owner should also understand the level of proof provided to indicate that findings have been closed out. All Category 'A' findings should be closed out by a comprehensive documentation package including suitable test results confirming correct operation and compliance with the requirements of the redundancy concept. This package should be supplied to the FMEA provider. The FMEA provider should close out the relevant entry in the concerns register and update the FMEA narrative to reflect the close-out, providing review of the documentation package indicates the solution to be acceptable. Documentation and test packages may also be appropriate in the case of Category B and C findings however a written statement detailing the extent of the changes and the outcome of any testing may be accepted as sufficient. Classification society representation may be required at testing to prove the modification or remedial work. It may also be beneficial to invite a representative from the FMEA provider.

APPENDICES

APPENDIX A EXAMPLE FMEA SPECIFICATION

1 SPECIFICATION

1.1 GENERAL

1.1.1 *A Failure Modes and Effects Analysis (FMEA) and supporting proving trials program will be prepared for the Dynamic Positioning system.*

1.1.2 *The FMEA shall be performed by an independent third party to the following specification.*

1.1.3 *The FMEA practitioner should produce a narrative FMEA covering all systems related to the DP redundancy concept. The purpose of the FMEA is to indicate whether or not the DP system meets the requirements of the relevant DP class notation (as interpreted by the FMEA practitioner) and compliances with the vessel's Worst Case Failure Design Intent.*

1.1.4 *The FMEA practitioner should explain the design philosophy of DP essential systems in considerable detail before explaining their failure modes and effects. This provides the necessary transparency in the analysis, which proves that the analyst has understood the operation of the system correctly and allows independent verification of the process.*

1.2 DELIVERABLES

1.2.1 *The following documents will be issued as part of the FMEA process.*

1. *Preliminary FMEA at a time to be mutually agreed when there is sufficient information to make meaningful comment on the design.*
2. *Preliminary DP FMEA proving trials at a time to be mutually agreed before sea trials.*
3. *Final DP FMEA proving trials document to be complete after DP FMEA proving trials.*
4. *Final DP FMEA.*
5. *FMEA companion document.*
6. *Progress reports at mutually agreed internals. - with concerns register.*
7. *Completed MTS Gap Analysis for relevant deliverables.*
8. *DP Annual Trials Program – upon request.*

1.3 LANGUAGE

1.3.1 *All reports will be written in English using a formal report writing style.*

1.4 REFERENCES TO FIGURES

1.4.1 *All figures, tables etc. will be referenced from the text.*

1.5 SUMMARY

1.5.1 *Following the title page, the FMEA report will start with a summary of the main points and findings of the analysis. In particular, it will provide:*

1. *A brief description of the vessel, discuss the vessel's worst-case failure design intent and state whether the analysis has confirmed or disproved it.*
2. *A summary of all the various manifestation of the worst-case failure will be given when the same effect can be obtained in number of ways.*
3. *Reference to any outstanding concerns.*

1.6 ABBREVIATIONS

1.6.1 *A list of all abbreviations used will follow the Summary or provided in an appendix if large.*

1.7 SUB-SECTIONS WITHIN THE FMEA

1.7.1 Refer to Appendix A.

1.8 APPLICABLE REFERENCES

1.8.1 The following rules, standards and guidelines (or their latest revisions) should be used as reference material in the preparation of the FMEA or FMECA:

1. *IMCA M247 Guidance to Identify DP System Components and Their Failure Modes'*
2. *IMCA M166 – Guidelines on Failure Modes and Effects Analyses.*
3. *IMCA M103 – Guidelines for the Design and Operation of DP Vessels.*
4. *IMCA M206 – A Guide to DP Electrical Power and Control.*
5. *IMCA - DP Incident Reports – Various.*
6. *MTS Learning From Incidents (LFIs).*
7. *MTS TECHOPs – Various.*
8. *MTS Gap Analysis Tools.*
9. *MTS DP Vessel Design Philosophy Guidelines.*
10. *IMO MSC 645 – Guidelines for Vessels with Dynamic Positioning Systems 1994.*
11. *IMO MSC 1580 – Guidelines for Vessels with Dynamic Positioning Systems 2017.*
12. *DP Rules of the appropriate Classification Society.*

1.9 LIMITATIONS OF THE ANALYSIS

1.9.1 The limitations of the analysis should be stated.

1.10 SYSTEM CONFIGURATION

1.10.1 The introduction should state the various vessel/power plant configurations that are being analyzed – for example, busties open/busties closed and different number of generators online.

1.10.2 Each section on the various sub-systems should also give more detailed configuration information appropriate to the analysis including the position of circuit breakers and valves.

1.11 SYSTEM SOFTWARE

1.11.1 The FMEA document should record DP related software revisions levels installed at the time of the FMEA proving trials.

2 REPORT FORMAT – MAIN BODY

2.1 GENERAL

2.1.1 *The main body of the report is divided up into the various systems that are being analyzed as outlined in Section 0 below. The following points should be discussed under the relevant subsection headings for each sub-system of the DP systems.*

2.2 SYSTEM DESCRIPTION

2.2.1 ***Drawing/Manual References:*** *Each section of narrative dealing with a particular system should begin by referencing the appropriate drawings with full Title, Drawing Number, and Revision Level or date if available. It is also acceptable to reference various drawings as the narrative proceeds if there are many drawings to be discussed.*

2.2.2 ***Description of redundancy concept:*** *A reasonably detailed but concise description of the how the system operates with particular attention to those parts that are essential to DP. Clearly identify those elements of the design intended to provide redundancy. It is useful to provide details of equipment manufacturers, types and ratings. Where the description includes aspects of the design that are not intended to be redundant, such as fuel transfer systems, discussions should focus how these systems impact the redundancy concept through potential common mode failures such as fuel contamination etc.*

2.3 DISCUSSION WITHIN SYSTEM DESCRIPTION

2.3.1 ***Location:*** *Where the system is physically located e.g. in the port switchboard room or the starboard pump room etc.; particularly for Class 3 vessels.*

2.3.2 ***Configuration:*** *How the system is normally configured. Main and alternate configurations if there are a number of possible configurations.*

2.4 SIMPLIFIED SYSTEM DIAGRAMS

2.4.1 *This should normally show only those parts of the system essential to DP. It should also show, in so far as is reasonably practical, the interfaces with other DP essential systems but only to such an extent as is necessary to explain the failures modes under discussion. It should also show the position of circuit breakers and valves where these are important to the analysis. It should identify those elements that are intended to be redundant with respect to each other. For marine auxiliary systems it is essential that the power supplies to pumps, fans, and other loads are shown even though this may be discussed again in the power distribution section. Where remotely operated valves are part of the system, the failure mode of important valves can also be shown. See detailed guidelines below.*

2.4.2 *For Class 3 analysis, the simplified system drawings should show compartment boundaries as dashed lines round parts of the diagram to show the limitation of the effects of fire and flood. Note this can also be useful in demonstrating how faults can be transferred out of the faulty compartment by the effects of short circuits on cables etc.*

2.4.3 *Drawings are to be produced using a suitable drawing package such as MS Visio. All text on drawings to be in Arial font – choose size to suit application. See 0 for details of format for sketches to be included in the FMEA.*

2.5 ANALYSIS OF SINGLE FAILURES AND THEIR EFFECTS

2.5.1 *Failures to be discussed in this section are those that have an immediate effect on system operation and would include the failure of redundant elements if both elements were continuously active.*

2.6 ANALYSIS OF HIDDEN FAILURES

2.6.1 Secondary failures are those that do not have an immediate impact on station keeping but which remove its fault tolerance or redundancy. Failure of redundant elements are included here if they are inactive at the time of failure. These will be discussed in a separate section for secondary and hidden failures such as backup supplies, offline redundancy or any protective functions on which redundancy depends. There may also be discussion of the fact that online redundancy may be expected to operate at or above its nominal rating.

2.7 ANALYSIS OF POTENTIAL COMMON MODE / CAUSE FAILURES

2.7.1 Discussion should focus on any common points between equipment intended to provide redundancy and how failures at the common points could affect the whole system. Discuss whether the sub-system is vulnerable to the usual common mode failures such as environmental control (heat), voltage spikes, voltage dips or sags, MBC in fuel, etc.

2.8 DESCRIPTION OF POTENTIAL PLANT CONFIGURATION ERRORS THAT COULD DEFEAT REDUNDANCY

2.8.1 These are essentially hidden acts of maloperation. In this section any operator errors in configuring the sub-system should be discussed with particular attention to those that would defeat the redundancy concept. Particular reference should be made to cross-connections between redundant components such as 'switchable' backup supplies being on the wrong connection or disarmed. Cross-connections for maintenance purposes, UPS bypass switches, valves for cross-connecting fuel, lube oil, compressed air and cooling water systems etc.

2.9 ACTS OF MALOPERATION

2.9.1 IMO guidelines require consideration of acts of maloperation if such an act is reasonably likely. These items should be discussed under a separate heading for each sub-system reviewed.

2.10 DESCRIPTION OF MAINTENANCE OR TESTING RELATED ISSUES

2.10.1 Discussion should be included the need for testing of alarms and protective functions if it is clear that an acceptable outcome is heavily dependent on the action of the automation system, operator or other protective functions. Such functions need periodic maintenance/testing to ensure that there is a high degree of confidence that they will operate on demand.

2.11 DESCRIPTION OF WORST-CASE FAILURE FOR SUB-SYSTEM

2.11.1 ***Worst-case Failure:*** *At the end of each section on a particular sub-system, there should be discussion of the worst-case failure identified for that sub-system and how it relates to the overall worst-case failure (equal or lesser). These sections for each sub-system will be gathered into the Executive Summary at the beginning of the FMEA report as it nears completion. This is necessary as there are often a number of failure modes where the effect on positioning is of equal magnitude or severity so there may be several worst-case failures separated only by their probability of occurrence.*

2.12 PRESENTATION OF CONCLUSIONS AND CONCERNS

2.12.1 The conclusion section should provide a general statement of the work done and discussed the DP system configuration(s) to which the conclusions apply. The worst case failure revealed by the analysis should be presented There should a clear 'Compliance statement' that indicates whether or not the design complies with the rules and guidelines referenced in the scope.

2.12.2 All concerns raised during the process of developing the FMEA should be logged in a 'concerns register' which should be issued periodically during the course of the FMEA project to provide feedback on issues in a timely manner. The concerns register should be created in spreadsheet (Excel) format and record the concern ID number, the date raised, discussion of the issue and any action taken to close it out. The concerns register should also record the initials of the person responsible for addressing the issues and the date of any close out.

2.12.3 ***Preliminary FMEA*** *- The concerns register may be included as an appendix in the preliminary FMEA.*

2.12.4 ***Final FMEA*** *- In the final FMEA the concerns register should be transferred to the FMEA companion document which should be referenced from the final FMEA document. The FMEA should state the number of outstanding category A concerns.*

2.12.5 The concerns identified should be categorized using the definitions below:

2.12.6 Concerns arising from analysis:

- ***Category A*** *The failure effects exceed the worst case failure design intent or some aspect of the design is non-compliant with the ….insert classification society… rules for notation …Insert DP notation… Improvement is recommended.*
- ***Category B*** *The failure effects equal the worst case failure design intent. The design complies with the ….insert classification society… rules for notation …Insert DP notation… but should be reviewed to determine whether a cost effective improvement can be made.*
- ***Category C*** *Observations, comments and suggestions associated with DP safety and reliability, which …insert client… may consider.*

2.13 PROGRESS REPORTS

2.13.1 These should be issued on a monthly basis but may be suspended with notification once the preliminary FMEA and FMEA proving trials have been issued if no further work is being carried. The progress report should contain a register of all technical quires raised and closed during the FMEA project, the concerns register, a register of any assumptions made in the process of developing the FMEA and the concerns register. Where the FMEA has identified that the redundancy concept depends on testing or periodic maintenance these issues should also be logged in an appropriate register.

2.14 FMEA COMPANION DOC

2.14.1 A companion document should be issued along with the final revision of the FMEA which provides details of all documents' issues in the course of the FMEA project and all the TQ, concerns, assumptions and maintenances issues registers at the conclusion of the FMEA project. The FMEA companion document should be referenced from the concerns section of the final FMEA. The FMEA companion documents in effect the final progress report.

EXAMPLE - APPENDIX A SECTION HEADINGS

THE FOLLOWING SECTION HEADINGS WILL BE USED

SUMMARY

TABLE OF CONTENTS

HEADINGS IN INTRODUCTION

Within the INTRODUCTION section there are the following headings, drawings and associated discussion.

1.3.1 Objectives of FMEA

1.3.2 Limitations of FMEA

1.4 FMEA PROCEDURE AND METHODOLOGY

1.4.1 Method

1.4.2 Structure of the FMEA narrative

1.4.3 Management of the FMEA process

1.4.4 Procedural and technical assumptions – (Reference to register)

1.5 REDUNDANCY CONCEPT

1.5.1 Worst case failure design intent(s)

1.5.2 Overview of redundancy concept with figures for overall SLD and Thruster arrangement. – (Discussion of how redundancy is achieved in each subsystem)

1.5.3 Operational configuration of the DP system – (related to WCFDI , all subsystems, all modes)

1.5.4 Common points between redundant systems

1.5.5 Protective functions upon which redundancy depends.

1.6 POWER AND PROPULSION CAPABILITY

1.6.1 Relationship between power and thrust.

1.6.2 Effect of worst case failure on power generation and thrust capability.

HEADINGS FOR EACH SUBSYSTEM

Within each subsystem there are the following headings. – Replace the word 'system' with appropriate name e.g. ENGINES AND AUXILIARY SYSTEMS. Replace 'subsystem' with the appropriate name e.g. FUEL OIL SYSTEM.

2 SYSTEM

2.1 SUBSYSTEM

2.1.1 Document reference

2.1.2 Description, and redundancy concept – (including simplified sketch of subsystem)

2.1.3 Location

2.1.4 Configuration for DP

2.1.5 Failure modes of the subsystem

2.1.6 Effects of subsystem failures

2.1.7 Hidden subsystem failures

2.1.8 Common mode failures

2.1.9 Configuration errors

2.1.10 Acts of maloperation.

2.1.11 Worst case failure of the subsystem

HEADINGS WITHIN THE CONCLUSIONS AND CONCERNS SECTION

The conclusions and recommendations section has the following headings:

11 CONCLUSIONS AND CONCERNS
11.1 CONCLUSIONS
11.1.1 General – (Statement of the work done)
11.1.2 DP system configuration for analysis
11.1.3 Other system configurations
11.1.4 Worst case failure – (for configuration analysed)
11.1.5 Compliance with rules and guidelines
11.2 CONCERNS
11.2.1 FMEA companion document
11.2.2 Concerns categories - (By severity in relation to the WCFDI)
11.2.3 Category A
11.2.4 Category B
11.2.5 Category C

EXAMPLE - APPENDIX B SPECIFICATION FOR SKETCHES

SLDs AND SKETCHES OF MARINE AUXILIARY SYSTEMS

1. *The drawing is to be split along the lines of the redundancy concept by using a dashed line to indicate equipment intended to be redundant – easy for port, starboard split – multi-way split may need several dashed lines – the two (or more parts) to be clearly identified e.g. PORT: STARBOARD.*
2. *For Class 3 FMEAs – dashed lines to be used to show compartment boundaries.*
3. *All pumps to show source of electrical supply at the pump symbol – if it is not clear from the switchboard nomenclature, add additional text to make it clear which part of the split it belongs to, e.g. MSB A or MSB B if it is clear that A is Port and B is starboard etc.*
4. *All pumps to show field station number that controls the pump e.g. FS 32 at the pump symbol.*
5. *All remotely controlled valves to show their failure mode on loss of power and signal e.g. F.S., F.O. and F.C. at the valve symbol.*
6. *All remotely controlled valves to show the source of power for actuators – air supply, hydraulic, electric and where it originates e.g. DB9 A at the valve symbol.*
7. *All remotely controlled valves to show the field station which controls them e.g. FS 42 at the valve symbol.*
8. *All fire dampers to show their failure modes on loss of control signal and actuator power at the damper symbol.*
9. *All Quick Closing Valves (QCVs) to show their failure modes on loss of control signal and actuator power at the valve symbol.*
10. *If tag numbers are available and it is important to the discussion to be able to identify particular components then these should be appended to the valve symbol (only for those valves that need to be discussed). If tags are not available then appropriate labels can be made up allow the component to be referenced.*

SIMPLIFIED OVERALL SLD TO BE INCLUDED IN THE INTRODUCTION SECTION OF FMEAS AND FMECAS

1. *All text on drawings will be in Arial at an appropriate font size for the drawing scale.*
2. *The overall SLD should be arranged in landscape and be legible on an A4 sheet.*
3. *Switchboards should be represented by a heavier solid line than the cables which attach to them.*
4. *It may be useful to arrange the drawing such that the thrusters can be shown at their physical locations within a dashed outline representing the shape of the vessel. Optionally, a vessel outline indicating thruster location should be included somewhere on the same sheet as space permits.*
5. *All voltage levels will be shown from the power generation level right down to the lowest control voltage level e.g. 11kV to 24Vdc.*
6. *Dashed lines will be used to divide up the drawing into groups of equipment intended to provide redundancy – e.g. Port switchboard and Starboard switchboard.*
7. *Dashed lines will be used to represent separate compartments for DP 3.*

8. *Main switchboards will show all generators, service transformers and thrusters, grounding systems, busties etc. – process consumers such as pipelay or drilling can be represented by a feeder.*
9. *The power, frequency, voltage and power factor will be shown at the generator symbol. Where identical generators are used, this information may be spread across several generators to save space.*
10. *The kVA rating and voltage ratio of service transformers should be shown e.g. 11kV/480V 1000kVA.*
11. *The voltage rating of switchboards will be noted at the switchboard (optionally the continuous current rating may also be noted).*
12. *The normal configuration of all busties should be given (N.O or N.C) at the bustie symbol.*
13. *A normally open contact symbol will be used to indicate a circuit breaker.*
14. *Cable tie lines will be indicated by a straight solid line.*
15. *Recognized symbols should be used for transformers and consumers such as thruster drives, starters, etc. It may be appropriate to use the same symbols as used on the vessel's schematics in some cases.*
16. *Thrusters will be indicated by a circle containing a propeller symbol. The designation used by the vessel for that thruster (e.g. ST1 for Stern Thruster 1) will be shown next to the thruster symbol.*
17. *The power of each thruster in MW (optionally kW) will be shown next to the thruster symbol.*
18. *Generators will be indicated by a circle containing the letter G and the generator's number e.g. G5.*
19. *Switchboards for marine auxiliary systems will show all DP essential consumers such as pumps, fans, UPSs, dc supplies etc. A mixture of symbols and labels (consumer list under switchboard symbol) can be used as space permits.*
20. *Switchboards for lighting and small power need only be shown if they supply a DP essential consumer (only DP essential consumers need be shown).*
21. *All UPS consumers essential to DP will be listed below the symbol for each UPS.*
22. *All consumers fed from rectifier/battery supplies should be listed below the symbol for the power supply.*
23. *The Field Station controlling each generator will be noted next to the generator symbol.*
24. *The Field Station controlling each switchboard will be noted next to the switchboard symbol.*
25. *Automatic and manual changeovers will be identified as such – next to the symbol.*
26. *Interlocks will be identified by connecting circuit breaker symbols with a dashed line (where it is important to do so).*

APPENDIX B EXAMPLE REDUNDANCY CONCEPT

MARINE TECHNOLOGY SOCIETY

DP VESSEL DESIGN PHILOSOPHY GUIDELINES

APPENDIX B

DP SHUTTLE TANKER REDUNDANCY CONCEPT PHILOSOPHY DOCUMENT

APRIL 2021

REVISIONS & CHANGES SUMMARY

Rev. No.	Date	Reason for Issue	Prepared by	Verified by	Approved by

Rev. No.	Section	Description of Changes

SUMMARY

CONTENTS

FIGURES

TABLES

APPENDICES

FIGURES IN APPENDICES

TABLES IN APPENDICES

1 INTRODUCTION

1.1 OVERVIEW

1.1.1 The objective of this Redundancy Concept Philosophy Document (RCPD) is to communicate the redundancy concept and supplement the vessel's build specification in matters related to dynamic positioning. The intended audience for this RCPD includes all stakeholders involved with the design and build of the vessel including:

- Classification society
- Shipyard
- Equipment vendors
- 3rd party verifiers (FMEA supplier)
- Vessel Technical Operator's shore-based staff (Owner)
- Vessel crew

2 VESSEL INDUSTRIAL MISSION(S)

2.1 OVERVIEW

2.1.1 The vessel is to be a DP class 2 shuttle tanker carrying out crude oil offtake from FPSOs operating offshore Brazil.

3 VESSEL OVERVIEW

3.1 PRINCIPLE DIMENSIONS

3.1.1 The vessel has a conventional monohull tanker configuration with engine room, bridge and accommodation aft and cargo tanks forward. design outlined in this RCPD is a concept design for the purpose of obtaining Approval in Principle for DP Shuttle Tankers with a power plant arrangement based on autonomous thrusters and generators.

3.1.2 Table 3-1 provides details of the vessel's main particulars.

Table 3-1 Vessel Specification

Name	DPST - Concept	**Length O.A.**	285.0m
Shipyard	TBA	**Beam**	45.0m
Hull/Project No.	TBA	**Design Draught**	18 m
Construction	TBS	**Dead Weight**	150000 tonnes
Owner	TBA	**Speed Max.**	16.0 knots

3.2 DP RELATED EQUIPMENT AND SYSTEMS

3.2.1 The DP system's five independent equipment groups and thruster arrangement are shown in Figure 3-1. Figure 3-2 provides an overview of the power distribution system. The main features of this design include:

- A main engine driving a single controllable pitch propeller with rudder located at the stern. The propeller and rudder are integral to the DP capability of the DPST.
- A 6kV diesel electric power plant consisting of four diesel generators on four switchboard bus sections, provides power for the thrusters and all auxiliary systems (including those of the main engine, controllable pitch propeller and the steering gear).

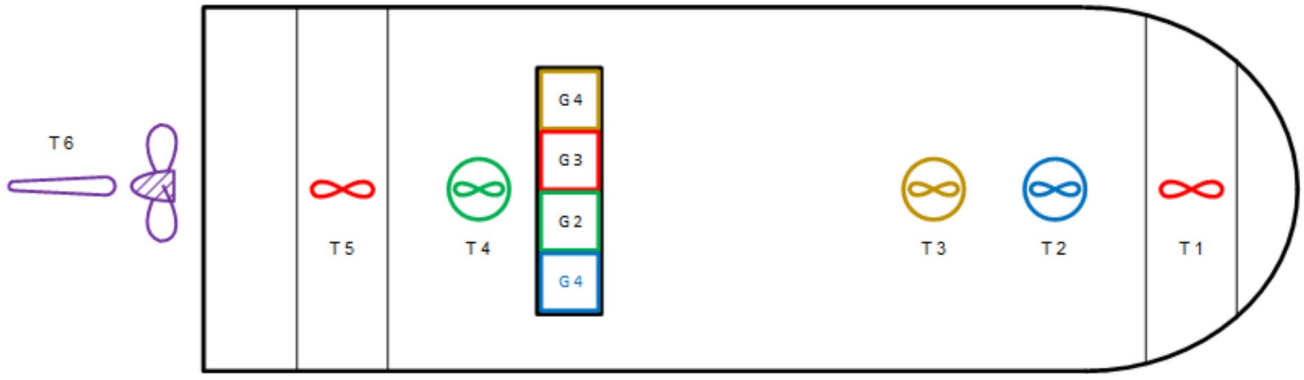


Figure 3-1 Independent DP Equipment Groups

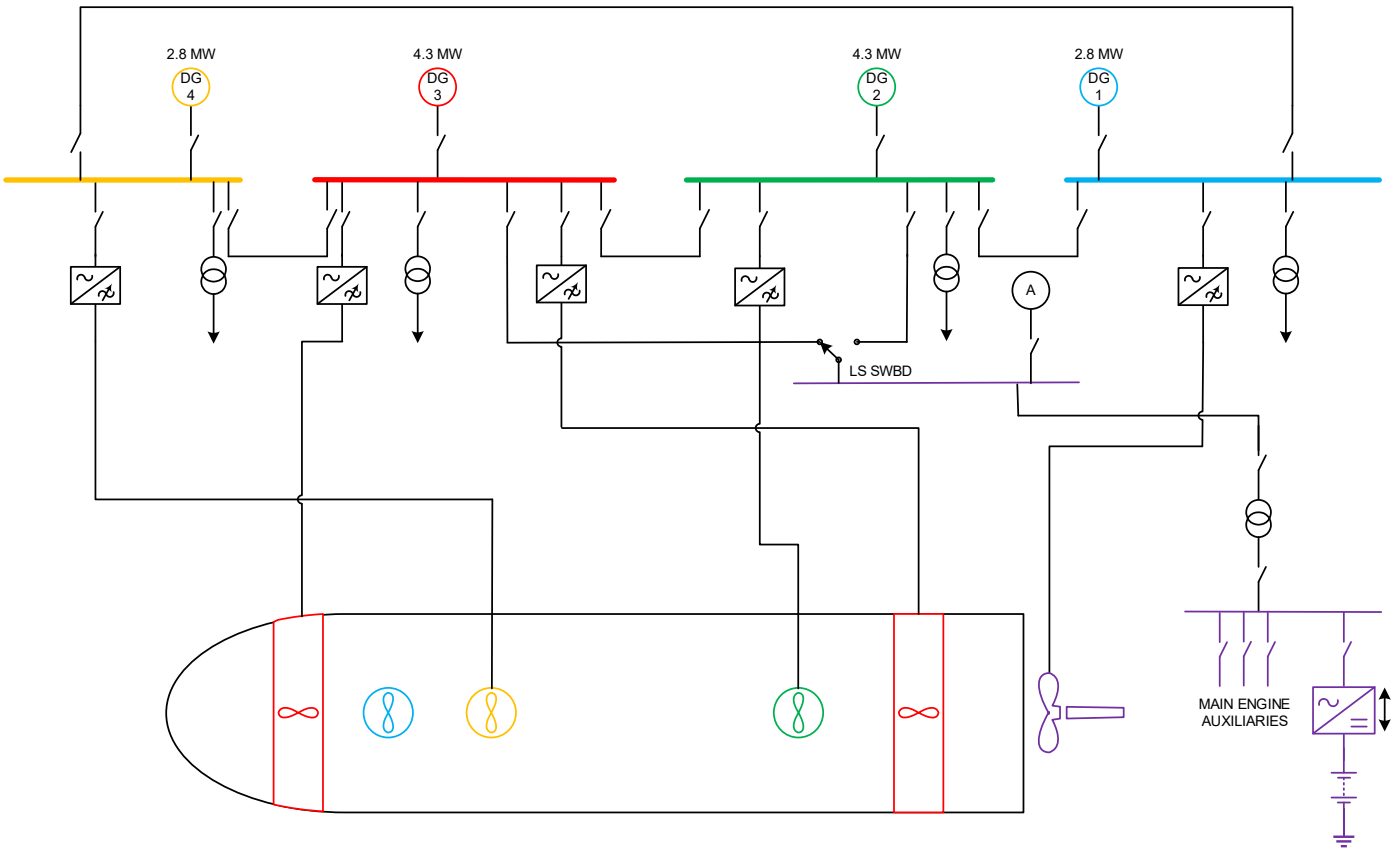


Figure 3-2 Redundancy Design Intent – (5 – Groups)

Table 3-2and Table 3-3 provide details of the generators, thrusters and main propulsion.

Table 3-2 Generators

Generator No.	Description	Red. Group	Power MW	Voltage	Frequency
G4	Port Outer	D	2.8	6kV	60Hz
G3	Port Inner	C	4.3		
G2	Stbd Inner	B	4.3		
G1	Stbd Outer	A	2.8		

Table 3-3 Thrusters

Thruster No.	Description	Red. Group	Power MW	Speed	Pitch
T1	Bow Tunnel Thruster	C	2.5	Variable	Fixed
T2	Bow Azimuth Thruster 1	A	2.5		
T3	Bow Azimuth Thruster 2	D	2.5		
T4	Stern Azimuth Thruster	B	2.5		
T5	Stern Tunnel Thruster	C	2.5		
T6	Main Propeller	E	16	Fixed	Variable
	Rudder	E			

4 CLASSIFICATION / EQUIPMENT CLASS

4.1 RULES

4.1.1 The vessel's DP system is to be built to DNVGL rules for rules for Dynpos AUTR. The vessel will have the following class notation:

+1A, Tanker for oil ESP, CSR, E0, DYNPOS(AUTR), BOW LOADING, TMON, NAUT(OC), BIS BWM(T), SPM, VCS(2), COAT-PSPC(B,C), RECYCLABLE, LCS, CMON, CLEAN, ER (SCR, Tier III)

The design of the vessel's DP system will comply with IMO MSC 1580 'Guidelines for Vessels and Units with Dynamic Positioning Systems. The DP systems consists of five equipment groups which can be considered to be independent in respect of common causes of failures when the failure criteria for Dynpos AUTR are applied.

5 DP SYSTEM OPERATING CONFIGURATIONS

5.1 GENERAL

5.1.1 The DP system will be designed to operate in the following configurations:

- Common power system - Closed Ring
- Any combination of 2 to 4 independent power systems - Open Busties

6 CODES, STANDARDS AND GUIDANCE

- Common Structural Rules for Double Hull Oil Tankers, July 2012
- DNVGL rules for Ships (RU-SHIP 2020)

7 OWNER'S/END USER-CHARTERER'S REQUIREMENTS

- Shell specification for DPST
- MTS DP Design Philosophy Guidelines
- MTS TECHOPs

8 REDUNDANCY DESIGN INTENT(S) & WORST-CASE FAILURE DESIGN INTENT(S)

8.1 DP SYSTEM REDUNDANCY DESIGN INTENT

8.1.1 The DP System's redundancy design intent, in Table 8-1, describes the effects of losing any one of the independent equipment groups. It is based on five independent equipment groups. The thrusters and generators are colour coded as indicated in Figure 3-1 and Figure 3-2.

Table 8-1 Redundancy Design Intent

Failure Status	Thrusters Available	Redundancy Type
Intact	T1 T2 T3 T4 T5 T6	Active
Failure of A	T1 T3 T4 T5 T6	None
Failure of B	T1 T2 T3 T5 T6	None
Failure of C	T2 T3 T4 T6	None
Failure of D	T1 T2 T4 T5 T6	None
Failure of E	T1 T2 T3 T4 T5	None

8.2 LIFE CONCEPT

8.2.1 The LIFE concept was developed by applying the principle autonomy, independence and segregation. The LIFE concept also utilises the principle of critical and non-critical redundancy to increase the reliability of each independent DP equipment group. The terms are defined as follows:

- The loss of critical redundancy will impact the vessel's post failure DP capability.
- Non-critical redundancy has no effect on post failure DP capability but improves the reliability and maintainability of the independent or redundant DP equipment group to which it is applied.

8.2.2 In newbuild LIFE Concept designs the Worst Case Failure Design Intent (WCFDI) does not consider the possibly of faults acting directly on the HV bus bars – This exemption is only valid when the switchboards have been specifically designed to be short circuit proof – Thus the WCFDI for Dynpos AUTRO may differ from that defined for LIFE concept Two WCFDIs will be maintained throughout the vessel's operational life.

8.3 MARINE SYSTEMS

8.3.1 In the case of marine auxiliary systems this involves providing two 100% duty /standby pump pairs and two 100 heat exchangers. The pumps power supplies both originate within the same independent equipment group. The philosophy of proving dual pumps is to be able to tolerate failure of a pump and not failure of its power supply. However, the two pump supplies are arranged from separate distribution board providing a degree of resilience to local power supply failure.

8.3.2 In the case of control power supplies, additional 24Vdc power supplies or additional UPS all within the same indecent equipment group.

8.4 WORST CASE FAILURE DESIGN INTENT – DYNPOS AUTR

8.4.1 The vessel's worst-case failure design intent is derived from the Redundancy Design Intent and is defined as follows:

'No single failure as defined for DNVGL notation Dynpos AUTR will have a greater effect on the vessel's ability to maintain position and heading than the loss of independent group C.'

- This intent applies in all defined power plant configurations.
- For this intent to be valid, all equipment must be capable of its defined performance and all protective functions must operate successfully on demand.

8.5 WORST CASE FAILURE DESIGN INTENT – LIFE CONCEPT

8.5.1 The vessel's worst-case failure design intent is derived from the Redundancy Design Intent and is defined as follows:

No single failure as defined for LIFE Concept will have a greater effect on the vessel's ability to maintain position and heading than the loss of one generator or one thruster.

- This intent applies in all defined power plant configurations.
- For this intent to be valid, all equipment must be capable of its defined performance and all protective functions must operate successfully on demand.
- WCFDI for LIFE concept on a DP Class 2 Vessel does not consider the possibility of a faut acting directly on the main switchboard bus bars.

9 EXPECTATIONS FOR VERIFICATION AND VALIDATION

9.1 INTENTION TO VALIDATE

9.1.1 The following tests will be carried out whether or not they are required by Dynpos (AUTR):

- All compensating provisions used to address common points will be tested for effectiveness. In particular:
  - Protective functions (electronic, electrical and mechanical)
  - Automatic changeovers
  - Diode isolation of dual supplies
  - Standby redundancy
- Short circuit and ground fault testing on all power distribution systems where cross connections exist.
- Network storm and throughput testing on data communication networks.
- All DP system components will be tested to prove their performance.

Note: In the absence of instructions in the vessel owner's specification, the shipyard will take owner's instruction on what verification and validation testing is required.

Thus, testing may be required even if:

- It is not specified in the rules for the DP notation.
- It is not carried out as established custom and practice.

Often it is possible to make a technical argument for why such testing is actually required by the class rules.

10 CONCLUSIONS

10.1 OVERVIEW

10.1.1 The DP redundancy concept described in this RCPD is based on 5 independent DP equipment groups which rely for their fault tolerance on:

- A range of protective function designed to prevent faults propagating through closed busties.
- Stored energy assigned to keep the main engine auxiliary systems running.
- Exemption of certain mechanical components from consideration in the FMEA

APPENDICES

APPENDIX 1. SYSTEM SKETCHES

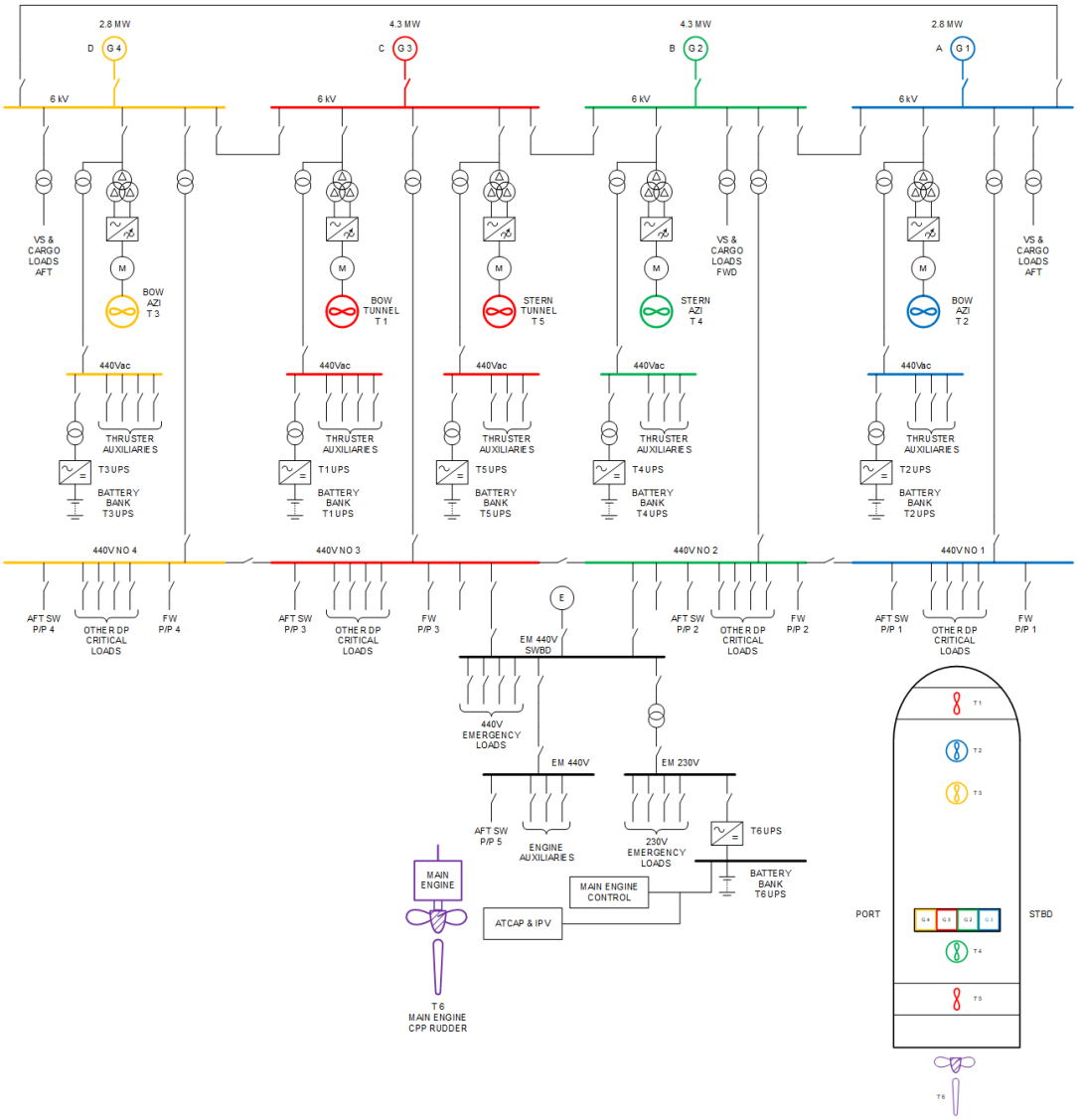
A1.1. INTRODUCTION

A1.1.1. The section which follows provided sketches which illustrate how the redundancy design intent is implemented on a system by system basis.

A1.2. POWER GENERATION AND DISTRIBUTION

A1.2.1. The Redundancy Concept is most readily visible in design of the Power Generation and Distribution systems which consists of four autonomous 6kV power systems and a LV power system for the Main Engine auxiliaries featuring a Battery Energy Storage System (BESS).

A1.2.2. Each power systems powers a single thruster with the exception of System C which powers the two tunnel thrusters.



Appendix 1 - Figure 1 Power Distribution System

A1.3. AUTONOMOUS GENERATORS AND THRUSTERS

A1.3.1. All power for the thrusters is derived from the HV feeder. A step-down distribution transformer supplies the thrusters' auxiliaries. Each generator has a dedicated MCC suppling power to its auxiliary systems. Power for this MCC is reduce form the appropriate section of the 440V bus.

A1.3.2. Autonomous designs lend themselves to the development of compact self-contained generators and thrusters which are modular in nature. This has the effects of:

- Creating well defined and easily understood system boundaries.
- Minimising the interface to other systems
- Minimising the number of potential fault propagation paths
- Reducing the opportunity for configuration errors
- Minimising the number of integration issues
- Maximizing the opportunity for pre-assembly, pre-commissioning and testing at an advanced stage of completion
- Reducing the verification and validation burden and simplifying the FMEA process
- Reducing the periodic reverification burden

A1.4. TREATMENT OF THE MAIN ENGINE

A1.4.1. DP shuttle tankers will typically have a large slow speed main engine for use during transit. From a DP perspective the main engine, CPP and rudder are treated as a transferable engine driven thruster which is intended to be independent in so far as it should only ever fail on its own and not with any other thruster.

A1.4.2. Difficulties in creating a truly autonomous design arise when the main engine has no dedicated independent source of electric power. In such design the main engine power is supplied from the main power generations system by way of duals supplies, auto changeover over or duty-standby pump arrangements. All these methods introduced potential fault propagation paths or increase exposure to hidden failures. They also add to the initial verification and reverification burden.

A1.4.3. In this design there are four sources of supply for the main engine auxiliary systems as follows:

- Redundancy Group C – Main supply
- Redundancy Group D – Backup supply by way of smart fail-safe auto changeover
- An auxiliary generator
- A battery energy storage system of limited capacity

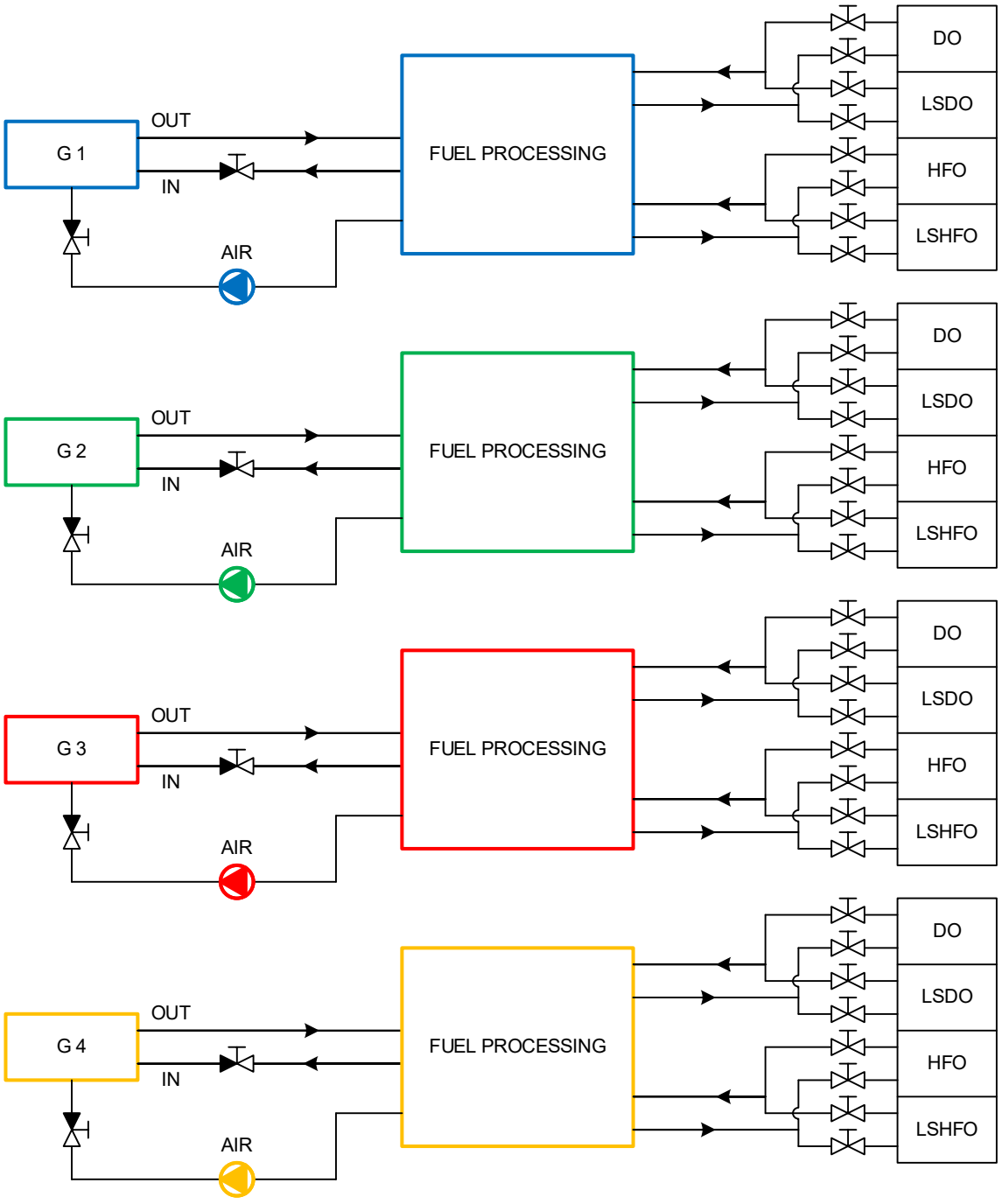
Note: *In this case the auxiliary generator could potentially be the Emergency Generator (Subject to classification Society approval)*

- A dedicated auxiliary generator
- A shaft generator driven from the main engine.

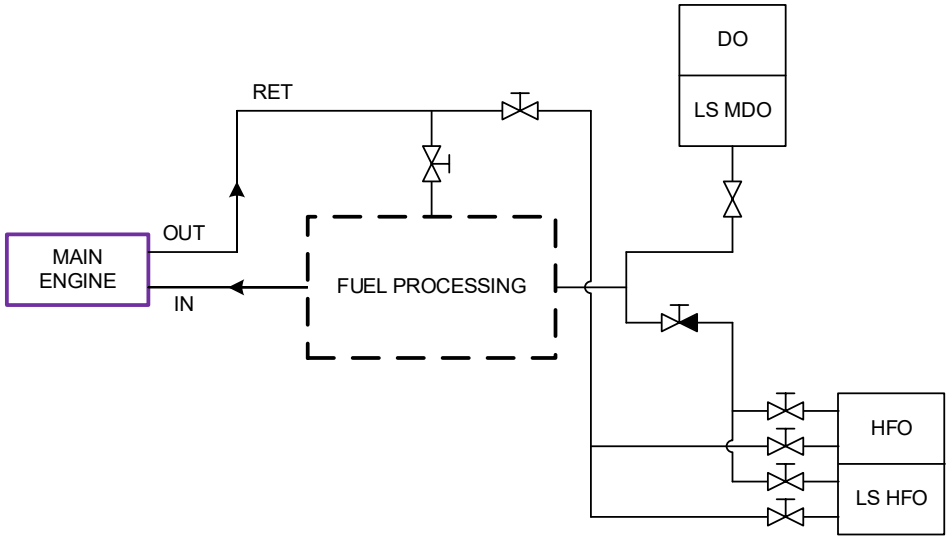
A1.4.4. Use of the emergency generator as part of the main engine redundancy concept might be possible, in some class notations, but not in others. Where it is not allowed by the rules, it may be necessary to provide a dedicated generator for the main engine. A shaft generator is another possibility.

A1.5. FUEL SYSTEM

A1.5.1. Appendix 1 - Figure 1 and Appendix 1 - Figure 2 show a fully segregated fuel system capable of maintaining segregation of four different grades of fuel.



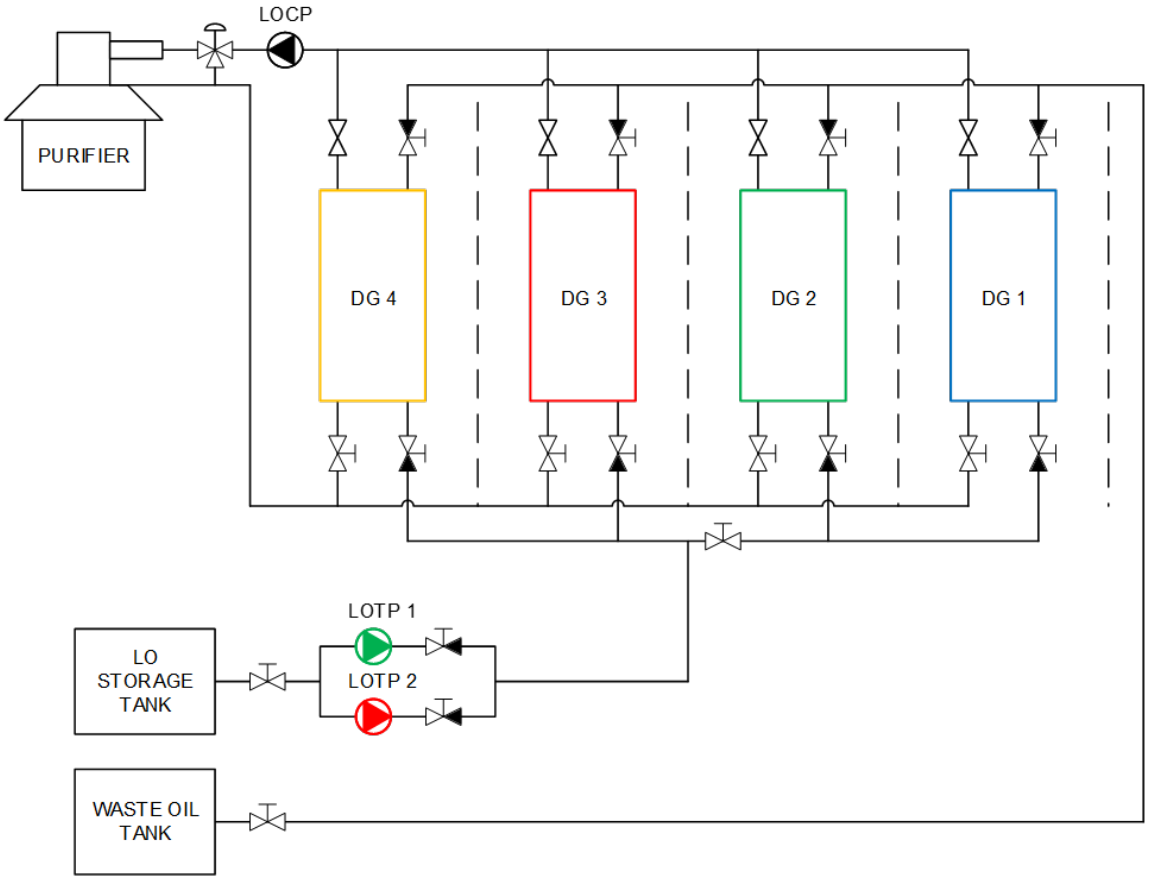
Appendix 1 - Figure 2 Fuel System



Appendix 1 - Figure 3 Main Engine Fuel System

A1.6. LUBRICATING OIL SYSTEM

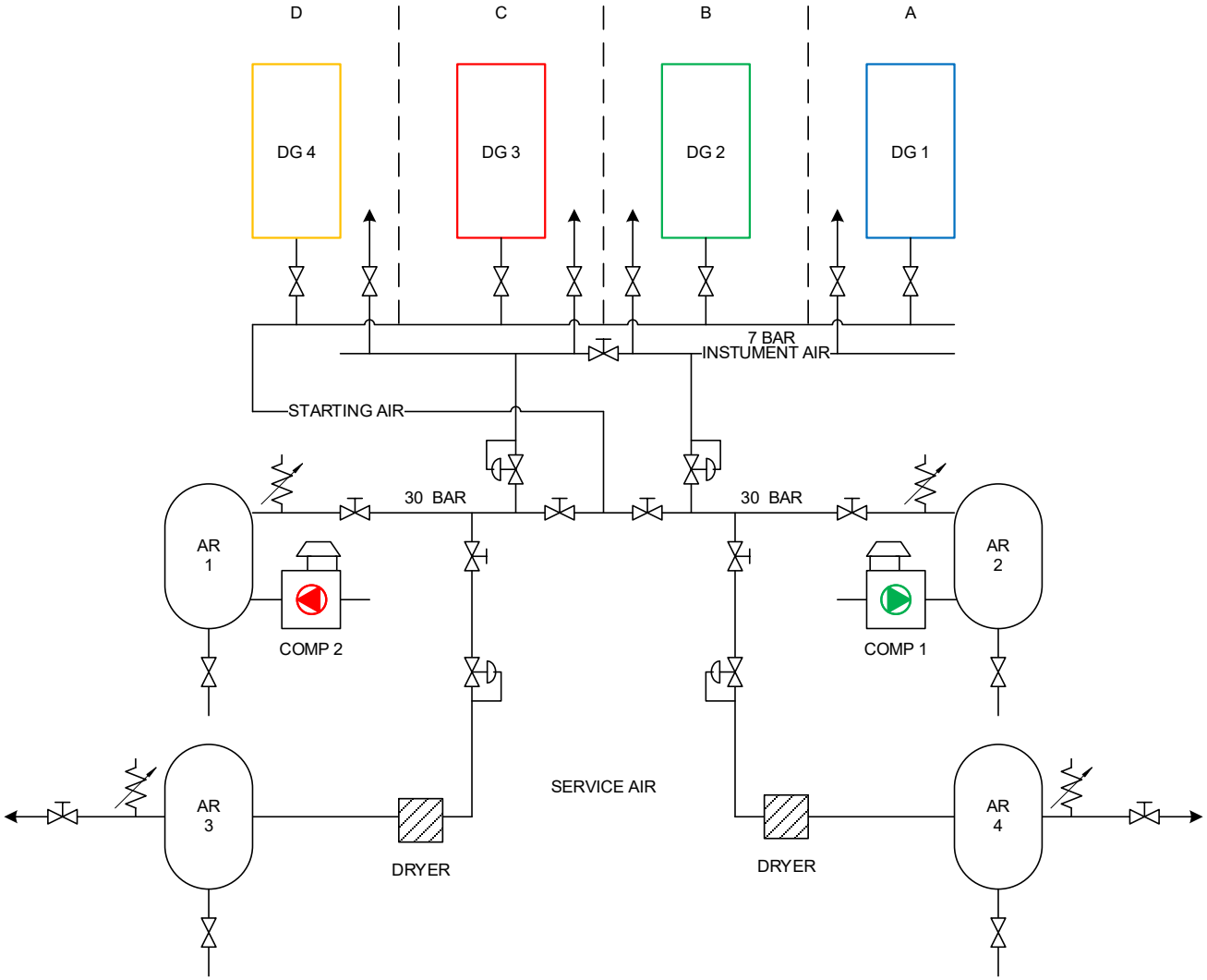
A1.6.1. Appendix 1 - Figure 4 shows the Lubricating Oil transfer and purification system is common to all four diesel generators. Procedures and oil sampling are used to mitigate the effects of the commonality so introduced.



Appendix 1 - Figure 4 Lubricating Oil System

A1.7. COMPRESSED AIR SYSTEMS

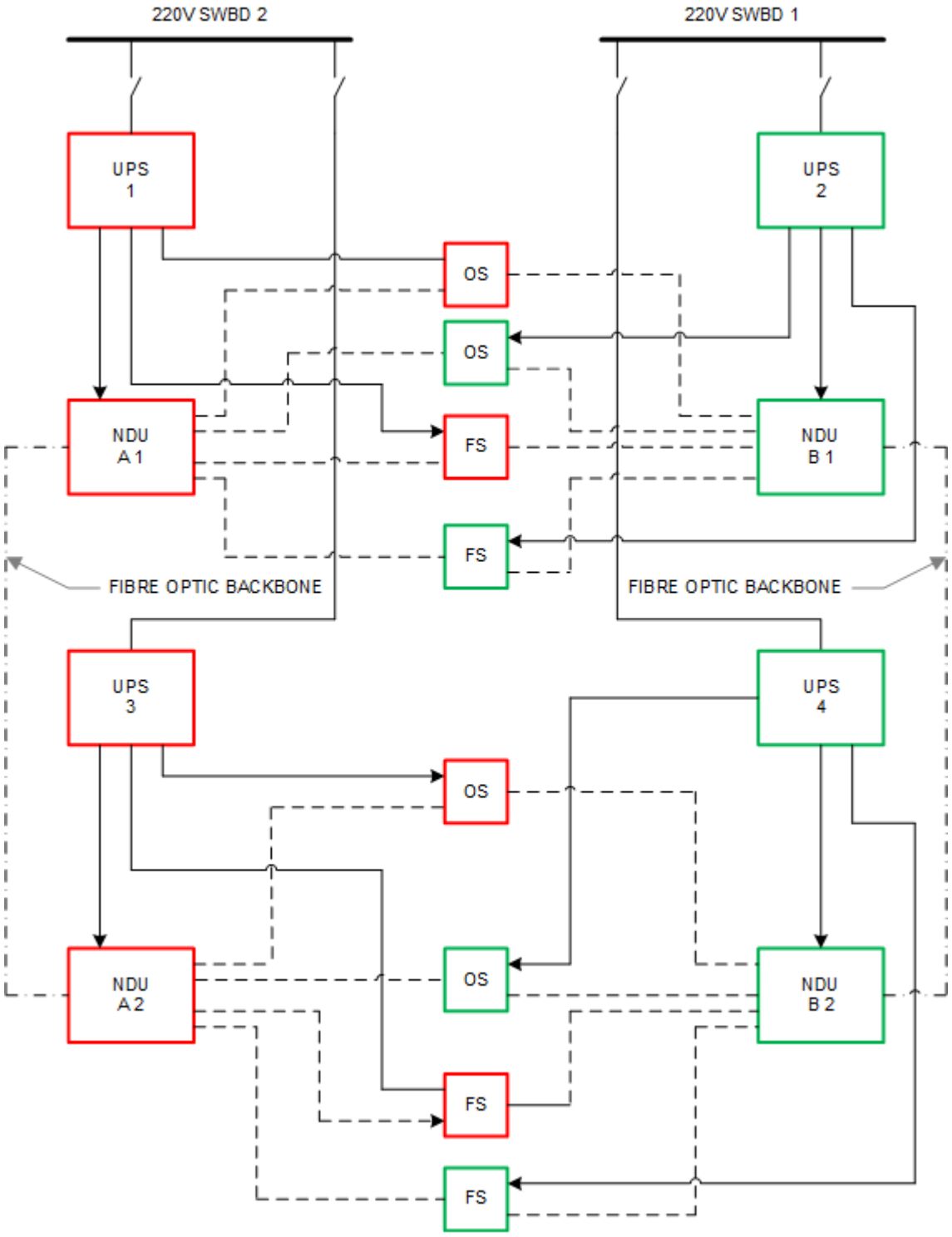
A1.7.1. Appendix 1 - Figure 5 shows the compressed air systems are common to all four diesel generators. The commonality so introduced is mitigate by the fail-safe nature of the equipment served by the compressed air systems. Engines and thrusters all continue to operate without compressed air. Risks associated with overpressure are mitigated by pressure relief valves.



Appendix 1 - Figure 5 Compressed Air System

A1.8. DATA COMMUNICATION NETWORKS

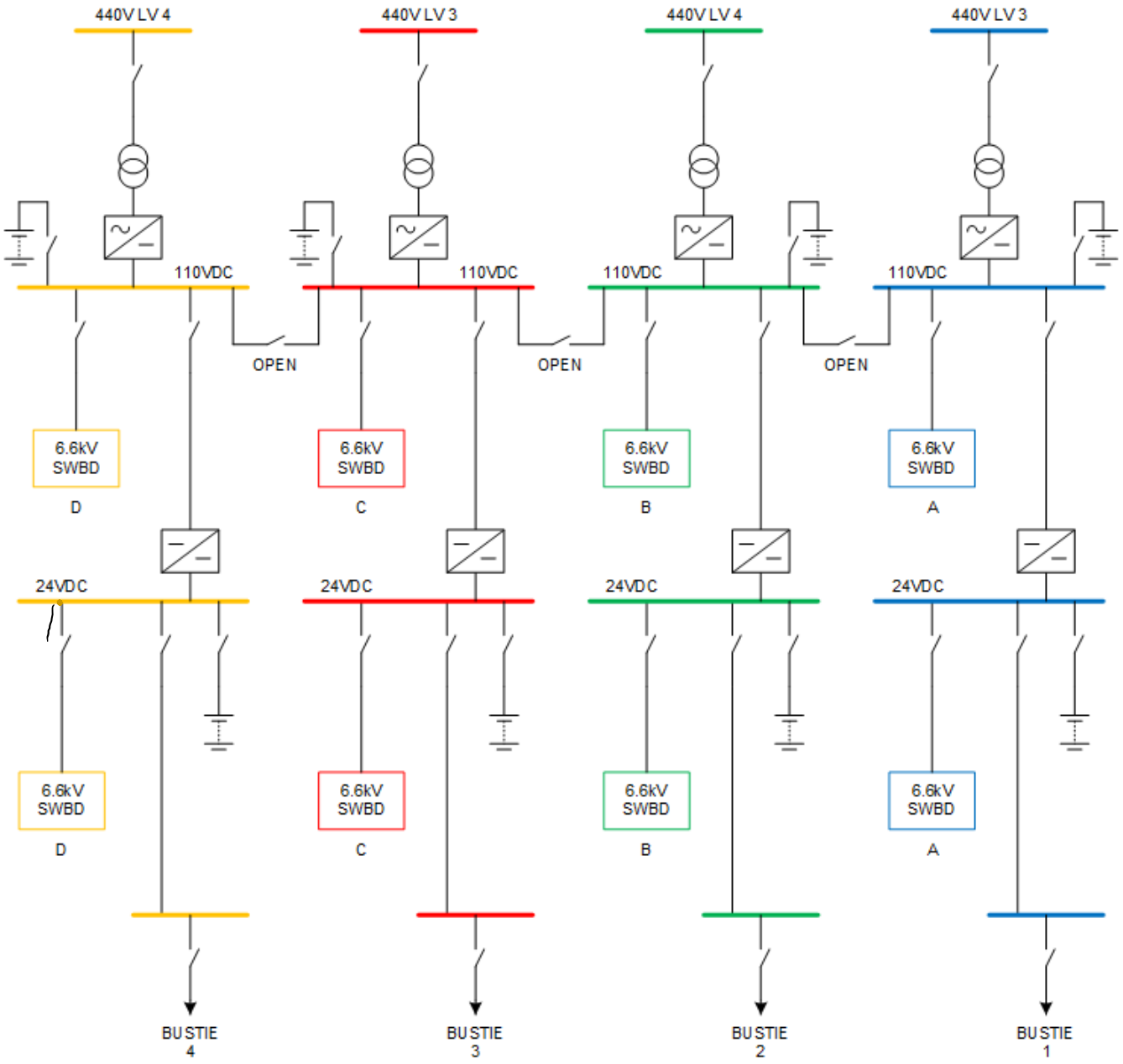
A1.8.1. Appendix 1 - Figure 6 shows the data communication networks. are arranged as a dual redundant data highway. A dual-star type arrangement is used with Network Distribution Units connected by a Fibre Optic backbone. Every field station and operators station form a common point between the A Network and the B network, and each network is connected to every data consumer / producer in the DP System. Verification and validation testing will include Network Storm testing to prove the protection against common mode failures is effective. Performance testing will be carried out to prove both networks are capable of their rated performance.



Appendix 1 - Figure 6 Data communication Networks

A1.9. 110VDC & 24VDC CONTROL POWER

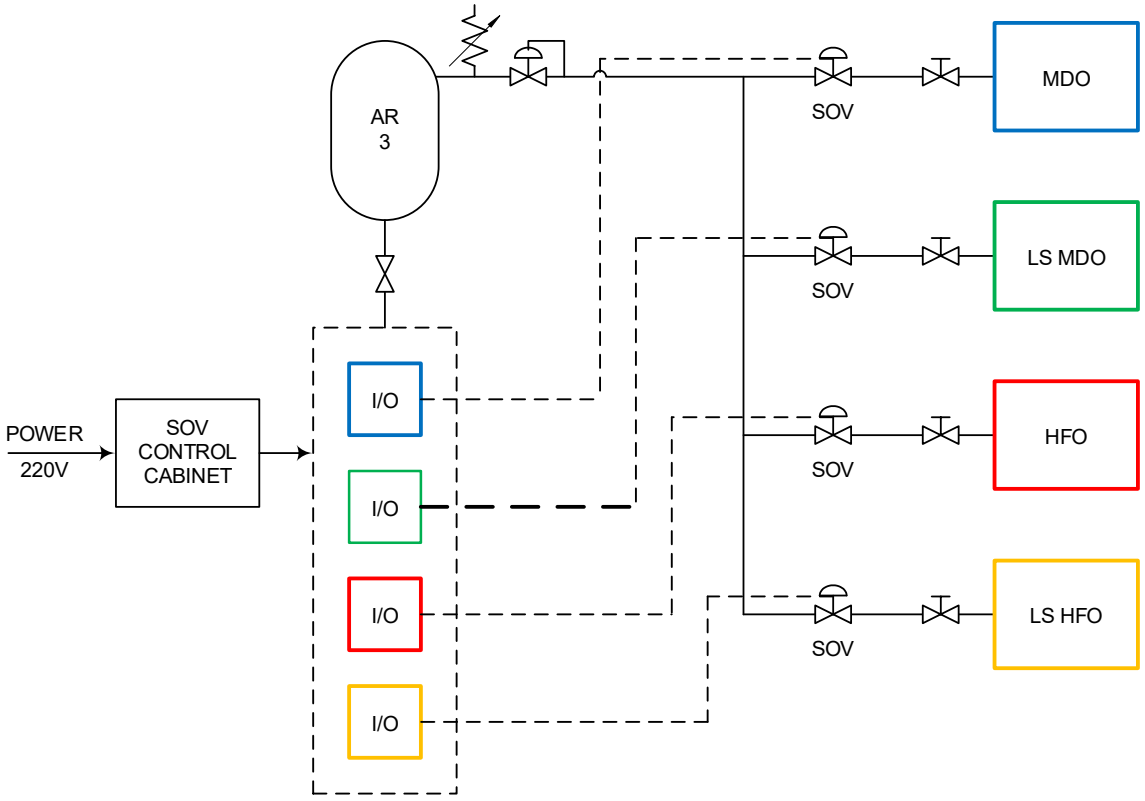
A1.9.1. Appendix 1 - Figure 7 shows a fully segregated control power supply system. Additional robustness has been added by provide the 24Vdc section with its own stored energy.



Appendix 1 - Figure 7 110Vdc and 24Vdc Control Power

A1.10. REMOTE CONTROLLED VALVES

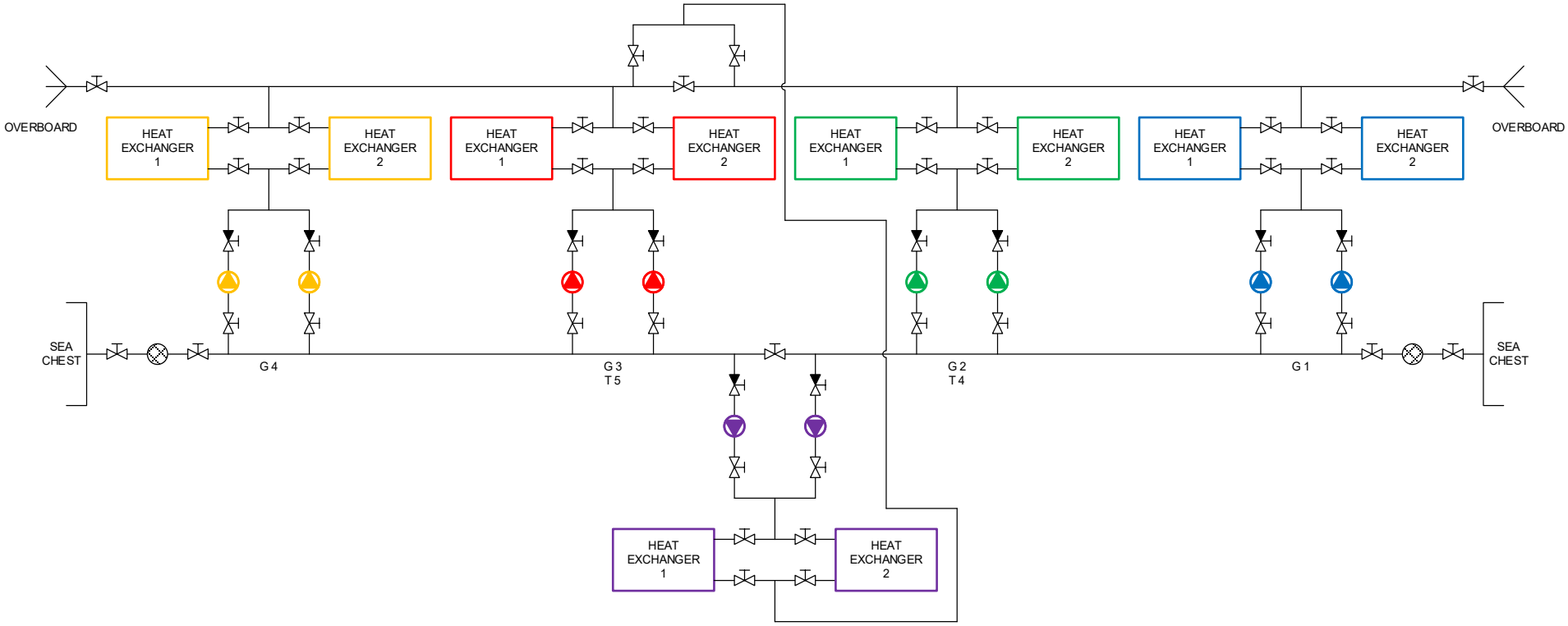
A1.10.1. Appendix 1 - Figure 8 shows a revised system for the fuel system QCVs. In this design the common air supply has been proven to be acceptable because of the fail-safe nature of the valves on loss of air pressure. The risk of a single point failure within the control cabinet commanding all the valves to close has been addressed by ensuring that valves for more than one independent DP equipment group are not located on the same I/O card.



Appendix 1 - Figure 8 QCV Control Power and signal

A1.11. MAIN SEAWATER COOLING SYSTEM

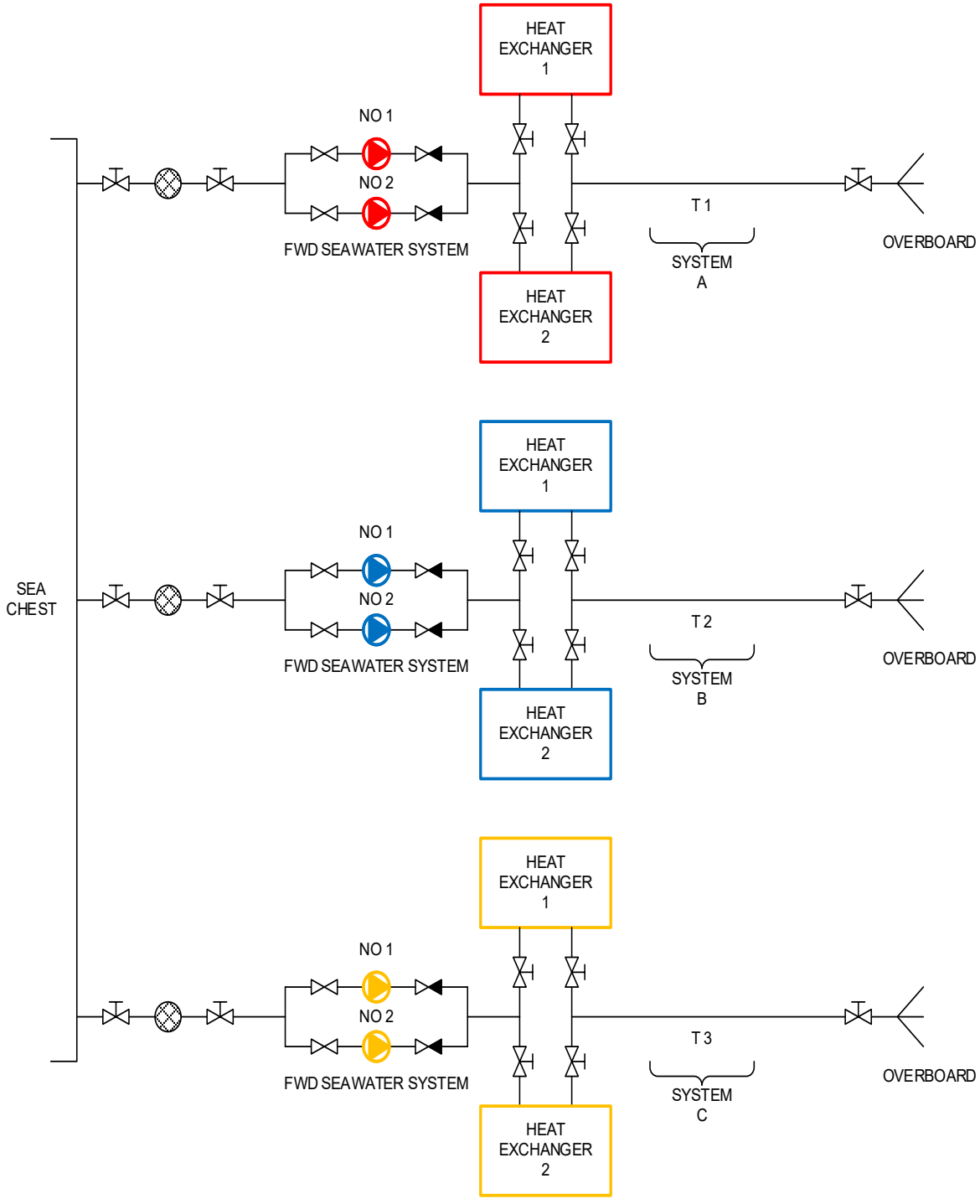
A1.11.1. Appendix 1 - Figure 9 shows the main seawater cooling system. Some commonality exists in this design as it is accepted that the risks of pipework failure in a seawater system lower and there is typically a substernal time lag before the effect of failure is felt in the freshwater cooled systems. The system has redundancy in overboard discharge and the ability to segregate a faulty section. It also provides for dedicated duty standby pumps and heat exchangers removing reliance on active elements and exposure to hidden failure.



Appendix 1 - Figure 9 Main Seawater Cooling System - Aft

A1.12. FORWARD SEAWATER SYSTEM

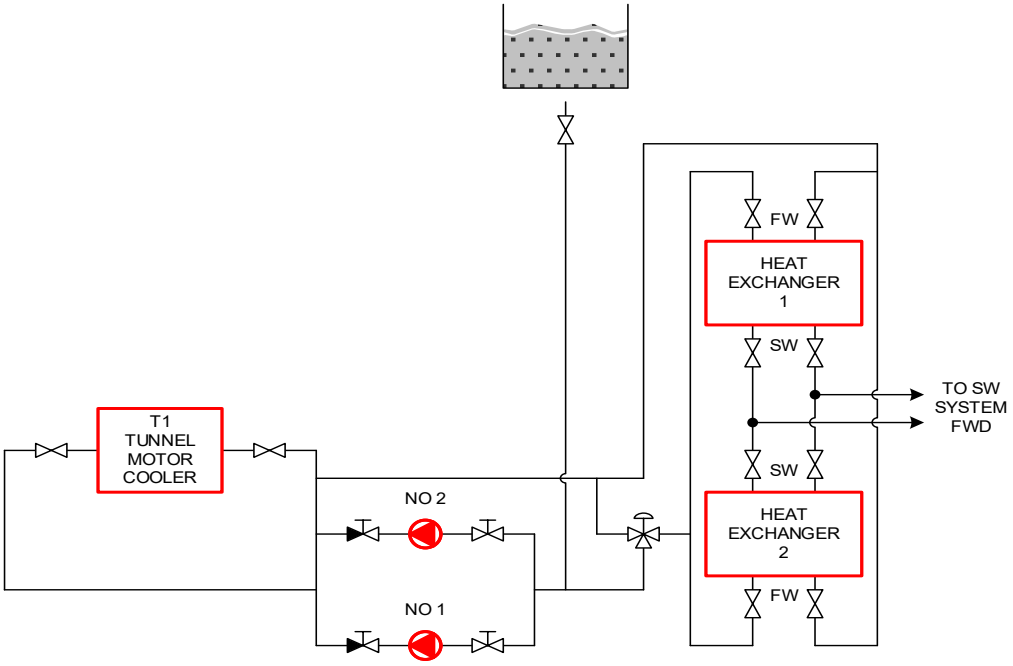
A1.12.1. Appendix 1 - Figure 10 shows the forward seawater cooling system. This design has full segregation and lends itself to a modular self-contained approach. As with the main seawater system, the use of non-critical redundancy is not essential but improves operability and maintainability.



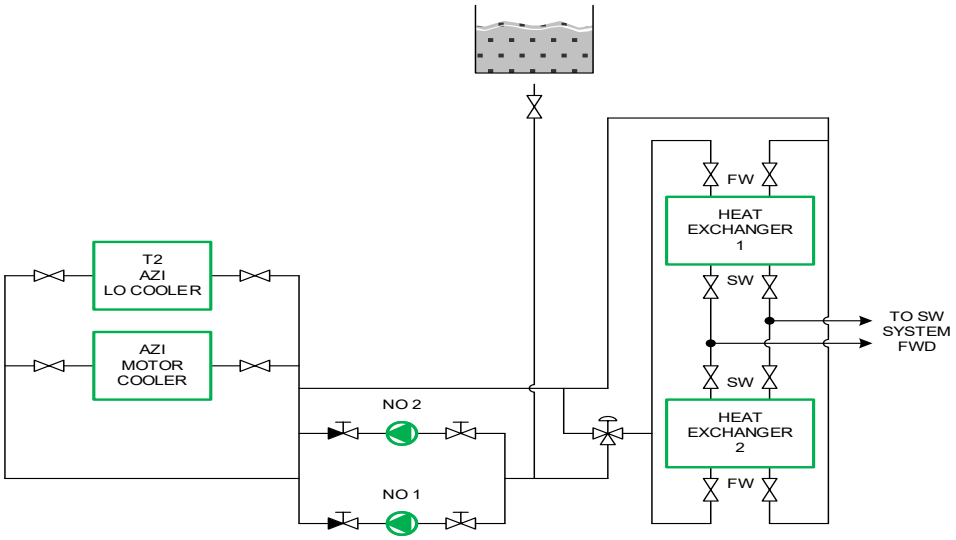
Appendix 1 - Figure 10 Main Seawater Cooling System - Fwd

A1.13. FORWARD FRESHWATER COOLING SYSTEM

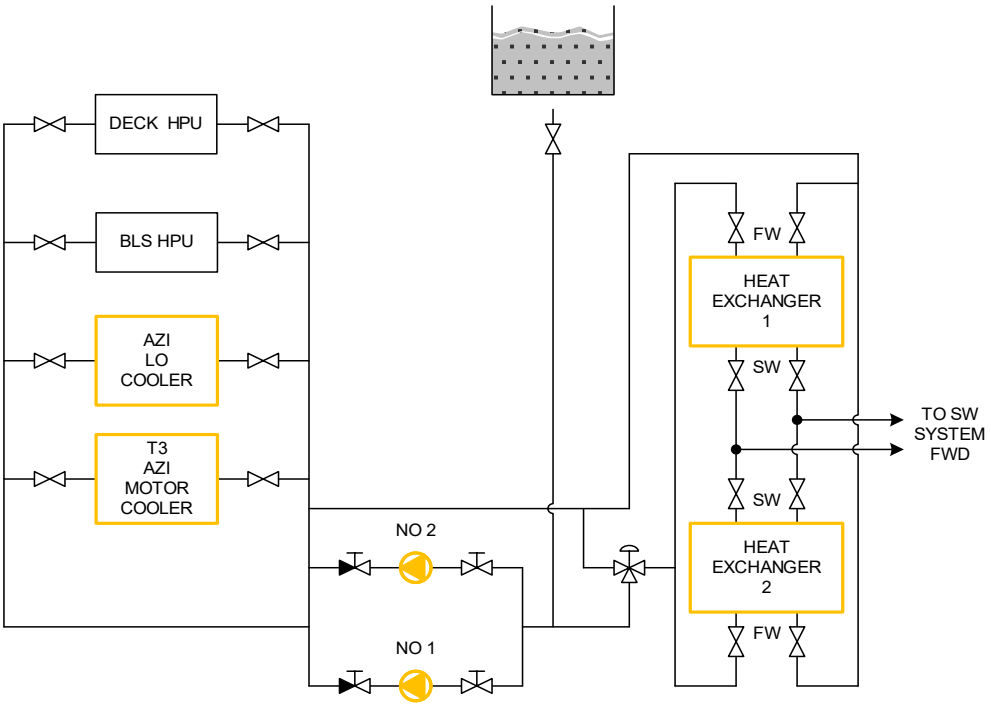
A1.13.1. Appendix 1 - Figure 11 to Appendix 1 - Figure 13, show the freshwater cooling system for the three forward thrusters, T1 T2 and T3.



Appendix 1 - Figure 11 Forward FW Cooling System T1



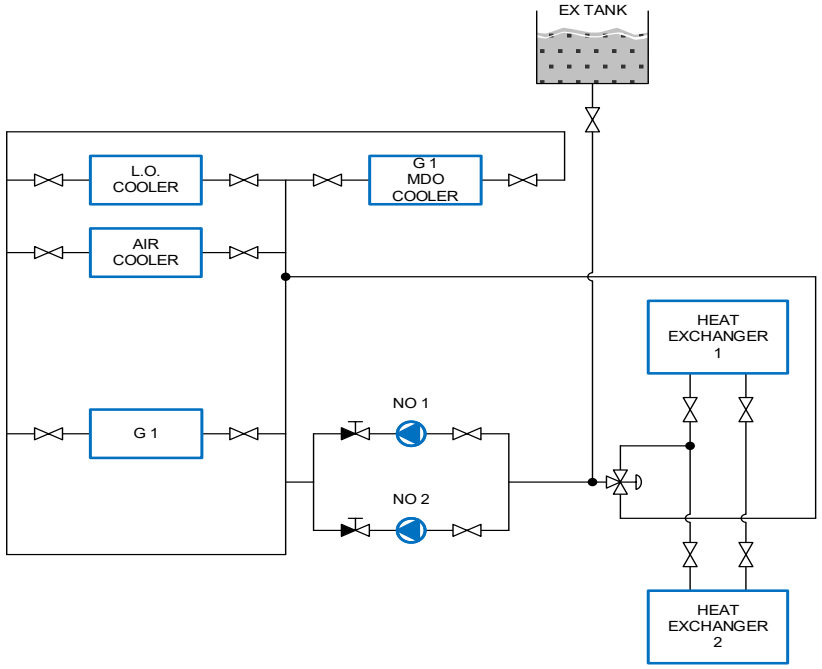
Appendix 1 - Figure 12 Forward FW Cooling System T2



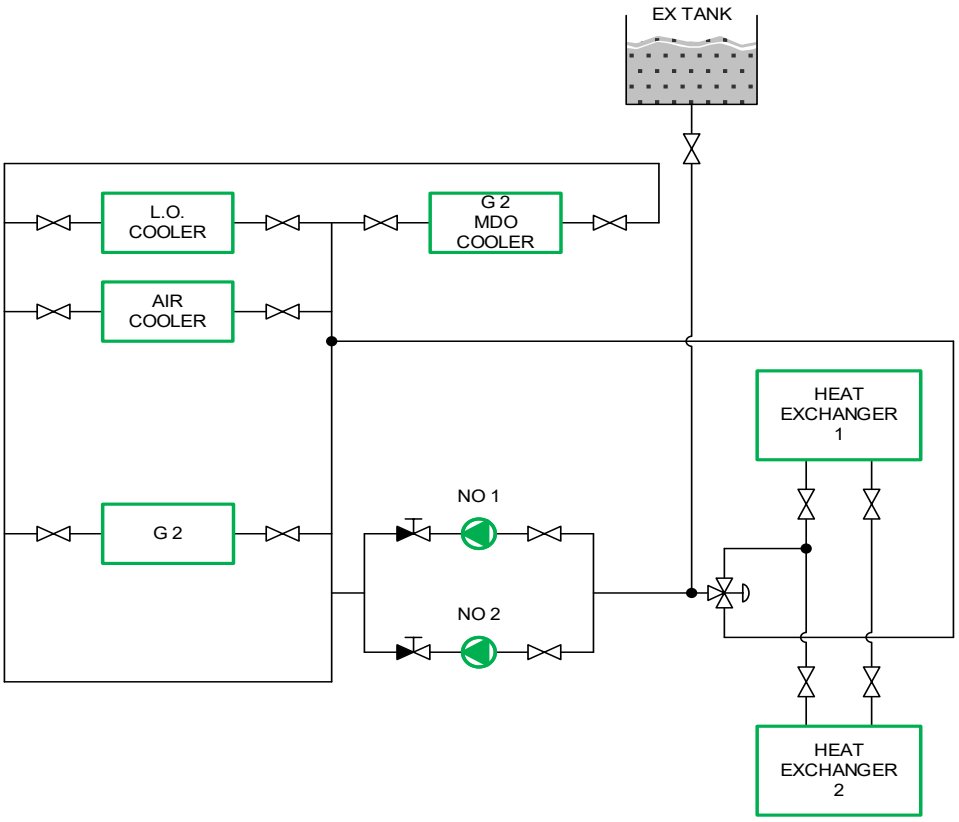
Appendix 1 - Figure 13 Forward FW Cooling System T3

A1.14. MAIN FRESHWATER COOLING SYSTEMS

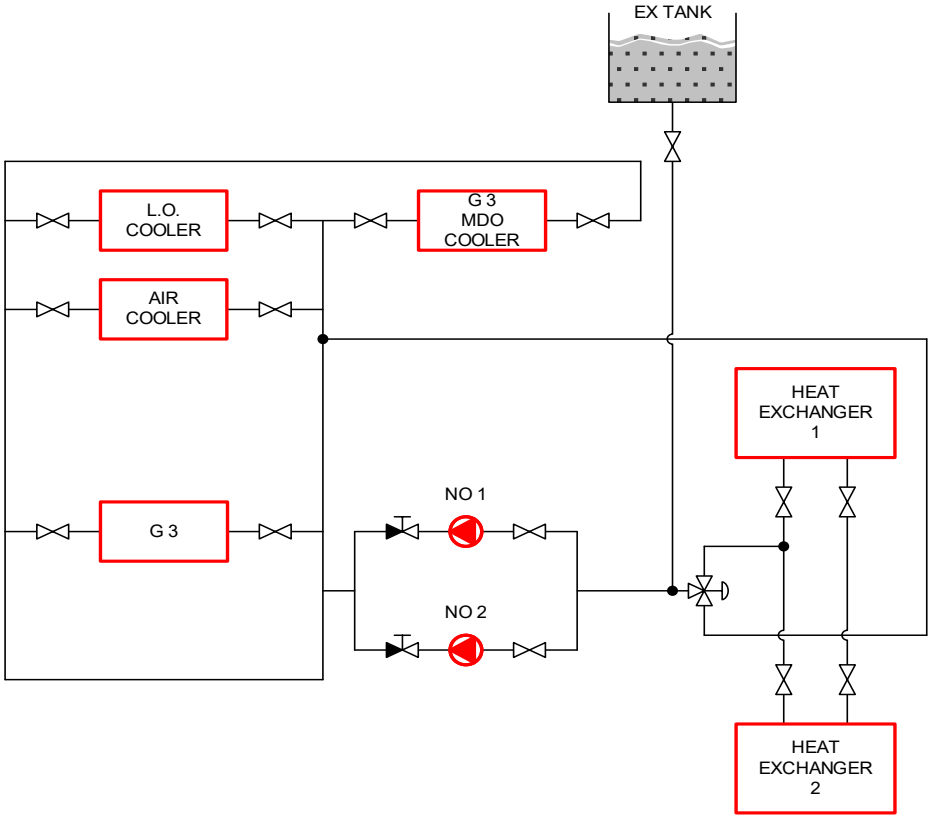
A1.14.1. Appendix 1 - Figure 14 shows the freshwater cooling systems for diesel generator G1. An identical design, based on segregation has been applied to the freshwater cooling system for all the main generators as shown in Appendix 1 - Figure 15, Appendix 1 - Figure 16, Appendix 1 - Figure 17.



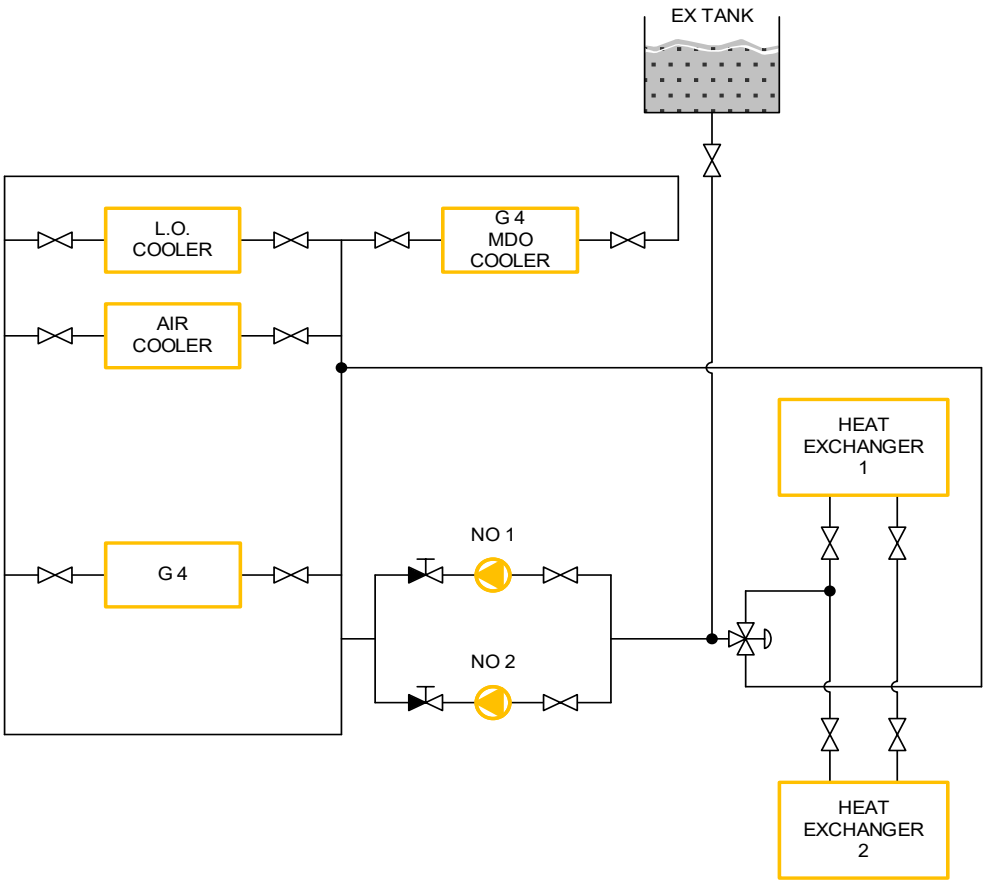
Appendix 1 - Figure 14 Freshwater Cooling System G1



Appendix 1 - Figure 15 Freshwater Cooling System G2



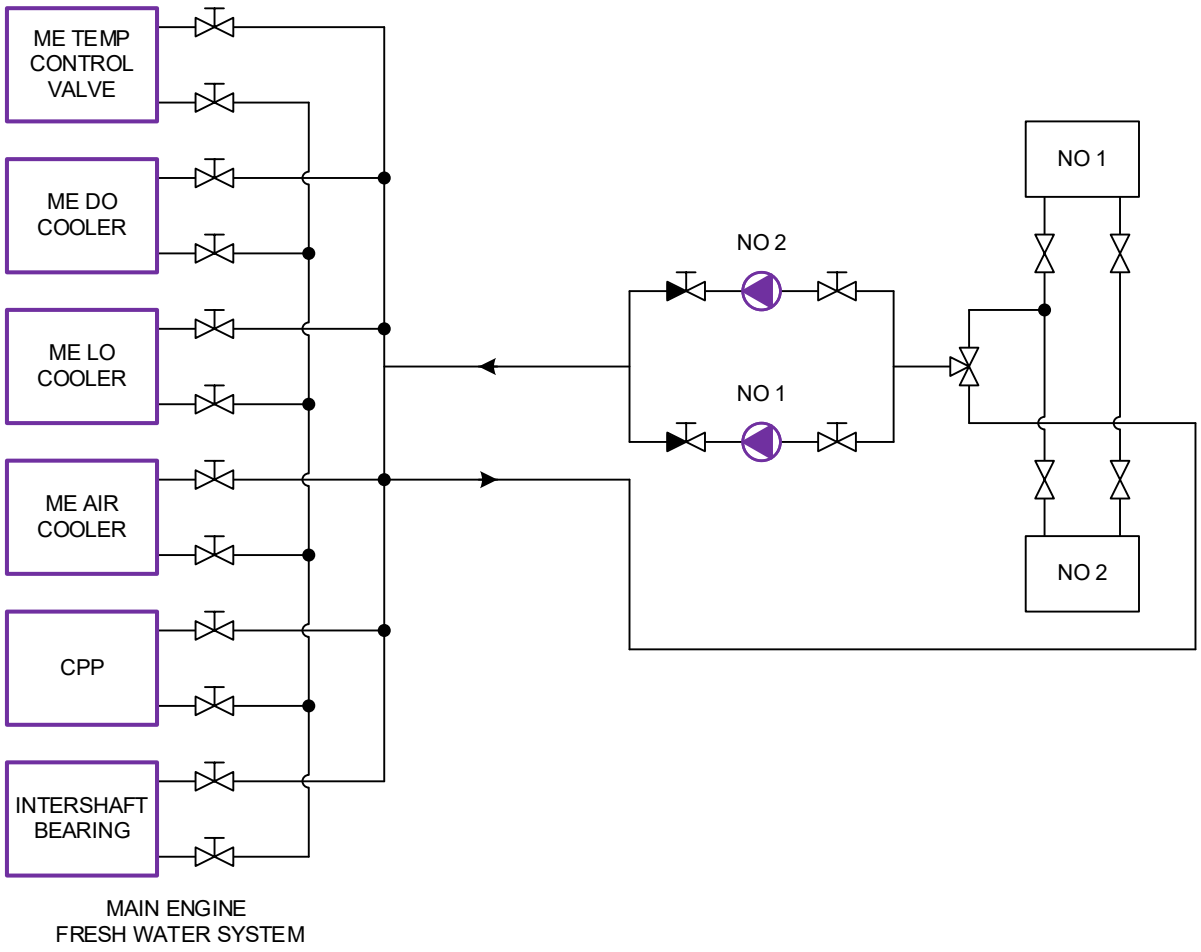
Appendix 1 - Figure 16 Freshwater Cooling System G3



Appendix 1 - Figure 17 Freshwater Cooling System G4

A1.15. MAIN ENGINE FRESHWATER COOLING SYSTEM

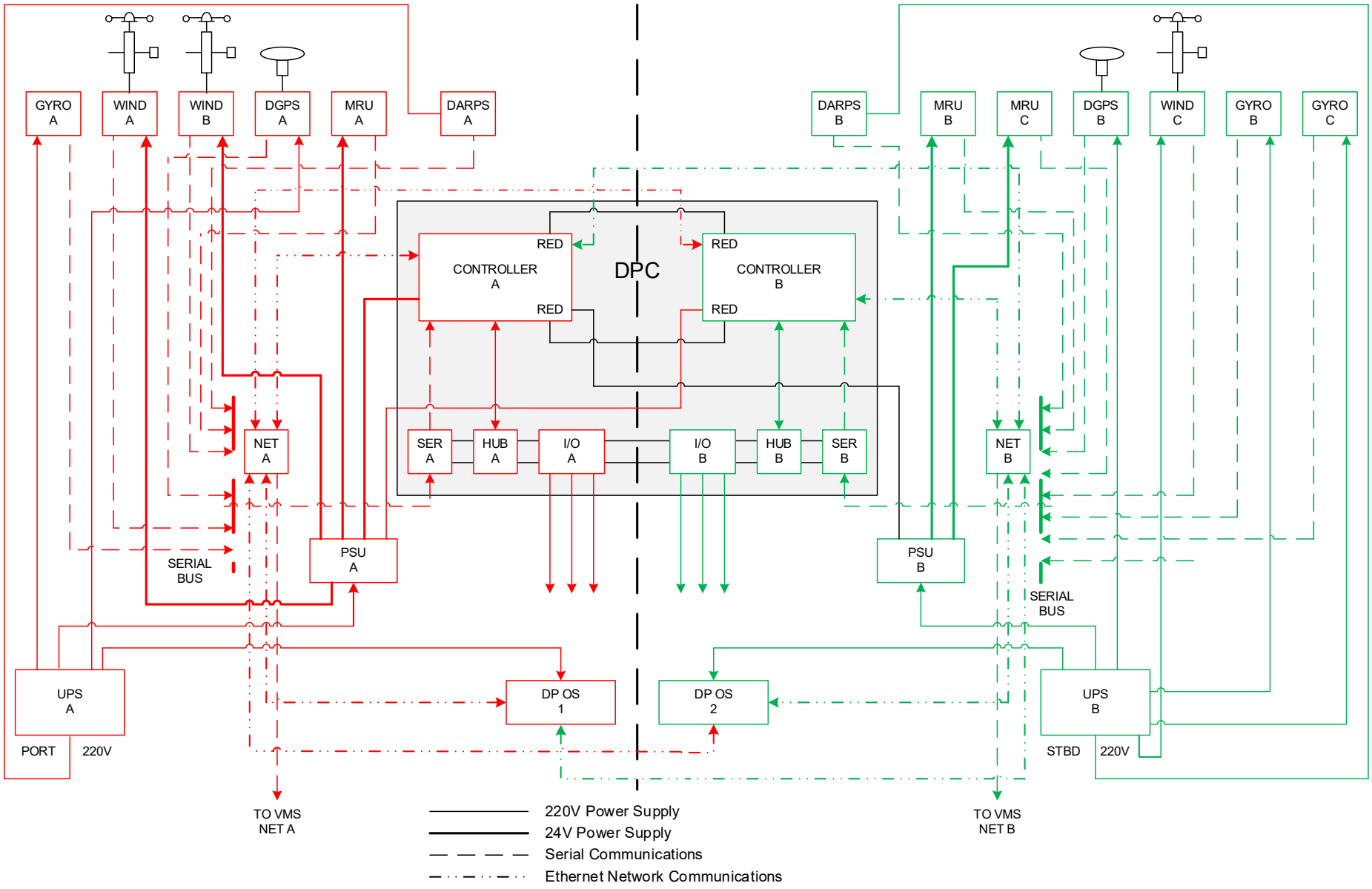
A1.15.1. The main engine cooling water system is independent as shown Appendix 1 - Figure 18.



Appendix 1 - Figure 18 ME Freshwater Cooling System

A1.16. DP CONTROL SYSTEMS

A1.16.1. Appendix 1 - Figure 19 shows the DP control system and its position references and sensors. Because standby redundancy is used to provide fault tolerance, a number of cross connections will be accepted in this system with the appropriate compensating provision to mitigate the risk of fault propagation. The rationale behind this is that the risk of a failed changeover to the standby controller is estimated to be higher than the risk from fault propagation (when properly mitigated).



Appendix 1 - Figure 19 DP Control Systems

APPENDIX 2. DIVERGENCE - LIST OF COMMON POINTS

A2.1. COMMONALITY IN MAJOR SYSTEMS

A2.1.1. The list of common points was extracted from the system sketches. There are no unmitigated common points other than seawater cooling system pipework which is considered to have a low risk of failure.

Colour Key	Meaning
	No Common Point
	Mitigated by Compensating Previsions
	Unmitigated but Considered Low Risk

Appendix 2 - Table 1 List of Common Points in Example 1

System	Nature of Common Point
110Vdc & 24Vdc control power	None
Fuel Systems DG & ME	None
Emergency MDO fuel systems	None
Lubricating Oil systems	Limited commonality in supplies to Lube Oil Transfer Pump power supplies - No direct connection
G1 to G4 FW cooling	None
Main Engine FW cooling Systems	None
Forward Freshwater Cooling System	None
Main SW cooling system (inc. Main engine)	Common Sea suction for Port Generations, common Sea Suction for Starboard Generators
Forward Seawater Cooling System	Common Sea Suction
Compressed air systems	Common but fail safe
Remote Valve Operating System	Common software and controllers but independent I/O – fail safe
DP Control System	Common Power supplies and I/O sharing references and sensors
Data Communication Networks	Commonality at each data consumer – Network storm protection

APPENDIX 3. ADHERENCE TO SEVEN PILLARS

A3.1. COMPARATOR TOOL

The comparator tool from MTS TECHOP (D-01 - Rev1 - Jan21) ADDRESSING C³EI² TO ELIMINATE SINGLE POINT FAILURES was used to produce a Heat Map for the Redundancy concept to assess the robustness of the design and its reliance on compensating provisions. Reference can be made to TECHOP (D-11 - Rev1 - Jan21) REDUNDANCY CONCEPT PHILOSOPHY DOCUMENT for further information on how the tool is used.

Appendix 3 - Table 1 Comparator Tool (INPUT)

Seven Pillars – Comparator			Independent Autonomy Independence Segregation	Common (Non-Independent) Closed Busties (Reliance on Protective Functions) Dual Feed (Reliance on Protection and ride-through) Reliance on Standby Start Reliance on Changeover Pipework (Reliance on protection against mechanical damage and performance attributes)		Remarks Percentage of common (non-independent) 'Yes' and 'No' entries in total DP system is an indicator of: · Reliance on active measure or exemption from consideration · Verification and validation burden
				Intention to Validate by Testing?		
System	Subsystem	Not Applicable	Yes	Yes	No	Percentage of Common (non-independent) 'No' entries in the total number of Common Systems is an indication of the robustness of the redundancy concept.
1. Select Not Applicable if necessary (✓) 2. Tick One Box in Each Row 3. Review Heatmap to check completion						
Marine Auxiliary Systems	Fuel MDO/HFO		✓			ME has independent power source
	Seawater Cooling			✓		Only main pipework is common
	Freshwater Cooling		✓			ME has independent power source
	Lubricating Oil			✓		Common system but robust measures in place to prevent contamination etc
	Service Air			✓		Compressed air consumers fail safe
	Starting Air			✓		Compressed air consumers fail safe

Seven Pillars – Comparator			Independent Autonomy Independence Segregation	Common (Non-Independent) Closed Busties (Reliance on Protective Functions) Dual Feed (Reliance on Protection and ride-through) Reliance on Standby Start Reliance on Changeover Pipework (Reliance on protection against mechanical damage and performance attributes)		Remarks Percentage of common (non-independent) 'Yes' and 'No' entries in total DP system is an indicator of: · Reliance on active measure or exemption from consideration · Verification and validation burden Percentage of Common (non-independent) 'No' entries in the total number of Common Systems is an indication of the robustness of the redundancy concept.
				Intention to Validate by Testing?		
System	Subsystem	Not Applicable	Yes	Yes	No	
1. Select Not Applicable if necessary (✓) 2. Tick One Box in Each Row 3. Review Heatmap to check completion						
Marine Auxiliary Systems	Instrument Air			✓		Compressed air consumers fail safe
	Combustion Air		✓			Independent from outside
	Ventilation			✓		Some commonality - Will be verified and validated
	HVAC			✓		Some commonality - Will be verified and validated
Power Generation	Engines		✓			All independent
	Engine Control Systems		✓			All independent
	Alternator		✓			All independent
	Governor		✓			All independent
	AVR		✓			All independent
	Protection Systems		✓			All independent
Power Distribution	Main Power Generation Level			✓		closed busties with comprehensive verification and validation
	Auxiliary Systems Power Distribution Level		✓			independent

Seven Pillars – Comparator			Independent Autonomy Independence Segregation	Common (Non-Independent) Closed Busties (Reliance on Protective Functions) Dual Feed (Reliance on Protection and ride-through) Reliance on Standby Start Reliance on Changeover Pipework (Reliance on protection against mechanical damage and performance attributes)		Remarks Percentage of common (non-independent) 'Yes' and 'No' entries in total DP system is an indicator of: · Reliance on active measure or exemption from consideration · Verification and validation burden Percentage of Common (non-independent) 'No' entries in the total number of Common Systems is an indication of the robustness of the redundancy concept.
				Intention to Validate by Testing?		
System	Subsystem	Not Applicable	Yes	Yes	No	
1. Select Not Applicable if necessary (✓) 2. Tick One Box in Each Row 3. Review Heatmap to check completion						
Power Distribution	Small Power and Lighting Level		✓			independent
	Control Power 110Vdc / 24Vdc		✓			independent
Power Management	Operator Stations		✓			Independent (common networks are considered separately)
	Field Stations		✓			independent (common networks are considered separately)
	Load Sharing		✓			Open busties no load sharing
	VAR Sharing (ac)		✓			
Energy Management	Battery Management Systems		✓			
	Battery / Capacitor Systems		✓			
	Energy		✓			
	Regeneration	✓				
	Dynamic Breaking	✓				

Seven Pillars – Comparator			Independent Autonomy Independence Segregation	Common (Non-Independent) Closed Busties (Reliance on Protective Functions) Dual Feed (Reliance on Protection and ride-through) Reliance on Standby Start Reliance on Changeover Pipework (Reliance on protection against mechanical damage and performance attributes)		Remarks Percentage of common (non-independent) 'Yes' and 'No' entries in total DP system is an indicator of: · Reliance on active measure or exemption from consideration · Verification and validation burden Percentage of Common (non-independent) 'No' entries in the total number of Common Systems is an indication of the robustness of the redundancy concept.
				Intention to Validate by Testing?		
System	Subsystem	Not Applicable	Yes	Yes	No	
1. Select Not Applicable if necessary (✓) 2. Tick One Box in Each Row 3. Review Heatmap to check completion						
Data Communication Networks	Networks			✓		common - Network storm and through-put will be carried out
	Network Power Supplies		✓			Independent
Thrusters	Thrust Magnitude Control		✓			Independent
	Thrust Direction Control		✓			Independent
	Thruster Control Mode Selection			✓		Still a common point but will be tested.
	E Stop		✓			Independent
DP Control System	Controllers			✓		Duty Standby C/O will be verified
	Operator Stations			✓		Operator stations are common to both controllers
	Power Supplies			✓		Power supplies are shared between A & B in standard delivery but will be tested
	UPS		✓			Independent UPS

Seven Pillars – Comparator			Independent Autonomy Independence Segregation	Common (Non-Independent) Closed Busties (Reliance on Protective Functions) Dual Feed (Reliance on Protection and ride-through) Reliance on Standby Start Reliance on Changeover Pipework (Reliance on protection against mechanical damage and performance attributes)		Remarks Percentage of common (non-independent) 'Yes' and 'No' entries in total DP system is an indicator of: · Reliance on active measure or exemption from consideration · Verification and validation burden Percentage of Common (non-independent) 'No' entries in the total number of Common Systems is an indication of the robustness of the redundancy concept.
				Intention to Validate by Testing?		
System	Subsystem	Not Applicable	Yes	Yes	No	
1. Select Not Applicable if necessary (✓) 2. Tick One Box in Each Row 3. Review Heatmap to check completion						
DP Control System	PRS			✓		Standard DP control system - will be tested
	Sensors			✓		Standard DP control system will be tested
Safety Systems	ESD	✓				
	F&G	✓				
	Fifi	✓				
	E Stop			✓		Common software but separate I/O - will be tested

A3.2. DP SYSTEM HEAT MAP

A3.2.1. Appendix 3 - Table 2 is the heat map produced by the comparator tool applied to the redundancy concept? Commentary on the results of the tool is provided in Section A3.3.

Appendix 3 - Table 2 Heat Map

DP System Heat Map

17								
Summary Score								
Fuel MDO/HFO								
Seawater Cooling								
Freshwater Cooling	6						11	
Lubricating Oil	**Summary Score**			3			**Summary Score**	
Service Air	Engines	5	4	**Summary Score**		5	Controllers	2
Starting Air	Engine Control Systems	**Summary Score**	**Summary Score**	Battery Management Systems		**Summary Score**	Operator Stations	**Summary Score**
Instrument Air	Alternator	Main Power Generation Level	Operator Stations	Battery / Capacitor Systems	3	Thrust Magnitude Control	Power Supplies	ESD
Combustion Air	Governor	Auxiliary Systems Power Distribution Level	Field Stations	Energy	**Summary Score**	Thrust Direction Control	UPS	F&G
Ventilation	AVR	Small Power and Lighting Level	Load Sharing	Regeneration	Networks	Thruster Control Mode Selection	PRS	Fifi
HVAC	Protection Systems	Control Power (110Vdc / 24Vdc)	VAR Sharing (ac)	Dynamic Breaking	Network Power Supplies	E Stop	Sensors	E Stop
Marine Auxiliary Systems	**Power Generation**	**Power Distribution**	**Power Management**	**Energy Management**	**Data Comm Networks**	**Thrusters**	**DP Control System**	**Safety Systems**

Total Score 56

Independence in Design	**60%**
Commonalities (Non-Independent) in design with intention to verify and validate	**40%**
Commonalities (Non-Independent) in design without intention to verify and validate	**0%**
Not Applicable	**5**
Total Completion	**100%**
Reliance on active mitigation, exemption from consideration and verification and validation burden	**41%**
Robustness of the redundancy concept (Analysis of common (non-independent) systems)	**100%**

A3.3. COMMENTRY HEAT MAP RESULTS

A3.3.1. Total Score: 56.

- 44 is a perfect score in a redundancy concept where all listed systems are applicable, and all systems are entirely independent.
- 132 indicates that every system has commonality and there is no intention to verify and validate the compensating provisions.
- This concept score 56 indicating a low level of commonality.

A3.3.2. Independence in design (60%): A figure of 60% indicates a moderate degree of commonality associated with lower risk commonality in system such as the main seawater because it is likely to be uneconomic and unnecessary to remove it.

A3.3.3. Commonalities in design with intention to verify and validate (40%): Indicated there are few commonalties of any kind in the design and all of them will be validated.

A3.3.4. Commonalities in design without intention to verify and validate (0%): The commitment to robust verification and validation.

A3.3.5. Not applicable (5): There are some additional ‘applicable; systems associated with the stored energy for the main engine, but they are all independent.

A3.3.6. Total completion (100%): The analyses was completed as indicted by the green banner in the tool output.

A3.3.7. **Reliance** on active mitigation, exemption, V&V burden (41%): This figure is commensurate with DP systems operating with closed busties are reliant on a wide range of protective functions.

A3.3.8. **Robustness** of the redundancy concept (100%): This high figure is entirely due to the commitment to comprehensibly verify and validate all compensating provisions.

APPENDIX 4. ALTERNATIVE MAIN SWITCHBOARD ARRANGEMENTS

A4.1. ADDITIONAL MAIN BUS CONFIGURATIONS

A4.1.1. The modular and autonomous nature of the AKA thruster and generator design means it can readily be adapted to different switchboard configurations.

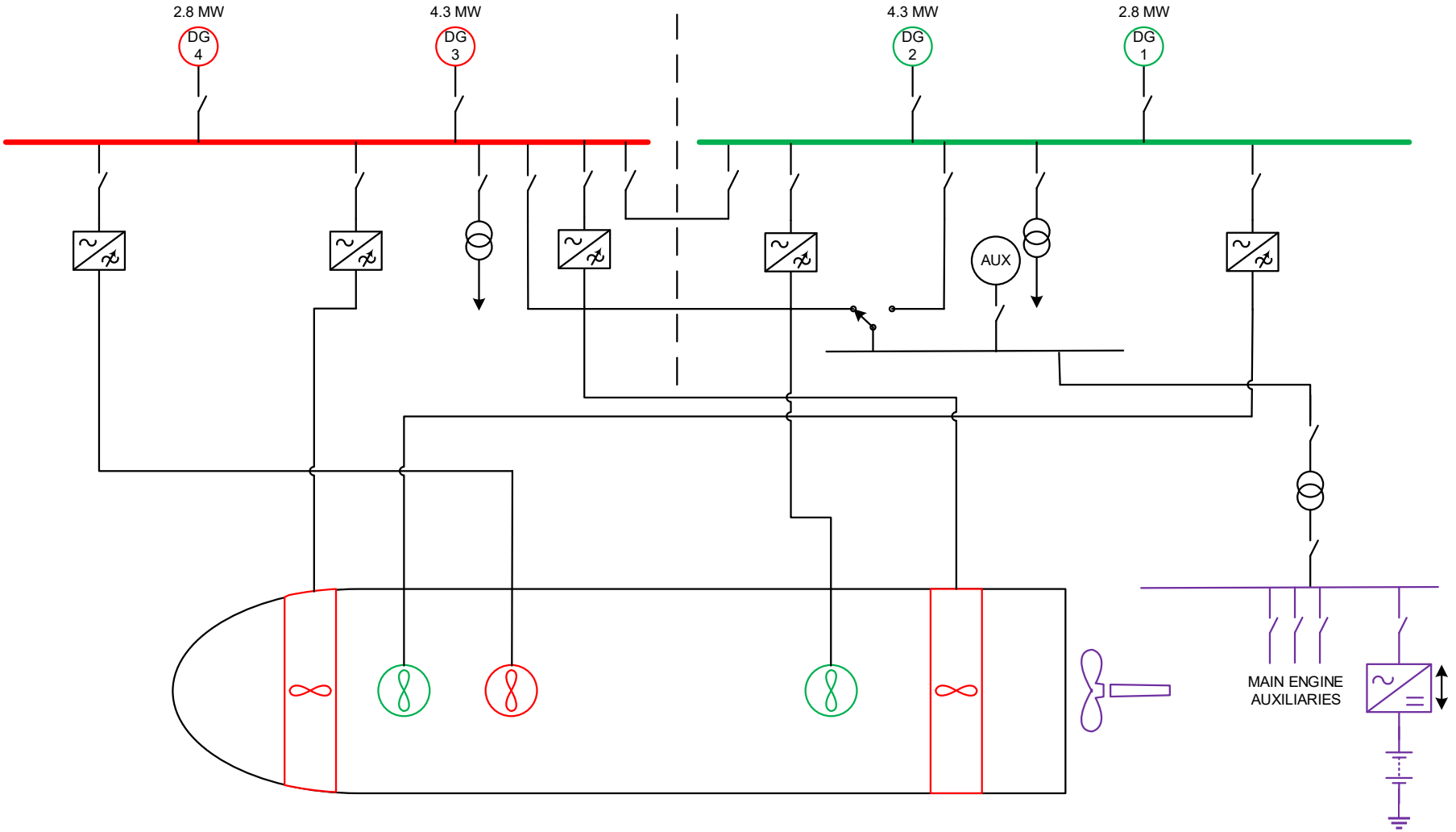
A4.1.2. A four-way split was used as the basis of the redundancy concept described in this RCPD. Alternative configurations for two-way split and three-way split are provided in the sections that follow.

A4.1.3. Although the post failure capability for Dynpos (AUTR) would change according to the bus bar configuration, the LIFE concept post failure capability would be determined by the capacity of the surviving generators and thrusters. Although the same thruster and main engine configuration has been retained. It is envisaged that there could be different numbers and ratings of generators.

A4.1.4. Changing the number of switchboards has little impact on the score obtained using the seven pillars comparator tool provided the same attention is paid to common points between redundant equipment groups.

A4.2. TWO-WAY SPLIT

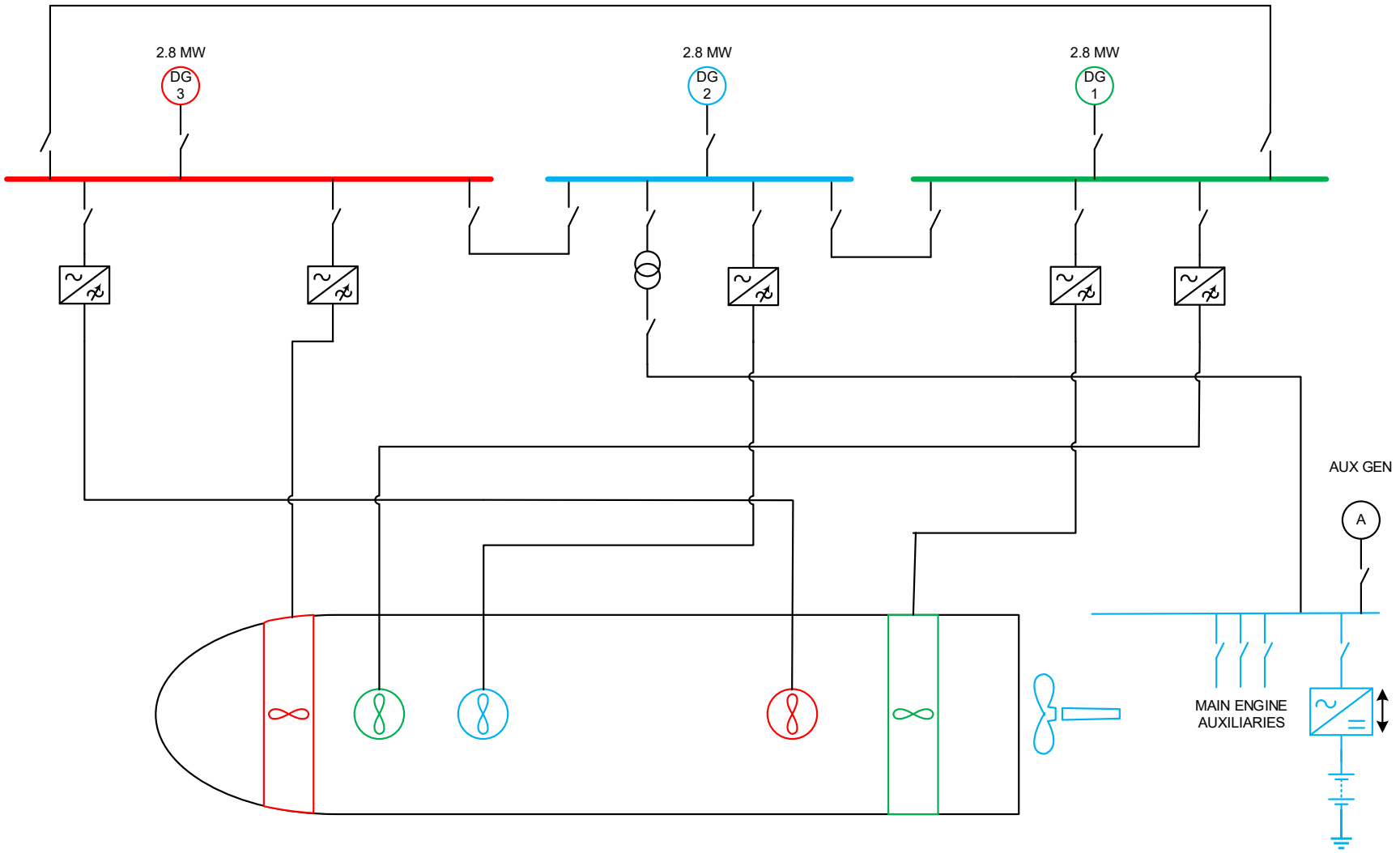
A4.2.1. Appendix 4 - Figure 1 shows an arrangement based on two main switchboards. All other aspects of the design remain the same including the thruster and main engine configuration. Although this appears to be based on three independent groups, everything except the main switchboards would be designed for five independent groups.



Appendix 4 - Figure 1 Two-way Split

A4.3. THREE-WAY SPLIT

A4.3.1. Appendix 4 - Figure 2 shows an arrangement based on three main switchboards. The same thruster and main engine configuration have been retained but the number of generators has been reduced from four (in two sizes) to three of the larger units. Alternatively, six smaller units may offer advantages. Although this appears to be based on four independent groups (three switchboards plus main engine, CPP & rudder), everything except the main switchboard bus sections would be designed for five independent groups.



Appendix 4 - Figure 2 Three-way Split