OCIMF

1970 50 2020

Dynamic Positioning Failure Mode Effects Analysis Assurance Framework

Risk-based Guidance

(First edition 2020)

Issued by the

Oil Companies International Marine Forum
29 Queen Anne's Gate
London SW1H 9BU
United Kingdom
Telephone: +44 (0)20 7654 1200
Email: enquiries@ocimf.org

www.ocimf.org

First edition 2020

The Oil Companies International Marine Forum (OCIMF)
Vision: A global marine industry that causes no harm to people or the environment.

Mission: To lead the global marine industry in the promotion of safe and environmentally responsible transportation of crude oil, oil products, petrochemicals and gas, and to drive the same values in the management of related offshore marine operations.

We do this by developing best practices in the design, construction and safe operation of tankers, barges and offshore vessels and their interfaces with terminals and considering human factors in everything we do.

Terms of Use

Contents

List of figures and tables

Glossary

The following are agreed definitions for terms used within this paper.

Aggressive Failure Modes Characterised by failures to an active state, such as failure of a speed regulator to the 'full fuel' condition or failure of an I/O terminal to logic high.

Annual DP trial A series of tests to verify the integrity of the DP System, conducted annually during a single period, as defined by the IMCA M190 publication.

Assurance document A standardised document used to facilitate an objective and effective assurance process. In the context of DP FMEAs, the information provided should be relevant to the vessel's redundancy concept. It can be a standalone document, or either incorporated into or an addendum to the FMEA.

Benign failure modes Failure to an inert or passive state. Examples include failure of an automatic voltage regulator to 'no excitation' or failure of an I/O terminal to logic low.

Common cause failure Failures that manifest on otherwise redundant DP equipment groups caused by external influences (including automatic interventions, such as ESD, or auto stops).

Common mode failure A subset of common cause failures in which redundant equipment groups fail in the same way.

Common points Elements that interface with or influence redundant groups and that can defeat the redundancy concept, including those presented by mission-specific equipment.

Compensating provisions Measures to prevent failure effects exceeding the Worst-Case Failure Design Intent (WCFDI). For example, protective functions or procedural barriers.

Comprehensive analysis Analysis is comprehensive when:

- All aspects of design and intended functionality are covered.
- The conclusions drawn from the analysis are unambiguous.
- The basis of the conclusion is clearly articulated and independently verifiable.
- Analysis and conclusions support the objectives of the testing required to satisfy verification and validation activities.
- The testing and analysis considered a comprehensive range of relevant failure modes including benign, aggressive and hidden failure modes.

Comprehensive documentation communicates the elements stipulated in this information paper effectively (with accompanying relevant sketches and tables). The analysis of each functional group should conclude on the 'end effect'. Documentation should be intuitive and facilitate the reader to arrive at the same conclusion as the author.

Configuration The vessel's allowed configuration(s), as defined, analysed and documented in the FMEA. Examples include:

- Bus configuration, configuration of all systems, including auxiliary systems, in line with the divisions in the redundancy concept.
- Control power supplies, fuel, cooling water isolation/crossover valves etc.

Vessels may have been provided with multiple DP system configurations to provide flexibility. Configurations that the vessel will operate in should be analysed and verified to be fault-tolerant, in accordance with the assigned equipment class.

Construction vessels All DP vessels that are not logistics vessels (engaged in pure platform supply operations) or MODUs.

Conventional fuels In marine applications, conventional fuels are typically Heavy Fuel Oil (HFO) and Marine Gas Oil (MGO).

Data centric Information that is derived from independently verifiable data (including those gathered and or recorded by digital means). See section 2.6 for more detail.

Design to test Systems designed to be verified by testing, and for which all types of testing necessary to verify the system's performance at its operational limits can be carried out without risk of equipment damage.

Digital survey application A digital tool where the complete, or specified parts of, the verification scope is incorporated and managed. The tool incorporates methods of gathering data that can be used as evidence for verification by a third party.

DP design philosophy A philosophy of how the redundancy objectives are achieved, along with the intended performance of the system to undertake its industrial mission, within the validated post-failure capability and WCFDI.

DP Shuttle Tankers (DPST) Trading tankers with DP systems onboard and with station-keeping functionality (such as heading, position, weathervane).

Failure Modes and Effect Analysis (FMEA) A systematic analysis to determine whether the redundant equipment groups in a DP system are independent of each other and fail to a safe condition. In this case, independence means not subject to a common cause of failure, and fail-safe* means not capable of causing a loss of position and/or heading.

**This is true when the vessel operates within its post-failure DP capability.*

Hidden failure A failure that is not immediately evident to operations and maintenance personnel.

Hybrid power Hybrid power systems use combinations of different technologies to produce power.

Incremental Tests According to IMCA M190, tests performed to verify the integrity of the DP system conducted over a defined period.

Independent Not subject to a common cause of failure. Sufficiently proven redundancy (with respect to the assigned equipment class) is generally considered to provide independence. Independence may be defined differently by other organisations.

Independent witness A suitably qualified and experienced individual removed from the day-to-day operational control of the vessel.

Independently verifiable The record of the test provided for review contains enough information for the verifier to independently conclude that the stated test result is accurate, that the test was properly executed, and that it met the test objective.

External Interfaces and influences Interfaces between the DP system and external systems, such as ESD, fire and gas, or tension (such as pipelay, moorings, cable lay, drilling equipment or draught sensors), failures of which may adversely affect the DP system, leading to exceedance of the WCFDI. The failure modes include failures of the external systems, sensors and interfaces, and should be analysed. External influences include electromagnetic interference, acoustic noise in the water column and dust or smoke drawing into the ventilation system.

Intuitive Easy to use and understand.

Peak shaving Providing peak power demand from an alternate power source. Typically, a battery or capacitor energy storage system is used to supply power peaks to allow diesel generators to operate at a relatively constant load.

Periodic (five-yearly DP trials) Periodic testing at intervals not exceeding five years to ensure full compliance with the applicable parts of the Guidelines, according to the IMO's MSC 645 and 1580.

Proving trials A series of tests carried out on DP to prove the conclusions of the DP System FMEA.

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

Redundancy concept The means by which single fault tolerance is achieved.

Redundancy Design Intent (RDI) The thrusters that are available to develop surge, sway and yaw, both in the intact condition and after worst-case single failure. Normally depicted in tabular format.

Redundancy Verification Table (RVT) Depiction of components (mechanical, electrical and control) of each functional group using a tabular format and colours to represent redundant groups. This makes it easier to identify common points.

Redundant equipment group Equipment groups which are capable of maintaining vessel position and heading (in limiting conditions) independently of other equipment groups either alone or in defined combinations.

Reliability The probability that an item can perform a required function under given conditions for a given time interval.

Remote testing Testing performed by crew or other owner's representative without the presence of (or remote witnessing by) a surveyor.

Remote witnessing Testing performed while being remotely witnessed by a surveyor through a live video and sound feed.

Resilience The ability of a system to withstand a failure and to continue operating following failure. This may include the ability to recover from a failure without suffering significant damage.

Rolling tests According to IMCA M190, tests on specified components or systems that have been identified as not being required annually, but which should be completed within a five-year period.

Separation design intent The physical separation of redundant equipment groups that constitutes the overall system design for a given configuration (DP equipment class 3).

Single failure propagation analysis A single failure propagation analysis is carried out to determine the failure effects and end effects of faults that may propagate from one redundant group to another through a common point. It may be necessary to use a formal FMEA table to properly document the range of failure modes and their effects. Suitable tables may be found in IEC 60812.

Sketches An intuitive way of communicating the functionality and the redundancy of a functional group, using a simplified diagram or drawing that captures relevant information pertinent to the redundancy concept, identifying common points and system boundaries.

Spinning reserve The reserve generating capacity in an electrical power system that can be available immediately without the need to connect additional generators. It can be provided by operating more generators than are required to supply the load, or by alternative power sources, such as battery energy storage systems.

State of Charge (SoC) The level of an electric battery's charge relative to its capacity.

State of Health (SoH) A measure of the condition of a battery compared to ideal conditions. A battery management system may use the divergence in one or more battery attributes to develop a figure of merit.

Supporting and Substantiating Documentation Technical drawings, studies and other information which support the analysis and conclusions required by this information paper.

Test on demand Systems with test-on-demand functionality have been specifically designed to be easy to test, so that initial and periodic verification and validation can be performed quickly and with limited use of resources.

Verification and validation processes Activities undertaken to ensure acceptance criteria have been met. Validation in this context is by testing and includes the effectiveness of compensating provisions.

Vessel Technical Operator (VTO) The owner or any other organisation, such as a vessel manager or bareboat charterer, that has assumed responsibility for the operation of the vessel, including all responsibilities as defined by the International Safety Management Code (ISM Code) or other legislative framework.

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

Worst-Case Failure Design Intent (WCFDI) The specified minimum DP system capabilities to be maintained following the WCF. The WCFDI is used as the basis of the design. This usually relates to the number of thrusters and generators that can simultaneously fail.

Abbreviations

ABS	American Bureau of Shipping
ASOG	Activity Specific Operating Guidelines
CAM	Critical Activity Mode
CW	Cooling Water
DGPS	Differential Global Positioning System
DP	Dynamic Positioning
DPC	Dynamic Positioning Controller
DNV	Det Norske Veritas
DNVGL	Det Norske Veritas Germanischer Lloyd
DP MODU	Dynamically Positioned Mobile Offshore Drilling Unit
DPST	DP Shuttle Tanker
ECR	Engine Control Room
EEP	Electrical Equipment Port
EES	Electrical Equipment Starboard
ESS	Energy Storage Systems
FMEA	Failure Mode and Effects Analysis
FS	Field Station
HPU	Hydraulic Power Unit
HV	High Voltage
IEC	International Electrotechnical Commission
IJS	Independent Joystick
IMCA	International Marine Contractors Association
IMO	International Maritime Organization
IRM	Inspection Repair Maintenance
LFI	Learning From Incidents
LNG	Liquid Natural Gas
LOP	Loss of Position
LTFW	Low Temperature Fresh Water
LV	Low Voltage
MRU	Motion Reference Unit
MSC	Maritime Safety Committee (IMO)
MTS	Marine Technology Society
NDU	Network Distribution Unit
OEM	Original Equipment Manufacturer
OVID	Offshore Vessel Inspection Database
OVMSA	Offshore Vessel Management Self-Assessment
PLC	Programable Logic Controller
PMS	Power Management System

PRS	Position Reference System
PSU	Power Supply Unit
RDI	Redundancy Design Intent
RP	Recommended Practice
RVT	Redundancy Verification Table
SoC	State of Charge
SOC	Statement of Compliance
SoH	State of Health
Stbd	Starboard
SWBD	Switchboard
TAM	Task Appropriate Mode
TCV	Temperature Control Valve
UKCS	United Kingdom Continental Shelf
UK HSE	United Kingdom Health and Safety Executive
UPS	Uninterruptable Power Supply
VMS	Vessel Management System
VTO	Vessel Technical Operator
WCF	Worst Case Failure
WCFDI	Worst Case Design Failure Intent
WSOG	Well-Specific Operating Guidelines

Bibliography

Classification Societies

Guidance notes on Failure Mode and Effects Analysis (FMEA) for classification (American Bureau of Shipping)

DNV-RP-E306: DNV GL recommended practice Dynamically Positioned Vessel Design Philosophy Guidelines (DNV GL)

DNV-RP-D102: DNV GL recommended practice for FMEA of redundant systems (DNV GL)

International Marine Contractors Association (IMCA)

M103 Guidelines for the Design and Operation of Dynamically Positioned Vessels

M166 Guidance on Failure Modes and Effects Analysis (FMEA) – Rev 2

M190 Guidance for Developing and Conducting DP Annual Trials Programmes – Rev 2

M247 Guidance on identifying DP system components and their failure modes (supersedes IMCA 04/04)

IMCA M250 Introduction to Battery Hybrid Systems for DP Vessels

Marine Technology Society (MTS)

DP Vessel Design Philosophy Guidelines (2019)

Technical and Operational Guidance (TECHOPS)

ODP 01(D): FMEA Testing (2013)

ODP 04(D): FMEA Gap Analysis (2013)

ODP 08(D): Annual DP Trials Gap Analysis (2014)

ODP 04(D): FMEA Gap Analysis

ODP 15(D): RP D102 FMEA Gap Analysis

ODP 17(D): Addressing C^3Ei^2 To Eliminate Single Point Failures (C^3Ei^2 – Cross-Connections, Commonality, External Interfaces and Influences)

MSC Circ.1580: Guidelines for vessels and units with dynamic positioning systems (International Maritime Organization (IMO))

Oil Companies International Marine Forum (OCIMF)

Dynamic Positioning Assurance Framework: Risk-based Guidance

Offshore Vessel Management Self-Assessment (OVMSA)

Offshore Vessel Inspection Questionnaire (OVIQ)

Offshore Vessel Particulars Questionnaire (OVPQ)

UK HSE RR195: Review of methods for demonstrating redundancy in dynamic positioning systems for the offshore industry (UK Health and Safety Executive and DNV)

1 Introduction

Failure Modes and Effects Analysis (FMEA) is a tool used by reliability engineers throughout the design process. Codes, standards and practices require dynamically positioned vessels to achieve single-fault tolerance by providing redundant systems. The objective of FMEA of redundant systems in a specified unit is to provide objective evidence of the required redundancy and fault tolerance.

Concerns about the safety and reliability of DP vessels were raised in 2002 following a series of DP incidents in the UK sector of the North Sea. These incidents brought the matter to the attention of the UK's Health and Safety Executive (UK HSE) Agency, which commissioned a study from Det Norske Veritas (DNV), suggesting that errors originated in vessel system design by shipyards, contractors and suppliers.

The UK HSE/DNV *Review of Methods for Demonstrating Redundancy in Dynamic Positioning Systems for the Offshore Industry* (2004) confirmed the above, concluding that vessel operators and managers were not always applying the guidance available and, in many cases, were not even aware of it. It also stated that some of the perceived weaknesses in the FMEA technique were due to the following:

- Review of FMEAs by Classification Societies is sometimes not thorough. Delayed FMEA submittal often makes it unnecessarily difficult for the Classification Society to deliver a quality approval. A lot of unnecessary difficulty can be avoided if the FMEA is started and shared/submitted to other parties at an earlier stage in the project.
- The three actual cases of loss of position through DP failure on the United Kingdom Continental Shelf (UKCS) in 2002 revealed deficiencies in the designed redundancy, which might have been detected by more thorough FMEAs and trials programmes, and therefore corrected.
- Lack of application of adequate FMEA expertise.
- Failure to follow a systematic procedure: weakness in the procedures for specifying, conducting and verifying the FMEA.
- The FMEA is commissioned too late to influence design.
- Failure to outline all operating modes when specifying the FMEA.

Various organisations took steps to address these identified weaknesses by:

- Improving the specification of what should be covered in an FMEA, including all the vessel's operating modes. IMCA 04/04: *Methods of Establishing the Safety and Reliability of DP Systems* has been superseded by IMCA M 247: *Guidance on identifying DP system components and their failure modes* and IMCA M 166: *Guidance on Failure Modes and Effects Analysis (FMEA) – Rev 2.*
- Updating and revising guidance documents where necessary and providing gap analysis tools to aid delivery of quality FMEAs. Some examples are:
  - MTS TECHOP_ODP_04_(D) (FMEA Gap Analysis).
  - MTS TECHOP_ODP_15_(D) (RP D102 FMEA Gap Analysis).
  - *Dynamic Positioning Assurance Framework, Risk-based guidance* (OCIMF; First edition 2006).
- Other examples by Classification Societies include:
  - The ABS *Guidance Notes on Failure Modes and Effects Analysis* (FMEA for classification, updated March 2018).
  - DNVGL's RP-D102: *FMEA of Redundant Systems.*
- Addressing competence through the IMCA DP Practitioner Accreditation Scheme (DP Trials and Assurance Practitioner).

1.1 Purpose and scope

Despite the above efforts, a significant number of FMEAs lack comprehensive analysis (revealed by subjecting a sample of FMEAs to an MTS DP FMEA gap analysis). The industry is not lacking guidance on how to produce comprehensive, quality FMEAs, but it is apparent that the guidance is not being implemented or adhered to consistently across the supply chain. This information paper addresses the assurance of DP FMEA quality by setting out how relevant information should be presented, in a prescribed format. Adherence to these requirements will be confirmed by OVID inspectors as part of the DP FMEA assurance processes commissioned by OCIMF members chartering DP vessels. The aim is that it will be used to strengthen and streamline the DP sections of OCIMF's Offshore Vessel Inspection Database (OVID)/Offshore Vessel Management Self-Assessment (OVMSA) process, including training of assurance providers.

This information paper does not prescribe the methodology for developing an FMEA. Instead, it prescribes a standardised format for presenting information relevant to the vessel's DP redundancy concept. This aims to facilitate an objective and effective assurance process. The information provided should be based on the vessel's verified design documentation.

This information paper aims to provide a pathway for effective assurance when ascertaining the quality of FMEAs by:

- Defining the important elements of a quality FMEA.
- Defining a standardised format for recording evidence confirming that the important elements of a quality FMEA have been addressed in the FMEA report under review. Examples of these elements include:
  - Common points.
  - Cross connections.
  - Fail-safe conditions.
  - Compensating provisions.
- Providing means for an assurance practitioner to confirm the validity of the evidence.

The second edition of the OCIMF publication *DP Assurance Framework: Risk-based Guidance* will be published in 2020, incorporating this information paper as an appendix.

1.2 Regulatory requirements

The International Maritime Organization (IMO)'s *Guidelines for Vessels and Units with Dynamic Positioning (DP) Systems* (Maritime Safety Committee (MSC) Circular 1580), defines FMEA and stipulates that vessels with DP Equipment Classes 2 and 3 should prove their DP redundancy concept through FMEA.

IMO MSC 1580 defines an FMEA in broad terms as: 'a systematic analysis of systems and subsystems to a level of detail that identifies all potential failure modes down to the appropriate subsystem level and their consequences.' IMO MSC 645, the predecessor of MSC 1580, made no reference to FMEA.

The FMEA should be comprehensive and identify the potential for hidden failures. MSC 1580 requires hidden failure monitoring to be provided in vessels with equipment classes 2 and 3.

1.3 History and use of FMEA in other industries

The origin of FMEA can be traced back to 1949 (US Armed Forces Military Procedures Document MIL-P-1629, Revised in 1980 as MIL-STD-1629A). This standard is no longer maintained. Aerospace and automotive industries adopted FMEA in the 1960s. In 1985 the International Electrotechnical Commission published International Standard 60812 *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*. It was revised in 2006 and 2018.

2 Methodology

2.1 Introduction

Codes, standards and practices applied to DP vessels are based on redundancy to ensure that no single failure leads to a loss of position and/or heading, for vessels assigned DP Equipment Classes 2 and 3. Loss of Position (LOP) incidents occur when the DP redundancy concept is defeated. Investigations have revealed that common points between redundant equipment groups are significant causal and contributory factors.

2.2 Failure Methods and Effects Analyses (FMEAs)

FMEAs are performed to:

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

FMEAs can be developed for redundant and non-redundant systems. FMEAs of redundant DP systems are focused on loss of position and/or heading, and can be defined as a systematic analysis to determine whether the redundant equipment groups in a DP system are independent of each other and fail to a safe condition. Where systems contain common points, the FMEA should clearly and unambiguously identify them. Such common points should be subject to a comprehensive single failure propagation analysis and draw conclusions about their impact on the redundancy concept. The effectiveness of compensating provisions and/or mitigations should be analysed, documented and validated by testing.

FMEAs should verify that Worst-Case Failure Design Intent (WCFDI) has been met, and the validation tests should prove that the severity of the Worst Case Failure (WCF) effects does not exceed the WCFDI. Failures with the potential to exceed the WCFDI should be addressed and mitigated by appropriate changes to the design. Vulnerabilities to failures that can propagate across redundant groups should be clearly identified so that appropriate corrective actions and compensating provisions are in place, including familiarising personnel with managing those vulnerabilities.

A comprehensive quality FMEA and proving trials program should achieve all the above objectives and provide relevant information in a transparent and intuitive manner, which facilitates:

- The development of:
  - DP annual trials programmes.
  - Periodic testing (a 5-yearly FMEA renewal trials program).
  - A DP operations manual.
  - Planned maintenance program/Inspection Repair Maintenance (IRM) activities.
  - Periodic verification of compensating provisions.
  - Effective decision support tools, such as Activity-Specific Operating Guidelines (ASOG) or Well-Specific Operating Guidelines (WSOG).
- Training of the vessel's operational and technical teams to ensure familiarisation.

2.3 Common failings in FMEAs

Common failings of FMEAs include:

- Lack of understanding and communication of the DP design philosophy, including system configuration (all systems and all configurations).
- Inadequate identification and assessment of common points because:
  - The system in which the common point occurred was not in the FMEA scope.
  - The system in which the common point occurred was part of the FMEA scope, but it was not identified.
  - The common point was identified, but the range of failure modes considered was not adequate or comprehensive.
- Lack of transparency:
  - Lack of understanding and communication of the redundancy design intent across all stakeholders and equipment providers.
  - Lack of understanding or inadequate overview of the system integration.
  - Lack of supporting or substantiating documents, such as Original Equipment Manufacturer (OEM) FMEAs or transient stability studies.
  - Lack of understanding and alignment with acceptance criteria at a system level (WCFDI).
- Inadequate identification of:
  - Hidden failures.
  - Configuration errors.
  - Acts of maloperation.
- Inadequate verification and validation, such as:
  - Lack of alignment between conclusions of the FMEA and FMEA proving trials.
  - Only benign failure modes are considered.
  - Lessons learned from incidents, such as LFIs and IMCA DP bulletins, are not incorporated.
  - Class approval may not prove that all relevant single failures or failure modes leading to a loss of position and/or heading have been adequately verified or addressed. Class rules for DP, in general, are intended to demonstrate achieving the objectives stated in the IMO MSC 645/1580 Guidelines for DP Equipment Class. The Classification Society rules continue to evolve based on insights gained from the experiences of DP vessels in service.

These failings contribute to masking the consequences of failures and thereby the potential risk and exposure from a loss of position and/or heading. A comprehensive quality FMEA should be able to identify key dependencies and residual vulnerabilities, which need to be managed effectively to achieve predictable outcomes.

2.3.1 Common points

It is well recognised and documented in industry guidance, codes, standards and practices that commonality spanning redundancy groups introduces potential failure pathways that could defeat the DP redundancy.

Common points cannot be eliminated completely in a redundant DP system. In some cases common points may be required to achieve specific objectives. Examples of common points are:

- Closed bus tie configuration for diesel electric power plant.
- Cross connected control power supplies, Uninteruptable power supplies, or commonality introduced by otherwise redundant networks.
- Some hybrid power designs.

Unnecessary common points should be avoided, by applying the principles of autonomy, independence and segregation. Designs that respect these principles can be more easily validated and verified, compared to highly integrated designs with many software and hardware dependencies.

Systems that incorporate the 'Design to Test' and 'Test on Demand' functionality bring efficiency to the validation and verification process.

If complexity is introduced into the design to achieve particular benefits, the verification and validation effort should match this complexity. The sophistication of the tools required to verify and validate a system is proportional to the complexity of the design.

Common points in a DP system also introduces additional assurance burden for the VTO, such as:

- Complexity of analysis, including single failure propagation analysis, verification and validation activities.
- Providing compensating provisions and proving their effectiveness (throughout the lifecycle of the vessel).
- Familiarisation and training of technical and operational teams.

2.3.2 Closed bus ties and cross-connections

The requirements for demonstrating the effectiveness of compensating provisions through comprehensive analysis, verification and validation testing should be well understood. Industry experience and guidance is available to draw upon. The requirements for demonstration of equivalent integrity of closed bus tie to that of open bus ties differ between Classification Societies, and continues to evolve. The following should be noted:

- MSC 1580 states that 'Bus-tie breakers should be open during equipment Class 3 Operations unless equivalent integrity of power operation can be accepted according to 3.1.4'. This shows recognition that operating with bus-tie breakers closed introduces a fault propagation path during DP operations. There is clear stipulation that failure in one system should never be transferred to the other redundant system. This is an expectation for systems with DP class 2 and 3 notation (single failure criteria does not include fire and/or flood events for DP class 2).
- When stipulated, end user/charterer's requirements should be met. Supporting and substantiating documentation, including the results of validation testing for charterer's requirements, should be available on board.

Typical end-user expectations include:

- Charterers may stipulate that the vessel be operated in open bus configuration. If so, all intended operating configurations should be analysed, verified and validated for their impact on the redundancy concept and post-failure DP capability.
- The scope of FMEAs and proving trials should include modes/configurations that vessel is capable of.
- The DP vessel should be operated within its post-failure capability in configurations that have been analysed and validated.
- Validation testing may be stipulated as a means of demonstrating equivalent integrity. The publication *MTS ODP_(D)_09: A method for proving fault ride through capability of DP vessels with HV power plant* provides general background information for vessel operators, class surveyors, power system vendors and shipyards involved in the process of proving fault ride-through capabilities of HV power plants on DP vessels.

2.3.3 Hybrid power

The advent of hybrid power systems using stored electrical energy sources can be used to achieve several objectives. For example:

- A reduction in greenhouse gas emissions, fuel consumption, and number of running generators, along with increased power plant efficiency.
- Meeting requirement for spinning reserve with stored electrical energy in lieu of energy traditionally provided by rotating sources.
- Load peak shaving with improved dynamic response to load applications.
- Improving resilience of the DP system (fault ride through capability for essential DP power consumers).

The objectives of installing hybrid power should be fully understood and clearly stated in the FMEA. Analysis should be comprehensive and demonstrate that the required functionality is available without compromising the DP system's redundancy concept.

The verification and validation process should focus on the essential elements of fault tolerant systems based on redundancy (performance, protection and detection).

There are too many permutations of hybrid power systems to consider every element in this information paper. Principally, hybrid solutions should be analysed in the DP system FMEA if they are included in the DP redundancy concept or if they are a common point of failure.

Verification and validation of hybrid systems

- **Performance**
  Hybrid power systems should be capable of their defined power delivery and energy storage capacity. This is essential if the hybrid system is to provide spinning reserve in lieu of diesel generators.

  Systems that are classified as hybrid due to the nature of fuel used to develop energy, such as dual fuel (Liquid Natural Gas (LNG)), should demonstrate through comprehensive analysis and validated testing that performance of the prime mover meets the design intent. Any divergences from the performance of conventional fuels should be clearly and unambiguously identified, along with affected performance attributes and post-failure capability criteria, in the FMEA and proving trials documents.

- **Protection**
  One of the most common uses of hybrid power is to provide spinning reserve more efficiently. Spinning reserve is a form of protection, and lack of spinning reserve is a potential hidden failure. Hybrid systems can also be used to enhance grid stability and provide voltage dip ride-through.

- **Detection**
  Hybrid power systems should have the means to detect degradation of performance on a continuous and periodic basis as required, including full power testing. This is true for any power generation system. For battery hybrid systems, alarms and indications for state of charge and state of health are Classification Society requirements. The IMO MSC.1/Circ. 1580, section 3.2.7 states that these measurements may be included in the DP control system consequence analysis.

2.4 Updates to the FMEA and five-yearly reviews/refreshes

The FMEA provides key input into the vessel's DP documentation, such as the DP operations manual (with all its checklists and decision support tools) and DP annual trials programme. Failure to keep it up to date can lead to these documents becoming inaccurate or irrelevant. This deterioration can negatively affect delivery of safe, reliable and predictable DP operations.

A systematic review of the DP FMEA and the associated trials programmes should be an ongoing process through the vessel's life cycle, and not restricted to the five-yearly review/refresh. Triggers for the review process are:

- Verification and validation to demonstrate compliance with relevant standards, codes and practices.
- Hardware or software modifications of the DP system that may affect the redundancy concept.
- Changes in operating procedures or deployment of the vessel on industrial missions that were not considered in the original design intent.
- Learnings from DP incidents (LFI), such as incidents that the Vessel Technical Operator (VTO) has experienced or been made aware of, or those published by industry bodies.

There should be positive confirmation that a review has taken place. Reviews should also be supported by documentation such as failure analysis, FMEA proving trials (when applicable), or evidence to confirm that the vessel's DP system and FMEA were reviewed for LFIs.

DP FMEAs that cannot be substantiated as outlined above are considered out of date.

Some Classification Societies may require that new revisions of FMEAs and FMEA test programmes are approved or reviewed.

2.5 Assurance of FMEAs

This information paper addresses the assurance of DP FMEA quality by stipulating requirements for pertinent information to be presented in a prescribed format, and providing a means to verify that:

- Common points between redundant DP equipment groups have been:
  - Identified.
  - Assessed.
  - Addressed by validated, verified and documented compensating provisions.
- The fail-safe condition of each redundant group has been considered. Fail-safe conditions are required to prevent drive-off (particularly for thrusters and their control systems). Information on the DP redundancy concept should be clearly and unambiguously presented in an intuitive and structured way, using tables and sketches. While this assurance process cannot physically confirm that the DP system FMEA is an accurate representation of the vessel, it does require that the sketches, tables and analysis are based on current, verified design documentation and not solely on the FMEA under review. Examples of the presentation format are provided in appendix A.

Focus areas from an assurance perspective are as follows:

- Supporting and substantiating documentation.
  The validity of the conclusions of a DP system FMEA rely on other engineering studies and documented test results (for example, a protection coordination study, harmonic analysis or test programs). These studies and programs should be referenced in the DP FMEA report. Substantiating and supporting documentation for the assurance document should be readily available on request and should include drawings that reflect the vessel's current state. The sketches and tables provided in the assurance document should be verified against the design documents of the vessel and not be solely derived from the FMEA. This applies to all documentation including that provided by OEMs.
- Common points.
  All common points between redundant DP equipment groups should be considered fault propagation paths with the potential to defeat the DP redundancy concept. Examples of common points include external inputs, such as:
  - Speed measurements.
  - Tension inputs.
  - Draught sensors.

  Mission-specific equipment is known to introduce common points and vulnerabilities with failure effects that exceed the WCFDI. The impact of mission-specific equipment failures on the DP system should be considered in the DP FMEA. Examples of mission specific equipment introducing common points include slip rings on cranes, or co-location of industrial mission equipment powered from different redundancy groups in a common space.
- Compensating provisions.
  The effects of fault propagation should be minimised or eliminated through compensating provisions. These should be applied to fault propagation paths, or to elements of the DP system that do not adopt a fail-safe condition. Such provisions may include protective functions, isolation strategies, alarms, monitoring, periodic testing or procedures to initiate operator intervention.

- Verification and validation processes.
  The assurance process requires evidence that verification and validation of the DP system has been carried out effectively. Verification is the process of confirming that the DP system has been built to the design. Validation is the process of confirming that the DP system achieves its design objectives by appropriate testing. The FMEA and proving trials represent a substantial part of the verification and validation processes for the DP system and its redundancy concept.

  The assurance document should include a statement of compliance from the VTO, to document self-assessment of the FMEA's quality. An example statement of compliance is in appendix B.

2.6 Assurance of periodic verification and validation

The FMEA should clearly identify the elements of performance, protection and detection that ensure that redundant equipment groups are independent and fail-safe.

MSC 1580 section 5 addresses surveys and testing as follows:

- A periodical testing at intervals not exceeding five years to ensure full compliance with the applicable parts of the guidelines. Testing should include a complete test of all systems and components and the ability to keep position after single failures associated with the assigned equipment class.
- The annual test (also called the annual DP trials) of all-important systems and components should be carried out to document the ability of the DP vessel to keep position after single failures associated with the assigned equipment class and to validate the DP FMEA and DP operations manual.
- The type of tests carried out and results should be recorded and kept on board.

2.6.1 Data-centric evidence

Evidence should be recorded and kept on board to confirm that periodic verification and validation processes are being applied as required and prove the conclusions of the DP system FMEA. All trial results, regardless of the method by which they were recorded, are to be data centric (derived from independently verifiable data, including those gathered and or recorded by digital means).

Digital records such as photos, or print-outs, do not meet the intent of data centricity as defined in this information paper, if they fail to:

- Provide the necessary details to corroborate test results, both local effect and end (global effect).
- Provide unambiguous evidence of meeting performance expectations.
- Measure relative performance of different sensors/systems.
- Provide data for triangulation (such as time, pressures, or temperatures).
- Do not facilitate independent verification.

Tests results recorded by manual means, such as handwritten notes, do not meet the intent of data centric as defined in this information paper unless supported by corroborating evidence. Test results which are limited to terms such as 'as expected', are not considered to provide corroborating evidence.

Applicable documentation from planned maintenance records may be used as evidence of achieving the test objectives provided it meets all other requirements of this information paper for such documentation. The recorded evidence should allow the OCIMF assurance provider to independently confirm the findings of the periodic verification and validation process. Periodic verification and validation test results that are not substantiated by data centricity and/or comprehensive documentation should not be submitted as evidence for assurance purposes.

From an assurance perspective it is emphasised that data centric evidence is essential. Such evidence should be capable of being verified independent of the person conducting the tests.

End user/charterer's standards/policies may preclude acceptance of non-data-centric results presented by remote testing as defined in this information paper. VTO's should engage with the end user and charterers and align on the acceptable methodology for periodic verification and assurance of the same.

2.6.2 Industry guidance on periodic verification and validation

Periodic verification and validation (reverification and revalidation) continue throughout the operational life of the DP vessel (including five-yearly periodical trials). The objective of such periodic verification and validation is to confirm that:

- The DP system remains in good order and responds to single failures as intended.
- The DP system complies with applicable codes, standards and practices.
- Lessons learned from incidents and new knowledge are addressed.

The assurance process requires evidence and confirmation that the FMEA has been subject to a review cycle (as detailed in section 2.4) and that all related documents, such as DP operations manuals and annual DP trials programmes, reflect the current revision of the FMEA.

Guidance on performing annual DP trials is provided in IMCA M190, which addresses and provides guidance on development, management and conduct of annual DP trials programmes.

The practice by some VTOs of performing 20% of the scope of the DP FMEA proving trial or DP annual trial programme every year does not meet the intent or objective of the annual DP trial as described by IMCA M190. End user/charterer's standards or policies may preclude acceptance of the above in lieu of the IMCA M190 annual DP trial. VTOs should confirm with the end user/charterer regarding acceptance of incremental tests in lieu of the annual DP trial, if the defined period of the incremental tests is specified to be within a year. The end user/charterer may elect to specify how the intent of the annual DP trial is achieved.

Terms such as digital survey application, remote testing (remote DP trials) and remote witnessing are also used by the industry. There is no unified accepted definition of these terms. Some Classification Societies accept that it is not essential for a surveyor to be physically on board, but do stipulate requirements for simultaneous remote witnessing when remote testing is conducted through live video and sound.

3 Potential impact of the assurance framework

The information to be presented in the standardised assurance document should already be available in the vessel's documentation, as it would have been essential to produce the FMEA. An example of an acceptable presentation format is provided in appendix A.

The process of providing the information in the prescribed standard format is estimated to take three to four working days if all relevant documentation is readily available and the assessment is carried out by a competent person.

The process of providing information in the standardised format may reveal gaps, inaccuracies, or lack of comprehensiveness in the existing FMEA. Additional staff skilled in FMEA processes may be needed to supplement the person carrying out the assurance. Gaps, if any, should be addressed by the VTO. Time-frames to close any gaps should be agreed between the VTO and end user/charterer. The requirements set out in this information paper should be included in the scope of work when commissioning a new FMEA (or a five-yearly refresh of an existing FMEA).

3.1 Assurance effort

A quality and comprehensive FMEA is an expectation for any DP vessel with DP equipment class 2 and 3, irrespective of the industrial mission the vessel is deployed for.

The assurance effort is summarised in the table below, which uses an intuitive heat map approach. The power plant and its configuration have been identified as a significant causal and contributory factors of DP incidents.

The heat map visually depicts the effort expected to be expended on the assurance of the FMEA based on the consequence of loss of position.

Assignment of the category LOW for logistics vessels does not necessarily mean that there are no consequences. LOP incidents on logistics vessels have resulted in collisions with the assets being supported. The FMEAs of logistics vessels are to be assured with the same level of diligence as any other vessel.

The term construction vessel means any DP vessel that is not a logistics vessel or a MODU.

The assurance effort and the verification and validation effort are also influenced by the nature of the barrier or compensating provision that is applied. Appendix E uses the familiar hierarchy of controls concept to provide guidance on the effectiveness, assurance and lifecycle burden that different types of compensating provisions impose.

The vessel's industrial mission, consequence of a loss of position and complexity of the power plant design or configuration dictates the effort in the assurance process and the technical depth of the assurance provider. For example, a vessel engaged in a logistics support function and operating in an open bus configuration needs less effort to assure fault tolerance than a logistics vessel operating in a closed bus configuration. In a similar vein, the consequence of a loss of position on a DP MODU will dictate a higher level of effort in the assurance process compared to a logistics vessel.

Assurance effort						
Vessel power plant design and configuration						
Vessel industrial mission and complexity	**MODU**	C	**HIGH**			
	Construction vessels and DPST	B	**MEDIUM**			
	Logistics vessels	A	**LOW**			
			1	2	3	4
	See section 3.1 for guidance on use of this table		**Open bus**		**Closed bus**	
			Conventional	**ESS**	**ESS (battery on thruster)**	**Conventional closed bus + ESS (battery on bus)**
			Assurance effort is low as redundant groups are separated and reliance on protective functions is minimal.	Assurance effort is relatively low as redundant groups are separated and reliance on protective functions is minimal. Batteries provide ride-through capabilities and an additional barrier to degradation of performance. Additional caution and precautions are necessary on single generator and battery configurations, which use cross-feeding.	Assurance effort is medium, as batteries providing station-keeping ride-through capabilities.	Highest assurance burden due to requirement to prove ride-through and protection. OR Assurance burden is high, as hybrid on bus provides ride-through capabilities and makes protection less critical; however, it has high requirements for verification and validation.

Table 3.1: *Guide to assurance effort*

4 Standardised format for presenting information

OCIMF has developed a standard format to facilitate assurance of the FMEA, proving trials and annual DP trials. Information relevant to the assurance of the DP redundancy concept should be documented in this standard format.

The focus of the standardised format is on common points, as they have been well established as a significant causal and contributory factor in DP incidents.

The intuitive presentation format uses a combination of set diagrams, tables and sketches to make such common points easily visible.

4.1 Set diagrams for redundancy concept

Set diagrams (commonly referred to as Venn diagrams) are an easy-to-understand and visually appealing way to represent the redundancy design intent within each functional group. These constitute:

- A unit (U) representing the system boundary of the functional group, or the entire vessel if the diagram is for the overall RDI.
- Circles or sets (A, B, C etc.), in different colours, representing each redundant group.
- A shaded area (A∩B) representing the points of intersection between redundant groups.
- The intersections (common points) represent potential fault propagation pathways and their effects should be proven to be acceptable, or compensating provisions made to mitigate their effects.

Set theory (Euler and Venn diagrams) is an intuitive way to represent the RDI of the functional groups. A Venn diagram is a specific type of Euler diagram, with an intersection representing every possible relationship between a given number of sets. However, due to the limitations of the graphical format, this methodology is only practical for DP redundancy concepts with four or fewer redundant groups. Euler diagrams use the concept of X-Groups to show similar information without such restrictions. Examples of the use of X-Groups are given in appendix A.

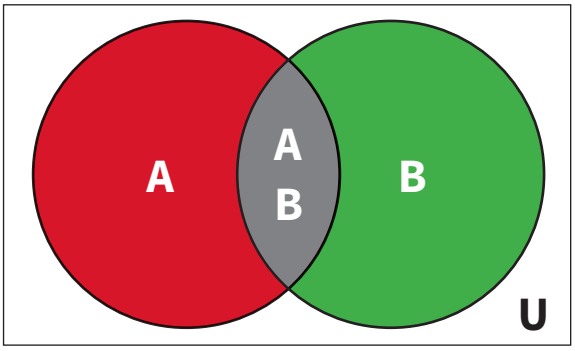

Figure 4.1: *Example of a Venn diagram*

4.2 Redundancy Verification Tables

The Redundancy Verification Table (RVT) is a tool that provides a systematic method to clearly identify and define components that:

- Belong solely to a particular redundancy group.
- Are common to more than one redundancy group.

These tables help to visually and unambiguously identify common points. An example of an RVT for a Low Temperature (LT) and High Temperature (HT) freshwater cooling system is shown in table 4.1 below and further examples are provided in appendix A.

LT and HT freshwater cooling system				
Subsystem	**Independent/ Common**	**Ref***	**Port**	**Starboard**
TCVs	Common	1	TV-2	TV-1
Heat exchangers	Independent		HE-2	HE-1
Pumps	Independent		PP-2	PP-1
Header tanks	Independent		HT-2	HT-1
LT pipework	Common	2	Pipework and isolation valve	
TCVs	Common	3	TV-4	TV-3
Heat exchangers	Independent		HE-4	HE-3
Pumps	Independent		PP-4	PP-3
Header tanks	Independent		HT-4	HT-3
HT pipework	Common	4	Pipework and isolation valve	

*The 'Ref' column provides an ID number that can be used to reference the discussion and analysis of common points in the single failure propagation analysis.

Table 4.1: *Redundancy Verification Table*

In an RVT, all of the identified components of the system are separated into their respective redundant groups based on:

- Their association with a particular redundant group, indicated by its column position.
- Their power supply assignment from a particular redundant group, indicated by its colour.

If the component is in the same colour as its column, then it is assessed as independent. Any other state identifies commonality, which may need further investigation. A white row spanning more than one column can also be used to indicate commonality.

The above example clearly identifies four common points in an LT and HT freshwater cooling system. As the other components are independent, only the identified commonalities are to be further analysed for failure modes and effects that have the potential to compromise the redundancy concept.

It is established practice to subdivide the DP system into its functional groups and analyse the redundancy within each functional group. Care should be taken in the analysis of common points that span redundant groups where the potential fault propagation path originates in one functional group and terminates in another. Further examples of sketches and RVTs for functional groups are provided in appendix C.

4.3 Single failure propagation analysis with FMEA worksheets

Once the common points have been identified using the RVT, they are analysed to ensure that the failure effects are acceptable or mitigated by appropriate compensating provisions. Each common point should have an analysis that demonstrates there are no unacceptable failure effects. The single failure propagation analysis may be accompanied by an FMEA worksheet where required. This worksheet should include:

- The component name/ID.
- Failure mode.
- Failure effect (local).
- Failure detection method.
- Effects on other subsystems.

- Failure causes.
- Compensating provision/barrier corrective action.
- End effect at unit level (also referred to as global effect).
- Severity of failure effect.
- Reference to test or verification.

IEC 60812 provides examples of suitable FMEA worksheets. Another example of a suitable worksheet is provided in appendix A. In simple cases (for example, a common point mitigated by closed isolation valves) a comprehensive narrative may be substituted for worksheets.

4.4 Sketches

Sketches are an intuitive way to communicate the functionality and the redundancy aspects of a functional group. They are an essential part of the assurance process. The main reason for using a simplified sketch is to capture information relevant to the redundancy concept, identifying common points and system boundaries. This information paper does not prescribe details such as which colours to use for the different redundancy groups. There will be variations in the sketches provided. This is acceptable provided the sketches are intuitive and convey the required information described above.

4.5 Other failure modes and considerations

A summary table for each subsystem should be provided to cover other failure categories, such as internal and external common-cause failures, hidden failures, configuration errors and acts of maloperations, where relevant.

4.6 Categorising and communicating the outcome of the auditor's assurance activity

The expectations of a standardised format should be communicated across the diverse stakeholders that influence the development and delivery of a comprehensive quality FMEA. For example, the OEM, integrators, assurance providers, or the VTO.

Auditors should be able to carry out and communicate the results effectively. The heat map described in appendix D allows auditors to communicate the outcome of the assurance process in a standard way and as objectively as possible. The end user/charterer should determine any follow-up action.

Providing guidance on the follow-up action is outside the scope of this information paper.

Appendix A: Examples of the presentation format

A1 Content of assurance document

This section explains what information should be included in an assurance document.

The DP system is subdivided into functional groups, each of which has a redundancy concept that aligns with the vessel's overall Redundancy Design Intent (RDI).A subsystem is not always divided into the same number of redundant DP equipment groups, but whatever physical division is used, the overall RDI should be satisfied.

The following information should be provided for the vessel:

- A table summarising limited, relevant vessel information.
- An overall RDI table.
- An overall Euler or Venn diagram. Venn or Euler diagrams may also be provided for individual systems.
- Configuration(s) of the DP system to subsystem level.

The FMEA and the assurance document should also include a section describing all intended technical system configurations and the corresponding WCFDIs, as well as a collected list of all prerequisites for achieving the RDIs, such as the set-up of subsystems.

The following information should be provided for each functional subsystem:

- A concise narrative describing how the subsystem functions.
- A colour coded sketch for each subsystem.
- A Redundancy Verification Table (RVT) for each subsystem (as per examples provided).
- A single failure propagation analysis of the common points.
- An FMEA (worksheet) table to analyse the common points where these are found. Such a table may only be required if the common point and its failure modes are so complex that more than a short paragraph is needed to describe all aspects of the failure effects and associated compensating provisions. Typically, a closed manual valve would require an FMEA table, but could be adequately addressed within the redundancy verification table and single failure propagation analysis. A closed bus tie, on the other hand, could require an extensive FMEA table with multiple entries.
- A table covering other failure categories, including:
  - Internal and external common-cause failures (if the format used does not address them in the RVT or FMEA worksheet).
  - Hidden failures.
  - Configuration errors.
  - Acts of maloperations.
- A statement for each subsystem that the redundant equipment groups are independent and fail-safe. (Independence and fail-safe may be achieved by compensating provisions)

Two examples below show the expected content and format of the assurance document. The examples are:

- Typical overall single line diagram of a DP construction vessel power system.
- Typical fuel oil system for a platform supply vessel.

Examples of acceptable variations in the presentation format for sketches and RVTs are also provided.

A2 Alternative graphical representations: shipyard drawings

The types of drawings produced by shipyards are not generally developed for the purpose of analysing and communicating the DP redundancy concept. Two examples of typical shipyard drawings are given in figures A2.1 Overall power system and A2.2 Fuel oil system. While the RDI may be more obvious from the Single Line Drawing (SLD), the fuel oil system is not presented in a way that makes the redundancy concept and its common points easily understandable.

These two drawings are the basis of the example analyses presented below. As a first step in developing an analysis of the DP system, it is helpful to develop simplified sketches based on the shipyard drawings that focus on highlighting the common points between redundant DP equipment groups. There will be variations in the way such sketches are developed, and this information paper does not intend to dictate the precise format to use, otherwise a beneficial innovation may be overlooked, or a limitation could be locked in.

Figures A2.3 and A2.4 show alternative ways of conveying the RDI. In this format, the redundancy groups are shaded zones surrounding the equipment belonging to a particular group. Common points are identified by the connections between the zones or by white areas within the zones.

Figures A2.5 and A2.6 show yet another presentation format. In these examples, the lines and symbols that represent the equipment are colour-coded according to the redundancy group to which they belong.

A third alternative for an acceptable presentation format is used in the full analysis of the power system and fuel oil systems that follows. In general, any format that uses similar methods to clearly and unambiguously identify the common points connecting redundant DP equipment groups is acceptable.

In some cases, the examples that follow conclude that compensating provisions are needed to achieved fault tolerance, such as isolation of power supplies to prevent fault transfer. The effect of these findings and implementation of the associated compensating provisions is that the original WCFDI is not achieved. This may require the vessel's post-failure DP capability to be reduced accordingly. However, it may be possible to develop other compensating provisions that allow the original RDI to be achieved.

In the assurance document, the WCFDI presented should already include the effect of all compensating provisions on the vessel's post-failure DP capability.

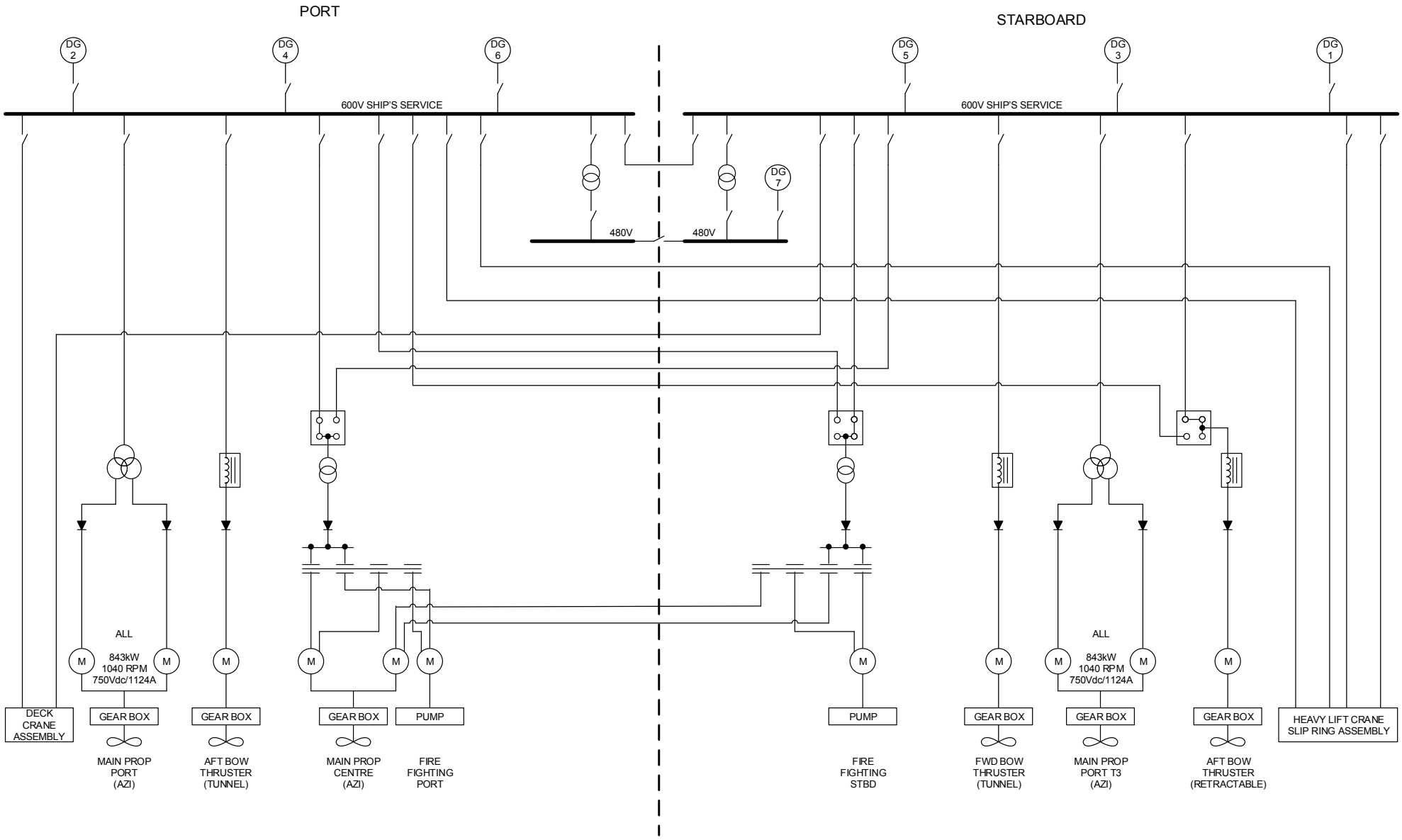

Figure A2.1: *Example shipyard-style drawing for a DP power system – construction vessel*

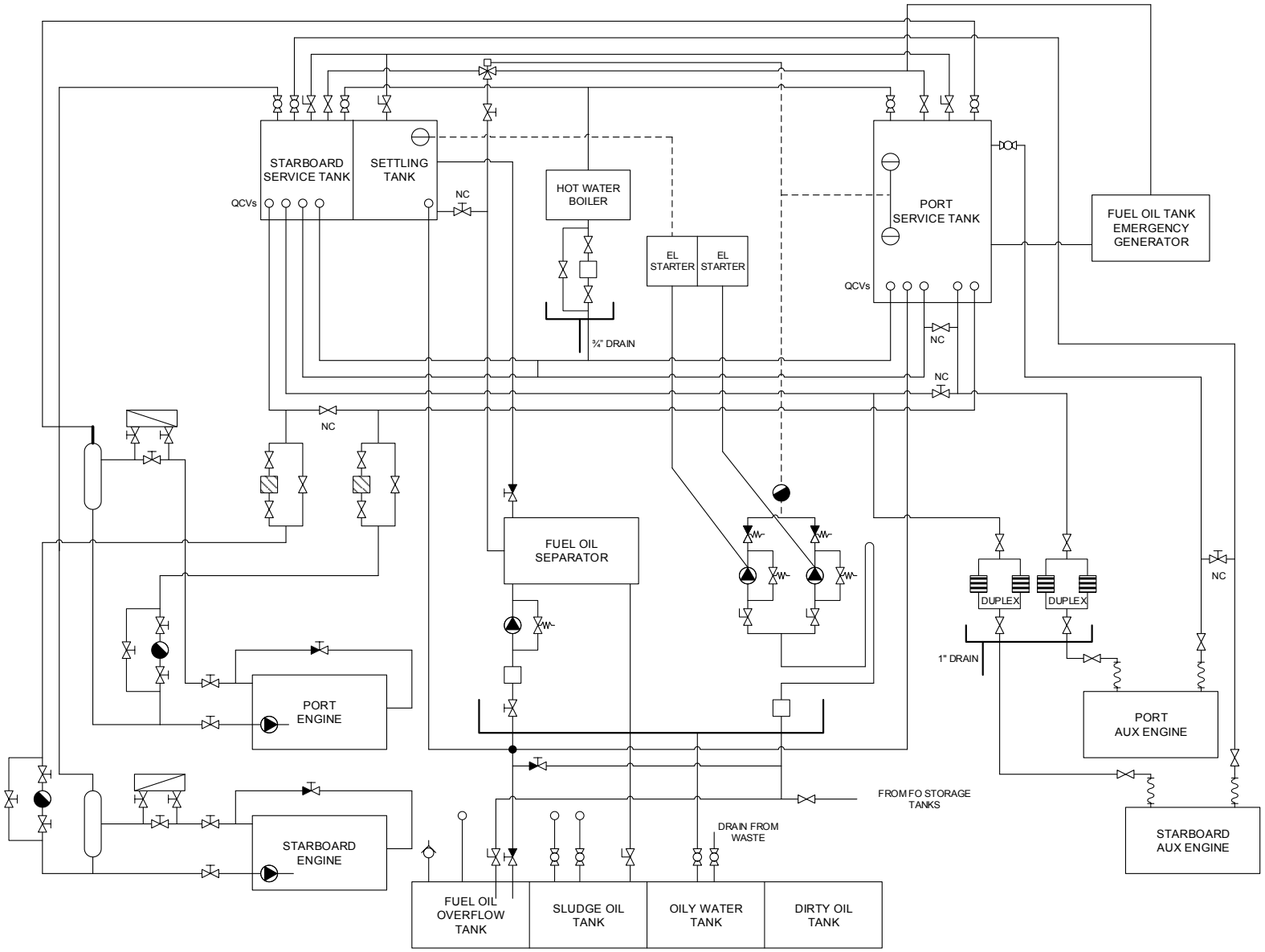

Figure A2.2: *Example shipyard style drawing for a fuel system – PSV*

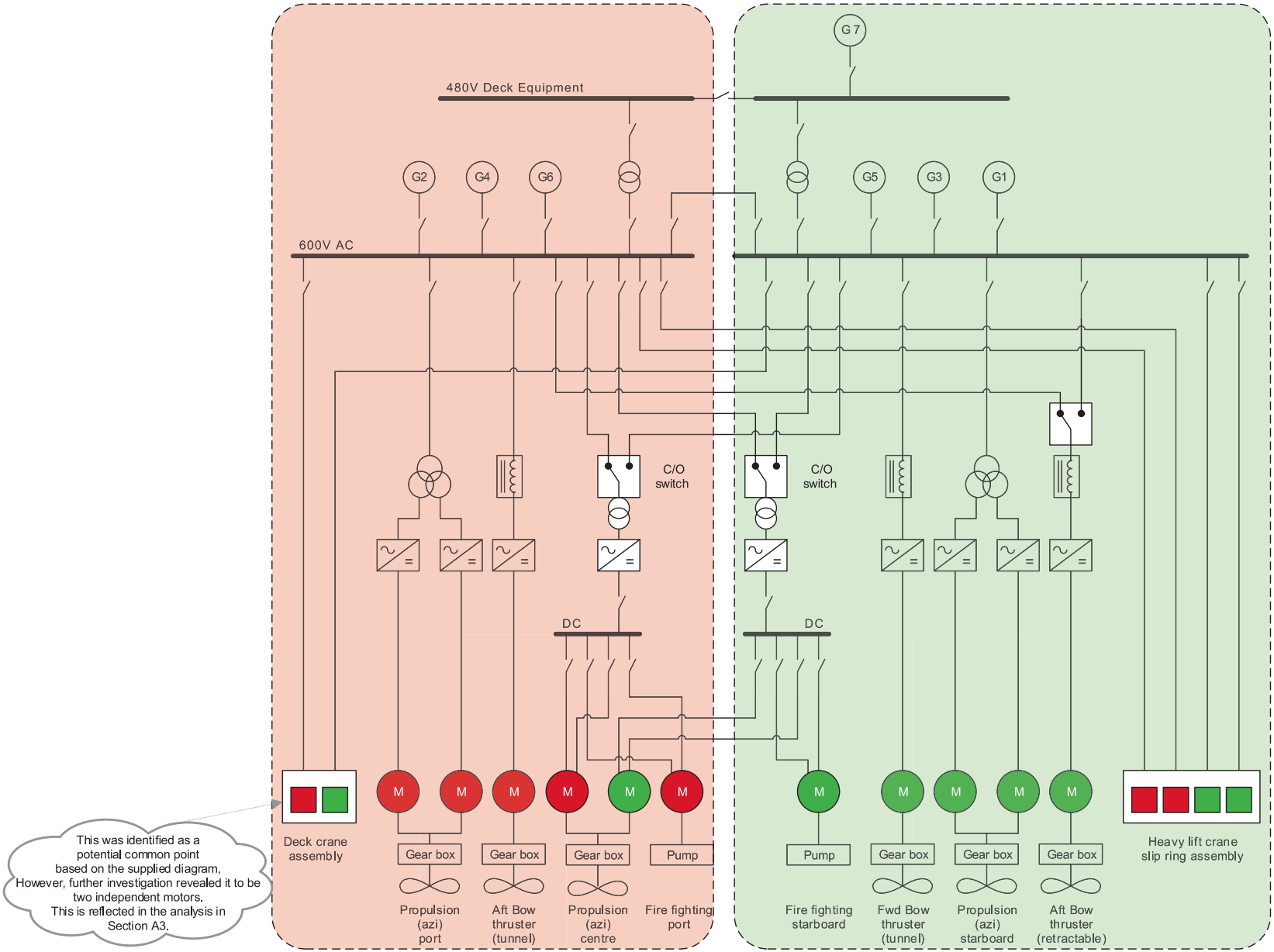

Figure A2.3: *Example sketch for a power system – construction vessel*

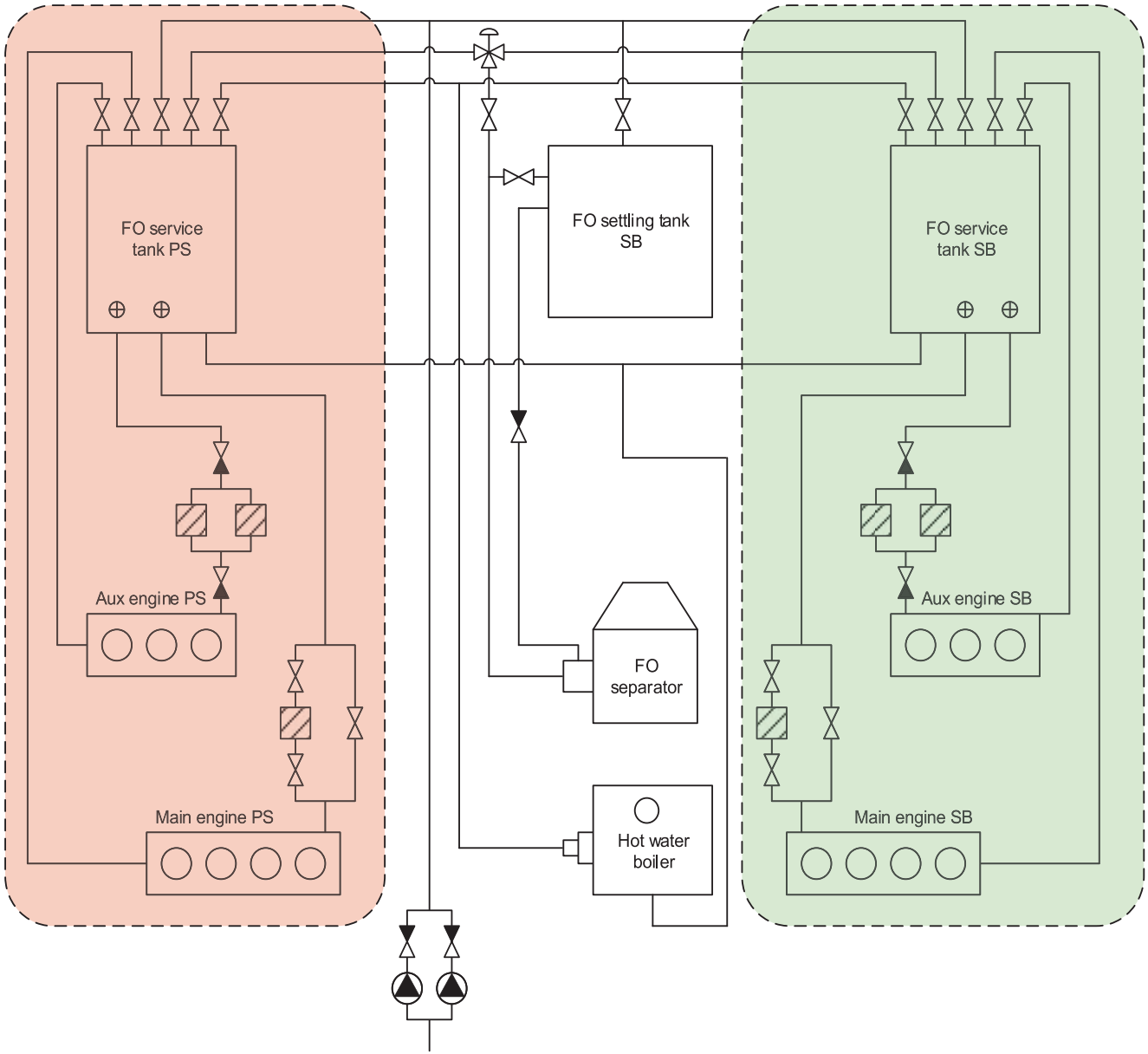

Figure A2.4: *Example sketch for a fuel system – PSV*

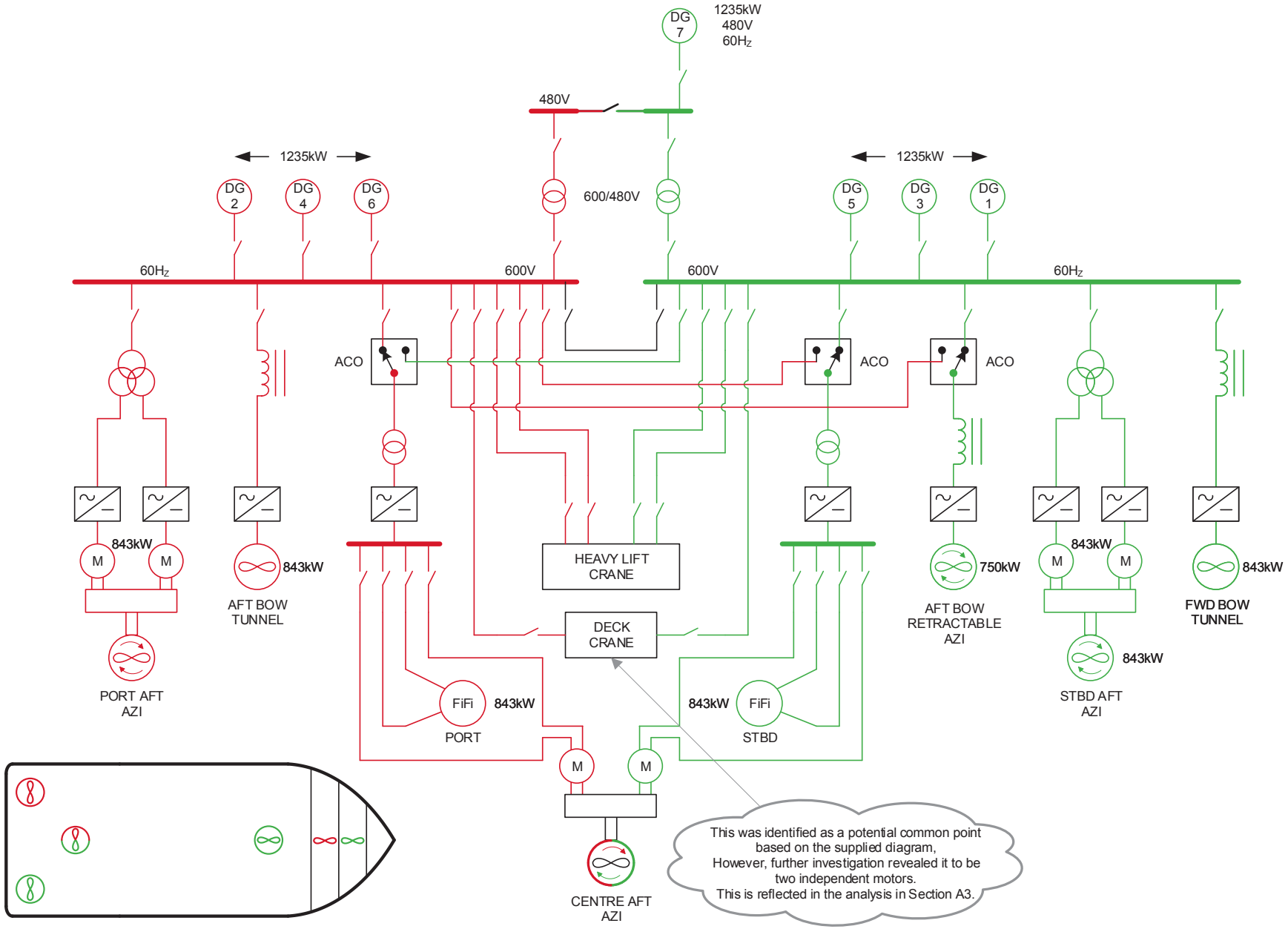

Figure A2.5: *Example sketch for a power system – construction vessel*

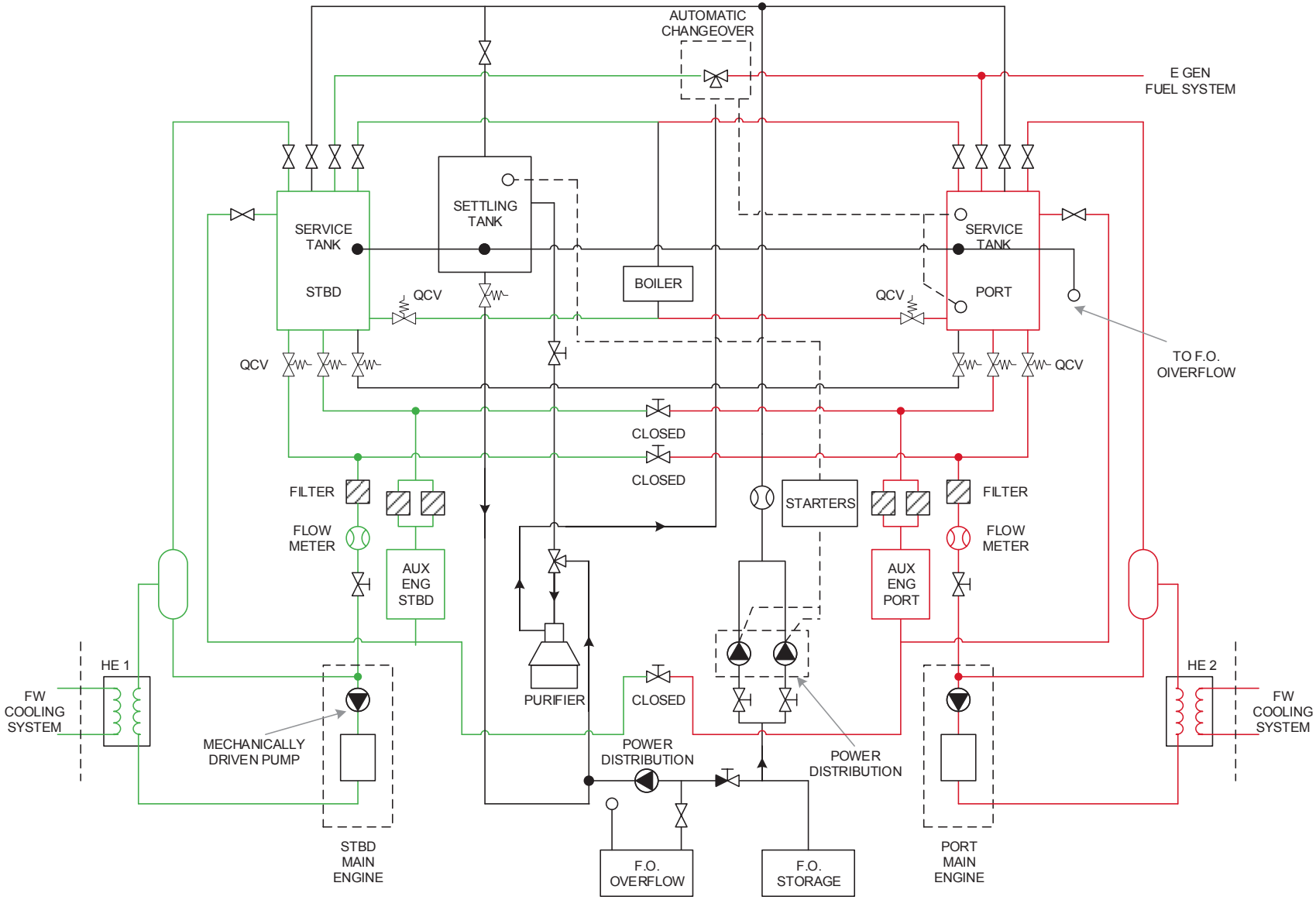

Figure A2.6: *Example sketch for a fuel system – PSV*

A3 Example power system analysis

A3.1 Vessel description

A3.1.1 The example vessel is a DP equipment class 2 multipurpose offshore construction vessel (fictious brand names have been used).

A3.1.2 The main particulars of the vessel are as follows:

- Length (overall): 145.00m
- Length (between perpendiculars): 133.80m
- Breadth moulded: 27.00m
- Depth moulded: 11.30m
- Draft (design): 7.50m

A3.1.3 Main power generation is provided by six ABC 8Q25Z marine diesel engines, each driving an EFG 1DC9999-8AL07-Z alternator through a flexible coupling. Each diesel generator produces 3 phase 600V AC and each is capable of delivering 1,235kW of electrical power at a lagging power factor of approximately 0.8.

A.3.1.4 One additional diesel generator of the same type (Diesel Generator No.7) is installed that can supply power to the deck equipment switchboards.

A.3.1.5 Three bow thrusters are installed in a common compartment forward: two HIJ QTT044 bow tunnel thrusters and one KLMN ATR9000 retractable azimuth thruster. The retractable azimuth thruster is installed aft of the two forward tunnel thrusters.

A.3.1.6 Three KLMN AT9040 FP propulsion azimuth thrusters are installed in a separate compartment aft.

A.3.1.7 All of the vessel's thrusters have fixed pitch propellers and are driven by variable speed electric motors through MOTORVAR SCRD converters.

A.3.1.8 The DP control system is an OPQ DP-2 dual redundant system, which includes two DPX 2 controller cabinets and two standard operator stations.

A.3.1.9 There is also a JSA1 independent joystick back-up system installed.

A.3.1.10 An iLIFT Lattice Boom Heavy Lift Crane is fitted aft at the main deck. The crane has main and auxiliary lifting systems and it is rated up to 1000T at a working radius of 28m.

A.3.1.11 An iLIFT Offshore Knuckle Jib Deck Crane is fitted aft at the starboard side of the main deck, forward. The crane has active heave compensation, main and auxiliary lifting systems and it is rated up to 150T at a working radius of 16m.

A3.2 Redundancy Design Intent

A.3.2.1 In order to meet the required single failure criteria, all systems supporting the DP system are separated into two redundant groups, as shown in table A3.1.

Condition	Positioning provided by	Type of redundancy
Normal operation (intact)	T1 T2 T3 T4 T5 T6	Standby redundancy T3 and one motor on T5 are required to change power supply
After single failure	T2 T3 T4 T5 or T1 T3 T5 T6	

Table A3.1: *Equipment in each Redundancy Design Intent*

The examples provided have been chosen to illustrate the treatment of common points and should not be considered viable or acceptable DP redundancy concepts. Post-failure DP capability based on power supply change-over is not accepted for inclusion in the DP control system consequence analysis by some Classification Societies.

A.3.2.2 For simplicity, each redundant group will be referred to either as the ‘port redundant group’ or the ‘starboard redundant group’. The main components of each redundant group are shown in table A3.2.

Port redundant group	Starboard redundant group
Diesel generator no.2	Diesel generator no.1
Diesel generator no.4	Diesel generator no.3
Diesel generator no.6	Diesel generator no.5
	Diesel generator no.7
Aft bow tunnel thruster (T2)	Forward bow tunnel thruster (T1)
Retractable bow azimuth thruster (T3)	Retractable bow azimuth thruster (T3)
Port propulsion azimuth thruster (T4)	Stbd propulsion azimuth thruster (T6)
Port 600V AC ship’s service switchboard	Stbd 600V AC ship’s service switchboard
Port 480V AC deck equipment switchboard	Stbd 480V AC deck equipment switchboard
Centre propulsion azimuth thruster (T5) motor 1	Centre propulsion azimuth thruster (T5) motor 2
Heavy lift crane slip ring assembly	
Deck crane assembly (port 300kW)	Deck crane assembly (stbd 300kW)

Table A3.2: *Equipment in each redundant DP equipment group*

A.3.2.3 The methodology of redundant equipment groups has been applied at a high level throughout the analysis to illustrate the overall RDI. This has also been applied for all relevant redundant component group auxiliary systems and subsystems.

Figure A3.1 represents the redundant groups within the overall boundary.

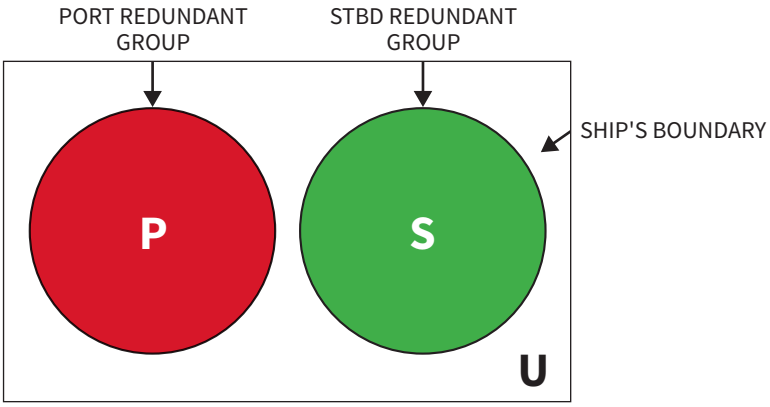

Figure A3.1: *Using set diagrams to describe redundant equipment groups*

Figure A3.2 represents the case where there are no connections between the port and starboard redundant groups.

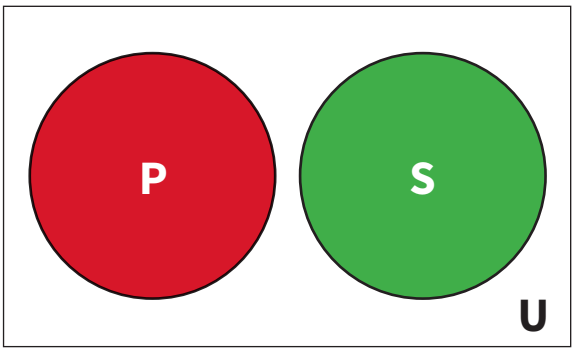

Figure A3.2: *Redundancy concept with no commonality*

Figure A3.3 represents a common component connection between port and starboard redundant groups.

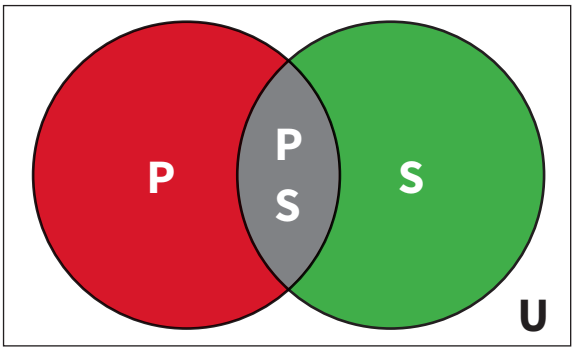

Figure A3.3: *Common component connection between port and starboard redundant groups*

Figure A3.4 represents an additional 'common component X' group that connects both redundant groups.

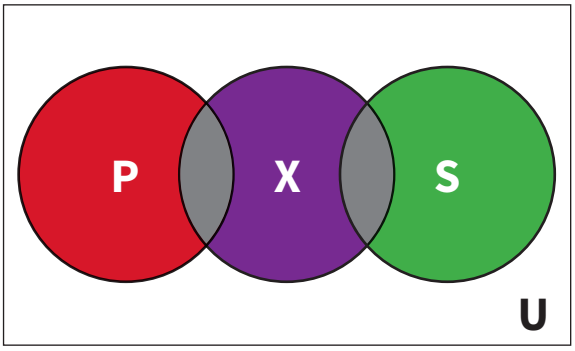

Figure A3.4: *Additional 'common component X' group that connects both redundant groups*

Legend

	Port redundant group
	Starboard redundant group
	Common points
	Common component X

A3.3 Main electrical power generation and distribution

A.3.3.1 The principle arrangements of the main switchboard and power distribution system are shown in figure A3.5.

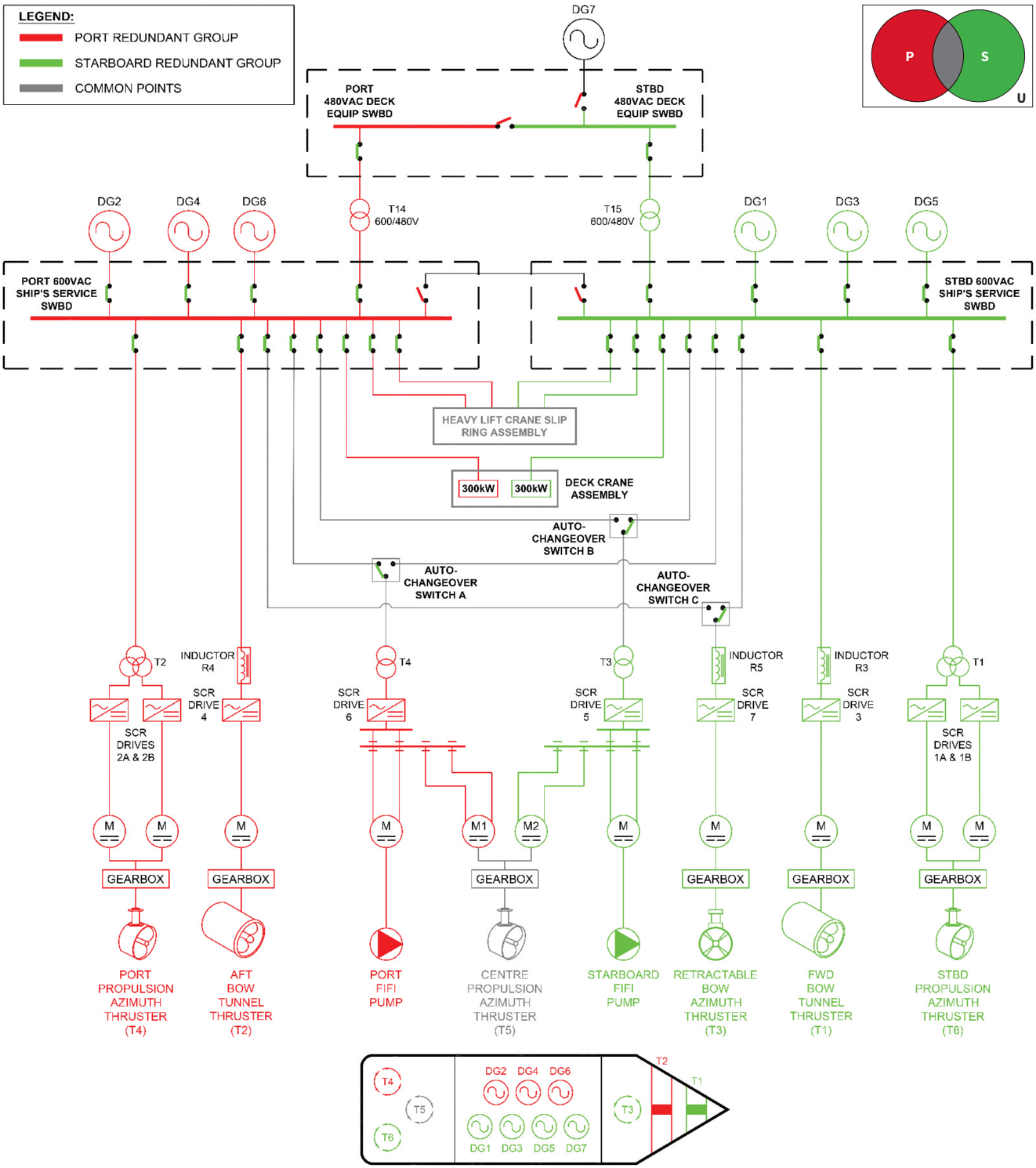

Figure A3.5: *Main switchboard and power distribution system*

A3.4 Main electrical power generation and distribution Redundancy Verification Table

A.3.4.1 The RVT for the main power distribution is shown in table A3.3.

Single Line Diagram				
Subsystem	**Independent/ Common**	**Ref**	**Port**	**Starboard**
Diesel generators	Independent		DG2, DG4 and DG6	DG1, DG3, DG5 and DG7
Automatic changeover switches	Common	1	Automatic changeover switches A, B and C	
Thrusters	Independent		T2, T4	T1, T6
	Common	2	T3 power supply	
	Common	3	T5 power supply and gearbox	
Ship's service switchboards (bus tie breakers open)	Independent		Port 600VAC	Stbd 600VAC
Deck equipment switchboards (bus tie breakers open)	Independent		Port 480VAC	Stbd 480VAC
Cranes	Common	4	Heavy lift crane slip ring assembly	
	Independent		Deck crane assembly port (300kW)	Deck crane assembly stbd (300kW)
FiFi pumps	Common	5	Port FiFi pump and starboard FiFi pump	

Table A3.3: *Redundancy Verification Table for main power distribution*

A3.5 Main electrical power generation and distribution single failure propagation analysis for common points

A.3.5.1 When an FMEA table is necessary to complete the single failure propagation analysis, each failure effect should be allocated a severity class that is defined in the FMEA. Examples of such classes are given below:

- **Severity Class 1 Catastrophic:** A major system failure that will cause total loss of DP capability regardless of any limitations placed on the vessel. This would mean a loss of position-keeping ability leading to an excursion, drive-off, or drift-off from position, resulting in possible asset loss or major environmental impact and which will lead to an emergency termination of the operation.
- **Severity Class 2 Critical:** A major system failure that will cause loss of DP capability if operational limitations are not adhered to. This will include loss of redundancy where a further failure may result in loss of position, requiring a controlled termination of the operation, such as loss of a main switchboard, and results in an extended shut-down of operations.
- **Severity Class 3 Serious:** A failure resulting in a temporary loss of availability or degradation of DP operational capability.
- **Severity Class 4 Minor:** A failure that has a negligible effect on the DP system or subsystem level, generally at component level, and results in minor unscheduled maintenance or repair.

A.3.5.2 The severity class allocation has been included within the FMEA worksheets for the common points in the main power distribution system. The single failure propagation analysis for the common points in the main power distribution system is included in A3.6 to A3.11.

A3.6 RVT Ref 1: Automatic changeover switch A, T5 supply port and port FiFi pump

A.3.6.1 Automatic changeover switch 'A' is supplied with power from the port 600V AC ship's service switchboard and is designed to supply power to the centre propulsion azimuth thruster (T5) motor 1 and the port FiFi pump through transformer T4 and SCR drive 6. In case the port 600V AC ship's service switchboard fails, it is designed to switch over the power supply to the starboard 600V AC ship's service switchboard.

A.3.6.1 An electrical fault, such as a short circuit at the changeover switch, transformer T4, a short circuit at the SCR drive 6 for T5 motor 1, or a failure at thruster T5 motor 1 or the port FiFi motor, causing high current or a power system disturbance, has the potential to cause loss of the port 600V AC ship's service switchboard.

A.3.6.2 There is no supporting or substantiating documentation to verify the discrimination and voltage transient ride-through capabilities of the power system when a short circuit occurs. There is no interlocking for automatic changeover switch A that prevents the automatic changeover function operating if a downstream fault occurs.

A.3.6.3 Therefore, following loss of the port 600V AC ship's service switchboard, due to a fault downstream of the automatic changeover switch A, the automatic changeover function may operate and transfer the fault to the starboard 600V AC ship's service switchboard. The result will be loss of both the port and starboard ship's service switchboards and loss of all the vessel's thrusters. This would exceed the WCFDI.

A.3.6.4 Compensating provisions to eliminate these failure modes are included in the FMEA worksheets (table A3.4, ref 1.1–1.5).

A3.7 RVT Ref 2: Automatic changeover switch B, T5 Stbd power supply and Stbd FiFi pump

A.3.7.1 Automatic changeover switch B is supplied with power from the starboard 600V AC ship's service switchboard and it is designed to supply power to the centre propulsion azimuth thruster (T5) motor 2 and the starboard FiFi pump through transformer T3 and SCR dive 5. In case the starboard 600V AC ship's service switchboard fails, it is designed to switch over the power supply to the port 600V AC ship's service switchboard.

A.3.7.1 A short circuit fault, at any of the following has the potential to result in loss of the starboard 600V AC ship's service switchboard.

- Changeover switch
- Transformer T3
- SCR drive 5 for T5 motor 2
- T5 motor 2
- Starboard FiFi motor

A.3.7.1 There is no supporting or substantiating documentation to verify the discrimination and voltage transient ride through capabilities of the power system if a short circuit occurs. There is no interlocking for automatic changeover switch B that would prevent the automatic changeover function operating if a downstream fault occurred. Therefore, following loss of the starboard 600V AC ship's service switchboard due to a fault downstream of the automatic changeover switch B, the automatic changeover function may operate and transfer the fault to the port 600V AC ship's service switchboard. The result will be loss of both starboard and port ship's service switchboards and loss of all the vessel's thrusters. This would exceed the WCFDI.

A.3.7.2 Compensating provisions to eliminate these failure modes are included in the FMEA worksheets (table A3.4, ref 1.6–1.10).

A3.8 RVT Ref 3: Automatic changeover switch C and T3 power supply

A.3.8.1 Automatic changeover switch C is supplied with power from the starboard 600V AC ship's service switchboard. It is designed to supply power to the retractable bow azimuth thruster T3 through inductor R5 and SCR drive 7 during DP operations. In case the starboard 600V AC ship's service switchboard fails, it is designed to switch over the power supply to the port 600V AC ship's service switchboard.

A.3.8.2 An electrical fault such as a short circuit at the changeover switch, inductor R5 or at the SCR drive 7 for the retractable bow azimuth thruster T3 has the potential to result in loss of the starboard 600V AC ship's service switchboard.

A.3.8.3 There is no supporting or substantiating documentation to verify the discrimination and voltage transient ride-through capabilities of the power system when a short circuit occurs. There is no interlocking for automatic changeover switch C that would prevent the automatic changeover function operating if a downstream fault occurs.

A.3.8.4 Therefore, following loss of the starboard 600V AC ship's service switchboard due to a fault downstream of automatic changeover switch 'C', the automatic changeover function may operate and transfer the fault to the port 600V AC ship's service switchboard. The result could be loss of both starboard and port ship's service switchboards and loss of all the vessel's thrusters. This effect would exceed the WCFDI.

A.3.8.5 The compensating provisions to eliminate these failure modes are included in the FMEA worksheets (table A3.4, ref 1.11–1.13).

A3.9 RVT Ref 4: T5 power gearbox

A.3.9.1 The centre propulsion azimuth thruster (T5) is driven by two electric motors. Motor 1 is supplied with power from the port 600V AC ship's service switchboard through transformer T4 and SCR drive 6. Motor 2 is supplied with power from the starboard 600V AC ship's service switchboard through transformer T3 and SCR drive 5.

A.3.9.2 Both motors will be simultaneously affected if the gearbox that they drive seizes. Seizure could be caused by a number of mechanical faults within the thruster gearbox. A propeller restriction, possibly caused by a rope, fishing net or similar object, would have similar effects. The effect of such failure would cause both motors to stall, meaning that they are overloaded, having reached their maximum torque. This will cause an electrical power system disturbance at both ship's service switchboards.

A.3.9.3 There is no supporting or substantiating documentation to verify the discrimination and transient conditions on the power system if this type of failure occurs. The result of this failure could be loss of both port and starboard ship's service switchboards and loss of all the vessel's thrusters. This would exceed the WCFDI.

A.3.9.4 The compensating provisions to eliminate these failure modes are included in the FMEA worksheets (table A3.4, ref 3.1–3.2).

A3.10 RVT Ref 5: Heavy lift crane slip ring assembly

A.3.10.1 Power to the vessel's heavy lift crane is supplied from both the port 600V AC ship's service switchboard and the starboard 600V AC ship's service switchboard through the cranes slip rings.

A.3.10.2 Both power supplies could be simultaneously affected by a failure at the sliprings, such as fluid leakage from the crane causing a short circuit between the two power supplies.

A.3.10.3 There is no supporting or substantiating documentation to verify the discrimination and voltage transient ride-through capabilities of the power system if a short circuit occurs. The result will be loss of both starboard and port ship's service switchboards and loss of all of the vessel's thrusters. This would exceed the WCFDI.

A.3.10.4 The compensating provision to eliminate this failure mode is included in the FMEA worksheet (table A3.4, ref 4).

A3.11 Main electrical power generation and distribution FMEA worksheets for common points

A.3.11.1 The effects of the individual failure modes relating to the common points in the main power distribution system are summarised in the FMEA worksheets (table A3.4).

A.3.11.2 The example FMEA worksheets in table A3.4 are provided to demonstrate presentation style and methodology. While their content is indicative of the type of failure modes that would be of concern, they are not intended to provide a comprehensive set of failure modes that can be applied to any changeover system or similar common point. Refer to other sources of engineering guidance on this subject if further information is required. A comprehensive range of failure modes should be considered in all cases.

Refs	Component(s)	Failure mode	Cause(s)	Local effect	Global effects (including subsystems)	Compensating provisions/barriers/ mitigation	Detection/ indication	Severity	Test reference
1.1 and 5	Automatic changeover switch A, T5 power supply port and port FiFi pump	Short circuit at changeover switch A	Insulation failure	Potential to damage changeover – auto changeover may operate unexpectedly	Supply CB at port ship's service switchboard trips DGs 2, 4 and 8 trip Loss of power to all consumers in port redundant group Auto C/O operates and fault transfers to starboard ship's switchboard DGs 1, 3 and 5 trip Loss of power to all consumers in starboard redundant group *Loss of all thrusters. Failure in excess of WCFDI.*	1 The automatic changeover function for automatic changeover switch A is to be inhibited. 2 The CB supplying power to automatic changeover switch A at the stbd ship's service switchboard is to be open and set to manual.	Supply protection operates to clear fault (on both supplies)	1	N/A due to compensating provision
1.2 and 5		Short circuit at transformer T4	Transformer T4 insulation/winding fault or water ingress	Potential damage to transformer			Various transformer and power system alarms	1	N/A due to compensating provision
1.3 and 5		Short circuit at the SCR Drive 6 for T5 Motor 1	Electrical component failure at drive/short circuit fault at drive or DC bus.	Potential damage to drive			Various drive and power system alarms	1	N/A due to compensating provisions
1.4 and 5		Failure at thruster T5 motor 1	T5 gearbox mechanical fault	Potential damage to thruster gearbox/ motor (seizure) T5 motor 1 draws excessive current from power source			Various motor and power system alarms	1	N/A due to compensating provisions
1.5 and 5		Port FiFi motor	Port FiFi pump mechanical fault.	Potential damage to pump gearbox/motor coupling (seizure). Port FiFi pump motor draws excessive current from power source.			Various motor and power system alarms	1	N/A due to compensating provisions

Table A3.4: *FMEA worksheets*

Refs	Component(s)	Failure mode	Cause(s)	Local effect	Global effects (including subsystems)	Compensating provisions/barriers/ mitigation	Detection/ indication	Severity	Test reference
1.6 and 5	Automatic changeover switch B, T5 power supply stbd and stbd FiFi pump	Short circuit at changeover switch B	Insulation failure	Potential to damage changeover – auto changeover may operate spuriously	Supply CB at stbd ship's service switchboard trips DGs 1, 3 and 5 trip Loss of power to all consumers in starboard redundant group Auto C/O operates and fault transfers to port ship's switchboard DGs 2, 4 and 6 trip Loss of power to all consumers in port redundant group *Loss of all thrusters. Failure in excess of WCFDI.*	1 The automatic changeover function for automatic changeover switch B is to be inhibited. 2 The CB supplying power to automatic changeover switch B at the port ship's service switchboard is to be open and set to manual.	Supply protection operates to clear fault (on both supplies)	1	N/A due to compensating provision
1.7 and 5		Short circuit at transformer T3	Transformer T3 insulation/winding fault or water ingress	Potential damage to transformer			Various transformer and power system alarms	1	N/A due to compensating provisions
1.8 and 5		Short circuit at the SCR drive 5 for T5 motor 2	Electrical component failure at drive/short circuit fault at drive or DC bus	Potential damage to drive			Various drive and power system alarms	1	N/A due to compensating provisions
1.9 and 5		Failure at thruster T5 motor 2	T5 gearbox mechanical fault	Potential damage to thruster gearbox/ motor (seizure) T5 motor 2 draws excessive current from power source			Various motor and power system alarms	1	N/A due to compensating provisions
1.10 and 5		Stbd FiFi motor	Stbd FiFi pump mechanical fault	Potential damage to pump gearbox/motor coupling (seizure) Stbd FiFi pump motor draws excessive current from power source			Various motor and power system alarms	1	N/A due to compensating provisions

Table A3.4: *FMEA worksheets*

Refs	Component(s)	Failure mode	Cause(s)	Local effect	Global effects (including subsystems)	Compensating provisions/barriers/ mitigation	Detection/ indication	Severity	Test reference
1.11 and 2	Automatic changeover switch C and T3 power supply	Short circuit at changeover switch C	Insulation failure	Potential to damage changeover – auto changeover may operate spuriously	Supply CB at starboard ship's service switchboard trips DGs 1, 3 and 5 trip Loss of power to all consumers in starboard redundant group Auto C/O operates and fault transfers to port ship's switchboard DGs 2, 4 and 6 trip Loss of power to all consumers in port redundant group. *Loss of all thrusters. Failure in excess of WCFDI.*	1 The automatic changeover function for automatic changeover switch C is to be inhibited. 2 The CB supplying power to automatic changeover switch C at the port ship's service switchboard is to be open and set to manual.	Supply protection operates to clear fault (on both supplies)	1	N/A due to compensating provision
1.12 and 2		Short circuit at inductor R5	Inductor R5 insulation/winding fault or water ingress	Potential damage to transformer			Various inductor and power system alarms.	1	N/A due to compensating provisions
1.13 and 2		Short circuit at the SCR drive 7 for T3	Electrical component failure at drive/short circuit fault at drive or DC bus	Potential damage to drive			Various drive and power system alarms	1	N/A due to compensating provisions

Table A3.4: *FMEA worksheets*

Refs	Component(s)	Failure mode	Cause(s)	Local effect	Global effects (including subsystems)	Compensating provisions/barriers/ mitigation	Detection/ indication	Severity	Test reference
3.1	T5 gearbox	Gearbox/motor coupling seizure	Gearbox mechanical component failure	Both thruster motors stall at maximum torque	DGs 1, 3 and 5 trip Loss of power to all consumers in starboard redundant group DGs 2, 4 and 6 trip Loss of power to all consumers in port redundant group *Loss of all thrusters. Failure in excess of WCFDI*	1 The CB supplying power to automatic changeover switch B at the stbd ship's service switchboard is to be open and set to manual. 2 See also compensating provisions for Refs 1.5–1.8. T5 motor 2 will therefore be isolated and thruster T5 will only be supplied with power from the port ship's service switchboard via SCR drive 6/motor 1.	Various drive and power system alarms	1	N/A due to compensating provisions
3.2			Propeller restriction						
4	Heavy lift crane slip ring assembly	Short circuit at crane slip rings	Fluid leakage from crane	Loss of power to heavy lift crane. Load suspended if in use.	DGs 1, 3 and 5 trip Loss of power to all consumers in starboard redundant group DGs 2, 4 and 6 trip Loss of power to all consumers in port redundant group *Loss of all thrusters. Failure in excess of WCFDI*	One power supply to the heavy lift crane should be isolated; either the power supply from the port ship's service switchboard or the power supply from the stbd ship's service switchboard	Various power system alarms	1	N/A due to compensating provision

Table A3.4: *FMEA worksheets*

A3.12 Main electrical power generation and distribution conclusions

A.3.12.1 The FMEA of the main power generation and distribution systems are concluded in table A3.5, considering implementation of the compensating provisions identified within the FMEA worksheets.

Main electrical power generation and distribution
Worst case single failure
Loss of one main switchboard section in one redundant group (considering compensating provisions).
Possible causes of the worst-case single failure (failure modes)
1 Failure of port 600V AC ship's service switchboard section. 2 Failure of port 480V AC deck equipment switchboard section. 3 Failure of starboard 600V AC ship's service switchboard section. 4 Failure of starboard 480V AC deck equipment switchboard section. 5 Diesel generator speed of voltage control fault.
Potential hidden failures
None.
Common cause failures
None.
Common mode failures (internal and external)
None.
Cross connections – common group X
Interconnecting bus tie breakers between 600V ship's service switchboards – normally open.
Cross connections – common component group
1 Interconnecting bus tie breaker between the port and starboard 480V AC deck equipment switchboards – normally open during DP operations. 2 T5 motor 1 power supply arrangement/auto changeover switch A. 3 T5 motor 2 power supply arrangement/auto changeover switch B. 4 T3 power supply arrangement/auto changeover switch C. 5 T5 thruster gearbox. 6 Heavy lift crane slip ring assembly. 7 T5 thruster gearbox.
External interfaces
1 Main switchboard control voltages. 2 Power Management System (PMS). 3 Alarm and monitoring system.
Configuration errors
Failure to implement compensating provisions identified on FMEA worksheets.
Acts of maloperation
There should be none, provided CAM/ASOG are followed. Inadvertent operation of the changeovers no longer possible.
Mitigations against failure modes
See FMEA worksheets.

Table A3.5: *FMEA of main power generation and distribution systems*

A.3.12.2 The redundant DP equipment groups are considered independent and fail-safe when the compensating provision are applied.

A4 Example fuel oil system analysis

A4.1 Vessel description

A.4.1.2 The vessel is a DP equipment class 2 platform supply vessel. The main particulars of the vessel are:

- Length (overall): 69.00m
- Length (between perpendiculars): 60.50m
- Breadth moulded: 15.50m
- Depth moulded: 7.00m
- Draft (design): 5.90m

A.4.1.3 The main propulsion is provided by two ABC 6Q30Z marine diesel engines, each developing up to 3,975kW of power at a speed of 750rpm, and each driving a controllable pitch propeller and a shaft generator that is capable of delivering 1,280kW, through a reduction gearbox.

A.4.1.4 Two DEF QTS042 CP bow tunnel thrusters with controllable pitch propellers are installed and located in the forward watertight compartment of the vessel.

A.4.1.5 Two GHI XTS032 CP stern tunnel thrusters with controllable pitch propellers are installed and located in an aft watertight compartment of the vessel.

A.4.1.6 Steering is provided by two JKL 30SGR high lift rudders, operated independently by hydraulic steering gears and located in the aftermost compartment of the vessel.

A.4.1.7 The DP control system is a MNO DP-2 dual redundant DP system, which includes two DPX 2 controller cabinets and two standard operator stations. There is also a JPA1 independent joystick back-up system installed.

A.4.1.8 Main electrical power is provided by the two shaft alternators, each generating 3 phase 440V AC and each capable of delivering 1,280kW at a lagging power factor of 0.8.

A.4.1.9 Two QRS T24L auxiliary diesel generators are provided.

A4.2 Redundancy Design Intent

A.4.2.1 In order to meet the required single failure criteria, all systems supporting the DP system are separated into two redundant groups. For simplicity, each redundant group will be referred to as the 'port redundant group' and the 'starboard redundant group'. The main components belonging to each redundant group are shown in table A4.1.

Port redundant group	Starboard redundant group
Port main engine	Starboard main engine
Port auxiliary diesel generator	Starboard auxiliary diesel generator
Starboard fuel oil settling tank	
Fuel oil separator	
Port fuel oil service tank	Starboard fuel oil service tank
Fuel oil transfer pump no.1	Fuel oil transfer pump no. 2

Table A4.1: *Redundant groups*

A.4.2.2 The methodology of redundant equipment groups has been applied at a high level throughout the analysis to illustrate the overall redundancy design intent. This has been applied for all relevant redundant component group auxiliary and subsystems.

A4.3 Fuel oil systems

A.4.3.1 The fuel oil systems consist of the fuel oil transfer system and the fuel oil service system. The principle arrangement of the fuel oil transfer system is shown in figure A4.1.

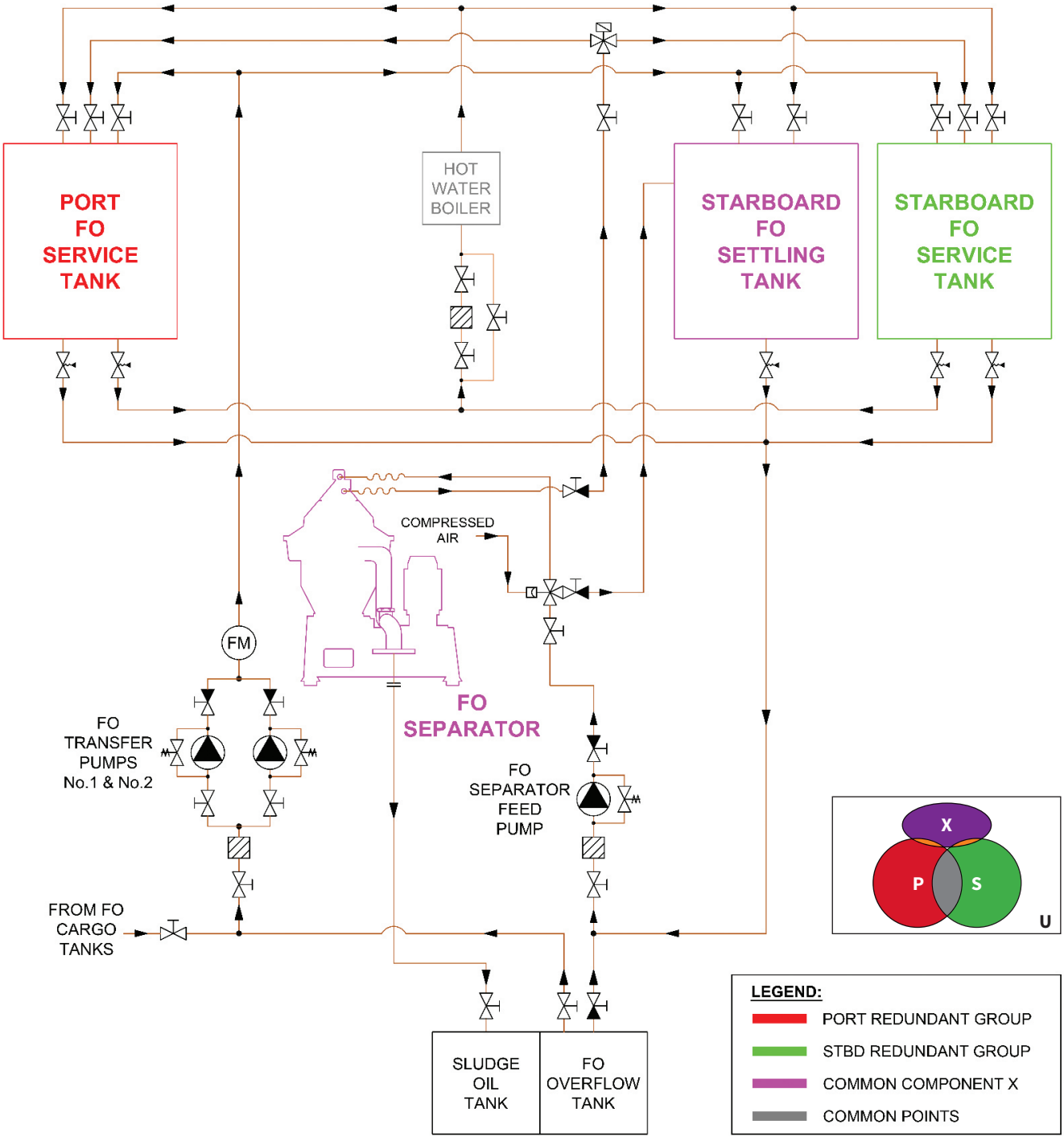

Figure A4.1: *Fuel oil transfer system*

A.4.3.3 The principle arrangement of the fuel oil service system is shown in figure A4.2.

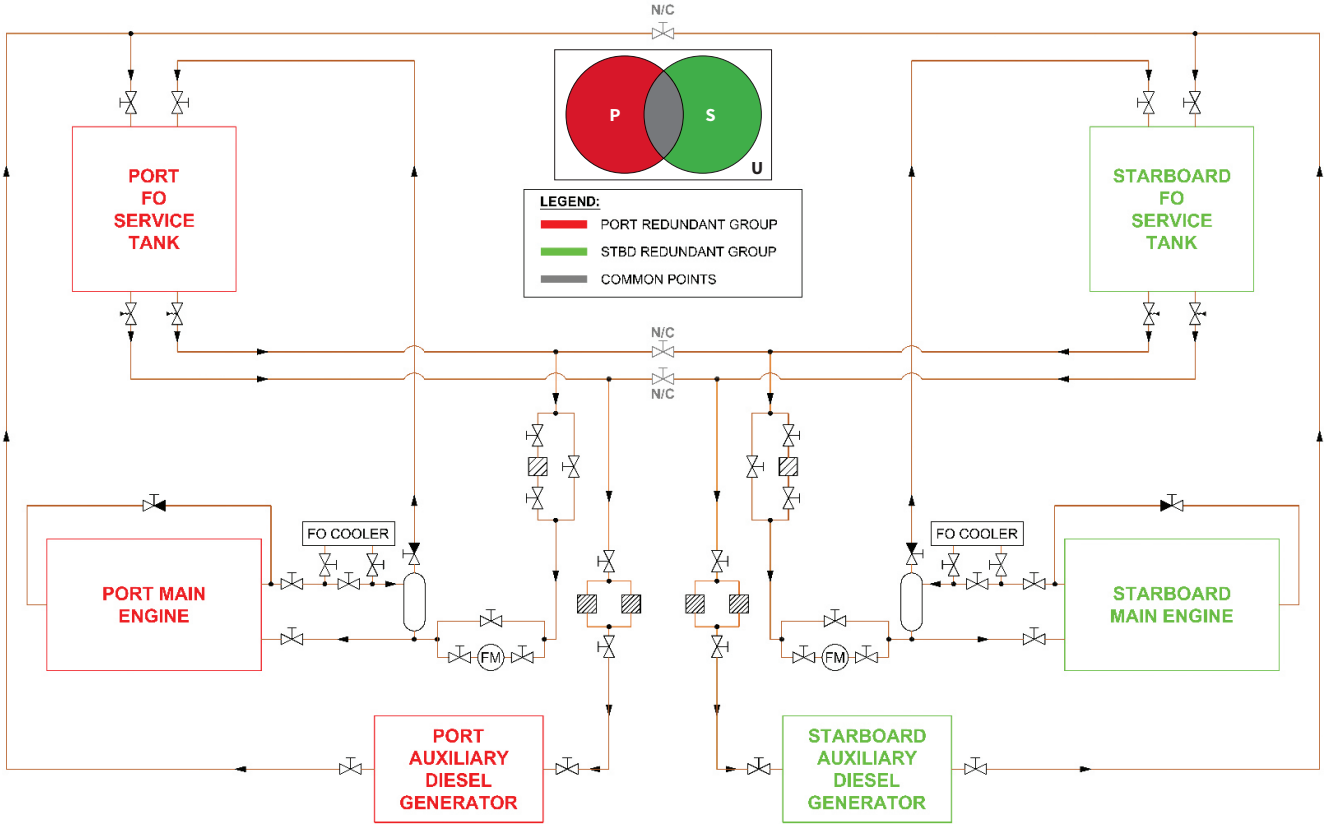

Figure A4.2: *Fuel oil service system*

A4.4 Fuel oil system redundancy verification table

A.4.4.1 The redundancy verification table for the fuel oil system is shown in table A4.2.

Fuel Oil System				
Subsystem	**Independent/ Common**	**Ref**	**Port**	**Starboard**
Service tanks	Independent		Port FO service tank	Stbd FO service tank
Settling tank	Common	1	Starboard settling tank	
FO separator	Common	2	One FO Separator for both FO service tanks	
FO transfer pumps	Independent		FO transfer pump no. 1	FO transfer pump no. 2
Pipework	Common	3	Pipework, isolation valves, three-way valve and crossover valves in supply and return piping to and from engines	
Engines	Independent		PME and port ADG	SME and stbd ADG
Hot water boiler	Common	4	Hot water boiler has common supply and return pipework from/to both FO service tanks	

Table A4.2: *Fuel oil system*

A4.5 Fuel oil systems single failure propagation analysis for common points

A.4.5.1 Each failure mode in the vessel's DP FMEA document has been allocated a severity class, which are defined as follows.

- **Severity Class 1 Catastrophic:** A major system failure that will cause total loss of DP capability regardless of any limitations put on the vessel. This would mean a loss of position-keeping, ability leading to an excursion, drive-off, or drift-off from position, resulting in possible asset loss or major environmental impact, and which will lead to an emergency termination of the operation.
- **Severity Class 2 Critical:** A major system failure that will cause loss of DP capability if operational limitations are not adhered to. This will include loss of redundancy where a further failure may result in loss of position, requiring a controlled termination of the operation, such as loss of a main switchboard, and results in an extended shut-down of operations.
- **Severity Class 3 Serious:** A failure resulting in a temporary loss of availability or degradation of DP operational capability.
- **Severity Class 4 Minor:** A failure that has a negligible effect on the DP system or subsystem level, generally at component level, and results in minor unscheduled maintenance or repair.

A.4.5.2 The severity class allocation has been included within the FMEA worksheets for the common points in the fuel oil system. The single failure propagation analysis for the common points in the fuel oil systems is included in section A4.6 to A4.8.

A4.6 Fuel contamination in both fuel oil service tanks

A.4.6.1 Fuel contamination can have serious repercussions on a DP vessel, or any vessel. If the source of the contamination is a storage tank, it is possible that both the running main engines and auxiliary diesel generators may be affected. Excess water in the fuel would cause erratic running and even loss of engines. Particle or bacterial contamination will result in filter clogging, and again, possible loss of engines.

A.4.6.2 Contamination of fuel in the port fuel oil service tank can affect the port main engine and the port auxiliary diesel generator. Likewise, contamination of fuel in the starboard fuel oil service tank can affect the starboard main engine and the starboard auxiliary diesel generator.

A.4.6.3 Water or particle contamination should be identified before it reaches the engines, through regular sampling and visual checks during draining of the fuel oil settling tank and service tanks, and regular visual checks on the fuel oil separator. It may also be identified through an increased need to clean the filters.

A.4.6.4 Good fuel treatment, prudent management of tanks and stringent bunkering/fuel transfer procedures should reduce fuel contamination in more than one fuel oil service system to a negligible risk.

A.4.6.5 A single fuel oil separator might allow both fuel oil service tanks to be simultaneously contaminated if both fuel oil service tanks are filled simultaneously and if the separator is carrying over excess water. However, a remote three-way valve is fitted at the discharge line between the two service tanks. The filling line isolation valve at the service tank not being filled should always be closed.

A.4.6.6 The hot water boiler can also be arranged to take suction from one or both service tanks and to discharge to one or both service tanks. The hot water boiler should always be arranged to take suction from one tank and return unused fuel to the same tank.

A.4.6.7 The fuel oil purifier can transfer fuel directly from the vessel's bunker fuel oil tanks to the port and/or starboard service tanks. This facility should not be used during DP operations.

A4.7 Fuel oil separator failure

A.4.7.1 Failure of a fuel oil separator can occur due to mechanical component failure, electrical motor failure or power loss. It can also occur due to other failures, such as failure of the associated feed pump, blockage of a fuel oil filter in the supply line, loss of compressed air or a control system failure. The engine room watch-keeper should be alerted by a fuel oil separator failure alarm.

A.4.7.2 Failure of a fuel oil separator should not present any immediate problems. Each fuel oil service tank has a volume that should provide enough time to repair a defective fuel oil separator. Enough spare parts for the fuel oil separator should be kept onboard.

A4.8 Main power distribution FMEA worksheets for common points

A.4.8.1 The effects of the individual failure modes relating to the fuel oil system are summarised in the FMEA worksheets (table A4.3).

Refs	Component(s)	Failure mode	Cause(s)	Local effect	Global effects (including subsystems)	Compensating provisions/barriers/ mitigation	Detection/ indication	Severity	Test reference
1.1 and 3	Fuel oil service tanks contaminated (both)	Particle or microbial bacterial, water contamination	Contaminated fuel loaded into FO bunker tanks	Erratic running of all engines over the same time period	Loss of main and auxiliary engines Loss of all thrusters and power *Loss of all thrusters. Failure in excess of WCFDI.*	1 Procedures and checklists for closing isolation and crossover valves. 2 Analysis of fuel oil at source. 3 Use of chemical decontamination on quarantined fuel. 4 Regular draining of water/sludge from setting tanks and service tanks. 5 Regular cleaning of FO separator. 6 Regular cleaning of filters. 7 Monitoring.	FO filter differential alarms at engines Low fuel oil pressure alarms at engines SG and ADG low frequency alarms during load changes	1	N/A due to compensating provisions
1.2 and 2		Water contamination	FO separator component failure			1 Procedures and checklists for closing isolation and crossover valves. 2 Maintenance. 3 Monitoring. 4 Alarms and water transducers.			
1.3 and 4			Heat exchanger component failure (hot water boiler or ME FO cooler)			1 Procedures and checklists for closing isolation and crossover valves. 2 Maintenance. 3 Regular draining of water/sludge from service tanks.			
2.1	Fuel oil separator	Failure/ceases to operate	Electronic component failure	FO separator not available to fill either FO service tank	Loss of filling capability for FO service tanks Eventual depletion of FO in service tanks and insufficient fuel to maintain continued DP operations	1 Maintenance and monitoring. 2 Spare parts.	FO separator failure alarm	4	51
2.2			Mechanical component failure					4	
2.3			Power loss					4	

Table A4.3: *Fuel oil system FMEA worksheets for common points*

A4.9 Fuel oil system conclusions

A.4.9.1 The FMEA of the main power generation and distribution systems are concluded in table A4.4, which considers the implementation of the compensating provisions identified in the FMEA worksheets.

Fuel oil systems
Worst case single failure
Loss of one main engine and/and or auxiliary diesel generator in one redundant group.
Possible causes of the worst-case single failure (failure modes)
1 Fuel contamination. 2 Filter blockage. 3 Flowmeter blockage. 4 Pipe leakage. 5 Failure of a quick closing valve.
Potential hidden failures
None.
Common cause failures
Actuation valves for quick closing valves are separated.
Common mode failures (internal and external)
Fuel contamination (see FMEA worksheets).
Cross connections – common component X
1 Fuel oil setting tank is common for both redundant groups. 2 Fuel oil separator is common for the both redundant groups.
Cross connections – common component group
1 Crossover valve between the supply line for the main engines – normally closed during DP operations. 2 Crossover valves between the supply and return lines for the auxiliary diesel generators – normally closed during DP operations.
External interfaces
1 Group emergency stop systems (FO transfer pumps and FO separator). 2 Quick closing valve controls (see section 14). 3 Alarm and monitoring system (see section 28).
Configuration errors
1 Any isolation valve at FO service tank which allows return of fuel from a fuel oil tank in the other redundant group. 2 Any normally closed crossover valve open.
Acts of maloperation
Possibility of inadvertent operation of quick closing valves – to be verified.
Mitigations against failure modes
Stringent bunkering, fuel transfer procedures and the following alarms and functions: 1 Fuel oil service and settling tanks low level alarms. 2 Main engine and auxiliary diesel generator low fuel oil pressure alarms.

Table A4.4: *FMEA of the main power generation and distribution systems*

A.4.9.2 The redundant DP equipment groups are considered independent and fail-safe when the compensating provision are applied.

Appendix B: Example statement of compliance

B1 Notes on statement of compliance

This information paper's framework requires a Statement of Compliance (SOC) from the VTO in the prescribed template, confirming that:

- The requirements to facilitate assurance activities are met.
- Verification and validation by the VTO's focal point accountable for DP operations have been undertaken, including:
  - Specific activities associated with certain requirements are carried out (such as periodic review/refresh of FMEAs or annual trials)
  - Specific references to sections, sub-sections, and documents where relevant information can be found to facilitate assurance.

The template is designed to facilitate the assurance process by requiring statements such as 'Yes' to be substantiated by references to specific sections of the FMEA and other DP-related documentation. Similarly, 'No' or 'Not Applicable' statements should be substantiated by documented reasons and references to where they are contained. Information that needs to be contained in the assurance document should be clearly identified in the SOC.

Completing the SOC will for the most part be a one-time effort. It can also be done during the compilation of the assurance document and the supporting and substantiating documentation. Additional effort may be needed following:

- Changes to FMEA (including renewal/refreshes).
- Periodic verification and validation by the VTO's DP focal point.

The SOC can also be leveraged to assist the VTO's self-assurance activities.

Entries in the SOC are annotated to indicate whether the subject in a particular row is a global issue (that applies to the whole vessel) or whether it applies to each subsystem. Compliance should be verified for each subsystem in the DP system.

B2 Vessel technical operator's statement of compliance

S. No.	Requirements of the OCIMF framework			Supporting evidence										Verified by VTO (DP accountable person and date)	VTO Remarks	Remarks
	Item	Compliance statement for specific activities/ requirements		Assurance document (items stipulated for the assurance document should be contained there)				If contained within FMEA and proving trials, reference applicable sections			If contained within other supporting documentation, reference applicable document and section					
		Specific activities under Item (reference to this information paper)	Comply (Yes/No) (substantiating evidence and references to be provided for Yes statements; No statements to be accompanied by clear unambiguous explanations)	Yes		No		Reference to FMEA section	Reference to FMEA page number	Reference to proving trials test number	Reference to document and section	Reference to page number	Reference to validation testing			
				Required (✓)	Verified by VTO	Contained within supporting documentation (✓)	Supporting documentation verified by VTO and references provided in compliance statement									
1	RDI	RDI (see section 2.2) (for vessel)		✓												Should be contained in the FMEA. An FMEA that does not contain the RDI should have other substantiating documents. Should be provided in the assurance documentation. DP design philosophy may be expressed in bullets to create a very high-level description of the redundancy concept. Generators and thrusters/open or closed bus.
2	WCFDI	WCFDI (see glossary) (for vessel)		✓												Should be contained in the FMEA. An FMEA that does not contain the WCFDI should have another substantiating document. This should not be driven by constraints, and if it is, it should be clearly defined. *For example, no single point failure as defined by class notation XYZ - 2 (DP equipment class 2) may lead to the loss of 2 generators and thereafter the loss of 3 thrusters when operated in the critical activity mode of operations. The WCFDI is applicable only when operating with all generators and thrusters online. XYZ is used a generic example of a notation and is not a real Classification Society.*
3	Worst-Case Failure (WCF)	WCF (see glossary) (for vessel)		✓												The FMEA should contain information comparing the verified and validated WCF to the WCFDI. *Each section of the FMEA should contain the WCF of the component group and compare this to the WCFDI.*

S. No.	Requirements of the OCIMF framework			Supporting evidence										Verified by VTO (DP accountable person and date)	VTO Remarks	Remarks
	Item	Compliance statement for specific activities/ requirements		Assurance document (items stipulated for the assurance document should be contained there)				If contained within FMEA and proving trials, reference applicable sections			If contained within other supporting documentation, reference applicable document and section					
		Specific activities under Item (reference to this information paper)	Comply (Yes/No) (substantiating evidence and references to be provided for Yes statements; No statements to be accompanied by clear unambiguous explanations)	Yes		No		Reference to FMEA section	Reference to FMEA page number	Reference to proving trials test number	Reference to document and section	Reference to page number	Reference to validation testing			
				Required (✓)	Verified by VTO	Contained within supporting documentation (✓)	Supporting documentation verified by VTO and references provided in compliance statement									
4	Configuration(s)	Configuration(s) (see section 3.3) (for vessel to subsystem level)		✓												Should be contained in the FMEA. An FMEA that does not contain the configuration should have other substantiating documentation. Ideally the FMEA should be updated with such information. *The vessel DP design philosophy and specifications should express the configuration for open bus/closed bus/ CAM/TAM etc.*
5	System sketches	System sketches (see section 4) (for all subsystems)		✓												Sketch should be a simplified representation focusing on the redundancy provided within the system and any common point.s *The FMEA should contain clear and concise sketches providing required information to the reader as outlined in this information paper.*
6	Redundancy Verification Tables (RVTs)	Redundancy Verification Tables RVTs (see section 4) (for all subsystems)		✓												Should clearly identify cross-connection and common points and lead to the single failure propagation items. *The analysis should contain colour-coded RVTs identifying component redundant groups with cross-connections and commonalities.*

S. No.	Requirements of the OCIMF framework			Supporting evidence										Verified by VTO (DP accountable person and date)	VTO Remarks	Remarks
	Item	Compliance statement for specific activities/ requirements		Assurance document (items stipulated for the assurance document should be contained there)				If contained within FMEA and proving trials, reference applicable sections			If contained within other supporting documentation, reference applicable document and section					
		Specific activities under Item (reference to this information paper)	Comply (Yes/No) (substantiating evidence and references to be provided for Yes statements; No statements to be accompanied by clear unambiguous explanations)	Yes		No		Reference to FMEA section	Reference to FMEA page number	Reference to proving trials test number	Reference to document and section	Reference to page number	Reference to validation testing			
				Required (✓)	Verified by VTO	Contained within supporting documentation (✓)	Supporting documentation verified by VTO and references provided in compliance statement									
7	Single failure propagation analysis	Single failure propagation analysis (see section 4) (for all subsystems)		✓												Should address technical failures and maloperation pathways and clearly identify compensating provisions and engineering/administrative barriers. Conclusions of no impact should be accompanied by a brief description of the rationale for the conclusion. *The analysis should identify impact on redundancy concept with reference to generators and thrusters (end effect).*
8	FMEA table	FMEA table (see section 2.3) (for all subsystems – where found necessary)		✓												This can be an IEC 60812 format component level failure analysis table looking at the common elements identified in the RVT and thereafter going through all its failure modes and effects, including end effect on generators and thrusters and providing details on compensating measures where necessary. *The analysis should provide a component level FMEA table to highlight the items in the single failure propagation analysis in detail.*

S. No.	Requirements of the OCIMF framework			Supporting evidence										Verified by VTO (DP accountable person and date)	VTO Remarks	Remarks
	Item	Compliance statement for specific activities/ requirements		Assurance document (items stipulated for the assurance document should be contained there)				If contained within FMEA and proving trials, reference applicable sections			If contained within other supporting documentation, reference applicable document and section					
		Specific activities under Item (reference to this information paper)	Comply (Yes/No) (substantiating evidence and references to be provided for Yes statements; No statements to be accompanied by clear unambiguous explanations)	Yes		No		Reference to FMEA section	Reference to FMEA page number	Reference to proving trials test number	Reference to document and section	Reference to page number	Reference to validation testing			
				Required (✓)	Verified by VTO	Contained within supporting documentation (✓)	Supporting documentation verified by VTO and references provided in compliance statement									
9	Hidden failures	Hidden failures (see section 2.3) (for all subsystems)		✓												The methodology by which the verification and validation is supported will need to be detailed. The analysis should include failures that do not make themselves visible to the operator and may remain hidden, such as degradation of performance *Another example of a potential hidden failure includes failure of on-demand functions such as protections that activate after a fault has occurred. Defence against hidden failures is usually accomplished by alarms and periodic verification and validation. For some notations, multiple redundant protective functions are provided. The significance of these are to be emphasised by documentation and familiarisation.*
10	Acts of maloperation	Acts of maloperation (see section 2.3) (for all subsystems)		✓												These should find their way into other documentation like the DP operations manual or checklists. *The analysis should provide links to acts of maloperation on common points. The triggers from common points should be assessed for both technical failures and maloperation. Technical failures need compensating provisions and maloperation can be mitigated through engineering or administrative controls. The undue reliance on operator intervention as a compensating provision to address technical failures should be avoided.*

S. No.	Requirements of the OCIMF framework			Supporting evidence										Verified by VTO (DP accountable person and date)	VTO Remarks	Remarks
				Assurance document (items stipulated for the assurance document should be contained there)				If contained within FMEA and proving trials, reference applicable sections			If contained within other supporting documentation, reference applicable document and section					
	Item	Compliance statement for specific activities/ requirements		Yes		No										
		Specific activities under Item (reference to this information paper)	Comply (Yes/No) (substantiating evidence and references to be provided for Yes statements; No statements to be accompanied by clear unambiguous explanations)	Required (✓)	Verified by VTO	Contained within supporting documentation (✓)	Supporting documentation verified by VTO and references provided in compliance statement	Reference to FMEA section	Reference to FMEA page number	Reference to proving trials test number	Reference to document and section	Reference to page number	Reference to validation testing			
11	Configuration errors	Configuration errors (see section 2.3) (for all subsystems)		✓												The analysis should contain information on the vessel redundancy concept, which depends on configurations that align all systems with RDI. Positive measures should be in place to ensure that potential erroneous configurations cannot be chosen. Control processes such as interlocks, control of work and familiarisation should be in place to ensure that this objective is achieved. *Identification and documentation of permissible configurations is essential to achieve the above objective.*
12	Separation design intent	Separation design intent (see glossary and appendix A) (for power and propulsion system and DP control systems)		Required only for DP3												This should be included in the FMEA to show that the analysis for DP equipment class 3 does analyse common cause failures of fire and flooding as required by the classification societies. These failures should not exceed the WCFDI and physical space will be a commonality. *The analysis and the validation processes should provide information on the physical separation of redundant equipment groups that constitutes the overall system design for the given configuration (DP equipment class 3).*

S. No.	Requirements of the OCIMF framework			Supporting evidence										Verified by VTO (DP accountable person and date)	VTO Remarks	Remarks
	Item	Compliance statement for specific activities/ requirements		Assurance document (items stipulated for the assurance document should be contained there)				If contained within FMEA and proving trials, reference applicable sections			If contained within other supporting documentation, reference applicable document and section					
		Specific activities under Item (reference to this information paper)	Comply (Yes/No) (substantiating evidence and references to be provided for Yes statements; No statements to be accompanied by clear unambiguous explanations)	Yes		No		Reference to FMEA section	Reference to FMEA page number	Reference to proving trials test number	Reference to document and section	Reference to page number	Reference to validation testing			
				Required (✓)	Verified by VTO	Contained within supporting documentation (✓)	Supporting documentation verified by VTO and references provided in compliance statement									
13	Validation of analysis through proving trials/testing/substantiating document	Proving trials (see section 2.5) (for vessel)		✓												The FMEA desktop analysis should be accompanied by a testing program, the results of which will drive the confirmation/ rewrite of the FMEA desktop analysis.
		Testing processes (see section 2.5) (for vessel)		✓												The verification and validation processes should be objective-driven, with clear and concise information. The objectives are defined with granularity in this information paper.
		Substantiating documentation (see section 2.5) (For all subsystems)		✓												The verification and validation processes and activities should include substantiating documentation as evidence of satisfactory completion.
14	Statements of independence and fail-safe	Statement of independence (see section 2.2) (for all subsystems)		✓												The validation process should confirm the independence and fail-safe condition of the redundant groups. This statement of independence and fail-safe condition is documentation concluding on the validated fault tolerance of the system. It is expected that this validation (for fail-safe) is in the form of validation testing. *Current practices do not always validate fail-safe condition of independent systems. In general, most systems (excluding control systems) can be concluded fail-safe by analysis and inspection and in some cases by validation testing. Concluding that control systems are fail-safe requires additional analysis and validation testing. This is seldom done comprehensively in an FMEA. The OEM should be required to provide supporting documentation.*
		Statement of compliance of fail-safe (see section 2.6) (for all subsystems)		✓												

S. No.	Requirements of the OCIMF framework			Supporting evidence										Verified by VTO (DP accountable person and date)	VTO Remarks	Remarks
	Item	Compliance statement for specific activities/ requirements		Assurance document (items stipulated for the assurance document should be contained there)				If contained within FMEA and proving trials, reference applicable sections			If contained within other supporting documentation, reference applicable document and section					
		Specific activities under Item (reference to this information paper)	Comply (Yes/No) (substantiating evidence and references to be provided for Yes statements; No statements to be accompanied by clear unambiguous explanations)	Yes		No		Reference to FMEA section	Reference to FMEA page number	Reference to proving trials test number	Reference to document and section	Reference to page number	Reference to validation testing			
				Required (✓)	Verified by VTO	Contained within supporting documentation (✓)	Supporting documentation verified by VTO and references provided in compliance statement									
15	Updates to the FMEA and five-yearly reviews/refreshes	Verification and validation efforts to demonstrate compliance with current industry standards, codes and practices (see section 2.4) (for vessel)		✓												The validation process should include updates to the FMEA and five-yearly reviews, with refreshes if required. The FMEA should follow industry guidance to categorise concerns and clearly document with supporting evidence. *Confirmation that review has been undertaken should be based on positive confirmation and substantiated by documentation such as failure analysis, FMEA proving trials when applicable, or documented evidence of process used to substantiate that the vessel's DP system and FMEA was reviewed for LFIs.*
		Hardware or software modifications of the DP system that have the potential to impact the redundancy concept (see section 2.4) (for vessel)		✓												
		Changes in operating procedures or deployment of the vessel on industrial missions not considered during the definition of the original design intent (see section 2.4) (for vessel)		✓												
		Learning from DP incidents (LFI) (such as incidents that the VTO has experienced or been made aware of, or those published by industry) (see section 2.4) (for vessel)		✓												

S. No.	Requirements of the OCIMF framework			Supporting evidence										Verified by VTO (DP accountable person and date)	VTO Remarks	Remarks
	Item	Compliance statement for specific activities/ requirements		Assurance document (items stipulated for the assurance document should be contained there)				If contained within FMEA and proving trials, reference applicable sections			If contained within other supporting documentation, reference applicable document and section					
		Specific activities under Item (reference to this information paper)	Comply (Yes/No) (substantiating evidence and references to be provided for Yes statements; No statements to be accompanied by clear unambiguous explanations)	Yes		No		Reference to FMEA section	Reference to FMEA page number	Reference to proving trials test number	Reference to document and section	Reference to page number	Reference to validation testing			
				Required (✓)	Verified by VTO	Contained within supporting documentation (✓)	Supporting documentation verified by VTO and references provided in compliance statement									
16	Assurance of periodic verification and validation	Periodic testing at intervals not exceeding five years to ensure full compliance with the applicable parts of the guidelines (see section 2.6) (for vessel)		✓												The assurance of periodic verification and validation should be supported by clearly identified closure pathways. Evidence should be recorded and kept on board to confirm that periodic verification and validation processes are being applied as required; to prove the conclusions of the DP system FMEA; and to achieve the other stated objectives.
		The annual test (also called the DP annual trial) of all important systems and components carried out (see section 2.6) (for vessel)		✓												
		The type of tests carried out and results recorded and kept on board (see section 2.6) (for vessel)		✓												
		Periodic verification and validation (reverification and revalidation) continue throughout the DP vessel's operational life (see section 2.6) (for vessel)		✓												
		Evidence and confirmation that the FMEA has been subject to review cycle (see section 2.6) (for vessel)		✓												
		Data-centric evidence is provided to support the above points (see section 2.6) (for each test)		✓												

S. No.	Requirements of the OCIMF framework			Supporting evidence										Verified by VTO (DP accountable person and date)	VTO Remarks	Remarks
	Item	Compliance statement for specific activities/ requirements		Assurance document (items stipulated for the assurance document should be contained there)				If contained within FMEA and proving trials, reference applicable sections			If contained within other supporting documentation, reference applicable document and section					
		Specific activities under Item (reference to this information paper)	Comply (Yes/No) (substantiating evidence and references to be provided for Yes statements; No statements to be accompanied by clear unambiguous explanations)	Yes		No		Reference to FMEA section	Reference to FMEA page number	Reference to proving trials test number	Reference to document and section	Reference to page number	Reference to validation testing			
				Required (✓)	Verified by VTO	Contained within supporting documentation (✓)	Supporting documentation verified by VTO and references provided in compliance statement									
17	Categorisation of concerns and concerns register	Categorisation of concerns and concerns register (for analysis and trials programmes)		✓												The categorisation of concerns should be in line with good industry practices for FMEAs. *Transparency/records to be maintained on how concerns are closed out so that this can be verified by any stakeholder. Sometimes these are closed out by class, but may affect delivery of the IM in a safe manner.*
18	Assumptions	Assumptions (for analysis and trials programmes)														The FMEA should provide a list of all assumptions and where it is not verifiable by testing, the OEM should provide supporting documentation.
19	Limitations	Limitations (for analysis and trials programmes)														Transparency/records to be maintained on the limitations of the FMEA/ supporting studies so that these can be verified by any stakeholder.
20	Constraints	Constraints (for analysis and trials programmes)														Transparency/records to be maintained on the constraints of the FMEA/supporting studies so that these can be verified by any stakeholder.
The VTO confirms that compliance has been verified and validated, the assurance document is complete and is accurate, and substantiating evidence and information is readily available to facilitate the assurance process.																

Name: _____

Designation: _____

Date: _____

Appendix C: Example sketches and Redundancy Verification Tables

C1 Redundancy Verification Tables and sketches for a range of subsystems

Identifying the redundant DP equipment groups and the common points connecting them is the most important part of any DP system FMEA. The sections that follow illustrate how the subsystem sketches and redundancy verification tables should appear for a variety of subsystems found on most DP vessels. A simple diesel electric concept with a two-way split is used, but the process can easily be adapted to a redundancy concept with any number of redundant equipment groups.

Table C1.1 describes the RDI for the vessel. The FMEA may prove that the original redundancy design intent is not achieved and should be revised. However, the RDI used at the outset of the design phase is the one that the FMEA will use to determine whether the intent has been achieved.

Condition	Positioning provided by	Type of redundancy
Normal operation (intact)	T1 T2 T3 T4	Active: no drift-off or drive-off of any thruster
After single failure	T1 & T3 or T2 & T4	

Table C1.1: *Redundancy Design Intent*

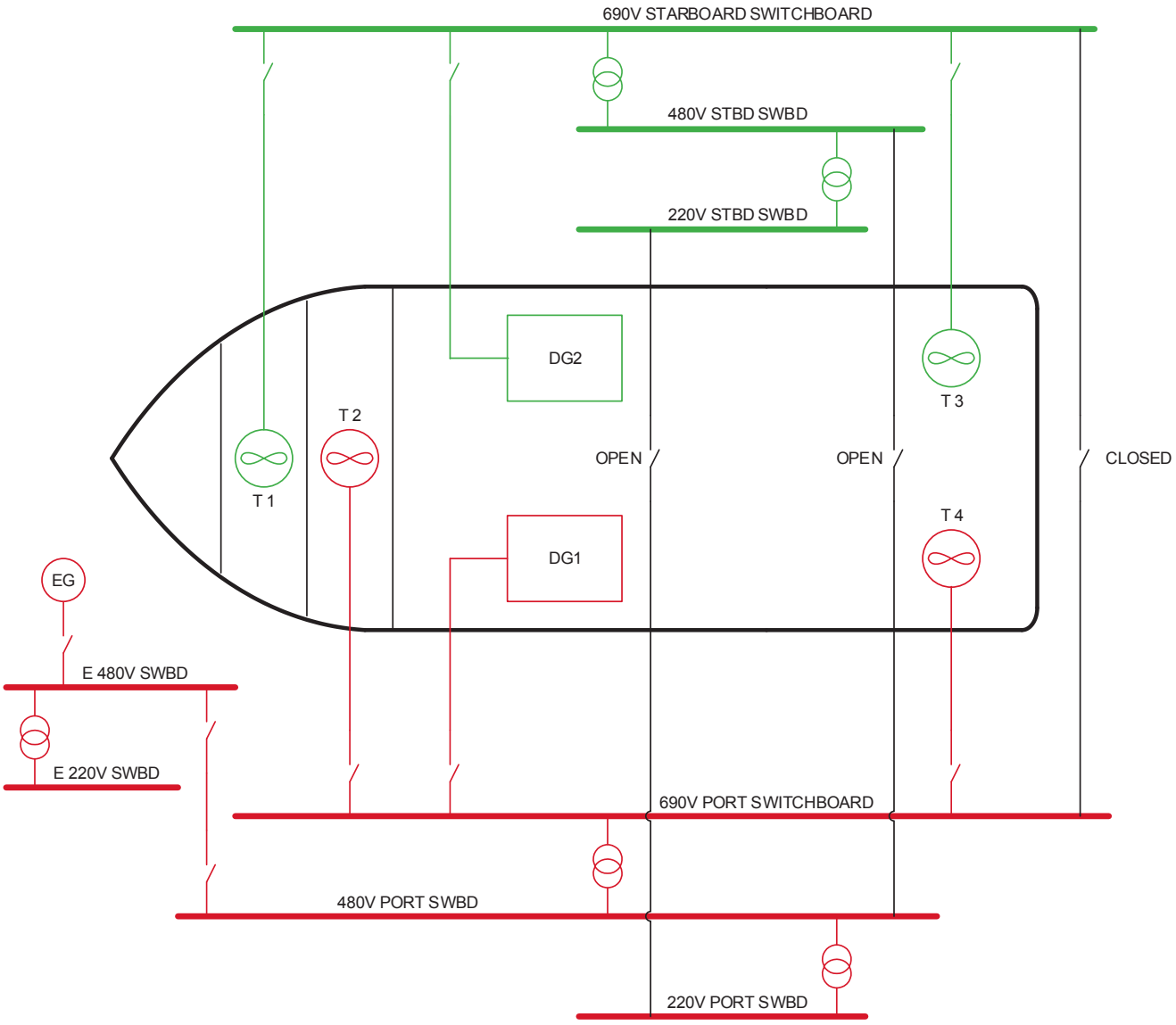

Figure C1.1: *Concept sketch for a DP vessel with simple redundancy concept*

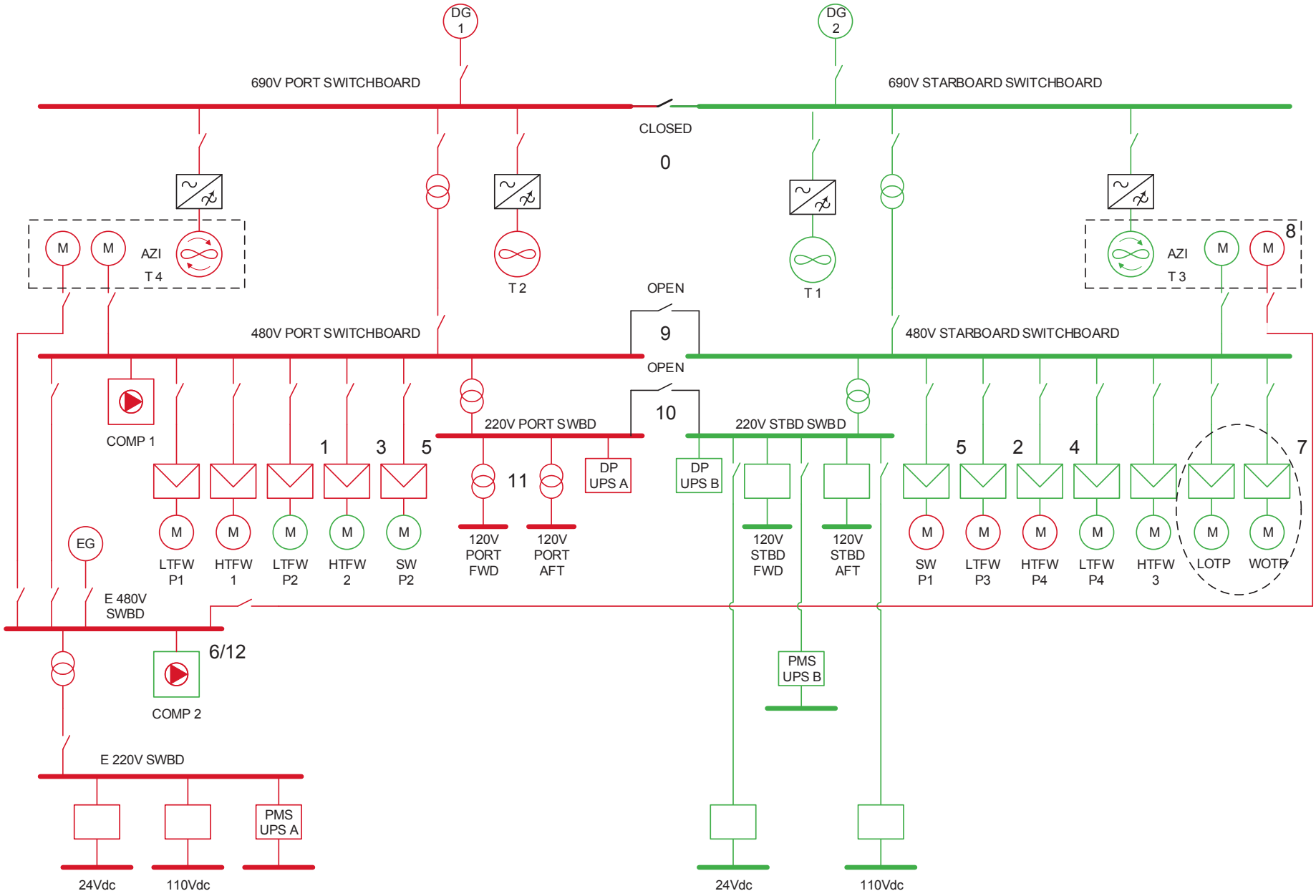

Figure C1.2: *Sketch of power system showing redundant equipment groups*

Subsystem	Independent/ Common	Ref	Port	Starboard
Generators	Independent		DG1	DG2
Thrusters	Independent		T2 / T4	T1 / T3
Transformers	Independent		690V/480V XFMR port	690V/480 XFMR stbd
Distribution	Independent		690V MSB port	690V MSB port
	Common	0	690V bus tie (closed)	

Table C1.2: *Power distribution systems – 690V*

Subsystem	Independent/ Common	Ref	Port	Starboard
Switchboards	Independent		480V Switchboard (SWBD) port	480V SWBD port
Low temperature cooling	Common	1	Low Temperature Fresh Water (LTFW) P1	LTFW P2
	Common	2	LTFW P3	LTFW P4
High temperature cooling	Common	3	HTFW 1	HTFW 2
	Common	4	HTFW P4	HTFW3
Seawater cooling	Common	5	SWP2	SWP1
Compressed air	Common	6	Comp 1	Comp 2
Lubricating oil	Common	7	LOTP WOTP	
Steering pumps	Common	8	T4 Steering P1 and P2 (E480V)	T3 Steering P1 / P2 (E480V)
Power distribution	Independent		Port 480V/220V XFMR	STBD 480V/220V XFMR
	Independent		ESWB 480V	
	Common	9	480V bus tie (open)	

Table C1.3: *Power distribution systems – 480V*

Subsystem	Independent/ Common	Ref	Port	Starboard
Power distribution	Independent		220V SWBD port	220V SWBD stbd
	Independent		Port Fwd 120V Xfmr	Port Fwd 120V Xfmr
	Independent		Port Aft 120V Xfmr	Port Aft 120V Xfmr
DP control	Independent		DP UPS A	DP UPS B
PMS	Independent		PMS UPS A (E220V)	PMS UPS B
Power distribution	Independent		24Vdc port (E220V)	24Vdc stbd
	Independent		110Vdc port (E220V)	110Vdc stbd
	Common	10	220V bus tie (open)	
Temperature control valves	Common	11	TCV1	TCV2

Table C1.4: *Power distribution systems – 220V*

Subsystem	Independent/ Common	Ref	Port	Starboard
Power distribution	Independent		EGEN	
	Independent		E 480V SWBD	
	Independent		E 480V to 220V Xfmr	
	Independent		Port 24Vdc	
	Independent		Port 110Vdc	
PMS	Independent		PMS UPS A	
Compressed air	Common	12		Comp 2

Table C1.5: *Emergency power distribution systems – 480V and 220V*

It is convenient to have the simplified system sketch and the RVT side by side for each cross reference. This is not always possible (for practical reasons) on larger or more complex systems. The two-column format should be used when it is practical to do so.

System sketch showing redundant DP equipment groups

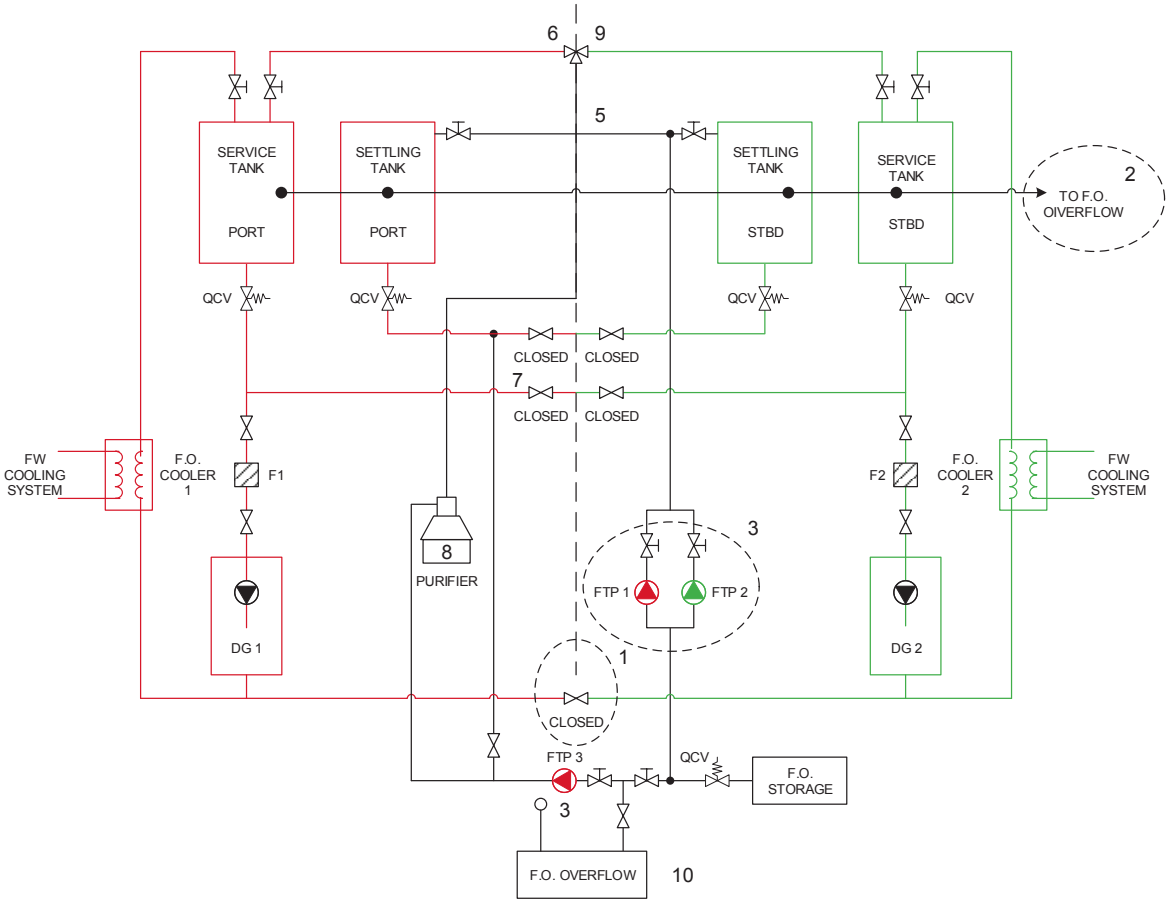

Figure C1.3: *Fuel oil system*

Redundancy Verification Table

Subsystem	Independent/ Common	Ref	Port	Starboard
FO selling	Independent		Settling tank port	Settling tank stbd
FO service	Independent		Service tank port	Service tank stbd
	Independent		DG1	DG2
	Independent		FO cooler 1	FO cooler 2
	Common	1	DG fuel return line	
FO distribution and transfer	Common	2	Fuel overflow line	
	Common	3	FTP 1	FTP 2 / FTP 3
	Common	4	Settling tank discharge line	
	Common	5	Settling tank fill line	
	Common	6	Service tank fill line	
	Common	7	Service tank transfer line	
Purification	Common	8	Purifier	
	Common	9	Purifier changeover valve	
Storage	Common	10	FO overflow and storage tanks	

Table C1.6: *Fuel oil system*

System sketch showing redundant DP equipment groups

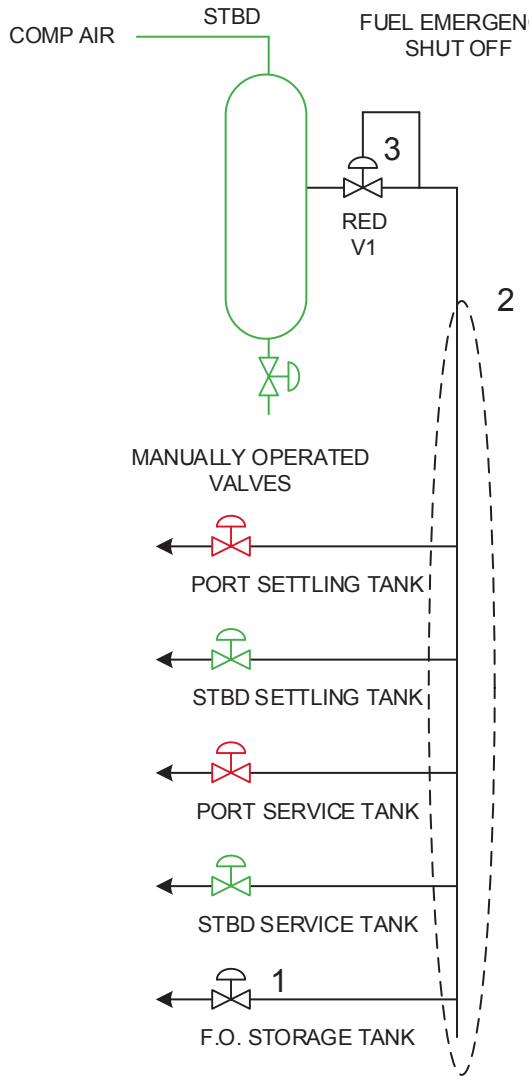

Figure C1.4: *Fuel shut off system*

Redundancy Verification Table

Subsystem	Independent/ Common	Ref	Port	Starboard
FO distribution	Independent		Port settling tank valves	Stbd settling tank valve
	Independent		Port service tank valve	Stbd service tank
FO storage	Common	1	FO storage tank and valve	
Compressed air distribution	Common	2	Pipework	
	Common	3	RED V1 (30 bar to 7 bar reducer)	

Table C1.7: *Fuel oil shut-off system*

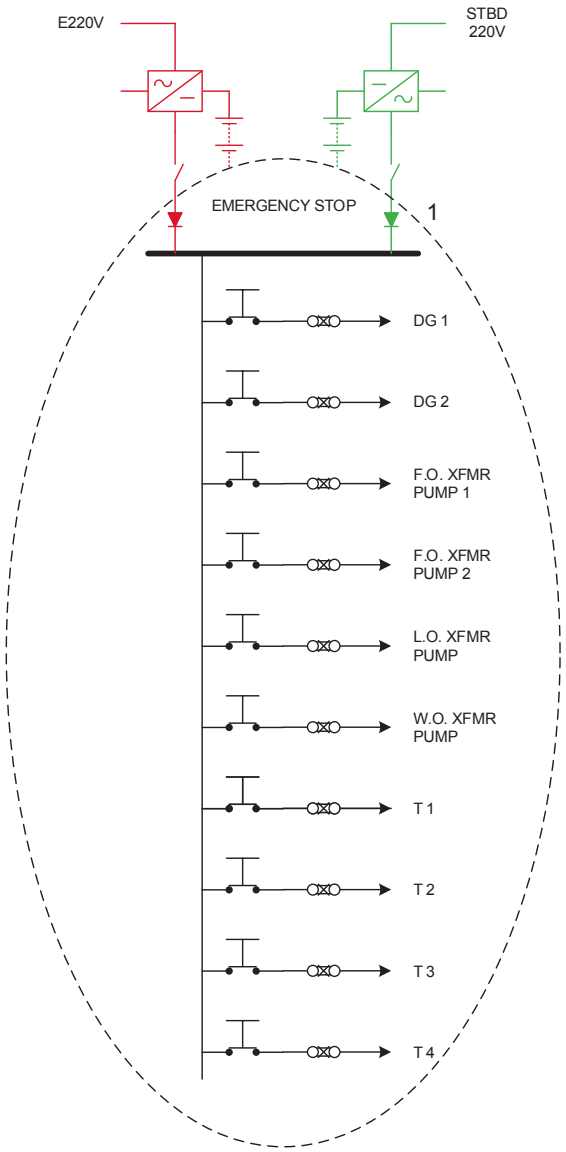

Figure C1.5: *Emergency stop system*

Subsystem	Independent/ Common	Ref	Port	Starboard
Power	Independent		Port PSU	Stbd PSU
Safety	Common	1	E STOP DB	
Engines	Independent		DG1	DG2
FO Xfr	Independent		FO Xfr 1	FO Xfr 1
LO Xfr	Independent			LO Xfr
	Independent			WO Xfr
Thrusters	Independent		T2	T1
	Independent		T4	T3

Table C1.8: *Emergency stop system*

System sketch showing redundant DP equipment groups

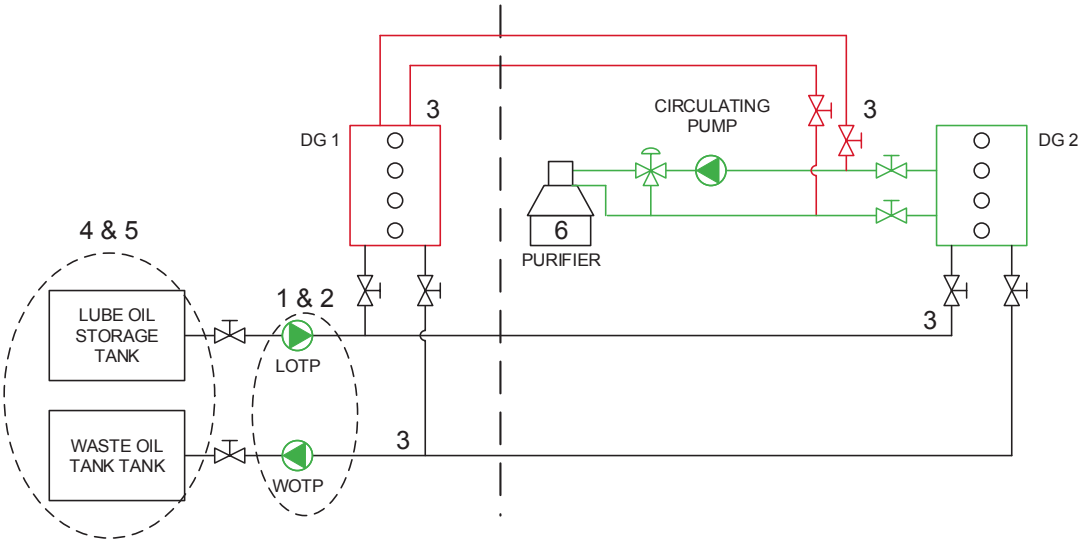

Figure C1.6: *Lubricating oil system*

Redundancy Verification Table

Subsystem	Independent/ Common	Ref	Port	Starboard
Engines	Independent		DG1	DG2
Transfer	Common	1	LOTP	
	Common	2	FOTP	
Distribution and storage	Common	3	Pipework and valves	
	Common	4	Waste oil tank	
	Common	5	Lube oil tank	
Purification	Common	6	Purifier	

Table C1.9: *Lubricating oil system*

System sketch showing redundant DP equipment groups

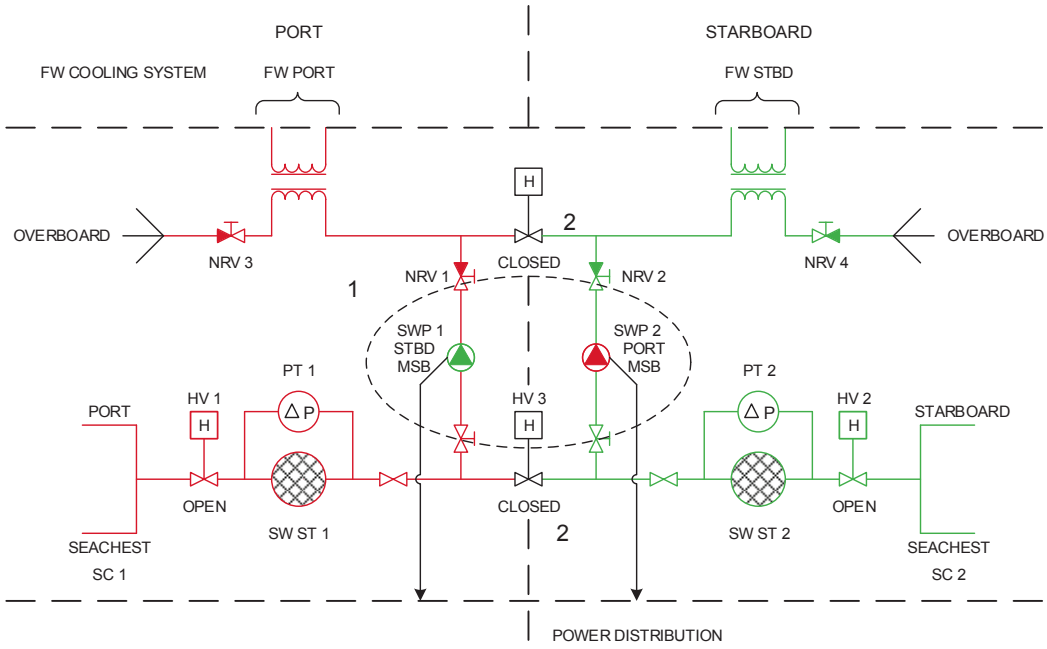

Figure C1.7: *Seawater cooling system*

Redundancy Verification Table

Subsystem	Independent/ Common	Ref	Port	Starboard
Sea chests	Independent		SC1	SC2
Strainers	Independent		SWST1	SWST2
Heat exchanges	Independent		SWHE 1	SWHE 2
Pumps	Common	1	SWP1	SWP2
Shell valves	Independent		HV1	HV2
Transducers	Independent		PT1	PT2
NRV	Independent		NRV 1 NRV3	NRV 2 NRV4
Piping	Independent		Port piping	Starboard piping
X-over valves	Common	2	HV3 HV4	

Table C1.10: *Seawater cooling system*

System sketch showing redundant DP equipment groups

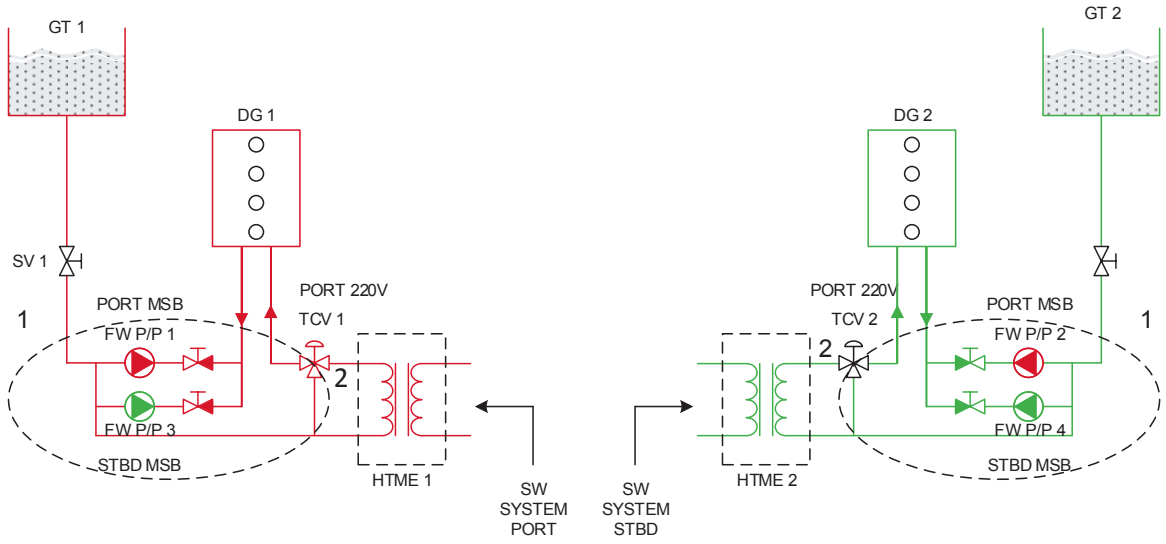

Figure C1.8: *High temperature freshwater cooling system*

Redundancy Verification Table

Subsystem	Independent/ Common	Ref	Port		Starboard	
Generator Cooling Water (CW) jacket	Independent		DG1		DG2	
Gravity tank	Independent		GT1		GT2	
Supply valve	Independent		SV1		SV2	
Motor/pump	Common	1	FW P/P 1	FW P/P 3	FW P/P 2	FW P/P 4
Discharge valve	Independent		DV1/DV3		DV2/DV4	
Temperature control valve	Common	2	HT TCV 1		HT TCV 2	
Heat exchanger	Independent		HTME 1		HTME 2	
Piping	Independent		From SW system port		From SW system stbd	

Table C1.11: *High temperature, freshwater cooling system*

System sketch showing redundant DP equipment groups

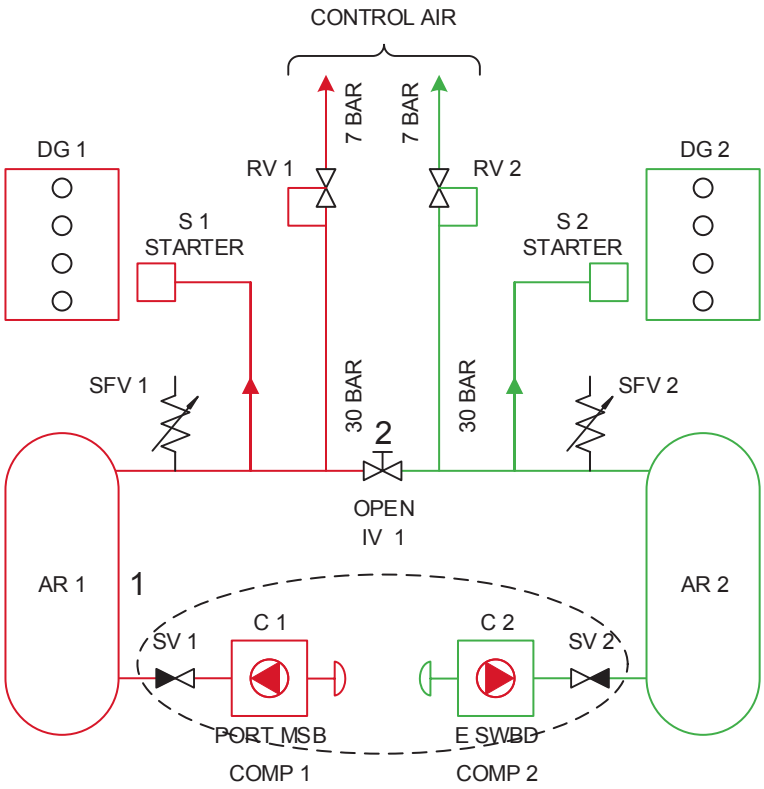

Figure C1.9: *Starting air system*

Redundancy Verification Table

Subsystem	Independent/ Common	Ref	Port	Starboard
Compressor	Common	1	Comp 1	Comp 2
Receiver	Independent		AR 1	AR 2
Supply valves	Independent		SV 1	SV 2
Relief valves	Independent		SFV 1	SFV 2
Isolating valve	Common	2	IV1	
Air starter	Independent		S1	S2
Reducing valve	Independent		RV1	RV2
Piping	Independent		Port pipework	Starboard pipework

Table C1.12: *DG starting air system*

System sketch showing redundant DP equipment groups

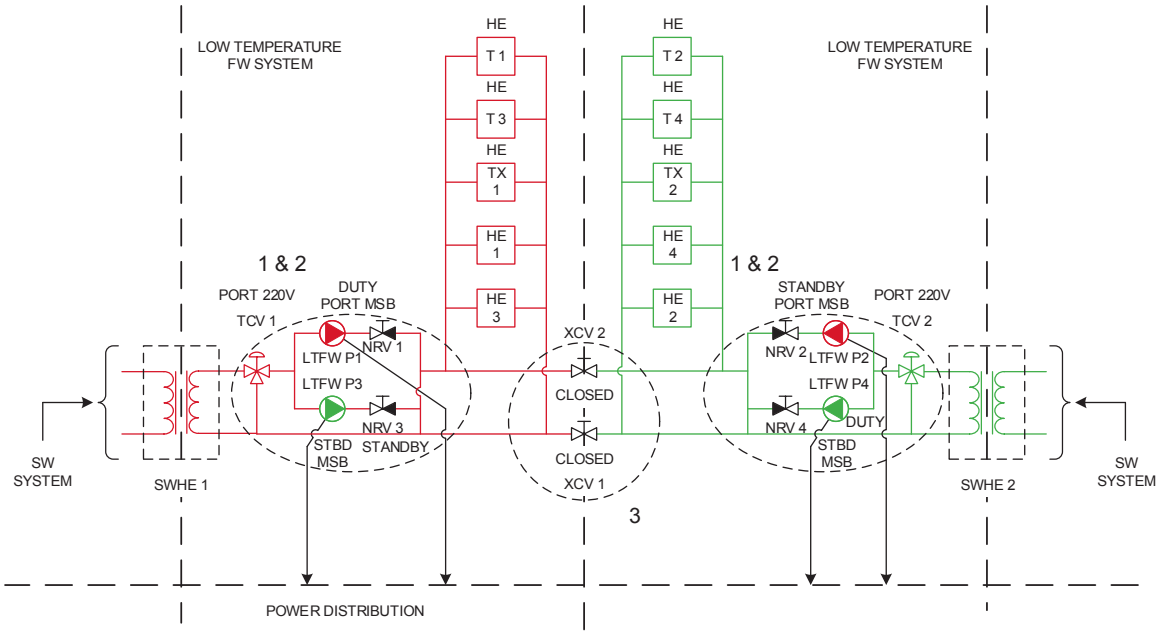

Figure C1.10: *Low temperature freshwater cooling system*

Redundancy Verification Table

Subsystem	Independent/ Common	Ref	Port	Starboard
Seawater system heat exchangers	Independent		SWHE1	SWHE2
Temperature control valves	Independent		TCV1	TCV2
LTFW pumps duty	Common	1	LTFWP1	LTFWP2
LTFW pumps standby	Common	2	LTFWP3	LTFWP4
NRV	Independent		NRV P1 NRV P3	NRV P2 NRV P4
X-over valve	Common	3	XCV 1 XCV2	
Consumer heat exchangers	Independent		HET1 HET3 HE TX1 HE1 HE3	HET2 HET4 HE TX2 HE2 HE4
Piping	Independent		Port pipework	Starboard pipework

Table C1.13: *Low temperature freshwater cooling system*

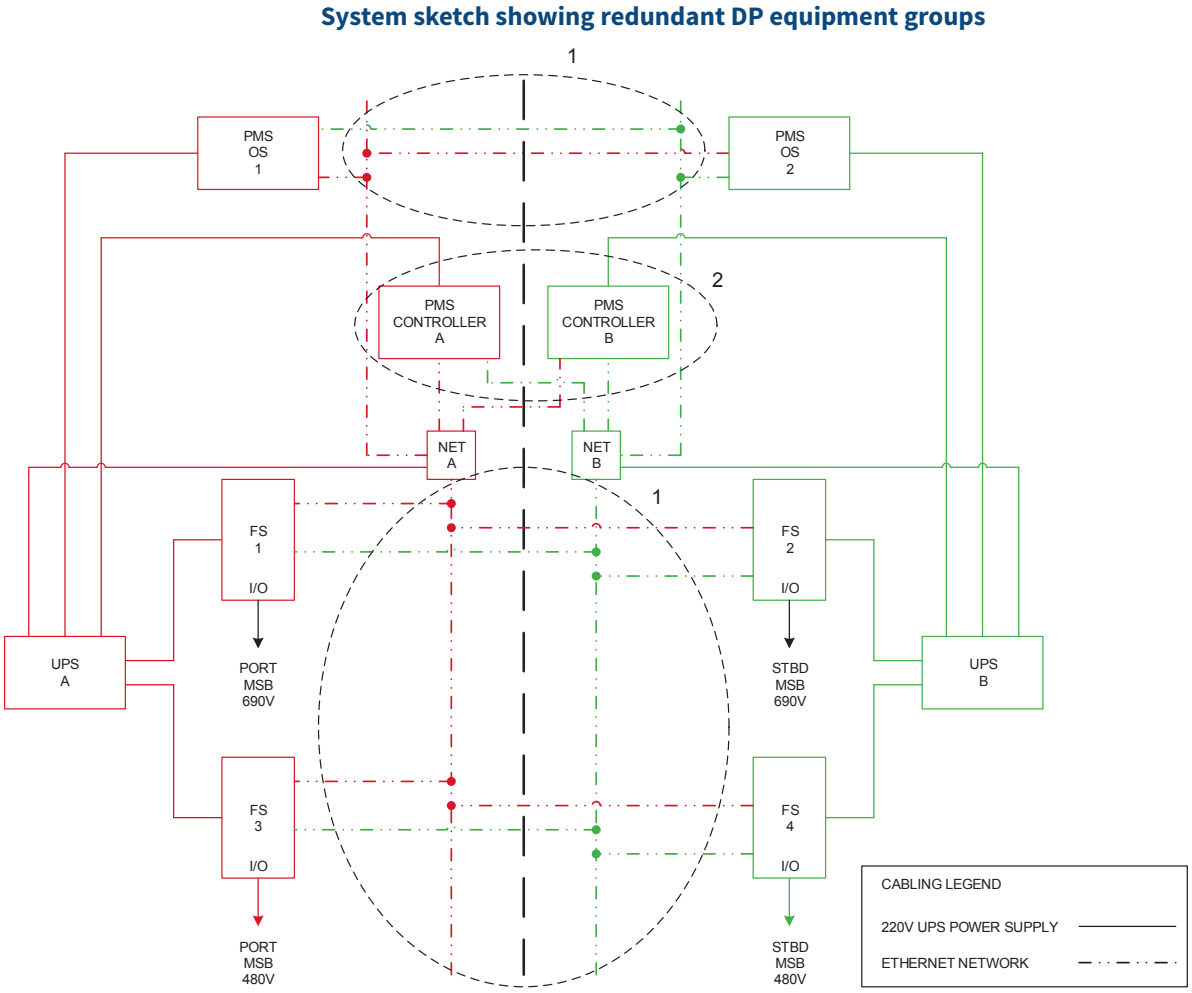

Figure C1.11: *Power management system*

Redundancy Verification Table

Subsystem	Independent/ Common	Ref	Port	Starboard
Operator stations	Independent		PMS OS 1	PMS OS 2
PMS controllers	Independent		PMS CON A	PMS CON B
Network hubs	Independent		NET A	NET B
Field stations	Independent		FS 1	FS 2
	Independent		FS 3	FS 4
Cables	Independent		OS 1 – NET A PMS A – NET A FS 1 – NET A FS 3 – NET A	OS 2 – NET B PMS B – NET B FS 2 – NET B FS 4 – NET B
Cables	Common	1	OS 1 - NET B PMS A – NET B FS 1 – NET B FS 3 – NET B OS 2 - NET A PMS B – NET A FS 2 – NET A FS 4 – NET A	
Controller	Common	2	Online controller	

Table C1.14: *Power management system*

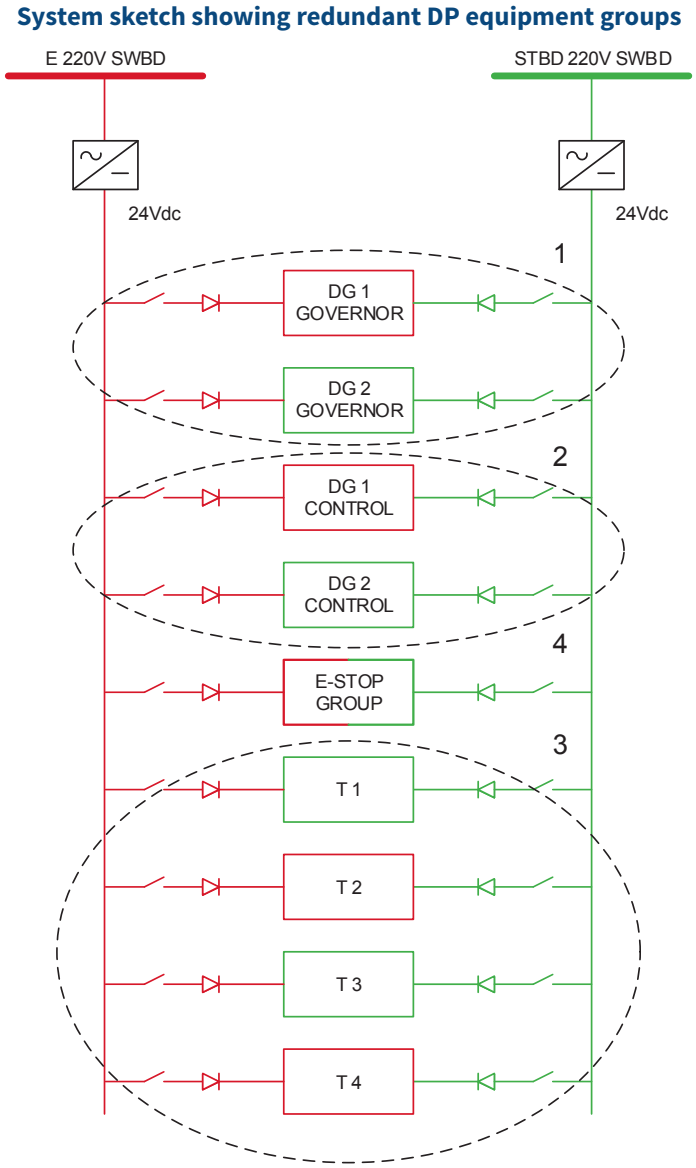

Figure C1.12: *24Vdc Power distribution system*

Redundancy Verification Table

Subsystem	Independent/ Common	Ref	Port		Starboard	
Governor	Common	1	24V Port	24V Stbd	24V Port	24V Stbd
			DG1 Gov		DG2 Gov	
Engine control	Common	2	24V Port	24V Stbd	24V Port	24V Stbd
			DG1 Con		DG2 Con	
Thrusters	Common	3	24V Port	24V Stbd	24V Port	24V Stbd
			T2		T1	
			24V Port	24V Stbd	24V Port	24V Stbd
			T4		T3	
Safety	Common	4	ESTOP			

Table C1.15: *24Vdc Power distribution system*

System sketch showing redundant DP equipment groups

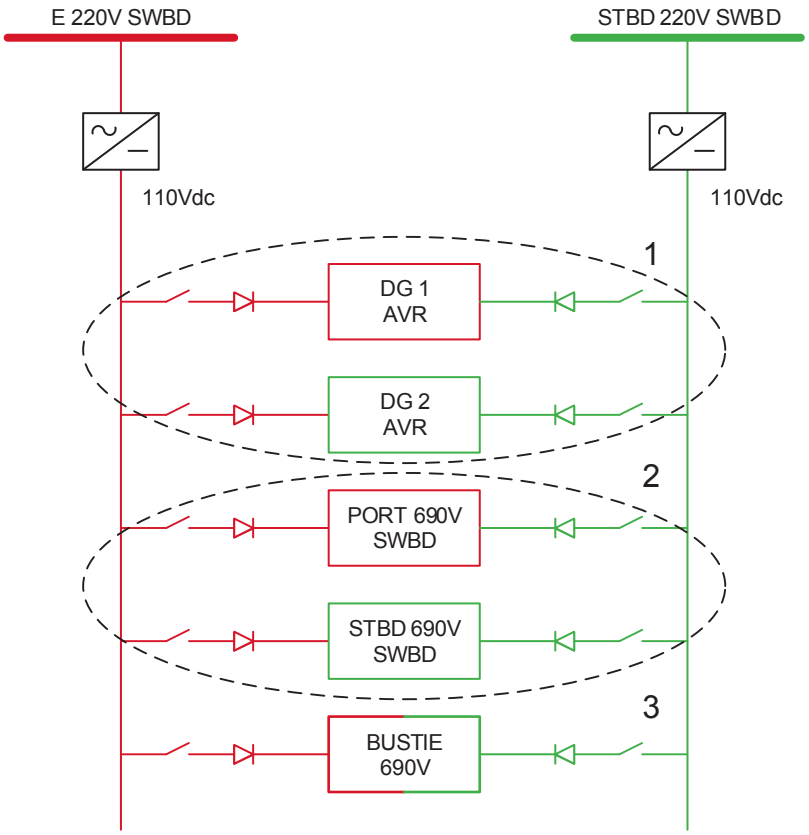

Figure C1.13: *110Vdc Power distribution system*

Redundancy Verification Table

Subsystem	Independent/ Common	Ref	Port		Starboard	
AVRs	Common	1	110V Port	110V Stbd	110V Port	110V Stbd
			AVR1		AVR2	
690V MSB	Common	2	110V Port	110V Stbd	110V Port	110V Stbd
			Port 690V SWBD		Stbd 690V SWBD	
Bus tie	Common	3	110V Port		110V Stbd	
			690V bus tie			

Table C1.16: *110Vdc Power distribution system*

System sketch showing redundant DP equipment groups

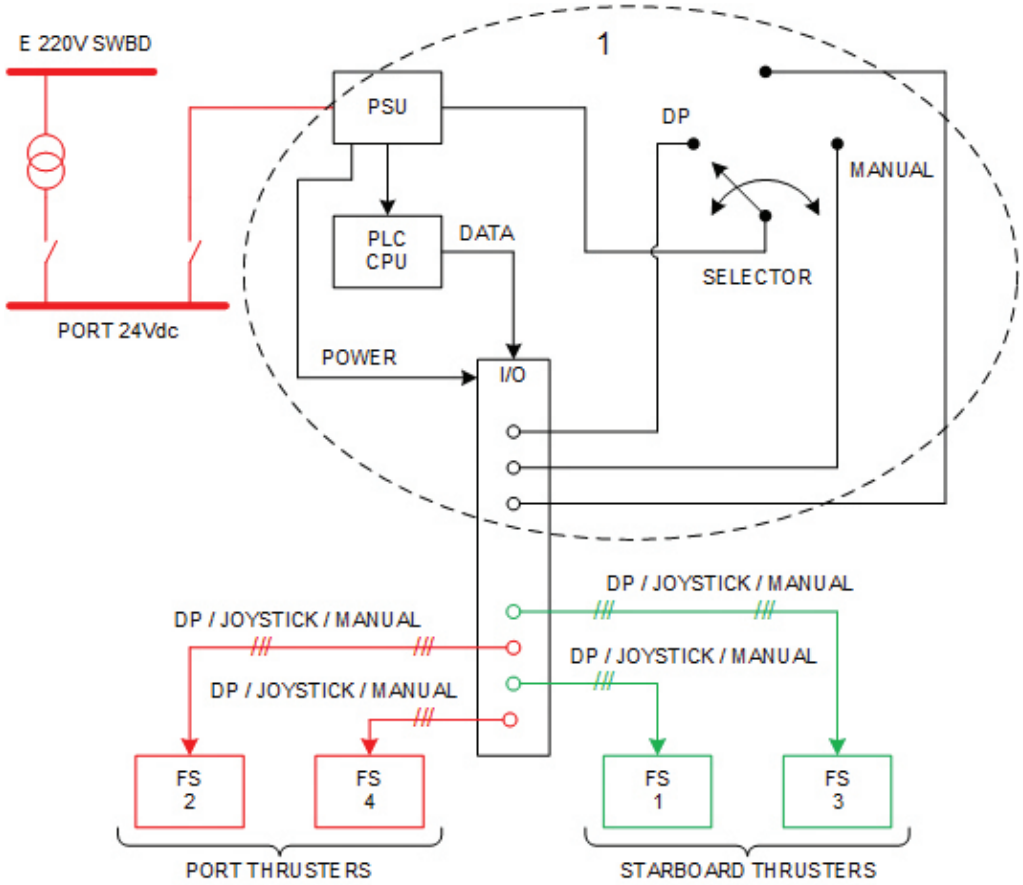

Figure C1.14: *Control mode selector*

Redundancy Verification Table

Subsystem	Independent/ Common	Ref	Port	Starboard
DPCS	Common	1	Power Supply Unit (PSU) Programmable Logic Controller (PLC) rotary switch I/O interface	
PMS/VMS	Independent		FS 2	FS 1
	Independent		FS 4	FS 3

Table C1.17: *Mode selector system*

System sketch showing redundant DP equipment groups

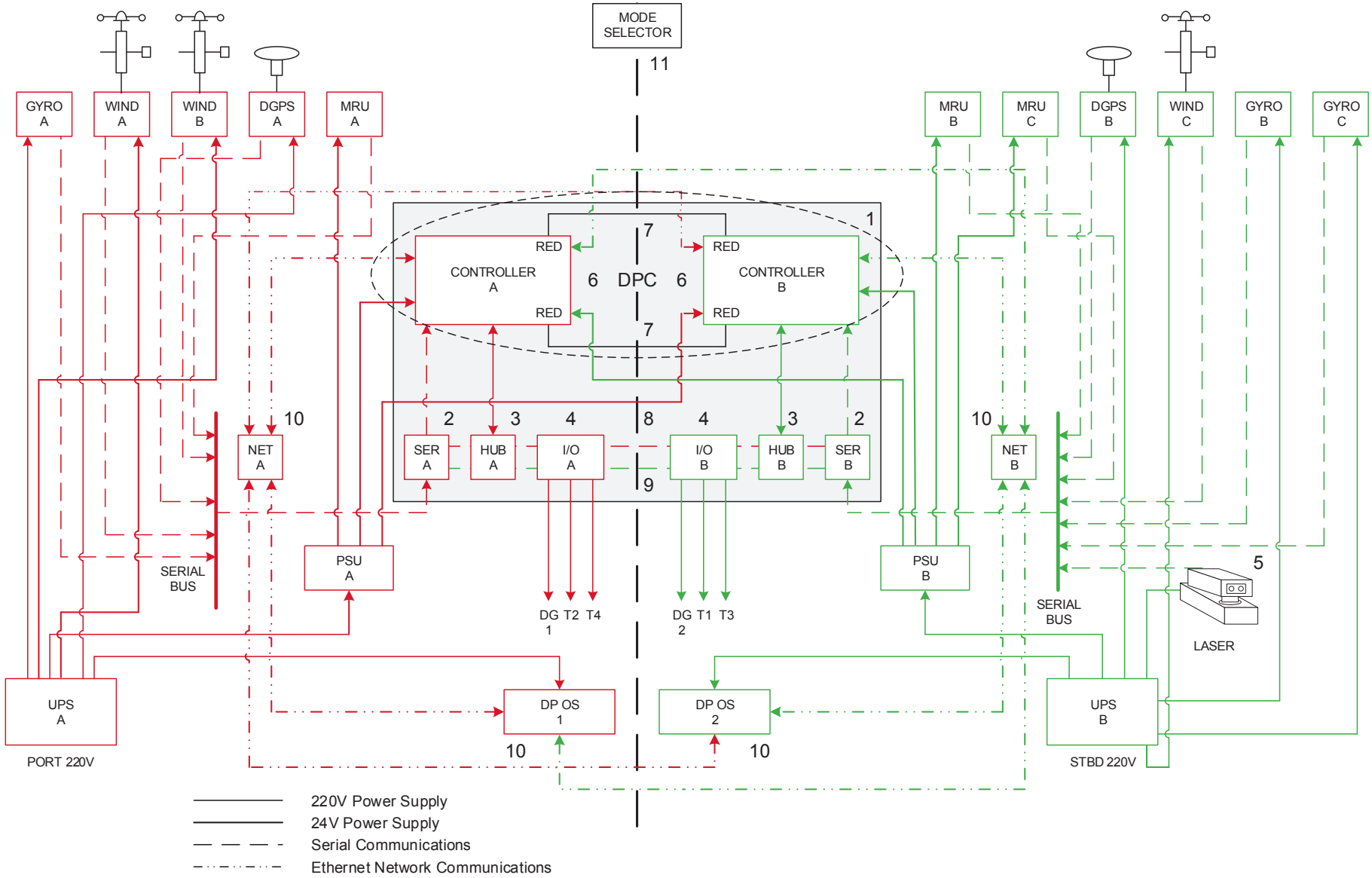

Figure C1.15: *DP control system*

Redundancy Verification Table

Subsystem	Independent/ Common	Ref	Port		Starboard	
Gyros	Independent		Gyro A		Gyro B & C	
Anemometers	Independent		Wind A & B		Wind C	
DGPS	Independent		DGPS A		DGPS A	
MRU	Independent		MRU A		MRU B & C	
Networks	Independent		NET A		NET B	
Power supplies	Independent		PSU A (input)		PSU B (input)	
Controllers	Common	1	PSU A	PSU B	PSU A	PSU B
			Con A		Con B	
Serial hubs	Common	2	PSU A	PSU B	PSU A	PSU B
			Ser A		Ser B	
Network hubs	Common	3	PSU A	PSU B	PSU A	PSU B
			Hub A		Hub B	
I/O interface	Common	4	PSU A	PSU B	PSU A	PSU B
			I/O A		I/O B	
Laser Position Reference System (PRS)	Common	5			Laser PRS	
Controller	Common	6	Online controller			
Redundancy network	Common	7	RED Nen (A to B) & (B to A)			
I/O	Common	8	Internal I/O bus A			
	Common	9	Internal I/O bus B			
	Common	10	Network			
Thruster control mode	Common	11	Mode selector			

Table C1.18: *DP control system*

C2 Example separation intent and analysis for DP class 3 vessels

Figures C2.1 and C2.2 show an example separation design intent for a DP class 3 vessel. This example has two tunnel thrusters forward and two azimuthing thrusters aft. It has a diesel electric power plant consisting of four diesel generators in two A60/WT engine rooms, two pump rooms and two fuel oil tanks at the tank top levels. The vessel always operates with the power plant configured as two independent power systems.

On the tween deck, there are four variable speed drives for the thrusters in individual compartments, two High Voltage (HV) switchboard rooms, two Low Voltage (LV) switchboard rooms and an engine control room.

On the main deck within the accommodation, there are two electrical equipment rooms containing UPSs for the main DP system. Above that is the navigation bridge, containing the main duplex DP system with one Differential Global Positioning System (DGPS), a fan beam laser, two Motion Reference Unit (MRUs), two wind sensors and two gyros. The backup simplex DP system is located in the engine control room, along with a DGPS, a gyro, an MRU, a wind sensor and a UPS. An isolation box allows all DP control systems to share all position reference systems and sensors.

There are two separation design intents to be proven:

1. Power and propulsion: The separation between the two redundant DP equipment groups normally under control of the duplex main DP systems.
2. DP control: The separation between the main and backup DP systems.

The separation verification tables are given in Table C2.1: Separation analysis for power and propulsion 1 and C2.2.

The physical installation of the power and control cabling to all components is the most challenging to verify and document. The level of analysis required by this information paper is limited to confirming that the location of equipment aligns with the separation design intent, and that there are viable and separate cable and pipe routes to locations intended to be physically separated from each other.

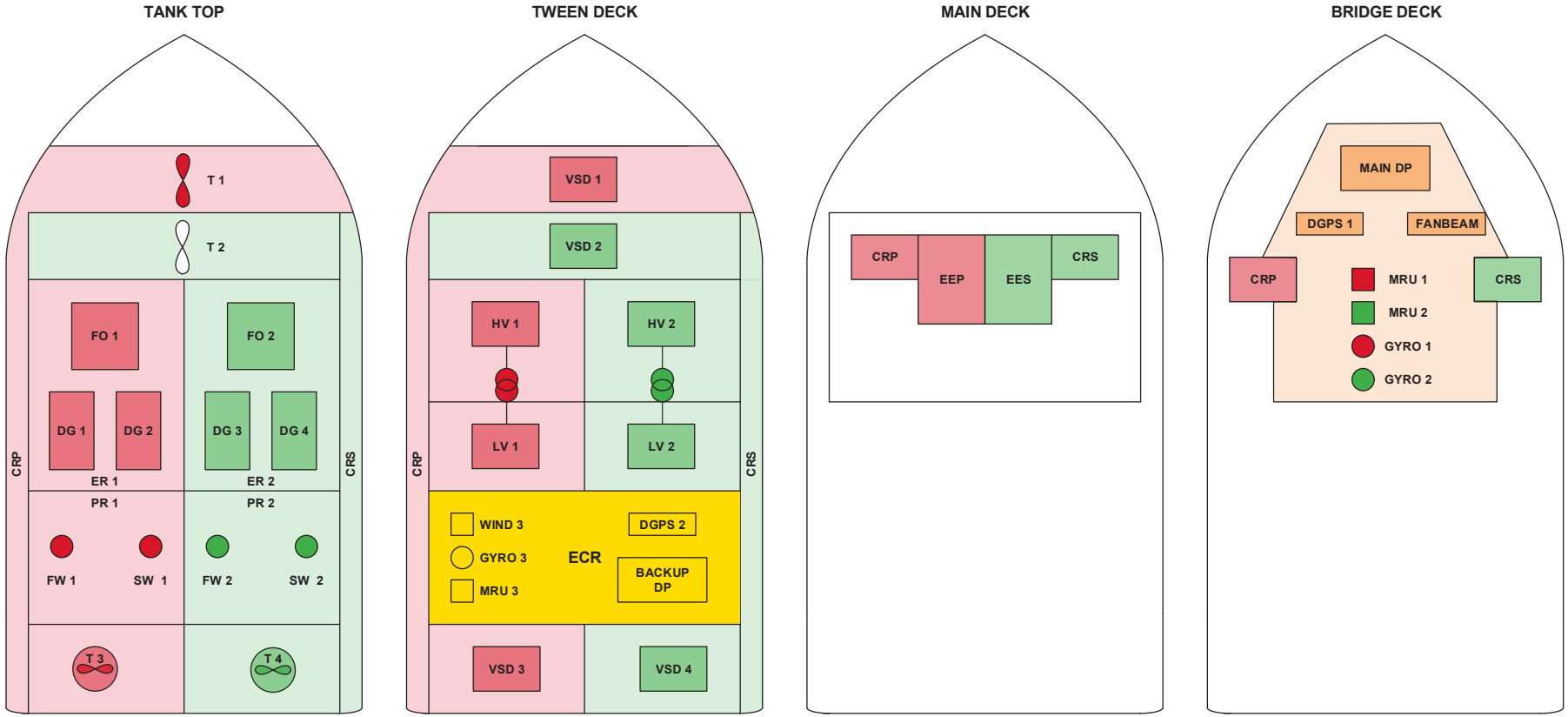

Figure C2.1: *Arrangement of port and starboard DP equipment groups*

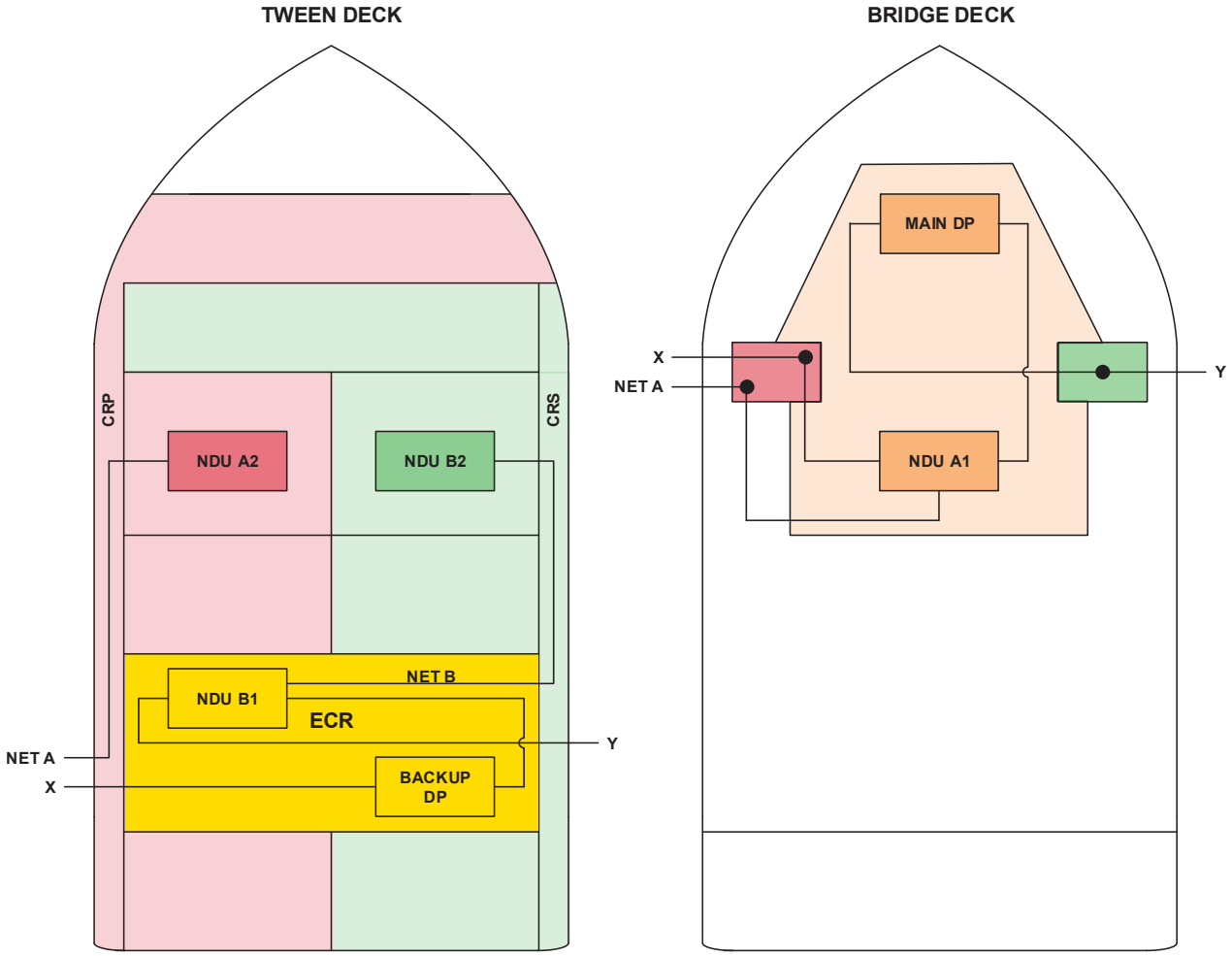

Figure C2.2: *Arrangement of DP control networks*

Separation – POWER and PROPULSION					
	Port DP equipment group			Stbd DP equipment group	
Deck	Compartment	Components	Colocation	Components	Compartment
Tank top	T1 – LOWER	T1, Motor and HPU	NDU A2 cables to FS in STBD GROUP NDU B2 cables to FS in PORT GROUP	T2, Motor and HPU	T2 – LOWER
	ER1	FO1 DG1 DG2		FO2 DG3 DG4	ER2
	PR 1	FW1 SW1		FW2 SW2	PR 2
	T3 – LOWER	T3 and Motor		T4 and Motor	T4 – LOWER
Tween deck	T1 – UPPER	VSD1		VSD2	T2 – UPPER
	HV – PORT	HV1 HV XFMR1		HV2 HV XFMR2	HV – STBD
	LV – PORT	LV1 LVXFMR 1		LV2 LVXFMR 2	LV – STBD
	T3 – UPPER	VSD3		VSD4	T4 – UPPER
Main deck	EEP	UPS1		UPS2	EES

Table C2.1: *Separation analysis for power and propulsion*

Separation: DP control			
DP control system	Deck	Compartment	Components
Main DP control	Tween deck	ECR	NDU B1 MRU 1 and 2 WIND 1 and 2 GYRO 1 and 2 DPC 2
Colocation	Main deck Tween deck	Port cable route	Cable for fire backup switch Cable for sensor isolation box Backup DP system to NDUA1 Net A
		Stbd cable route	Main DP system to NDUB1
Backup DP control	Main deck	Forward bridge	NDU A1 MRU 3 WIND 3 GYRO 3 UPS 3 DPC 1

Table C2.2: *Separation analysis for DP control*

Appendix D: Operating instructions for FMEA sense check (heat map generator)

An FMEA should contain certain components. The expected components are listed in the first column of table D1.2.

Concluding upon the absolute accuracy of an FMEA would require the analysis to be repeated and the findings compared. However, it is possible to infer its accuracy, to some extent, from the degree of consistency between:

- Analysis components within each subsystem.
- Analysis components in the subject subsystem and other subsystems to which it may have an interface.
- The analysis components in the subsystem and the overall redundancy design intent.

An assessment mechanism is provided in table D1.2, FMEA sense check. This process should be performed on each subsystem (functional group) to provide a series of subsystem scores which can then be averaged over all subsystems to provide a score for the FMEA itself. Although the overall average score provides a general indication, it is important that every subsystem is properly analysed. In this respect, the subsystem score and individual elements within the heat map are more important.

The Y-axis of the FMEA sense check (table D1.2) contains the anticipated analysis components. The X-axis is an indication of both consistency and intuitiveness. Consistency is considered to be more important than intuitiveness.

The concept of the heat map was chosen because it provides an overall assessment and granular detail in a compact format. The colours provide specific detail on deficiencies to offset the smoothing effect of the average score, and therefore reducing the possibility that a high average score masks a serious deficiency in an important system.

An FMEA with many omissions or inconsistencies is likely to draw unreliable conclusions about the DP vessel's station-keeping integrity. VTOs are encouraged to use this tool for initial assessment of the FMEA FMEA before preparing the assurance document in order to determine where focus is required.

Individual subsystem scores can be used to generate a heat map of the FMEA, as shown in tables D1.1 and D1.2.

	Auxiliary systems					Distribution		Gen	Safety	Control		Score
	FO	LO	Air	SW	FW	690V	480V			PMS	DPC	
Doc	0	0	0	0	0	0	0	3	3	3	3	12
Sketch	4	4	4	4	4	4	4	4	0	0	4	36
Test	1	2	3	4	5	4	3	0	2	1	0	25
CP	5	4	3	2	1	1	0	4	2	3	4	29
SFP	5	0	1	3	5	1	3	2	5	4	2	31
CP	2	1	3	1	5	5	5	1	1	1	1	26
RVT	0	0	0	0	0	1	3	1	5	2	1	13
RC	3	3	3	4	5	5	5	4	4	4	4	44
Con	1	2	3	4	5	4	3	0	2	1	0	25
ACTUAL	21	16	20	22	30	25	26	19	24	19	19	
	109					51		19	24	38		Average 48.7%
Completion	48.4%					56.7%		42.2%	53.3%	42.2%		
Weight	0.1					0.25		0.3	0.2	0.15		1
	4.8%					14.2%		12.7%	10.7%	6.3%		Weighted average 48.7%

Table D1.1: *Example 1 heat map for DP system FMEA*

	Auxiliary systems					Distribution		Gen	Safety	Control		Score
	FO	LO	Air	SW	FW	690V	480V			PMS	DPC	
Doc	3	3	3	3	3	1	1	3	1	2	2	25
Sketch	4	4	4	4	4	4	4	4	0	0	3	35
Test	1	2	3	4	5	3	3	0	2	1	0	24
CP	5	4	3	2	1	1	0	4	2	3	4	29
SFP	5	0	1	3	5	1	3	2	2	4	2	28
CP	2	1	3	1	5	2	2	1	1	1	1	20
RVT	3	3	3	3	3	1	3	1	2	2	1	25
RC	3	5	5	4	5	5	5	4	4	4	4	48
Con	5	5	4	3	5	4	3	0	2	1	0	32
ACTUAL	31	27	29	27	36	22	24	19	16	18	17	
	150					46		19	16	35		Average 53.7%
Completion	66.7%					51.1%		42.2%	35.6%	38.9%		
Weight	0.1					0.25		0.3	0.2	0.15		1
	6.7%					12.8%		12.7%	7.1%	5.8%		Weighted average 45.1%

Table D1.2: *Example 2 heat map for DP system FMEA*

Review of tables D1.1 and D1.2 indicates that these FMEAs have predominantly warm colours and the average score is around 50% of the possible marks for consistency and comprehension. This result suggests a more in-depth review of the FMEA may be warranted before presenting the information in the assurance document.

Further refinement of this process is possible using a weighted average. The examples in table D1.1 and D1.2 have been extended to show the effect of:

- Reducing the contribution from those systems that are historically less likely to contain common points that are not revealed through analysis, such as auxiliary systems.
- Boosting the contribution of those systems that are known to feature more prominently in DP incidents.

In example 1, the weights produce no significant difference between the average and the weighted average. However, in example 2 the weighted average is significantly lower when weighting is applied to the systems that are more commonly associated with DP incidents as causal or contributory factors. It should be noted that errors and omissions in the analysis of power generation, power distribution and power management systems may have a greater impact on the station keeping integrity of DP vessels operating with their bus ties closed. For this reason, it is reasonable to increase the weighing applied to these subsystems in the assessment of FMEAs for closed bus tie configurations.

Example weighting factors are given below. Any appropriate weighting scheme can be applied, but the justification for applying the chosen weights should be recorded in the assurance document.

Subsystem	**Weighting factor**
Auxiliaries	10%
Control (PMS DPCS and networks)	15%
Safety (F&G ESD)	20%
Power distribution (including control power)	25%
Power generation	30%

Although the average score may be of general interest, the individual scores for each analysis element in each subsystem should be the focus of any remedial work.

FMEA sense check for each functional group								
Analysis Components	**Substantiating documentation** (document from which the analysis was generated and/or supports its conclusions)	0	1	2	3	4	5	
	System sketches (Intuitive means of communicating the functionality and the redundancy of a functional group)	0	1	2	3	4	5	
	Link to validation (testing and other activities undertaken to ensure acceptance criteria have been 0 1 2 3 4 5 met. Validation in this context is by testing and includes effectiveness of compensating provisions.))	0	1	2	3	4	5	
	Compensating provisions (compensating provisions are mitigations in place to prevent failure effects exceeding the WCFDI)	0	1	2	3	4	5	
	Single failure propagation analysis (the analysis carried out to determine the failure effects and end effects (impact on thrust) of the identified common points)	0	1	2	3	4	5	
	Identification of common points (common points selected from subsystems sketch)	0	1	2	3	4	5	
	Redundancy Verification Table (identify components and common points in each subsystem)	0	1	2	3	4	5	
	Redundancy concept (for each subsystem)	0	1	2	3	4	5	
	Configuration (vessel's intended configuration for operations, as documented in the FMEA)	0	1	2	3	4	5	
		Omitted	**Provided but inconsistent with:**			**Consistent**		
			RDI	**Analysis components**	**Other subsystems**	**But not intuitive**	**And intuitive**	**Subsystem Score**
		Analysis component not provided	Provided but inconsistent with overall DP RDI	Consistent with RDI but inconsistent between analysis components for same subsystem	Consistent with RDI and between analysis components but inconsistent between subsystems	Consistent with RDI and between components and subsystems, but not presented in an intuitive format	Consistent with RDI and between components and subsystems, and presented in an intuitive format	

Table D1.3: *Heat map generator*

Appendix E: Hierarchy of controls heat map

			Commonalities in systems				
Hierarchy of controls applied	**Elimination**	E	Removal of any physical connection between the bus sections	Supply from same redundant group eliminating cross-connections, changeovers, and other common points.	Elimination of networks that do not play an active part in the DP control system and redundancy concept	Elimination of the reliance on supervisory control system to ensure no fault propagation pathways exist. Control system can be autonomous and at the lowest level, thus removing the need to communicate information such asDP on each thruster.	Removal of any physical connection between the redundant groups
	Substitution	D	Proven better technology to replace the bus tie-breaker	N/A	Profibus or fibre optic networks to mitigate common protocol/medium vulnerabilities	Proven better technology to replace the control system with a system that is more autonomous and fault tolerant	N/A
	Engineering controls	C	Verified and validated effective protections in place to mitigate fault transfers	Verified and validated effective protections in place to mitigate fault transfer	Verified and validated effective protections in place to mitigate fault transfer, e.g. network storms	Verified and validated effective protections in place to mitigate fault transfer	Verified and validated effective protections in place to mitigate fault transfer. Effective design changes made to address commonalities.
	Administrative controls	B	Procedures/checklists to ensure correct bus configuration is set up for operations	Isolations of cross-connections or changeover using checklists	Procedures/checklists to ensure no alarms are hidden. Fall back to Independent Joystick(IJS) on complete network failure.	Procedures/checklists to ensure no alarms are hidden. Ensure no default/debug modes setup after software updates.	Procedures/checklists to ensure no alarms are hidden. Isolations of cross-connections and changeover using checklists.
	No controls	A	Bus configuration has no controls	No controls over distribution cross-connections, changeovers and other common points.	No protection in place to prevent fault transfer/loss of communication	No protection in place to prevent fault transfer/loss of communication	No controls over distribution cross connections, changeovers. No protection in place to prevent fault transfer/loss of communication.
	Functional groups		1	2	3	4	5
			Power generation (bus configuration)	**Power distribution** (control power/ups distribution, cross-connections/changeovers)	**Networks** (network storms/ communication failures)	**Control system** (communication failures/PLC failures/supervisory control)	**Auxiliary systems** (cross-connections/ mechanical changeover)
	Causal and contributory factors of incidents (sequenced by frequency)						

Oil Companies
International Marine Forum
29 Queen Anne's Gate
London SW1H 9BU
United Kingdom

T +44 (0)20 7654 1200
E enquiries@ocimf.org

ocimf.org