



**TECHNICAL AND OPERATIONAL GUIDANCE
(TECHOP)**

TECHOP (D-01 - Rev1 - Jan21)

**ADDRESSING C³EI² TO ELIMINATE SINGLE POINT
FAILURES
(C³EI² - CROSS-CONNECTIONS, COMMONALITY,
EXTERNAL INTERFACES AND INFLUENCES)**

JANUARY 2021

DISCLAIMER

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

CONTENTS

SECTION	PAGE
1 INTRODUCTION	6
2 SCOPE, IMPACT AND COMMON MISCONCEPTIONS	7
2.1 SCOPE	7
2.2 IMPACT ON PUBLISHED GUIDANCE	7
2.3 COMMON MISCONCEPTIONS	8
3 CASE FOR ACTION	10
3.1 FAULT TOLERANT SYSTEMS BASED ON REDUNDANCY	10
3.2 EXAMPLE DP INCIDENTS CAUSED BY CROSS-CONNECTIONS	11
3.3 EXAMPLE DP INCIDENTS CAUSED BY COMMONALITY	12
3.4 EXAMPLE DP INCIDENTS CAUSED BY FAILURES IN EXTERNAL INTERFACES	12
4 VISUALISING COMMONALITY	14
4.1 PRACTICAL DP SYSTEMS	14
4.2 INFLUENCE OF CAM AND TAM	15
4.3 TYPICAL CONTROL POWER ARRANGEMENTS	15
5 TAXONOMY OF CROSS-CONNECTIONS	18
5.1 RISK ASSOCIATED WITH CONTROL POWER CROSS-CONNECTIONS	18
5.2 LOAD AND SUPPLY SIDE	20
5.3 HIGHEST RISK & HIGHER RISK	21
5.4 HIGH RISK	23
5.5 FURTHER EXAMPLES	25
6 EVALUATING CONTROL POWER CROSS-CONNECTIONS	28
6.1 INITIAL EVALUATION	28
6.2 CATEGORISING CONTROL POWER CROSS-CONNECTIONS	29
7 PENALTIES OF ISOLATION	32
7.1 AVOIDING ASSUMPTIONS	32
7.2 CAUTIONARY NOTES	32
7.3 EFFECT OF ISOLATION ON POST FAILURE DP CAPABILITY	33
7.4 HIDDEN FAILURES	39
7.5 ASSESSING THE RELATIVE RISK	39
7.6 TWO-WAY SPLIT	39
7.7 MULTI-WAY SPLIT	40
8 VERIFICATION AND VALIDATION	41
8.1 ANALYSIS	41
8.2 TESTING	41
8.3 COMMONALITY AT UPS INPUT SIDE	41
8.4 OVERVOLTAGE	41
8.5 MAIN CLASS REQUIREMENTS FOR SAFETY SYSTEMS	42
8.6 ALARMS	42

APPENDICES

APPENDIX A CROSS-CONNECTIONS

- A.1 CROSS-CONNECTIONS - GENERAL
- A.2 CROSS-CONNECTIONS IN CONTROL POWER SUPPLIES
- A.3 TOOLS FOR EVALUATION
- A.4 CLOSED BUSTIES

APPENDIX B COMMONALITY

- B.1 ADDRESSING COMMONALITY
- B.2 COMMONALITY IN DP CLASS 3 DESIGNS
- B.3 GROUND FAULTS – PROPAGATION THROUGH SHIP'S HULL
- B.4 MARINE AUXILIARY SERVICES
- B.5 NETWORKS
- B.6 NETWORK TESTING

APPENDIX C EXTERNAL INTERFACES & INFLUENCES

- C.1 EXTERNAL INTERFACES & INFLUENCES
- C.2 FIRE & GAS AND EMERGENCY SHUTDOWN (ESD)
- C.3 OTHER EXTERNAL INTERFACES

FIGURES (IN MAIN DOCUMENT)

Figure 3-1	Generalised DP Redundancy Concept	10
Figure 4-1	Degrees of Commonality	14
Figure 4-2	Not Cross-connected in Any Way	15
Figure 4-3	Circuit Breakers Allow Isolation of Dual Supplies	16
Figure 4-4	No Protection Unless Circuit Breakers are Opened at One Supply	16
Figure 4-5	Protection Against Some Types of Faults by dc/dc Converter	17
Figure 4-6	Limited Protection by Diodes	17
Figure 5-1	Example of Highest Risk Categorisation Using a Diode Type Cross-connection	19
Figure 5-2	Example of Higher Risk Categorisation Using a Diode Type Cross-connection	19
Figure 5-3	Example of a High-Risk Categorisation Using a Diode Type Cross-connection	20
Figure 5-4	Cross-connections in Supply and Load Side	21
Figure 5-5	Highest / Higher Risk Cross-connections	22
Figure 5-6	Common Negative Power Supply Rail on Floating Systems – Highest Risk	23
Figure 5-7	High Risk Cross-connections	24
Figure 5-8	Common Point With No Over-current Protection	25
Figure 5-9	Dual Supply to a Field Station is Protected by Redundancy Modules	26
Figure 5-10	Misalignment in ac Side	27
Figure 6-1	Initial Evaluation	28
Figure 7-1	Cross-connections Spanning the Redundancy Groups in a Three-way Split	36
Figure 7-2	Cross-connection Isolated – Three-way Split Becomes Two-way Split	37
Figure 7-3	Effects of Isolation on Post Failure DP Capability	38

1 INTRODUCTION

1.1 PREAMBLE

1.1.1 The guidance documents on DP (Design and Operations and People) were published by the MTS DP Technical Committee in 2011, 2010 and 2012, respectively. Subsequent engagement has occurred with:

- Classification Societies (DNV, ABS)
- United States Coast Guard (USCG)
- Marine Safety Forum (MSF)
- Oil Companies International Marine Forum (OCIMF)

1.1.2 Feedback has also been received through the comments section provided in the MTS DP Technical Committee Web Site.

1.1.3 It became apparent that a mechanism needed to be developed and implemented to address the following in a pragmatic manner.

- Feedback provided by the various stakeholders.
- Additional information and guidance that the MTS DP Technical Committee wished to provide and a means to facilitate revisions to the documents and communication of the same to the various stakeholders.

1.1.4 The use of Technical and Operations Guidance Notes (TECHOP) was deemed to be a suitable vehicle to address the above. These TECHOP Notes will be in the following categories:

- General TECHOP (G)
- Design TECHOP (D)
- Operations TECHOP (O)
- People TECHOP (P)

1.2 TECHOP NAMING CONVENTION

1.2.1 The naming convention, TECHOP (CATEGORY (G / D / O / P) – Seq. No. – Rev.No. – MonthYear) TITLE will be used to identify TECHOPs as shown in the examples below:

Examples:

- TECHOP (D-01 - Rev1 - Jan21) Addressing C³EI² to Eliminate Single Point Failures
- TECHOP (G-02 - Rev1 - Jan21) Power Plant Common Cause Failures
- TECHOP (O-01 - Rev1 - Jan21) DP Operations Manual

Note: Each Category will have its own sequential number series.

1.3 MTS DP GUIDANCE REVISION METHODOLOGY

1.3.1 TECHOPs as described above will be published as relevant and appropriate. These TECHOP will be written in a manner that will facilitate them to be used as standalone documents.

1.3.2 Subsequent revisions of the MTS Guidance documents will review the published TECHOPs and incorporate as appropriate.

1.3.3 Communications with stakeholders will be established as appropriate to ensure that they are notified of intended revisions. Stakeholders will be provided with the opportunity to participate in the review process and invited to be part of the review team as appropriate.

2 SCOPE, IMPACT AND COMMON MISCONCEPTIONS

2.1 SCOPE

2.1.1 Cross-connections continue to be a significant causal and contributory factor of DP incidents despite the guidance on cross-connections published in the various documents by the MTS DP Committee.

2.1.2 This TECHOP is an amalgamation of parts of three previous TECHOPs on similar subjects augmented by new information pertinent to delivery of predictable incident free DP operations:

- TECHOP_ODP_10_(D) (EXTERNAL INTERFACES)
- TECHOP_ODP_11_(D) (CROSS_CONNECTIONS)
- TECHOP_ODP_13_(D) (CONTROL POWER SUPPLIES & AUTO CHANGEOVERS)

2.1.3 The TECHOP, by design, is comprehensive and contains examples demonstrating issues prevalent in experienced DP incidents associated with:

1. Cross-connections between redundant equipment groups.
2. Commonality shared between redundant groups.
3. External interfaces & influences (affecting DP system as a whole).

2.1.4 Evidence from DP incident data and learnings from incidents (LFIs) confirms that cross-connections, commonality, external interfaces and external influences (in and on all parts of the DP system) continue to be significant causal and contributory factors in DP incidents. They are often the reason that failure effects exceed anticipated consequences and sometimes the worst-case failure design intent.

2.1.5 This TECHOP subdivides vulnerabilities into three themes to facilitate ease of dissemination of information. These three themes are (with examples):

1. **Cross-connections between redundant equipment groups:**
 - a. Control power supplies.
 - b. Closed bus-ties.
2. **Commonality shared between redundant groups:**
 - a. Power consumers that are associated with more than one redundancy group.
 - b. Networks (redundant and non-redundant including networks introduced for providing Human Machine Interface (HMI) and perceived to be devoid of DP control functionality).
 - c. Marine auxiliary systems - Ventilation systems, fuel distribution system etc.
3. **External interfaces & influences (affecting DP system as a whole):**
 - a. ESD, Fire & Gas safety shutdown systems including E-Stops for fuel pumps.
 - b. Draught sensors.
 - c. Fuel (quality), atmosphere, ionosphere, water column.

2.2 IMPACT ON PUBLISHED GUIDANCE

2.2.1 This TECHOP supplements information provided in the MTS DP Vessel Design Philosophy Guidelines.

2.2.2 This TECHOP has appendices which contain detailed information including diagrams to illustrate the problems which may be encountered. Diagrams provided in this TECHOP are intended to illustrate the problems associated with cross-connections, commonality and interfaces. It is emphasised that they are not intended to represent practical or good examples of how such connections or interfaces could be created.

2.3 COMMON MISCONCEPTIONS

2.3.1 Each of the three themes listed above is discussed in a dedicated appendix. A significant part of this TECHOP is devoted to vulnerabilities introduced into the DP system by cross-connections which are often introduced with the best of intentions.

Cross-connections are usually introduced:

- To allow functionality to be maintained after a failure, often to reduce the severity of the effects of higher probability failures. However, such cross-connections do not restore fault tolerance, and seldom reduce vulnerability to non-productive time.
- for compliance (perception based?) with other requirements (example – main class / main propulsion rules, SOLAS etc.)

Note:

1. *Requirements of main class / main propulsion rules have evolved to address issues prevalent on vessels which may not have been designed to the same principles of redundancy as DP vessels. An example is the requirement for a secondary source of supply (examples - power, hydraulics). DP vessel designs which do not consider the consequences of such secondary sources of supply crossing redundancy groups may introduce unwarranted vulnerability to failures that could exceed the Worst Case Failure Design Intent (WCFDI).*
2. *Early identification of such requirements which could introduce vulnerability to the redundancy concept and engagement with class for alternate proposals can lead to solutions which satisfy main class requirements without compromising DP redundancy by introduction of cross-connections.*

2.3.2 A common misconception is to confuse cross-connections with added redundancy without recognising that such cross-connections have the potential to defeat the redundancy concept by weakening attributes of fault resistance, fault tolerance and fault ride-through.

2.3.3 Another prevalent misconception is that opening bus-tie circuit breakers at the highest power distribution level is adequate to isolate all fault transfer paths and adhere to the principles of independence and segregation. The cross-connections that are left within any system and / or distribution level become potential fault transfer paths compromising fault tolerance, fault resistance and fault ride-through. Segregation strategies to align with the redundancy concept should be applied at all power distribution levels.

2.3.4 Several solutions are offered as potential mitigations of the risks posed by cross-connections. The most effective and least burdensome mitigation is of course not to introduce them where this can be avoided. Where cross-connections are unavoidable or are introduced to achieve stated objectives (such as emission reduction, lowering running hours etc.), mitigations against fault propagation should include validation testing for benign and aggressive failures. In such cases, these cross-connections should be clearly identified and documented in the FMEA along with the compensating provisions, verification and validation testing (requirements and results) including periodic testing.

Note: Cross-connections and auto changeovers in control power supplies continue to be a cause of DP incidents. The potential threat they pose is often overlooked in DP system FMEAs. Even when they are identified, analysis may focus only on benign failure modes. It can be difficult to prove that such cross-connections do not compromise the DP redundancy concept by analysis alone. There can be significant reluctance to carry out validation testing to prove that failure effects do not exceed the WCFDI. Such reluctance could be a result of shortage of time, lack of awareness of failure effects and consequences including fear of testing and impacts on equipment etc.

2.3.5 Designs which incorporate mitigations of fault propagation paths should be verifiable and effectiveness validated by testing. Examples of such mitigations are isolation valves in auxiliary systems, and diodes, fuses, circuit breakers, dc/dc convertors, and other forms of galvanic isolation in electrical systems. It should be recognised that there is a wide range of variability in the effectiveness of such mitigations spanning from 'not effective' to 'partially effective' and 'effective'.

2.3.6 Non-verifiable methods of mitigation, which cannot be validated by testing, should not be proposed.

Note: For systems that have been designed with avoidable cross-connections, common power supplies and automatic changeovers, demonstrating the robustness of systems may be difficult. Especially if they have not been subjected to a rigorous system engineering design process and effective testing. Mitigating the risks in the available time scale and satisfying stakeholder's concerns is likely to involve isolating backup supplies and locking changeovers in the most favourable position for CAM. These actions may place limitations on vessel operability and post failure DP capability that should be managed.

Such limitations can be avoided by using alternative solutions (as an example, alternate supplies from same redundancy group). Such alternate solutions are potentially more cost effective than trying to prove fault tolerance and more effective in building confidence in the robustness of the system.

3 CASE FOR ACTION

3.1 FAULT TOLERANT SYSTEMS BASED ON REDUNDANCY

3.1.1 Loss of position may occur in several ways:

- **Drift off** – Insufficient thrust following a failure.
- **Drive off** – Exceeds thrust requirements or thrust in the wrong direction following a failure.
- **Large excursion** - Vessel returns to set point after a failure but with an unacceptably large deviation.
- **Force off** – The vessel has insufficient thrust in the intact condition to maintain position in the prevailing environmental conditions.

3.1.2 DP vessels of equipment classes 2 and 3 are intended to be single fault tolerant. This requirement is satisfied by the provision of redundant systems each capable of developing surge, sway and yaw forces either alone or in combination as shown in Figure 3-1. In an ideal system, DP equipment Groups A and B would be completely independent with no cross-connections or commonality. In a practical design, it is not possible to achieve absolute separation of the two systems and cross-connections generally exist between the two groups to allow common control of generators, switchboards and thrusters. The fault tree in Figure 3-1 shows the two ways in which a DP vessel can lose position because of a fault, which are 'drift-off' and 'drive-off'. A drive-off can occur if either group fails in such a way that it causes too much thrust to be developed or thrust in the wrong direction. For a drift-off to occur, both redundant groups have to fail in some way. For this to occur when the DP redundancy concept was intact, before a single failure occurred, there must be a mechanism that allows a fault in one group to propagate to the other redundant group causing it to malfunction. Cross-connections or commonality between redundant groups are the means by which failure effects propagate between redundant groups. Either the fault occurs in the cross-connection or common point itself or the failure effects propagate by way of the connection or common point.

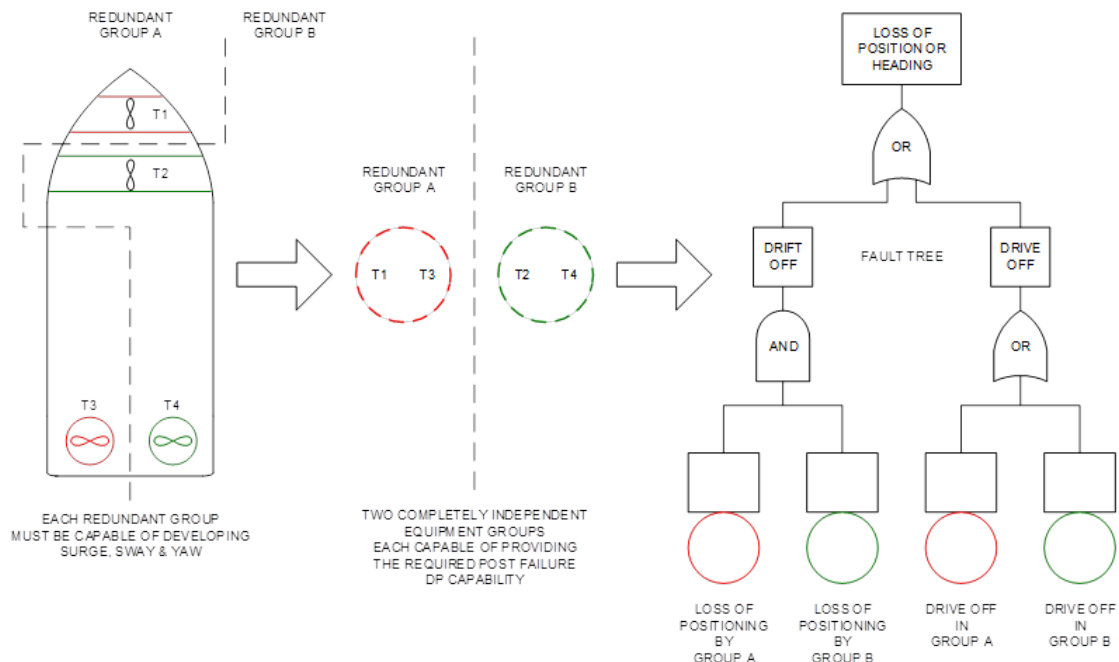


Figure 3-1 Generalised DP Redundancy Concept

3.2 EXAMPLE DP INCIDENTS CAUSED BY CROSS-CONNECTIONS

3.2.1 Failure effects propagating by way of cross-connections have caused DP loss of position incidents. The examples below provide some insight into how and why these incidents occurred.

1. A DP class 2 semi-submersible had two sources of supply to each thruster's control system. The main source of supply was the emergency switchboard. When the emergency switchboard lost power, the thruster control panels changed over to the backup supply but the small glitch during changeover caused thrusters to stop exceeding the worst-case failure design intent.
2. A large crane / pipelay vessel had a common 24Vdc distribution system for all engine governors with multiple sources of supply. This design was accepted on the basis of the high reliability of the distribution system. Unfortunately, the same distribution system was used for non-DP-related functions throughout other parts of the vessel and an electrical fault developed which caused all the engine governors to malfunction, leading to blackout.
3. A ROV support vessel had four independent 24Vdc control supplies connected through a common switchboard control system wiring. An earth fault on one generator control power supply caused all online generators to stop.
4. A DP class 2 construction vessel had two 110Vdc supplies for switchboard controls that were connected by diodes and fuses. One fuse became intermittent and went open circuit. Thus, both main switchboards were found to be running from one supply with no alarm and no fault-tolerance in the event of failure.
5. A well stimulation vessel had individual UPSs for each thruster control system and a common backup 24Vdc supply from a charger / rectifier on the emergency switchboard by way of diodes. The charger suffered an internal fault and coupled a much higher voltage on to the 24Vdc supply. All thruster controllers were damaged.
6. A DP class 2 drilling rig had two independent control power supplies that could be cross connected by a manual changeover switch. A fault in the changeover switch caused the failure of both control supplies and blackout.
7. A DP class 3 diving support vessel had an auto changeover on the ac control power supplies to the thruster control systems that allowed the centre bow thruster to be powered from the same control supplies as either the forward or aft bow thrusters. A test to simulate a short circuit in the centre control panel proved that all bow thruster control supplies would trip leaving the vessel with no thrust at the bow.
8. A large DP class 2 pipe laying vessel has engines with electrical governor actuators. Fuel rack position feedback was provided as part of the actuator control loop. The feedback failed on one actuator causing the actuators to advance to the full fuel position. The faulty engine took the entire system load tripping other engines on reverse power before tripping itself causing a blackout.
9. A DP class 2 diving vessel had governors with speeder motors controlled from a centralised power management system. The vessel operated with its busties closed. The generator governors were trimmed by a pilot motor controlled by a dry contact relay. The relay contacts on the speed-raise function welded together and caused one engine to trip all others on reverse power leading to blackout.
10. A DP class 2 pipe laying vessel suffered a short circuit fault in a generator. The bustie opened but unfortunately all low voltage supplies were lost on under voltage leading to loss of all thrusters.

3.3 EXAMPLE DP INCIDENTS CAUSED BY COMMONALITY

3.3.1 Failure effects propagating by way of common points have caused DP loss of position incidents. The examples below provide some insight into how and why these incidents occurred.

1. A DP class 3 diving vessel suffers intermittent loss of all bow thrusters when a network storm causes them to transfer spuriously to lever control.
2. A DP class 3 diving vessel had a common compressed air system for engine controls. This was accepted on the basis that the engines continued to run on loss of pressure. This control air supply was derived from the starting air supply by way of a single pressure regulator. The regulator failed and allowed high pressure through to the low-pressure side which forced its way through the solenoid valves operating the engine stop cylinders blacking out the vessel.
3. A DP class 2 diving vessel suffered a fault in the dual communication bus used to connect references and sensors to the DP computers. An interface module failed in such a way that it prevented other modules from using both networks. Neither DP computer could control the thrusters and position was lost.
4. A DP class 2 pipe laying vessel had a common engine alarm and shutdown system for both engine rooms. The alarm panel had an auto-changer between two sources of supply. However, a fault downstream of the changeover caused total loss of power to the panel and shutdown of all engines.
5. A platform supply vessel was being tested at annual DP trials. During the network storm test both controllers stopped, and the vessel suffered a drift off. The investigation revealed the hubs were not properly configured rendering the storm protection ineffective.
6. A DP class 3 diving vessel had a centralised power management system. The phase-back control lines for both main propellers located on a single I/O card. This card failed in such a way as to phase back both main propellers.
7. A DP class 3 diving vessel has a Master-Slave power management system. Normally, the master controls the entire vessel. A terminating resistor broke in the network used to update the slave with the status of the master. The slave received corrupted status data on the master. On the day the master failed the slave took over control and reconfigured the power plant using this corrupted data. As a result, the power management system tripped both service transformers. Causing loss of all auxiliary services and the vessel blackout.

3.4 EXAMPLE DP INCIDENTS CAUSED BY FAILURES IN EXTERNAL INTERFACES

3.4.1 Failure or malfunction of external interfaces have caused DP loss of position incidents. The examples below provide some insight into how and why these incidents occurred.

1. Pipe layer - Failure of external force compensation input leading to buckling of pipe.
2. Drillship - Failures of draught measurement system affects DP system model leading to drive off.
3. Semi-submersible – Failure of industrial power control interface allows regenerated power from drawworks to trip all generators on reverse power leading to blackout.
4. Drillship - Failure of ESD system- Communication errors in dual redundant remote I/O imitate activation of external ESD 0 causing the whole vessel to shut down.
5. Drillship - Failure of ESD system – Poor design of ventilation system combined with lack of robustness in declaring a confirmed fire. Automatic ESD 0 shutdown triggered by tank cleaning activities.

6. Semi-submersible - Failure of ESD system – Excessive commonality introduced by using a single I/O card for all ESD pushbuttons – Software error trips all diesel generators when one card loses power and is reconnected.
7. Pipe layer – Failure of water mist control system shuts down all three engine rooms when false pressure switch signals indicate water mist is being released.
8. Pipe layer - Erroneous application of external force compensation led to loss of position and buckling of pipe.

4 VISUALISING COMMONALITY

4.1 PRACTICAL DP SYSTEMS

- 4.1.1 An ideal redundant system is one that has no cross-connections or common points between (or external interfaces with) the redundant DP equipment groups. This condition is shown as 'A' in Figure 4-1. Validation and verification requirements for systems designed in this manner are limited to proving the performance of each redundant group and proving the means to detect degradation of that performance in service. However, such designs are impractical because some common points cannot be eliminated (examples - DP control systems spanning both redundant groups – commonality introduced by vessel hull, water column, atmosphere etc).
- 4.1.2 Practical implementation of redundancy thus introduces some commonality. However, design choices are available and that is depicted as 'B' and 'C' in Figure 4-1. The visual representation intuitively draws attention to 'B' as the design of choice since it restricts the commonality to the extent unavoidable or needed in order to achieve the functional aspects of the desired objectives (example – efficiency, reduction in emissions etc).
- 4.1.3 Design choices reflected in 'C' in Figure 4-1 will result in a greater burden of engineering studies, comprehensive analysis and verification and validation activities as a consequence of introducing unwarranted or unnecessary commonality and / or cross-connections (initially and during the vessel's lifecycle).
- 4.1.4 Design choices reflected in 'D' in Figure 4-1 are sometimes found in vessels and usually are reflective of a desire to maximise uptime by reducing the perceived failure effects without realising that the consequences of such design choices could lead to a loss of position. In some cases it is justified, often without basis, that such commonality has no impact on the DP system.

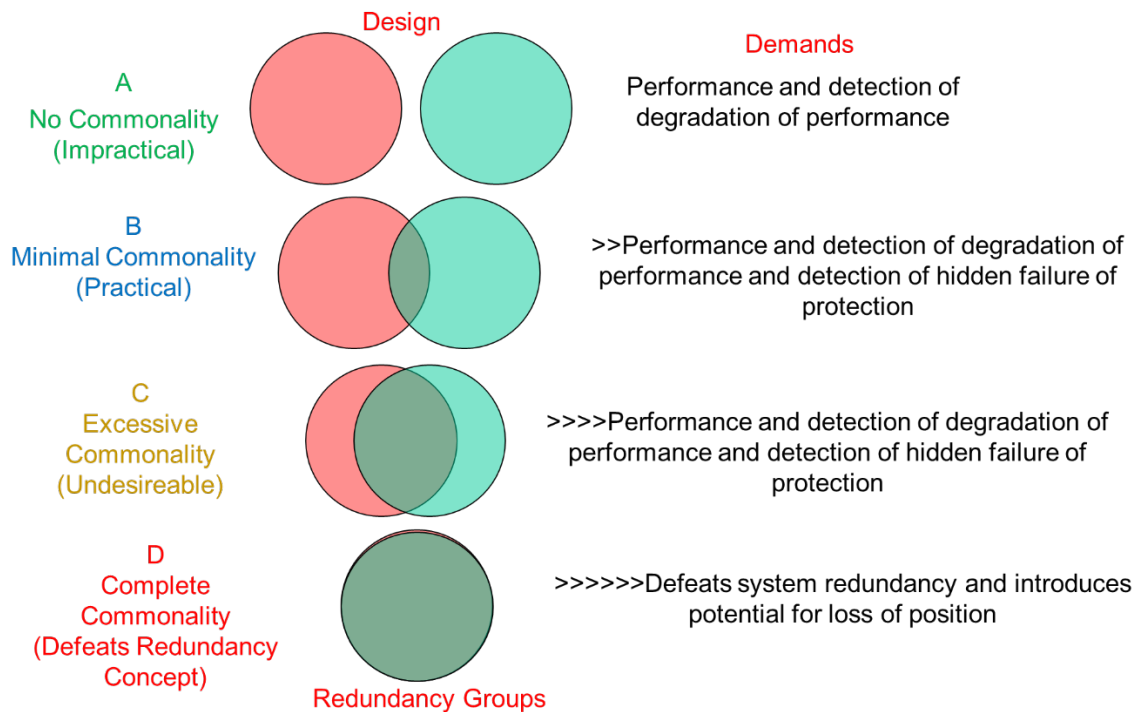


Figure 4-1 Degrees of Commonality

4.2 INFLUENCE OF CAM AND TAM

- 4.2.1 The concepts of CAM and TAM are central to MTS DP Operations Guidance but also strongly influence design philosophy. Critical Activity Mode is the DP system configuration that provides the highest level of station keeping integrity. Isolating cross-connections with the potential to transfer failure effects during critical DP activities would be part of the process of setting up the vessel for operations in CAM. Reducing reliance on unvalidated protective functions would also be part of that process.
- 4.2.2 In Task Appropriate Mode (TAM) the consequences of a loss of position are known and acceptable and do not include risk to life, asset or the environment. Essentially, there may be a defined and acceptable commercial risk associated with failure to complete the work on time, equipment damage or the need for remedial work. In this mode of operation greater flexibility may be considered to achieve the vessel uptime objectives including the use of cross-connections and reliance on protective functions.

4.3 TYPICAL CONTROL POWER ARRANGEMENTS

- 4.3.1 Where control power cross-connections exist between redundant groups, different forms of fault isolation are used such as diodes or dc to dc convertors. In a few cases, there is no fault isolation at all (redundant supplies simply hardwired together).
- 4.3.2 In the completely isolated supply arrangement in Figure 4-2 there is no electrical connection between the power supplies for the two redundancy groups.

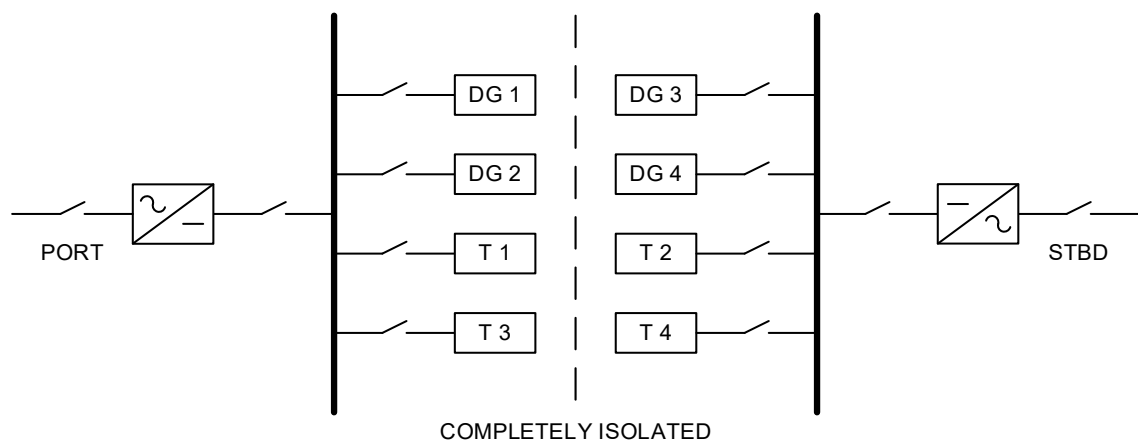


Figure 4-2 Not Cross-connected in Any Way

- 4.3.3 In Figure 4-3, there are two supplies to each of the generators and thrusters but it is possible to isolate one of them to make the power supply arrangement match the overall division in the redundancy concept.

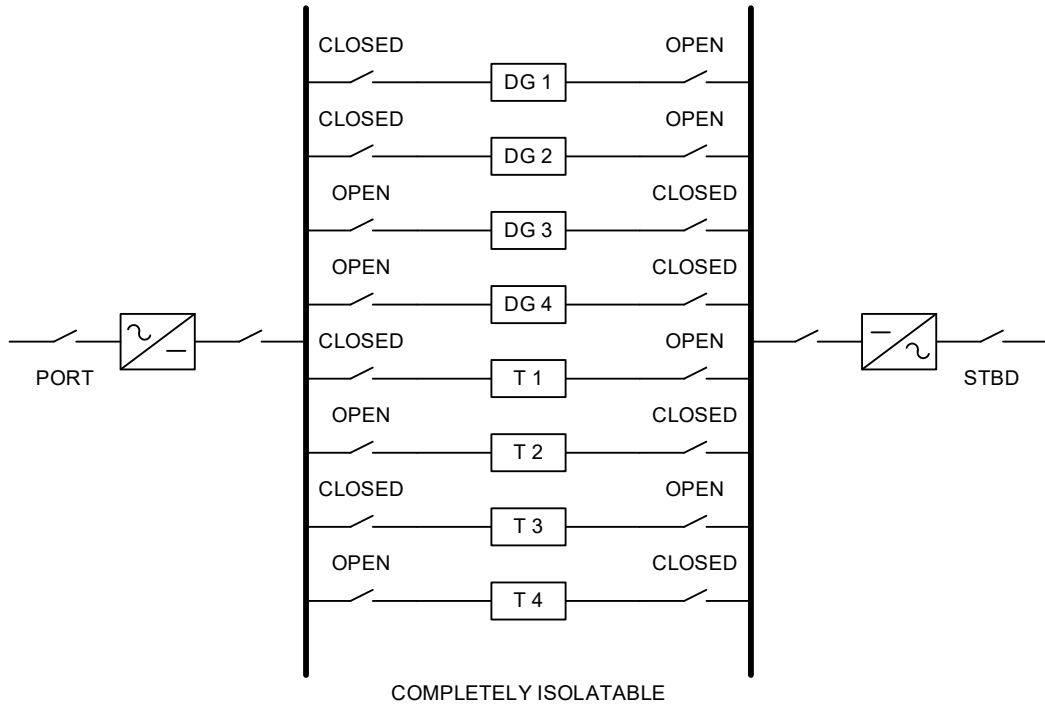


Figure 4-3 Circuit Breakers Allow Isolation of Dual Supplies

4.3.4

If the circuit breakers remain closed as shown in Figure 4-4 then any fault anywhere in the dc power distribution system will cause a voltage dip everywhere. The action of the circuit breaker may clear the fault but does not guarantee predictable failure effects.

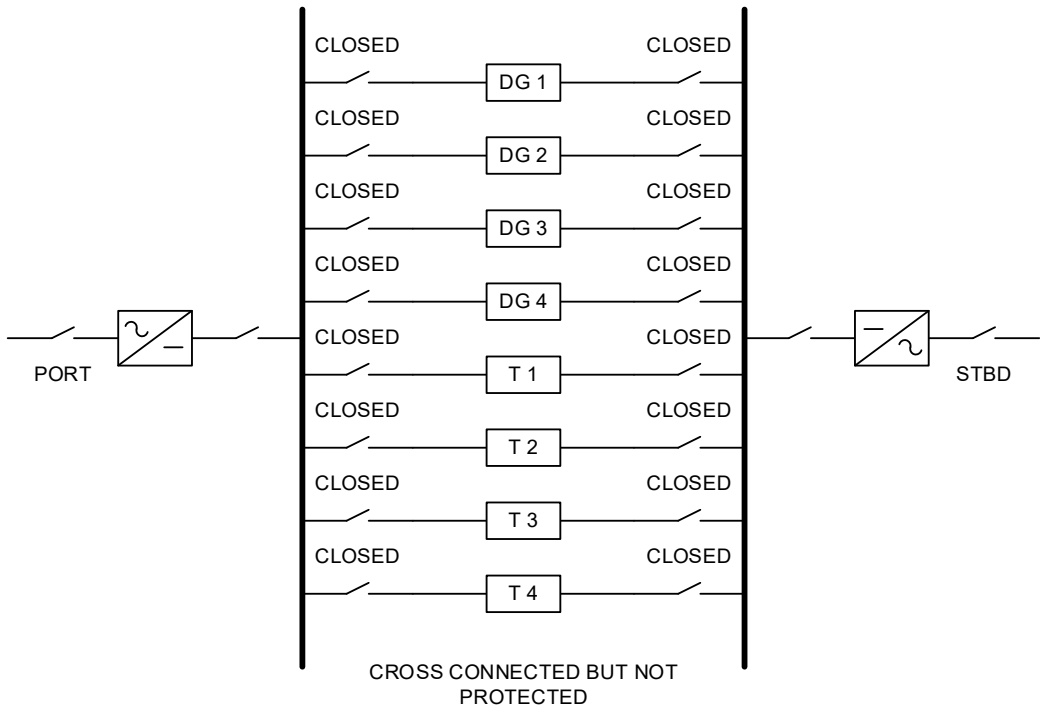


Figure 4-4 No Protection Unless Circuit Breakers are Opened at One Supply

4.3.5

In Figure 4-5 dc/dc convertors are used to provide a degree of isolation that is typically better than that provided by diodes but unless there is a full understanding of the functionality provided within the dc/dc converter it cannot be assumed to be fully fault tolerant.

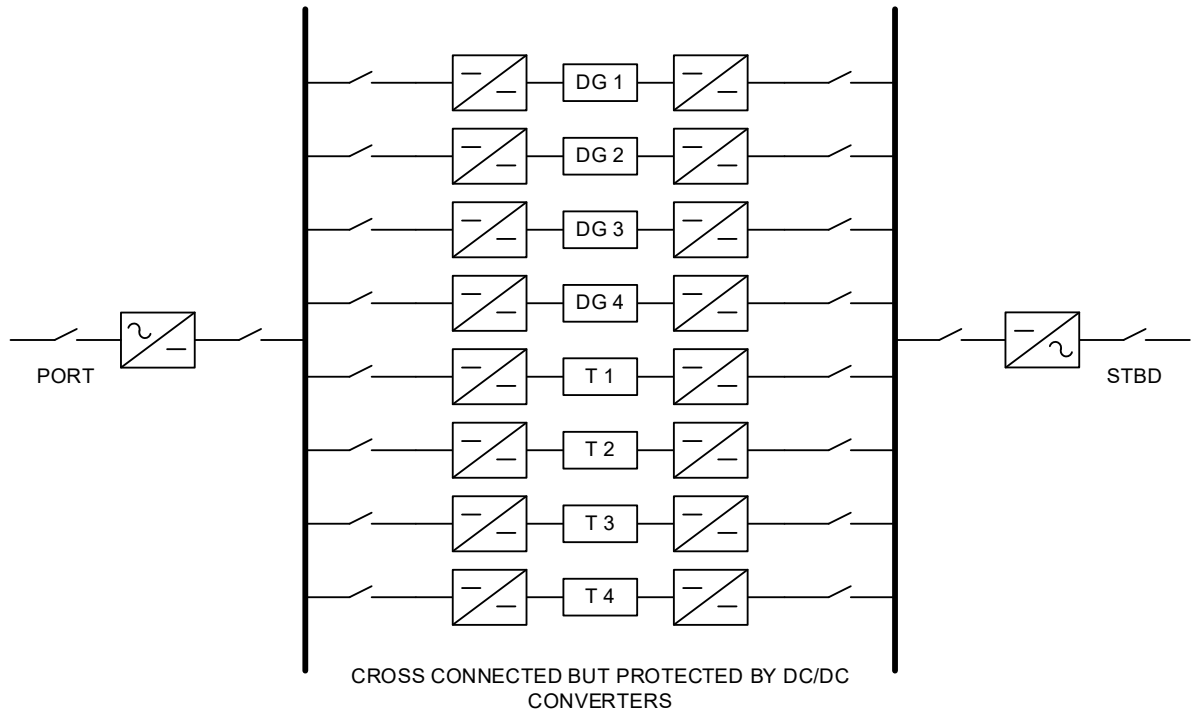


Figure 4-5 Protection Against Some Types of Faults by dc/dc Converter

4.3.6

In Figure 4-6, diodes are used to provide a limited degree of isolation against faults in either of the two rectifiers but the diodes do not prevent over voltages destroying sensitive loads or prevent voltage dips at any one consumer propagating back to the rectifiers and affecting all consumers.

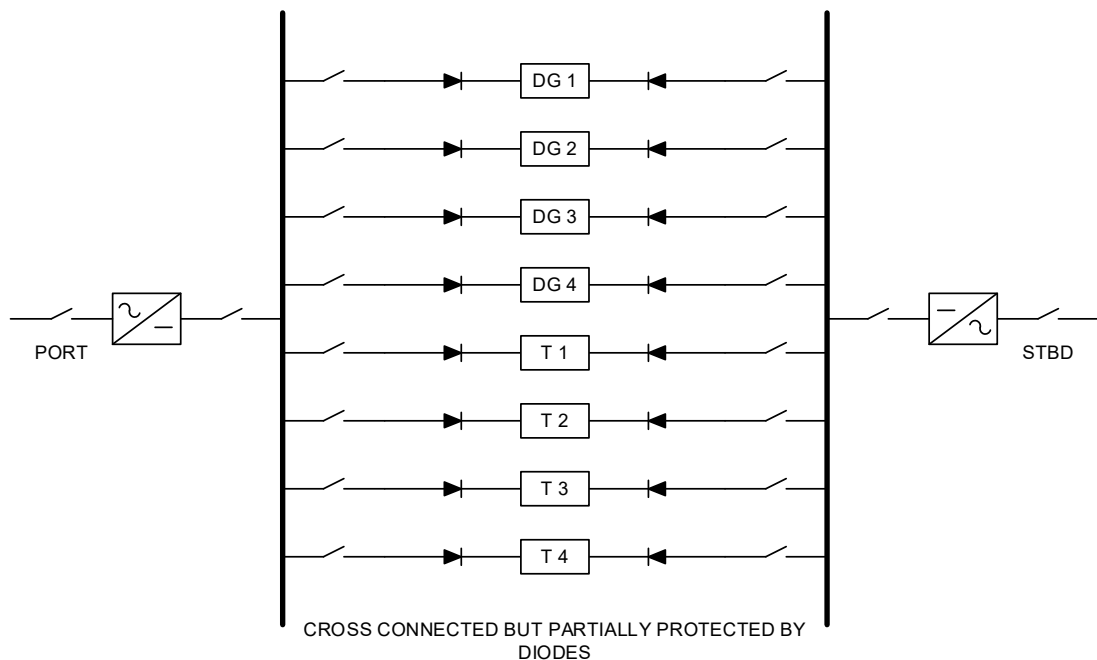


Figure 4-6 Limited Protection by Diodes

5 TAXONOMY OF CROSS-CONNECTIONS

5.1 RISK ASSOCIATED WITH CONTROL POWER CROSS-CONNECTIONS

5.1.1 All cross-connections represent potential fault-propagation paths. However, not all cross-connections pose the same degree of risk of loss of position. The discussion that follows is provided for the purpose of ranking the various types of control power cross-connections in terms of the likely threat they pose to DP station keeping.

Note:

The ranking methodology described herein is an example and is not intended to be prescriptive.

5.1.2 Four categories of cross-connection risk have been identified:

•	HIGHEST RISK
•	HIGHER RISK
•	HIGH RISK
•	MITIGATED

Notes:

In this example, the category labels 'High Risk', 'Higher Risk', and 'Highest Risk' were chosen in preference to the more common choices of 'low', 'medium' and 'high' to ensure that appropriate focus is placed on verifying and validating the risk and its mitigations. Categorisation as low risk should be based on verification and validation activities.

The categories 'Highest Risk' and 'Higher Risk' are treated as the same category for the purpose of determining the path to resolution, but they may require different degrees of mitigation and thus are separated.

5.1.3 The potentially easiest means of addressing an avoidable or unnecessary control power cross-connection is to isolate it. However, isolation should not be done without understanding the implications and proving the effects of the changes – See Section 7 for further explanation. If isolation is not possible (or is undesirable) the risk of fault propagation can be reduced by the application of protective functions to mitigate the failure effects and demonstrate the effectiveness of fault resistance, fault tolerance and fault ride through. The validation of these functions and attributes is used to categorise the risk posed by a particular design of cross-connection as follows:

Highest Risk Figure 5-1	The cross-connection has no protective functions to allow it to be isolated in response to an overcurrent fault or a failure to zero voltage in one source (blocking).
Higher Risk Figure 5-2	The cross-connection is protected against over current and reverse current faults but lacks means to prevent severe voltage dips being created, the consumers which share the distribution with the common point lack, the ride-through capability to prevent malfunction and this is not provided by batteries or other stored energy source.
High Risk Figure 5-3	The cross-connection is protected against overcurrent and reverse current faults, the consumers are provided with ride through capability whether intrinsically or by external means such as stored energy sources. However, the risks associated with an over voltage fault has not been addressed and there may be a vulnerability to hidden failures. The effects of failure have not been proven by testing.

5.1.4 The boundary between High Risk and Higher Risk arrangements is characterised by the presence of ride through capability for all DP consumers for the more frequently experienced types of fault such as supply interruptions and voltage dips. This attribute may be achieved by:

- batteries or other stored energy devices.
- limiting the fault current to prevent voltage dips.
- having consumers demonstrate resilience to the effects of voltage dips.

Notes:

Such arrangements do not remove all fault-propagation mechanisms. Current limiting methods and consumers with ride-through capability are most conclusively tested in-situ. Overvoltage concerns may be addressed to a large degree by analysis and inspection, but bench testing is a possibility if testing in situ is problematic.

Avoiding validation testing to demonstrate fault ride through capability may only be considered when all sensitive DP related consumers are protected by stored energy such as batteries (UPS or dc battery charger / power supply).

5.1.5 Figure 5-1 to Figure 5-3 below illustrate how this ranking is applied to an example using diodes. A and B are redundant groups and C is a common system powered from both A & B.

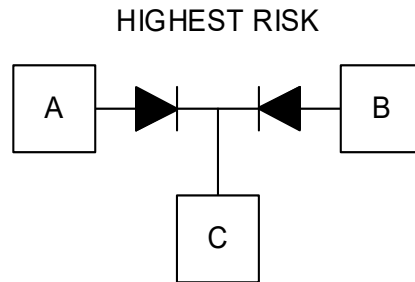


Figure 5-1 Example of Highest Risk Categorisation Using a Diode Type Cross-connection

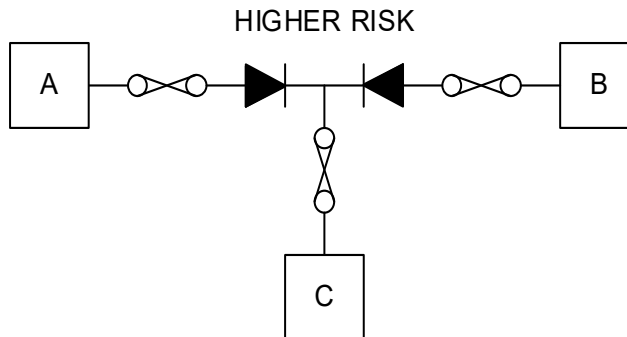


Figure 5-2 Example of Higher Risk Categorisation Using a Diode Type Cross-connection

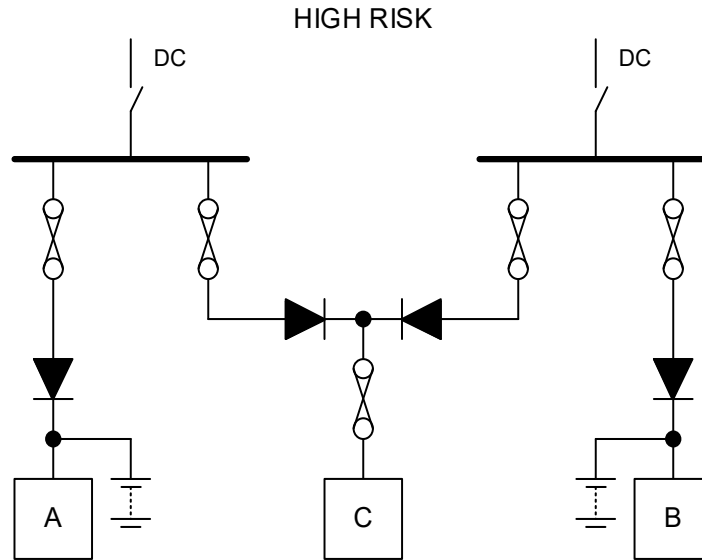


Figure 5-3 Example of a High-Risk Categorisation Using a Diode Type Cross-connection

- 5.1.6 The highest risk arrangement has diodes which protect against a reverse current fault but are not designed to protect against an overcurrent fault. There is nothing to prevent a fault at point C drawing a large fault current from A and B until they both malfunction or trip, and then all three systems fail.
- 5.1.7 In the higher risk example, fuses have been added which will at least disconnect A and B from C if it malfunctions, but the voltage dip created by the fault will persist until the fault is cleared. A & B will have to ride-through that dip without malfunction.
- 5.1.8 In the high-risk arrangement batteries have been added to ensure that A and B don't see a voltage dip when a short circuit fault occurs at C.
- 5.1.9 For the risk to be adequately mitigated it would be necessary to ensure there were means to detect hidden failures, prevent an overvoltage fault affecting more than one system and successfully complete comprehensive verification and validation. Alternatively, the decision could be taken to isolate one of the two feeds to C provided this change did not unacceptably affect the vessel's post failure DP capability.

5.2 LOAD AND SUPPLY SIDE

- 5.2.1 Cross-connections can be present on the load side or on the distribution (supply side) (Example common power supply) as shown in Figure 5-4 below.

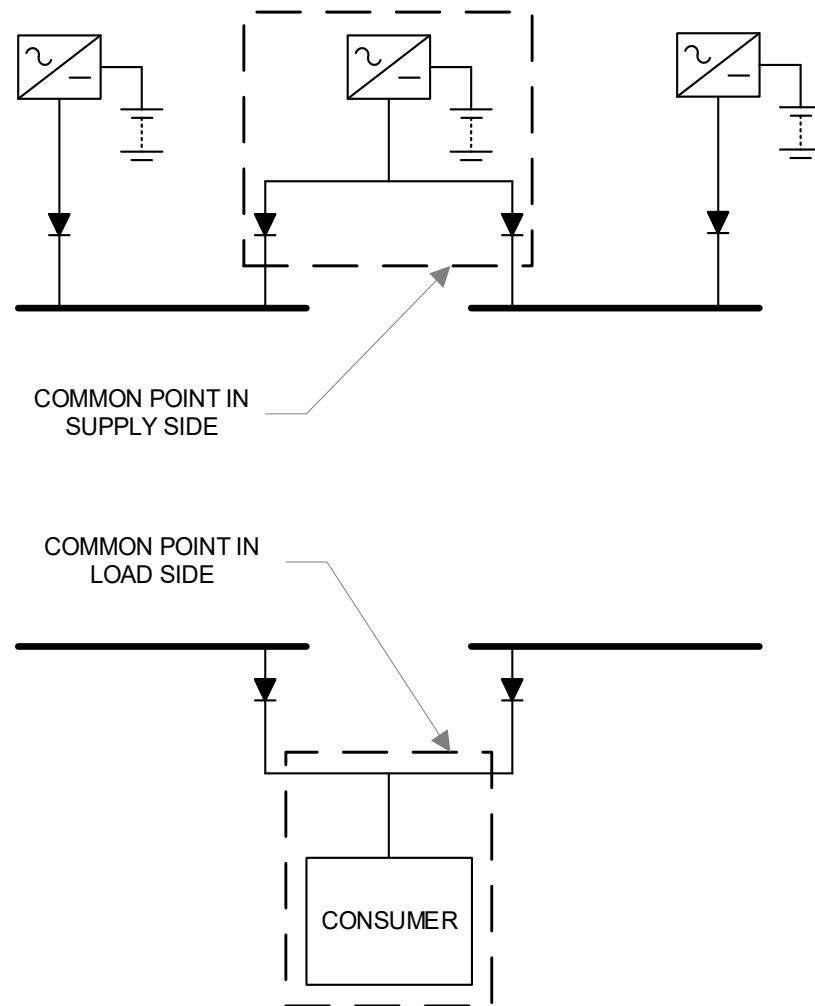


Figure 5-4 Cross-connections in Supply and Load Side

5.2.2 Although much of the guidance in this TECHOP was written from the 'Load Side' perspective, it is equally valid for common points introduced on the supply side.

5.3 HIGHEST RISK & HIGHER RISK

5.3.1 Categorisation of risks as 'Highest' or 'Higher' will be subjective without the benefit of validation testing. The default should be to consider such cross-connections as 'Highest' risk until demonstrated otherwise by validation testing.

5.3.2 Figure 5-5 shows an example which could be highest risk (the nature of the common point has yet to be revealed). Cross-connections which form direct connections to a common point between power distribution systems supplying DP related consumers for different redundancy groups are categorised as Highest Risk or Higher Risk. The common point may be formed by way of a direct (hardwired) connection, or auto-changeovers, diodes or dc to dc converters for example.

5.3.3 A fault at the common point can have the following undesirable effects:

1. Create a voltage dip that causes DP consumers in more than one redundancy group to malfunction.
2. Cause the main supply breakers at the power supply outputs to trip instead of the feeder breakers immediately upstream of the fault. This has the effect of isolating all DP consumers in all connected redundancy groups. (Selectivity / Coordination flaw)

3. An over-voltage on one supply may damage the associated redundancy group and the consumer at the common point – It may create a consequential over-current fault affecting both redundancy groups. This can cause voltage dips and exposure to possible selectivity-failure in the other redundant equipment groups.

Notes:

- *This failure mechanism may propagate by way of an auto changeover even though the initial over-voltage does not.*
- *Diodes and dc to dc convertors can block reverse current flow and voltage (up to a point) – For diodes, the limit is determined by their Peak Inverse Voltage (PIV) rating. They do not block if they have failed to a short circuit condition (hidden failure).*
- *Diodes do not block over voltage in the forward direction – dc to dc convertors may be able to prevent a forward overvoltage propagating up to a point. Switch-mode or similar ac power supplies may also do so.*

5.3.4

Some 'C-Form' changeover relays (e.g., single pole - three contacts with a common armature) can arc between the normally open and normally closed contacts particularly when breaking a high current (Incidents have been attributed to such designs). This forms a fault propagation path between redundancy groups.

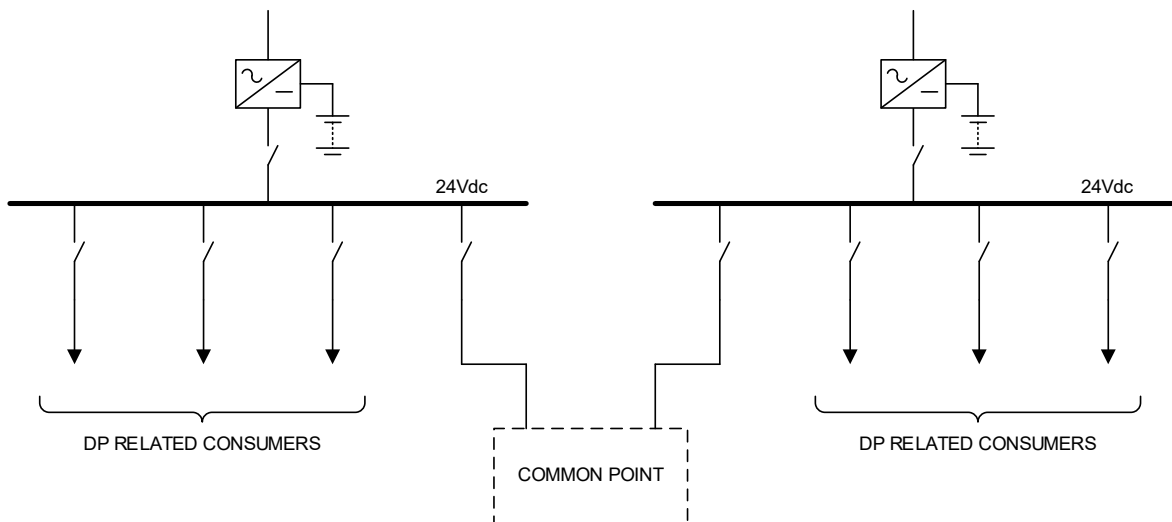


Figure 5-5 Highest / Higher Risk Cross-connections

5.3.5

Highest risk cross-connections include common negative supply rails for power supplies in different redundancy groups if these are not referenced to the ship's hull (floating) as shown in Figure 5-6.

Note:

Particular care is required to understand the failure effect of any common points created between floating dc power supplies on either the positive or negative supply rails or both. A mixture of floating and hull referenced equipment powered from the same source requires particular attention.

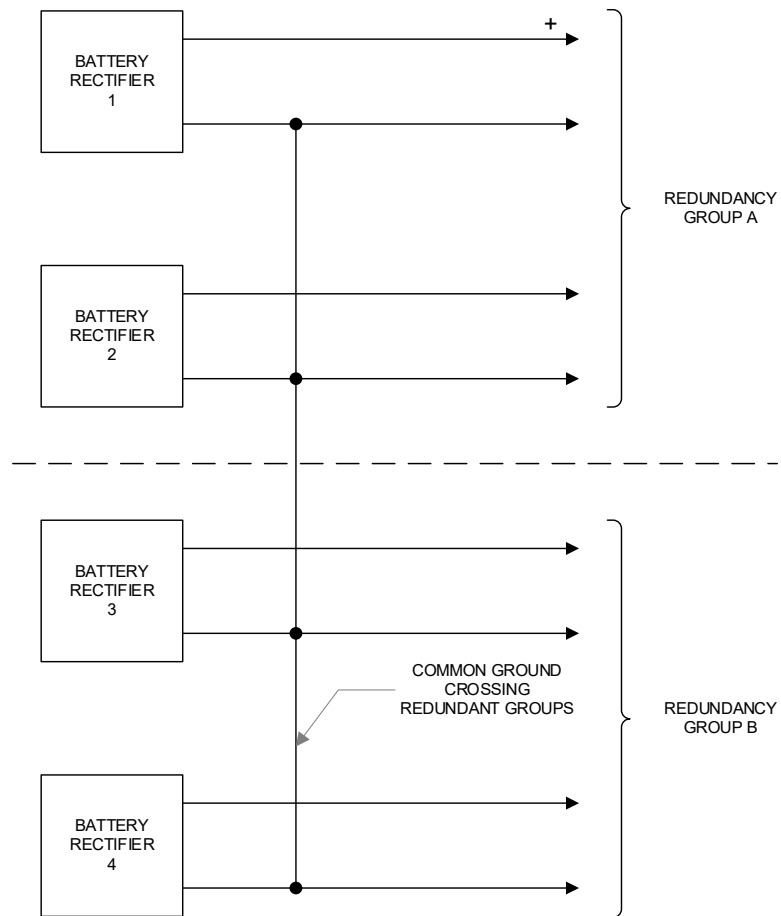


Figure 5-6 Common Negative Power Supply Rail on Floating Systems – Highest Risk

5.4 HIGH RISK

- 5.4.1 High risk cross-connections are considered to be undesirable but of lesser concern than the higher risk or highest risk type because all DP related consumers are isolated from the effects of the common voltage dip by a battery in a UPS (must be a double conversion UPS in the case of ac) or a battery rectifier supply (in the case of dc).

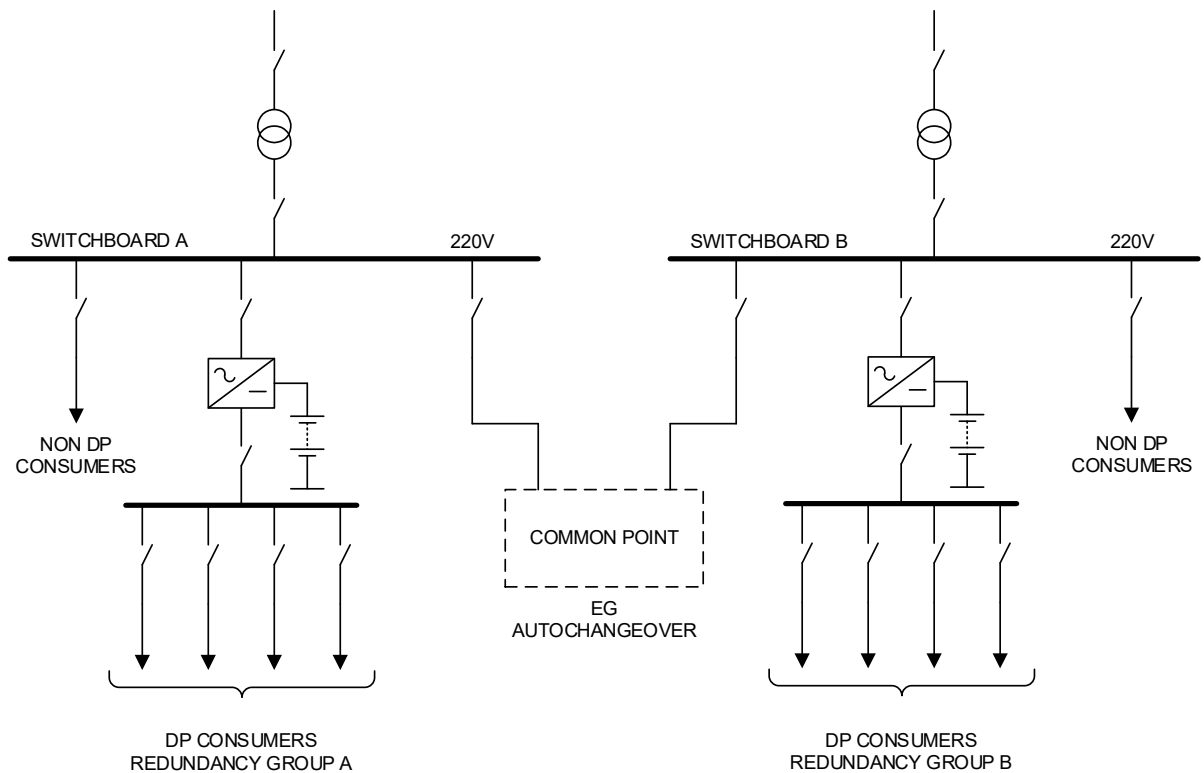


Figure 5-7 High Risk Cross-connections

5.4.2 In the High-Risk arrangement, a fault at the common point may cause voltage dips or disconnect all sources of power because the protection fails to work selectively but the DP consumers in all redundancy groups will continue to run without interruption from the batteries until such time as the main source of power can be restored or the batteries are exhausted.

5.4.3 There may be DP related consumers on distribution voltage levels above that at which the common point is created. For a categorisation of High-Risk to be valid (as opposed to Highest-Risk) there must be reasonable grounds to conclude with a high degree of confidence that any voltage dip created by a fault at the common point will not cause these consumers to malfunction in more than one redundant equipment group. Features and findings which may support this conclusion include:

1. The power distribution level is a robust, high capacity source intended for high power consumers.

Note:

The power frequency waveform at this point must be unlikely to be influenced by a failure at the common point because the fault current to the common point is very small compared to the capability of the source. This may be true for common points created for control power sources but not for high power consumers such as crane sliprings or dual fed HPUs etc.

2. One or more service transformers exist between the common point and the DP consumers on the higher distribution levels e.g. 6.6kV to 480V and / or 480V to 220V.

3. The DP related loads on the higher distribution level are not highly sensitive to voltage dips – e.g. pumps and fans – not variable speed drives for example. The true vulnerability may be difficult to determine, as a voltage interruption followed by a swift recovery, while motors are still turning, can create over-current conditions similar to crash sync on a generator. Thus, the nature of the worst-case disturbance needs to be understood.
4. The common point is supplied by a switch-mode power supply or dc to dc convertors which are of a type that will not pass a significant over-current or voltage dip to the supply side on failure at the common point.
5. The existence of long cable runs of low cross-section cable to the common point with fuses or circuit breakers of low current rating (typically 1A or less) from a very robust source – (stiff voltage regulation) – A fault at the common point is very unlikely to influence the power system voltage significantly.
6. The design of motor starters used for the loads on the higher voltage distribution levels has considered the possibility of voltage dips. Means have been provided to prevent contactors dropping; out such as dc coils for example.
7. The difference in load / fault currents between the DP consumers on the higher voltage distribution levels and the common point is very large; such that it is unlikely that a significant voltage dip would occur during operation or fault clearance at the common point.

5.4.4 If it is not possible to conclude that DP consumers at higher voltage levels would not be affected for the reasons listed above, then the risk posed by the cross-connection requires mitigation.

5.5 FURTHER EXAMPLES

5.5.1 Figure 5-8 is a HIGHEST RISK cross-connection. The dual supply to the EX UPS was installed without overcurrent protection. A fault in the supply line to the EX UPS has the potential to operate both 20A fuses disconnecting all the control power causing loss of port and starboard engine control systems.

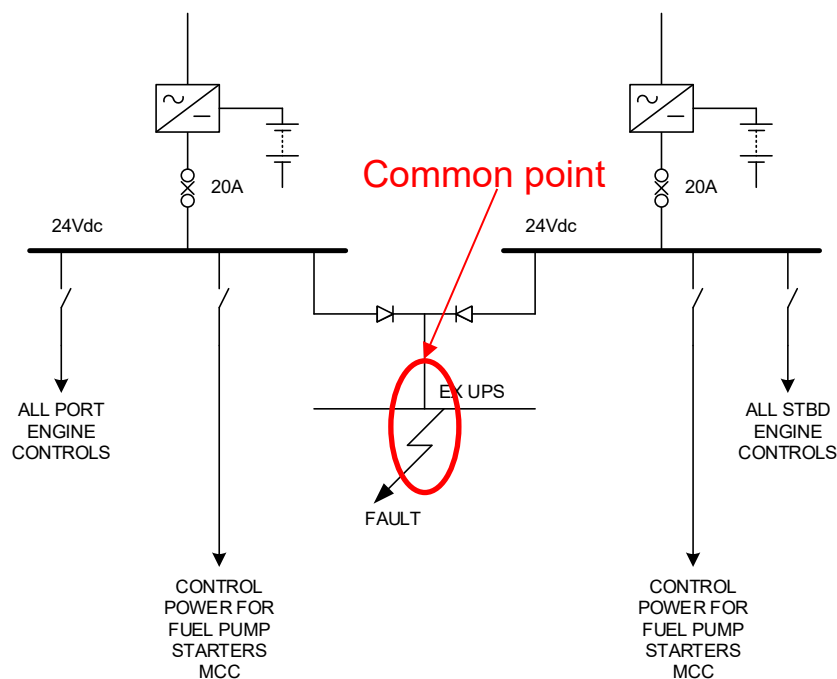


Figure 5-8 Common Point With No Over-current Protection

- 5.5.2 Figure 5-9 is a HIGHER RISK cross-connection. Although there are batteries in the system their location in relation to the fault means they cannot prevent a voltage dip causing the E Stop relays for the generators dropping out stopping all the engines. However, dc/dc 'redundancy modules' have been installed at the common point and these are of a type that will effectively limit the fault current and thus the voltage dip. These may need to be proven by testing.

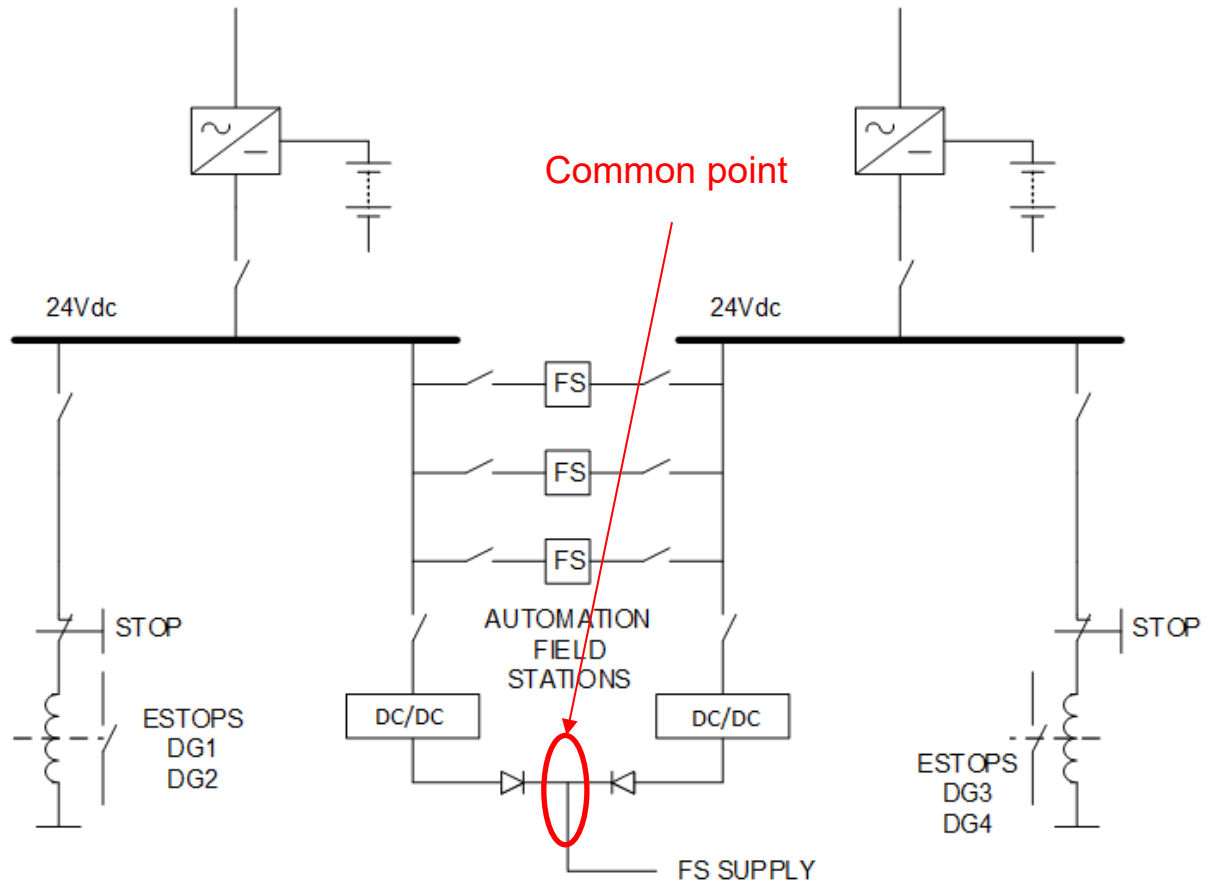


Figure 5-9 Dual Supply to a Field Station is Protected by Redundancy Modules

- 5.5.3 Figure 5-10 shows a typical two-way split with cross-connections. Cross-connections exist on the ac distribution and the dc distribution. This is a high-risk example. The cross-connection on the dc side is within the same redundancy group. If the cross-connection on the ac side were re-aligned, then the risk from an overvoltage passing through to both dc distributions and therefore all four generator control systems would be removed.

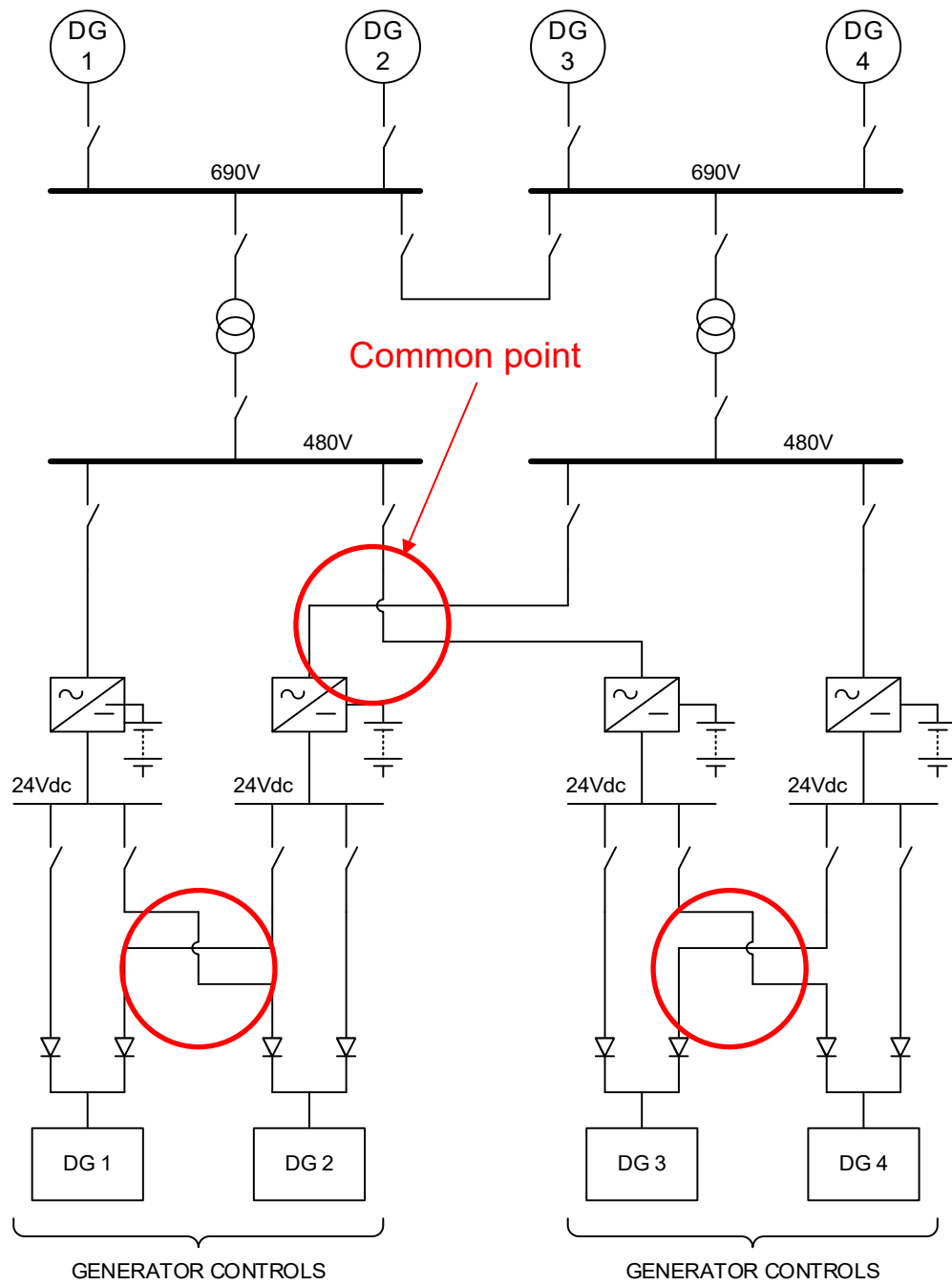


Figure 5-10 Misalignment in ac Side

6 EVALUATING CONTROL POWER CROSS-CONNECTIONS

6.1 INITIAL EVALUATION

6.1.1 The first step when cross-connections are identified is to unambiguously evaluate:

1. What are the effects of failures occurring at cross-connections to DP consumers and if it exceeds the analysed and validated worst case failure design intent? (Note even if it is not covered in the approved documents)
2. What are the threats and if they are credible and will result in failures occurring at the cross-connections?
3. Steps to resolution include:
 - Identification
 - Impacts
 - Addressing:
 - a. verify and validate
 - b. isolate
 - c. modify
 - d. leave as is (transparency – administrative controls)
 - e. opportunity for improvement
 - Operational controls (ASOG / WSOG impacts on post failure DP capability)

6.1.2 Figure 6-1 illustrates the initial evaluation to be carried out.

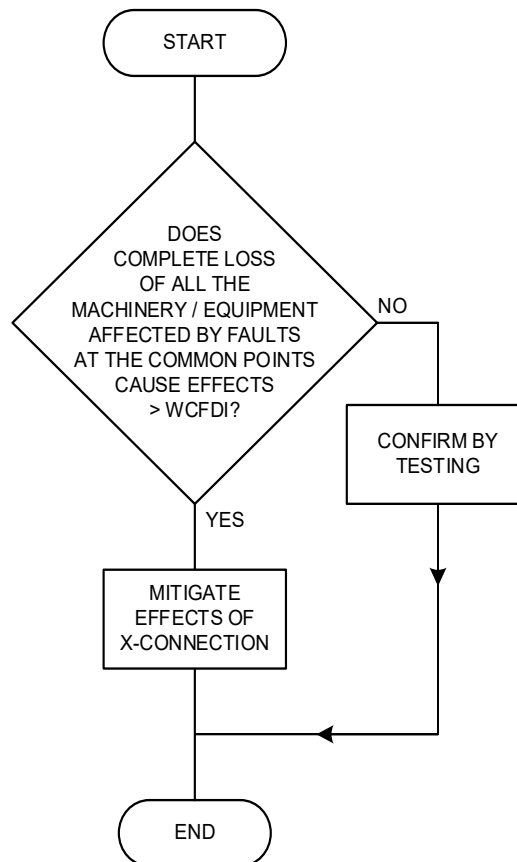


Figure 6-1 Initial Evaluation

6.1.3 If the initial evaluation confirms that further action is required, the pathways to resolution could include:

- Isolation in line with redundancy concept.
- Validation of the resilience to power system transients and / or fault ride through capability through testing (example - short circuit and ground fault test – through application and closure of a suitable circuit breaker).
- Consideration of over-voltage as a fault propagation mechanism.

Note: There is a possibility that time on DP following a fault may be limited by battery endurance where a High-Risk arrangement is not isolated (e.g. no mitigation has been deemed necessary following testing). Although several steps can be taken to increase confidence that the probability of this occurring is low, these measures may not be adequate to address the risk of loss of position in all industrial missions. Contingency planning for this eventuality and recovery from it should be developed. Example - means to restore input power to the UPSs.

6.1.4 High Risk cross-connections are unlikely to provide the station keeping integrity required for manned diving operations unless mitigated by isolation.

6.2 CATEGORISING CONTROL POWER CROSS-CONNECTIONS

6.2.1 Table 6-1 and Table 6-2 can be used together to assist in categorising the risk level of any identified cross-connection. Table 6-1 is the primary categorisation table. To use it, select the type of cross-connection from the bottom row (Example dc to dc converter). To determine the risk level, review the conditions A to E moving upwards through the table stopping at the first statement that is true. Select that as the risk level. For example, If the dc to dc convertor provided:

- Overcurrent protection.
- Current limiting to prevent voltage dip at the input side.
- Over voltage protection.

but had:

- No alarms for hidden failure of one supply.
- Not been validated by testing.

6.2.2 Then the arrangement would be categorised as **4D** (High Risk) and treated accordingly.

Table 6-1 Guide to Categorisation of Cross-connections



Mitigation of Fault Propagation in control power		Risks associated with common points formed by various type of components						
	Has been isolated or validated by analysis and testing	F						
Increasing levels of protective functions	Has not been validated by analysis and testing	E						 Stop at the first True Statement
	No alarms for detection of hidden failures	D			HIGH RISK			
	No resolution of overvoltage concerns	C						
	No current limiting and / or Batteries for ride through capability (Interlocks for Auto changeovers)	B		HIGHER RISK				
	No overcurrent & Ground Fault Protection or reverse current blocking	A	HIGHEST RISK					
Nature of the Common Point			1	2	3	4	5	
			Hardwired	Diodes	Auto changeover	dc to dc SMP QUINT etc.	Isolated or Manual Changeover	

Table 6-2 Explanation of Categorisation

Validation and/or isolation has been carried out F	<p>(STONE) Hardwired connection between redundancy groups with no fuses and no other forms of protection generally cannot prevent fault propagation. Available mitigations include:</p> <ul style="list-style-type: none"> Isolation or other engineering Change. Restricting in operations are. 	Isolated or - Successful live short circuit and earth fault testing has added significantly to confidence in the ride-through capability of consumers.			Generally free of fault propagation paths but failure effects may propagate between redundancy groups (that are electrically isolated) due to the effects of fire and flooding when equipment from redundant DP groups is collocated.
Validation by analysis and testing E		No validation testing and / or analysis carried out			
Alarms for detection of hidden failures D		Redundancy could be compromised if one of the diodes has failed.	Redundancy could be compromised. The autochanger may operate but the backup supply is unavailable.	Redundancy could be compromised. The converter or redundancy module on one of the supplies could be faulty.	
No resolution of overvoltage concerns C		Even if all the consumers that share the supply to the common point are protected against voltage dip there may still be the possibility that a severe overvoltage may propagate through the common point causing malfunction.	A severe over voltage may be able to jump the gap between the contacts in a dry contact relay or contactor.	A severe overvoltage may be able to propagate through the convector or modules and back up to the other redundancy group.	
No ride-through capability by current limiting or batteries – or prevented by interlocks in the case of auto changeovers B		consumers in other redundancy groups connected through the common point must be protected against the effects of the voltage dip. These consumers may be on a UPS or have intrinsic ride through capability.	Auto changeovers without interlocks to prevent them transferring when the fault is in the changeover or its consumers propagate significant overcurrent faults causing voltage dips with the potential to cause another consumer's malfunction.	Some dc to dc & redundancy convertors have a current boost functions to help blow fuses and operate MCBs selectively. This could cause a voltage dip on the supply side and ride through may depend on batteries or consumer attributes.	
No protection and selectivity for overcurrent or blocking function A		Redundant groups connected by diodes without fuses or MCBs will propagate significant voltage dips with the potential to cause malfunction – Without selectivity in overcurrent they may trip the supplies in both redundancy groups.	Redundant groups connected by an auto changeover which has no overcurrent protection of its own will operate the overcurrent protection on both redundant groups to which it is connected.	All these types units typically provide some kind of current limiting function and overvoltage protection but the extent to which it is suitable must be confirmed.	
	1 Hardwired	2 Diodes	3 Auto changeover	4 dc to dc, SMP	5 Isolated

7 PENALTIES OF ISOLATION

7.1 AVOIDING ASSUMPTIONS

7.1.1 Isolation is often considered to be the easiest option to address a cross-connection issue, but it is important not to jump to conclusions about how best to address a perceived risk before all the facts are understood. Isolating cross-connections to address perceived or low station keeping risk may introduce exposure to safety events increasing the overall risk profile. (e.g., isolations to address perceived or low station keeping risk compromising protective functions designed to address safety (protection against fire)). The discussion that follows attempts to illustrate that evaluation and risk management process using an example.

7.2 CAUTIONARY NOTES

7.2.1 Mitigations involving isolations will need additional verification and validation to demonstrate that isolation does not result in un-intended consequences such as compromising:

A. Protection schemes

Protection schemes are required to operate effectively during power system transients- Care should be taken to ensure that isolation does not disable the protective function by removing the fault ride through capability provided to that protective function by a supply with a battery backup. This is likely to manifest itself when isolation strategies result in power being supplied by a raw ac power supply.

B. Alarms

Control and protection power supplies are often monitored, and alarms given if the supply is disconnected or fails for any reason. Intentional isolation of the supply may cause the alarm to be permanently active. Such standing alarms may mask the occurrence of more important alarms. Attention should be given to means to prevent such standing alarms from occurring by addressing the relay logic or software used to generate them.

C. Industrial process continuity

Removal of battery back up from control and protection power supplies may have consequences for the correct operation of DP or industrial mission related equipment. Frequent malfunction or spurious operation of such equipment may hamper execution of the industrial mission. The potential for malfunction may not become apparent until the equipment experiences the distortion associated with the operations of industrial mission equipment and therefore may not be apparent during testing in more benign conditions where such machinery is not operating. Such interruptions to the industrial process are not desirable in the long run. While isolations may be the required strategy to address the issues in the short-term, alternate mitigations should be devised that will not result in such interruptions to industrial process continuity.

D. Automatic blackout recovery

Control systems used for blackout recovery depend upon continuity of power during blackout connections in order to restart machinery etc. Attention should be paid to the effect of isolations to ensure they do not deprive such control systems of the battery backup they require to effect the automatic recovery.

7.3 EFFECT OF ISOLATION ON POST FAILURE DP CAPABILITY

7.3.1 **Two-way Split:** In the case of a two-way split the cross-connections can generally be isolated with no reduction in the vessel's post failure DP capability. The cross-connection was helpful in reducing the impact of control power failure from 'loss of all generators (for example) in one redundancy group', to 'no effect' other than loss of redundancy. The other helpful feature is that it protected the DP system from hidden loss of capacity in the surviving machinery which would otherwise have to operate a high load.

7.3.2 **Multi-way Split:** Multi-way split with insufficient UPSs to allow alignment of the UPS distribution with the redundancy concept. In this case it is not possible to isolate cross-connection in a manner that retains the vessel's post failure DP capability. In the case of a typical DP MODU drillship with a three-way split and six thrusters, the best that can be done is to create a quasi-two-way split. However, this does not result in a 50% post failure DP capability but a rather a 33% post failure capability because two bow thrusters and two stern thrusters may be lost together. (Refer to Figure 7-1, Figure 7-2 and Figure 7-3)

7.3.3 isolation of back-up supplies, and other cross-connections is a useful tool to mitigate unacceptable failure effects that have a potential to exceed the WCFDI. Like any tool it has to be used with care and applied to situations for which it is the best choice. It is as important to know when a cross-connection should not be isolated. In some cases, making this judgment call is neither easy nor straightforward. This note intends to provide guidance that may help remove some of the subjectivity from the process.

7.3.4 Back-up power supplies are generally provided to reduce the severity of failure effects associated with more frequently occurring failure modes such as a failure to low or zero voltage at the output of a power supply. This is the way most power supplies fail. They can however fail in other ways such as ground fault, or to high voltage. Historically, failure to high voltage occurs less frequently than failure to low voltage.

7.3.5 A rough guide to the prevalence of the various types of faults that occur in single phase A/C or D/C power systems would be as follows (starting with the most prevalent):

- Earth (ground) fault
- Wire break, loose terminals
- Power supply fails to low or zero output voltage
- Short circuit (fuse or CB operates)
- Power supply fails to high voltage
- ac inverter fails to low or zero frequency
- ac inverter fails to high frequency.

Note: Lightning is sometimes referred to as a reason to isolate cross-connections, but the voltage associated with lightning is so high it may arc across any normal means of isolation such as a withdrawn fuse or open circuit breaker.

7.3.6 In the case of vessels with a simple two-way split in their redundancy concept, the cross-connections may be removed. This will remove the threat of total blackout but may make it more likely that a partial blackout will occur. However, in the case of a two-way split the effect is to add one more failure mode to many other that could cause failure effects of equal severity.

- 7.3.7 A different situation occurs when cross-connections are isolated in a redundancy concepts with multi-way splits. Cross-connections in multiway splits may be introduced to limit the number of UPSs and battery chargers required for control power. Typically, in a three-way split, it would be good practice to install at least one control power UPS for each redundancy group. However, it is possible to develop a design having only two UPS, provided the redundancy group without a dedicated UPS is provided with two supplies one from each of the two installed UPSs.
- 7.3.8 Such arrangements introduce certain vulnerabilities. Although they are effective in the case of wire breaks and failure of power supply, they actually create vulnerabilities to failure modes such as short circuit and overvoltage. They also introduce vulnerabilities associated with hidden failures in the supplies themselves. Such failures may mean that the vessel is operating in a condition which is not fully fault tolerant because backup supplies, upon which the redundancy concept relies, are in a failed state.
- 7.3.9 In the case of a three-way split, the worst-case failure for thrust and power is usually designed to be loss of about 33%. That is to say, the vessel should always be able to hold station in conditions that require the power and propulsion system to be operating at 66%. Unfortunately, that post failure capability depends on the dual supplies to control power consumers. Once these are isolated, the worst-case failure typically becomes 50% for power and 33% for thrust. The reason it is not 50% for thrust is that the capability is determined by being left with only one operational thruster out of the three at each end. One end of the vessel may have two thrusters operating but it won't be possible to make full use of that capability because only one thruster is online at the other end. Drill ships are heavily dependent on heading control to avoid going beam-on to the environment.
- 7.3.10 This change in the vessel's worst-case failure from loss of 33% to loss of 66% can:
- Significantly restrict operability.
 - Introduce additional requirements for number of generators connected.
 - Increase the frequency of experiencing the worst-case failure because it can now occur because of a more frequently experienced failure modes such as a 'wire break' or spurious trip of a circuit breaker.
 - Make the vessel vulnerable to hidden failures in the single surviving redundancy group.
- Note: The last point is perhaps the most significant and is expanded upon in greater detail below.*
- 7.3.11 Unlike the two-way split, where there is no reduction in post failure DP capability and the additional failure mode is just one of many with the same severity, the effect on the three-way split is to severely reduce the post failure DP capability. The new failure modes may be the only one capable of having this much larger effect. So, the risk profile from before isolation to after isolation has changed from:
- **Before** – Low risk of total loss of thrust capability
to,
 - **After** - Higher risk of 66% loss of thrust capability (Much more probable failure mode) – change from Low Impact Failure Effect to High Impact Failure Effect.
- 7.3.12 Operating the vessel within its revised post failure capability would appear to offer a solution but the increased frequency of failure has the potential to compound the effect of an undetected failure. leading to loss of position.

-
- 7.3.13 As drill ships rarely need to operate at their design post failure DP capability, the margin between theoretical capability and actual operating capability provides a margin which offers some protection against hidden lack of performance in surviving machinery. This margin is eroded if the failure effect causes a large reduction in available capability.
- 7.3.14 So, performing isolations in a multi-way split redundancy concept can have the effect of:
- making partial loss of capability more likely.
 - Increasing the severity of the failure effect.
 - Reducing the margin that protected against hidden failures or undetected reductions in performance.
- 7.3.15 Before performing isolations, it is necessary to conclude whether or not the risk profile is improved or worsened following the isolation.
- The decision to isolate is based on an assumption that there is a risk of total blackout or loss of all thrusters.
 - Isolations will not improve the real risk profile if that assumption is not valid.
 - Effort must be expended to determine to what extent that assumption is true.
 - If the concern is failure to over voltage, has overvoltage protection been provided?
 - If the concern is short circuit, do the consumers have fault ride-through capability?
 - If isolations were performed on the assumption that these attributes are missing when in fact, they are present, then the risk profile has almost certainly been made worse.

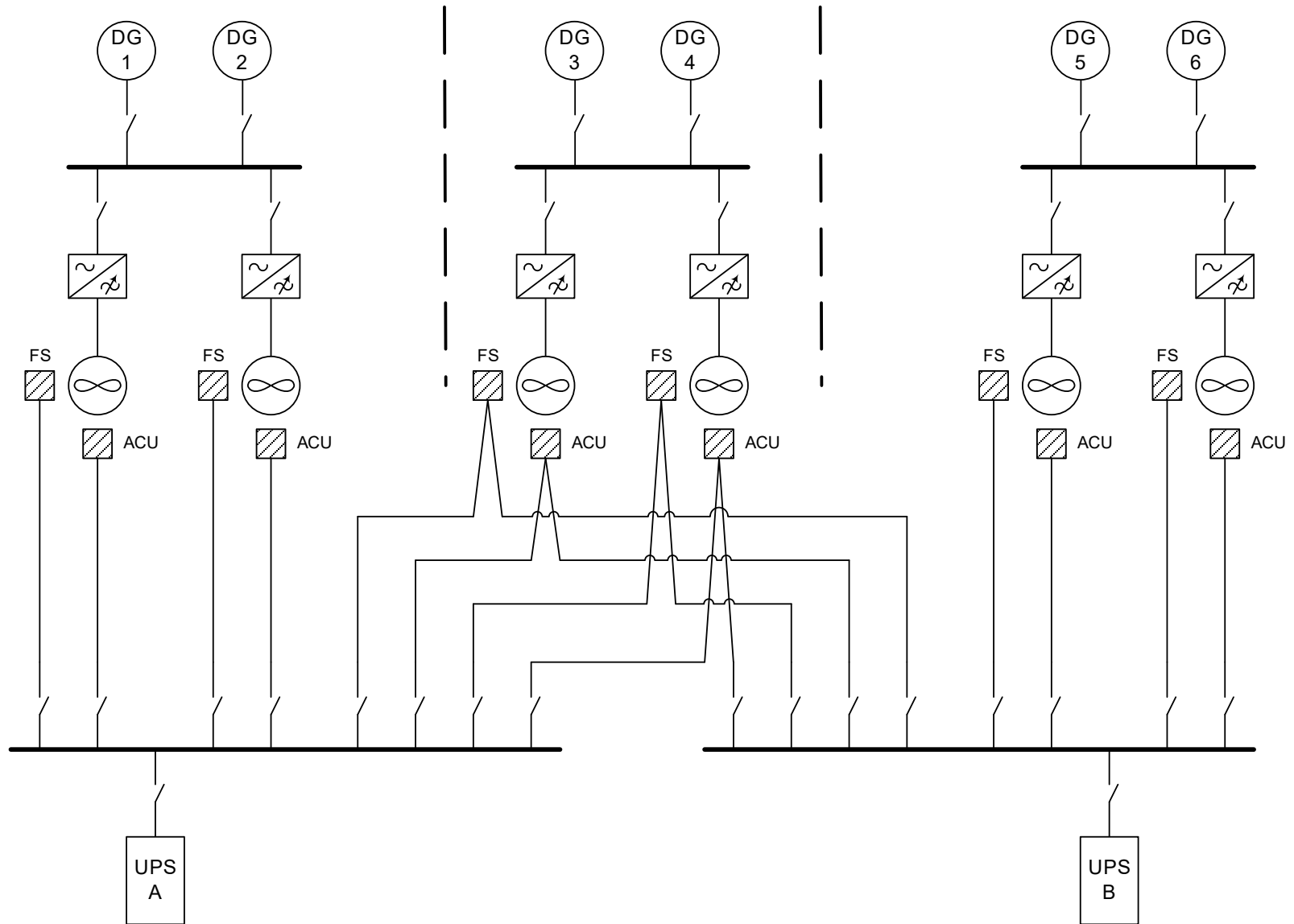


Figure 7-1 Cross-connections Spanning the Redundancy Groups in a Three-way Split

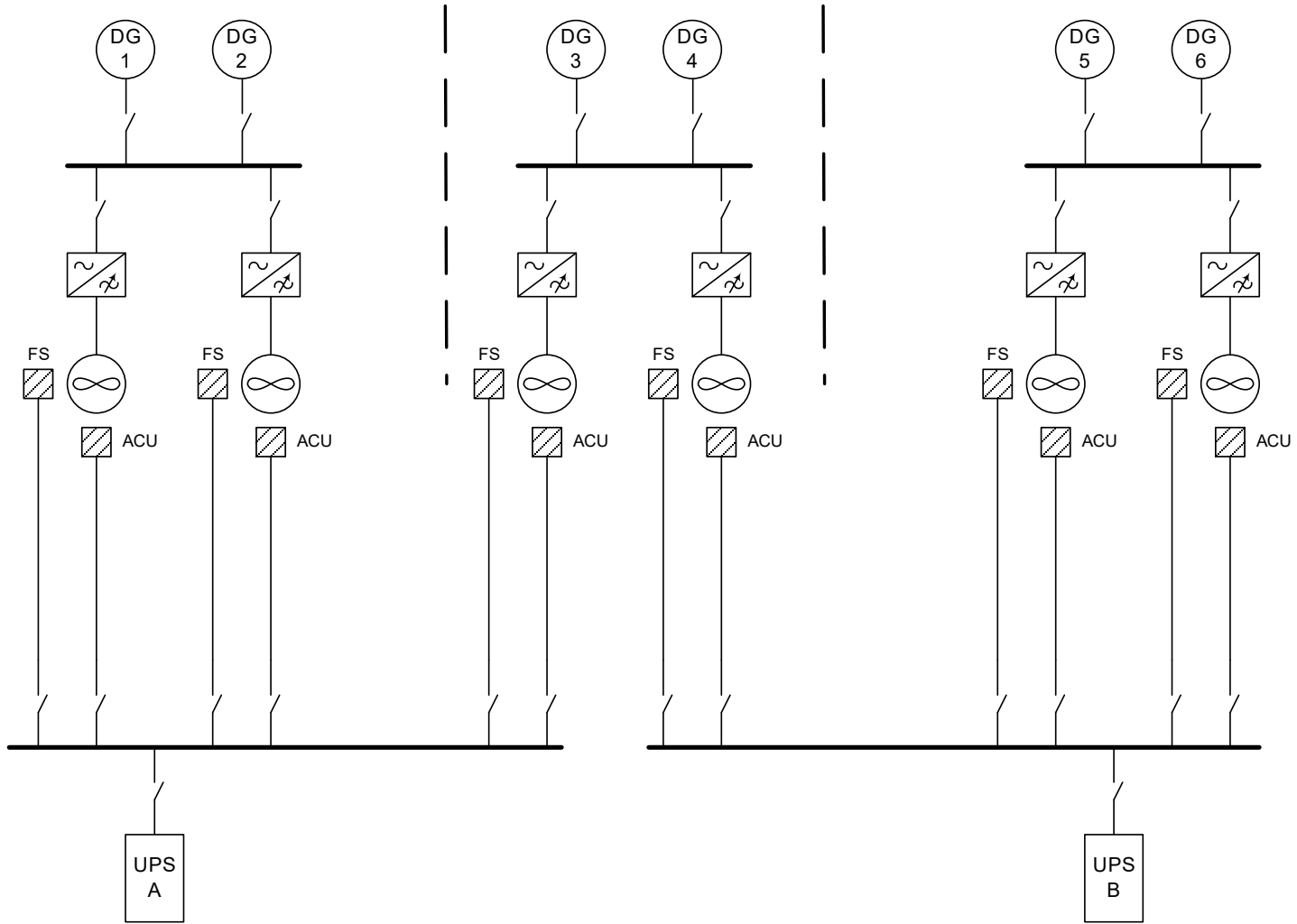


Figure 7-2 Cross-connection Isolated – Three-way Split Becomes Two-way Split

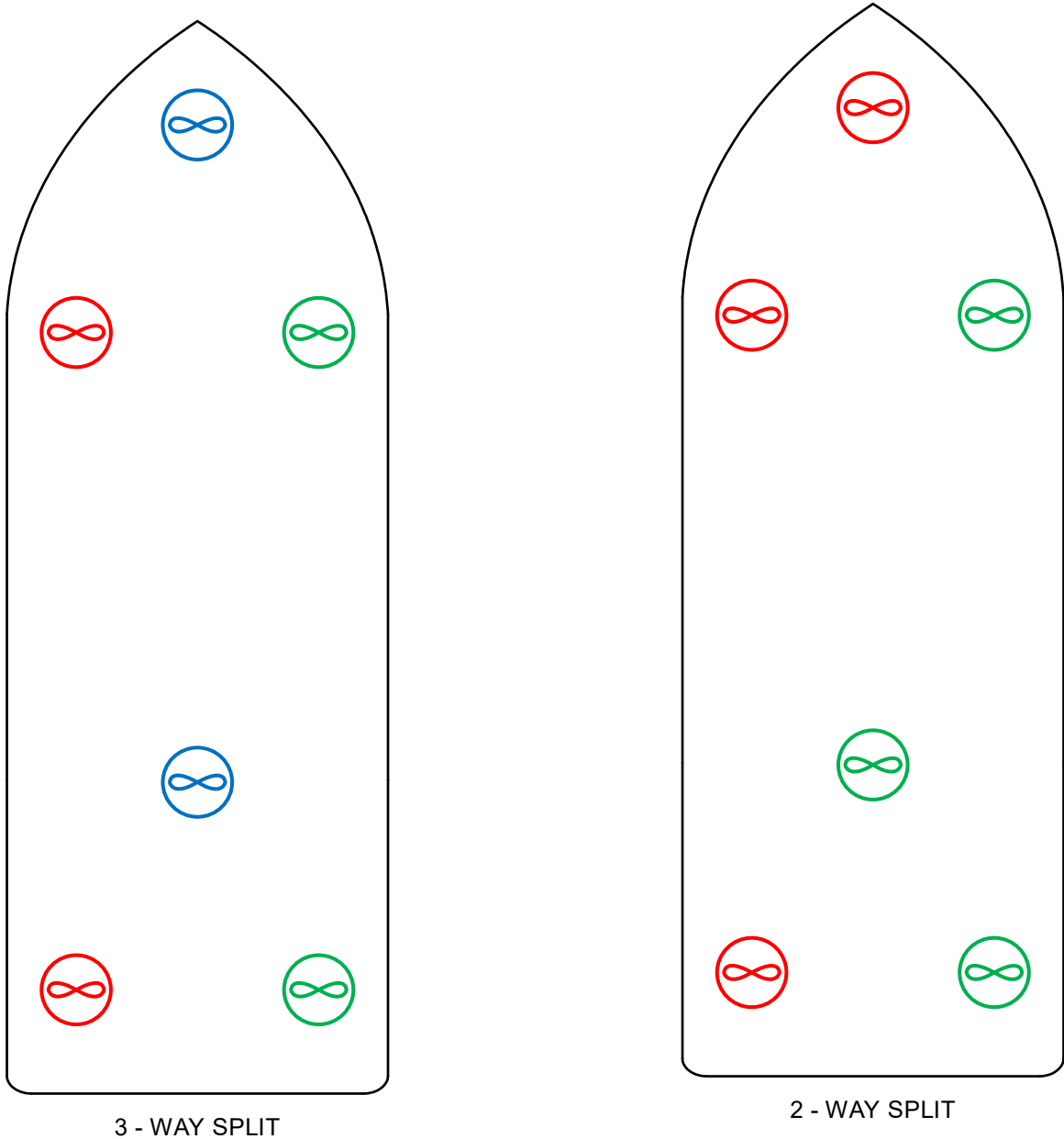


Figure 7-3 Effects of Isolation on Post Failure DP Capability

7.4 HIDDEN FAILURES

7.4.1 Hidden failures (or ignored failures) are very often causal and contributory factors in DP incidents. Pre-existing failures (hidden or otherwise) can defeat the DP redundancy concept. In some cases, it is claimed that such incidents were caused by double failures and therefore somehow excusable. This may have some validity but there is an expectation that means will be in-place to confirm the DP system is intact and that such measures will be deployed with a frequency which provides a high degree of confidence that pre-existing faults will be discovered in time to prevent them compounding another failure (to create more severe failure effects). There is no validity to the double failure argument if such measures have not been deployed.

7.4.2 Hidden failures can be addressed by two means:

1. Having an effective program to reveal them based on proving the attributes of performance, protection and detection in each redundant DP equipment group.
2. Increasing the reliability of the equipment so that demand on performance and protective functions is reduced.

7.4.3 Designs with very low impact failure effects also offer some degree of protection because they effectively increase the amount of time for which a hidden failure would not have a critical effect because the vessel is operating in benign environmental conditions.

7.4.4 Hidden failures can be detected by several means including:

- Alarms and monitoring.
- Planned maintenance & inspection.
- Condition monitoring (including cascade waveform injection testing).
- Annual DP trials.

7.4.5 Hidden failure may take several forms:

- Reduction or limitations in performance of a system which is only revealed when it is required to operate at higher load post failure capability.
- Faulty protective functions which do not operate on demand to mitigate the effects of fault propagation.
- faults in standby redundancy such that the standby unit does not take over from the duty unit.

7.5 ASSESSING THE RELATIVE RISK

7.5.1 Isolation of back-up supplies is a useful tool in the fight against fault propagation, but it also has the potential to significantly reduce the post failure capability, reliability and station keeping integrity if it is applied indiscriminately.

7.5.2 As is always the case in risk management, it is important to get an overview of the complete risk picture. Not all failure modes are equally likely and to focus on the less likely failure modes while ignoring the possibility that the isolations will expose the DP system to other risk (such as the effects of hidden failures) is not effective risk-mitigation.

7.6 TWO-WAY SPLIT

7.6.1 The effects of isolations in systems with a two-way split in the redundancy concept tends to be the most straight forward, has the greatest benefits and fewer side effects. In a simple two-way split, the isolation is unlikely to have any impact on the post failure capability (Transferable thrusters aside).

7.7 MULTI-WAY SPLIT

7.7.1 The situation in a multi-way split such as a three-way split or a four-way split can be very different. The effects of isolation in multi-way way splits require greater attention because:

- It can significantly reduce the vessel's post failure DP capability.
- It can create a new more probable **High Impact Failure Effect** with the potential to increase exposure to the effects of hidden failures.
- High Impact failures can create very significant power and thrust transients which have to be accommodated by protective functions such as drilling phase back and thrust reduction systems. These are all potential hidden failures, and some do not work particularly well.
- The isolation may impose restrictions on generator configurations that provide fault tolerance and therefore increase the risk of configuration errors.
- Before considering isolations, expend reasonable effort to determine whether or not the risks the isolation is intended to address actually exist (e.g., over voltage and lack of fault ride through). If the risk does not exist, then the isolations will likely worsen the risk profile.
- In redundancy concepts with multi-way splits the focus should always be on aligning the control power distribution with the divisions in the DP system's system redundancy concept. This will typically require the addition of UPSs and / or battery chargers.

8 VERIFICATION AND VALIDATION

8.1 ANALYSIS

8.1.1 The verification and validation process will only be effective if it considers a comprehensive range of failure modes including inter alia:

- Under voltage – including zero and intermediate voltage.
- Over voltage.
- Open circuit, short circuit, earth fault and combinations of same where relevant.
- Frequency excursions in ac systems including spikes and harmonic distortion.
- Diodes may fail to open circuit or short circuit – (burn-out and punch-through).

NOTE – The failure effects of various modes of failure may be quite different. For example, it is not valid to assume that a switchboard which fails ‘as set’ for failure of the control power supply to zero voltage will fail ‘as set’ for intermediate and elevated voltage modes of failure. This is because the control system may be deprived of the power to take action when power is removed. However, at intermediate or elevated voltage it may malfunction and still have power to take action such as open circuit breakers etc.

8.2 TESTING

8.2.1 Cross-connections shall be comprehensively proven to have no unacceptable failure effects. This will typically include live short circuit and earth fault testing and analysis. Diodes are unlikely to produce a satisfactory outcome but more sophisticated interfaces like dc to dc convertors, switched mode power supplies and commercially available redundancy modules may behave satisfactorily.

NOTES:

- In all cases where a cross-connection is not isolated. It will be necessary to conclude upon the possibility that an overvoltage may propagate through the common point. Testing this may prove challenging, but some means to achieve the required level of confidence must be found.
- Means to mitigate risk from hidden failures associated with remaining cross-connections will be established. These may include monitoring and periodic testing.

8.3 COMMONALITY AT UPS INPUT SIDE

8.3.1 Having all battery sources from a single power distribution (such as the emergency switchboard) is undesirable and exposes the vessel to risks from hidden loss of battery capacity. This may deprive consumers of their voltage dip ride through capability. Such lack of ride through capability may compound the effects of a failure elsewhere in the power distribution system leading to failure effects of a severity exceeding that of the worst-case failure design intent.

8.4 OVERVOLTAGE

8.4.1 The possibility that an overvoltage in one of the redundancy groups can propagate through the common point to affect another cannot be quantified without investigation. Similar considerations are required to those that apply on the Higher Risk connections.

8.4.2 A common point created by switch mode power supplies or dc to dc convertors may offer better protection against fault propagation than other means of creating common points.

8.5 MAIN CLASS REQUIREMENTS FOR SAFETY SYSTEMS

8.5.1 With very few exceptions, any requirements in main class rules for backup supplies do not require that the back-up power supply be taken from another redundancy group – It may be taken from a separate source within the same redundancy group. DNVGL rules for AUTRO specifically advise against control power circuits crossing the A60/WT divide between redundancy groups.

8.5.2 In a few cases, related to safety systems, there may be a requirement for a supply from the emergency source of power in addition to the one from the main source of power. If the main source of power is in a different redundancy group from the emergency source of power (for DP purposes), then this may create a cross-connection requiring mitigation. Two options are possible:

1. Comprehensively test and analyse the effects of a failure at the common point.
2. The vessel owner should be requested to seek confirmation from the relevant classification society regarding the possibility of modifying the power supply arrangement to resolve the potential fault transfer path between redundant DP equipment groups.

8.5.3 It should be anticipated that changes or modifications to the vessel will require class approval and adequate time should be allowed for that process.

8.6 ALARMS

8.6.1 Standing alarms may be created by isolations and it could be argued that these could be a distraction or hamper comprehension and diagnosis in a developing situation. There may be the potential for incorrect action to be taken. There are several options to remove or repurpose these alarms.

8.6.2 Possible options to remove or repurpose these include:

1. Reversing the logic by swapping from NO to NC contacts on the relay that generates the alarm or vice versa. This arrangement gives an alarm if the isolation has been overlooked or inadvertently connected.
2. Deleting the alarm from the I/O list – may require vendor automation engineer.
3. Powering the second power supply from the main supply feed if the current rating and protection settings of the main feed permit that. This restores a little redundancy in the case of a faulty power supply.

APPENDICES

APPENDIX A CROSS-CONNECTIONS

- A.1 CROSS-CONNECTIONS - GENERAL
- A.2 CROSS-CONNECTIONS IN CONTROL POWER SUPPLIES
- A.3 TOOLS FOR EVALUATION
- A.4 CLOSED BUSTIES

APPENDIX B COMMONALITY

- B.1 ADDRESSING COMMONALITY
- B.2 COMMONALITY IN DP CLASS 3 DESIGNS
- B.3 GROUND FAULTS – PROPAGATION THROUGH SHIP'S HULL
- B.4 MARINE AUXILIARY SERVICES
- B.5 NETWORKS
- B.6 NETWORK TESTING

APPENDIX C EXTERNAL INTERFACES & INFLUENCES

- C.1 EXTERNAL INTERFACES & INFLUENCES
- C.2 FIRE & GAS AND EMERGENCY SHUTDOWN (ESD)
- C.3 OTHER EXTERNAL INTERFACES

APPENDIX A CROSS-CONNECTIONS

FIGURES

Appendix A - Figure 1	Commonly Found dc Control Power Distribution Schemes	4
Appendix A - Figure 2	Over-voltage Failure Mode	5
Appendix A - Figure 3	dc to dc Converter	7
Appendix A - Figure 4	Dual Supplies Provided by dc to dc Converters (still cross connected – not preferred)	8
Appendix A - Figure 5	Simple Dual Supply Arrangement Using Diodes	9
Appendix A - Figure 6	Control Power Supplies without Cross-connections	12
Appendix A - Figure 7	Individual Supplies	13
Appendix A - Figure 8	Separating Main and Backup Supplies	14
Appendix A - Figure 9	Multi Split Systems	15
Appendix A - Figure 10	Common Battery Bank	16
Appendix A - Figure 11	Auto Changeover	17
Appendix A - Figure 12	LV Distribution System - Backup Supplies from Emergency Switchboard	18
Appendix A - Figure 13	LV Distribution System - Backup Supplies from Other Redundant DP Group	19
Appendix A - Figure 14	Dual Diode Connected Supplies to Engine Governors	21
Appendix A - Figure 15	Design with Additional Supplies and No Cross-connections	22
Appendix A - Figure 16	Generator Controls with Dual Supplies	23
Appendix A - Figure 17	Typical Diesel Electric DP Power Plant	30

TABLES

Appendix A - Table 1	Control Power Consumer and Source	24
Appendix A - Table 2	DP UPS Arrangement	24
Appendix A - Table 3	Control Power ac & dc Distribution (Two-way Split) - Example	25
Appendix A - Table 4	Control Power ac & dc Distribution (Four-way Split) - Example	26
Appendix A - Table 5	Control Power ac & dc Distribution (Two-way Split)	27
Appendix A - Table 6	Control Power ac & dc Distribution (Three-way Split)	28
Appendix A - Table 7	Control Power ac & dc Distribution (Four-way Split)	29

A.1 CROSS-CONNECTIONS - GENERAL

A.1.1 OVERVIEW

A.1.1.1 In the vernacular of DP vessel design, the term 'cross-connections' is used to mean physical connections between redundant equipment groups. Cross-connections occur for many different reasons. Some are unavoidable such as those in the DP control system which must control the thrusters in all redundant groups while others such as closed busties exist to provide advantages in terms of emissions, fuel consumption and maintenance.

A.1.1.2 The term 'cross-connections' is most commonly used to describe tangible connections which are intentionally installed. Fault propagation may occur through intangible connections such as the coupling of interference from power cables to control cables. This is generally controlled by good installation practice such as the cable segregation requirements in classification society rules.

A.1.2 STAKEHOLDER REQUIREMENTS

A.1.2.1 In addition to DP equipment class notation requirements, other stakeholders may stipulate their own requirements to address cross-connections.

A.1.2.2 It is of paramount importance to clearly identify the requirements of all stakeholders, assess impacts and develop appropriate plans to meet expectations.

A.1.3 FAULT PROPAGATION PATHS

A.1.3.1 All cross-connections are potential fault propagation paths that may have the ability to couple failure effects in one redundant equipment group to another. Such coupling may result in the failure of both systems accompanied by failure effects of a severity greater than that of the Worst-Case Failure Design Intent (WCFDI).

A.1.3.2 Where cross-connections are unavoidable, there must be a comprehensive set of protective functions designed to identify and isolate any failure effect propagating by way of the cross-connection. Typical examples of protective function applied for this purpose include:

- Generator and bustie protection designed to open closed busties on detection of:
 - a. Over current.
 - b. Under voltage.
 - c. Over voltage.
 - d. Under frequency.
 - e. Over frequency.
 - f. Unbalanced line currents.
 - g. Severe active power imbalance.
 - h. Severe reactive power imbalance.
- Net storm software in data communications systems.
- Pressure relief valves in common control air systems.
- Fuses and Miniature Circuit Breakers (MCBs) in main and backup control supplies.
- Diodes for fault isolation in main and backup control supplies.
- Interlocks and permissive designed to prevent acts of maloperation.
- Switchboard control, power and synchronising lines.

A.1.3.3 Unfortunately, protective functions are not always as effective or as comprehensive as they should be and may only be effective in isolating a subset of the faults that can propagate from one system to another. Every protective function is also a potential hidden failure. Alarms and periodic testing are required to improve confidence that they remain effective and will operate successfully on demand.

A.1.4 FAILURE MODES OF CROSS-CONNECTIONS

A.1.4.1 Electrical consumers may malfunction when exposed to interruptions, fluctuations and other transient phenomena on their power supplies. An excursion from the nominal supply voltage or frequency may have this effect depending on the sensitivity of the consumer (fault ride-through capability).

A.1.4.2 **Under-voltage** is arguably the most prevalent failure mode and may be caused by (inter alia):

- Supply interruption – No voltage.
- Voltage control issues at the power source – AVR etc.
- The effects of electrical faults such as short circuit and overload.
- Earth faults may cause excursions above and below the nominal line-to-earth voltage simultaneously at different points.

A.1.4.3 **Over-voltage** conditions may be experienced less frequently but may cause more severe and irrevocable damage when they do. Over-voltage may occur due to:

- Regulator failures
- Transformer faults
- Transient phenomena – spikes, commutation notches etc. – A power and propulsion system should be designed to cope with the normally occurring transient phenomena associated with its operation.
- Lightning.

A.1.4.4 **Over / Under frequency:** Excursions above and below nominal power frequency may occur due to speed regulator failures in generators and control system faults in UPSs and inverters.

A.1.4.5 **Distortion:** Waveform distortion may also cause malfunction – In particular, equipment that utilises the zero crossings in ac voltage waveforms for timing purposes. Harmonic distortion can be caused by failure of harmonic cancelation features or malfunctioning consumers and may be considered as another form of frequency-related failure.

A.2 CROSS-CONNECTIONS IN CONTROL POWER SUPPLIES

A.2.1 OVERVIEW

A.2.1.1 Cross-connections in control power supplies are very common in DP class 2 and DP class 3 designs, particularly in 110Vdc and 24Vdc supplies for switchboard and thruster controls. There are at least three reasons why this is the case.

- **Reliability:** There is a perception that dc power supplies based on battery rectifier arrangements are unreliable (thus backup is required).
- **International Regulations and Class rules:** There are SOLAS, MODU code and class rules requiring certain control power consumers to have a main and a backup supply or an emergency supply (these issues can generally be managed).
- **Severity of failure effect:** The failure effects of losing a battery rectifier supply may equal the worst-case failure design intent (WCFDI). See Section A.2.7.

A.2.1.2 The redundant supplies are usually cross connected by cables from one redundant system to another terminated by a protection device such as a fuse or miniature circuit breaker and some sort of device intended to limit the potential for fault propagation such as diodes or dc to dc converters. In some designs each consumer has a backup supply. In other designs the cross-connection is between the power supply distribution boards.

A.2.1.3 Most DP related equipment requires control power in some form or other and dc supplies with battery back-up are a popular way of fulfilling the requirements for:

- Clean power
- Fault ride-through capability
- Continuity of control power in a blackout.

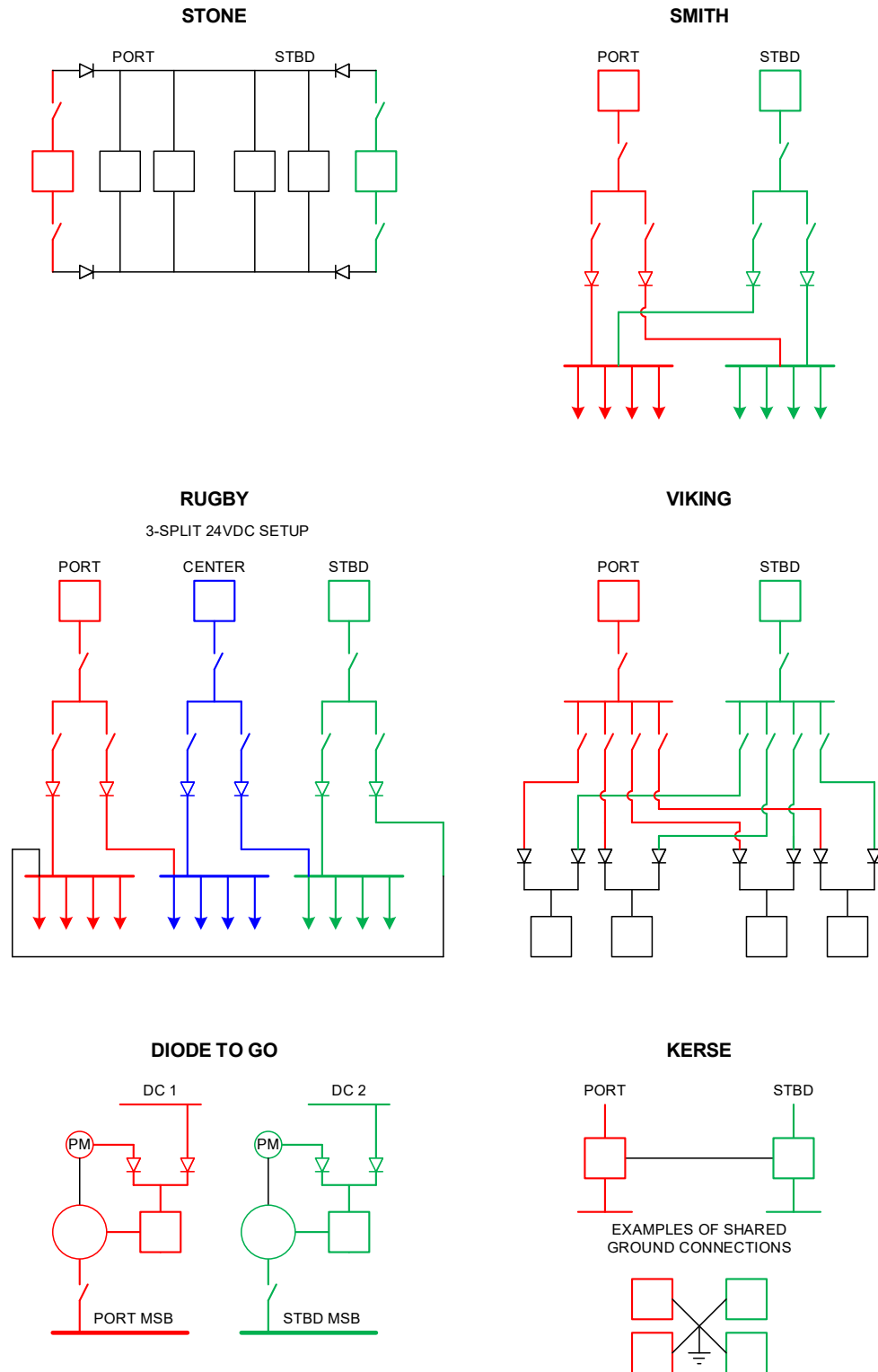
A.2.1.4 A minimum specification installation provides one dc power supply for all consumers on one redundant group. In practice, the requirement for different voltages and the practicality of providing low voltage power over long distances generally means there is more than one unit. Despite having multiple units, the failure effects of any unit are generally equal to the worst-case failure design intent. While it could be argued that the failure effects do not exceed the worst-case failure effect, the impacts of losing multiple generators, thrusters or entire switchboards, when it can be avoided at reasonable cost, is generally considered to produce a less robust redundancy concept.

A.2.1.5 Several of the major classification societies have rules under 'main class' which require backup supplies for essential consumers such as engine governors or system associated with propulsion and steering. These rules generally do not specify where the backup source of power comes from but in the case of DP vessels the requirement is often interpreted to mean from the dc supply in the other redundant equipment group. Another interpretation is that it should originate at the emergency switchboard. Requirements originating in SOLAS or IMO MODU code may also give rise to cross-connections for similar reasons and may require Flag State acceptance of any deviation.

A.2.1.6 Taking the supply from an existing source in another redundant group is traditional and perceived to be the most cost-effective way of complying with the rule requirements (or desire to improve reliability). This practice avoids the cost of installing a second power supply in each redundant group. However, this perception may prove erroneous when the full cost of purchasing, installing and commissioning the interconnecting cables is considered and it may be more economical to install additional power supplies within each redundant group. In particular, the cross section and thus the cost of cables required to avoid significant voltage drop is a factor in some LV distribution systems.

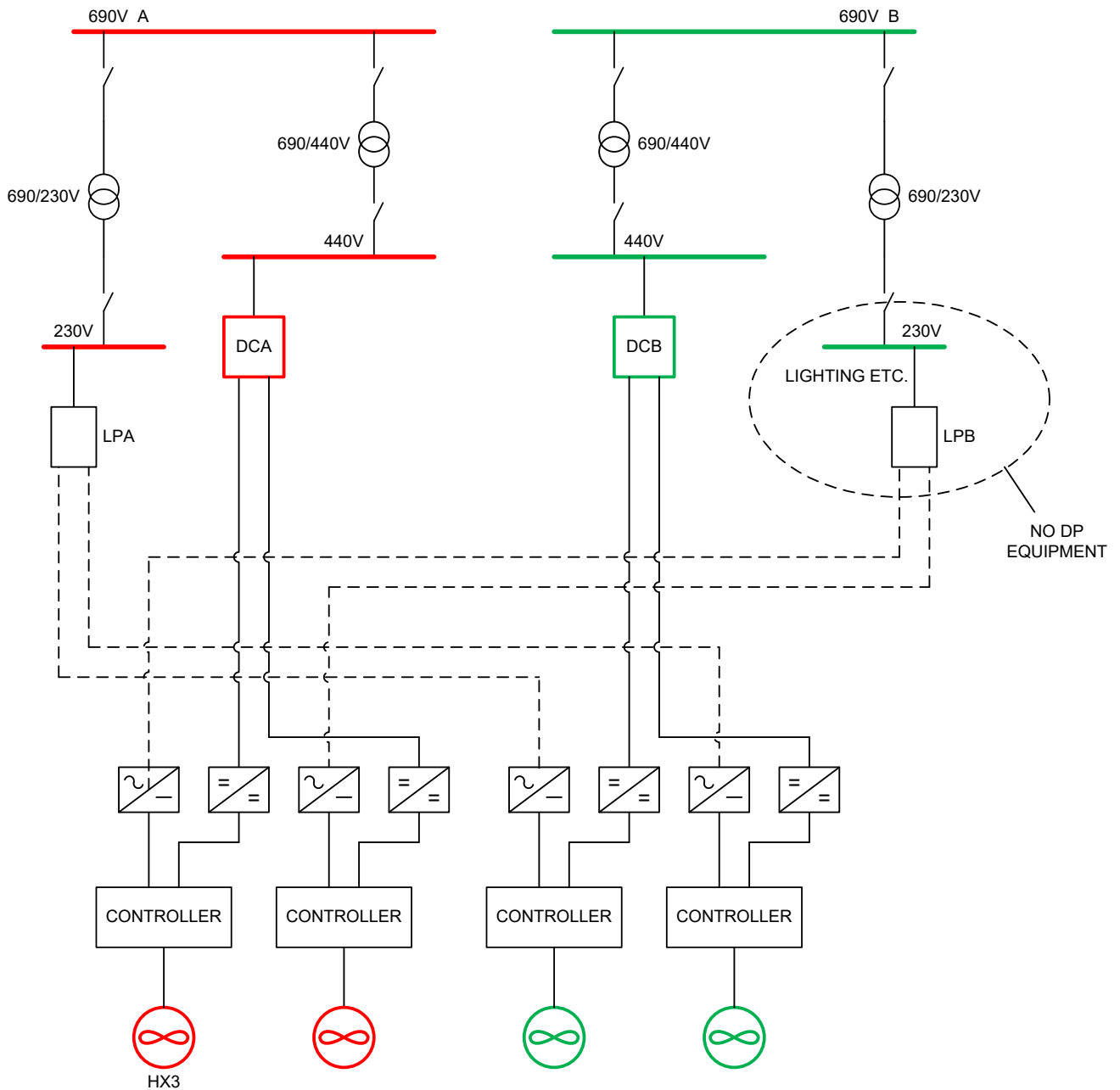
A.2.2 EXAMPLES OF COMMON CONTROL POWER ARRANGEMENTS

A.2.2.1 The sketches in Appendix A - Figure 1 below illustrate commonly found dc control power distribution schemes. Such schemes are typically used to provide power for generators and switchboards controls.



Appendix A - Figure 1 Commonly Found dc Control Power Distribution Schemes

A.2.2.2 Not all cross-connections occur within the same voltage distribution level. In the example in Appendix A - Figure 2 below, 230V lighting distribution boards provide dc power to thruster drive controllers by way of rectifiers. Sometimes these arrangements may be categorised as 'fault tolerant' because the supply originates from a source which has no other DP related equipment which could be subjected to voltage dips etc. However, issues associated with hidden failure of the normal supply and also the potential for over-voltages to be coupled from one redundancy group into the other need to be considered. These arrangements need the same scrutiny as other cross-connections.



Appendix A - Figure 2 Over-voltage Failure Mode

A.2.3 FAILURE MODES OF DIODES

A.2.3.1 Diodes are still commonly found, despite there being superior ways to provide redundant power. Diodes are power electronic devices that act as a one-way valve. Current flows in the direction of the arrow but cannot flow against it. In the direction of conduction, the diode exhibits a forward voltage drop of around 0.6V. The diode's current rating dictates the forward current it can tolerate. In the reverse direction, it will block reverse current flow from a voltage source up to the voltage at which it breaks down and conducts in the reverse direction. This point is referred to as the diode's peak inverse voltage.

A.2.3.2 Diodes used for cross connecting control power supplies are usually generously rated for current and voltage and often rated for many times the load current and voltage they experience in normal operation.

A.2.3.3 Diodes have the following modes of failure:

- Short circuit (conduct in either direction) – Typically caused by an overvoltage event called 'punch-through'.
- Open circuit (no conduction) – Typically caused by overcurrent event called 'burnout'.

A.2.3.4 It is important to remember that the failure of associated components can also defeat the redundancy concept. Loose terminals and broken conductors, fuse failures caused by vibration, etc. These types of failure are typically more common than failure of the power electronic device itself.

Notes:

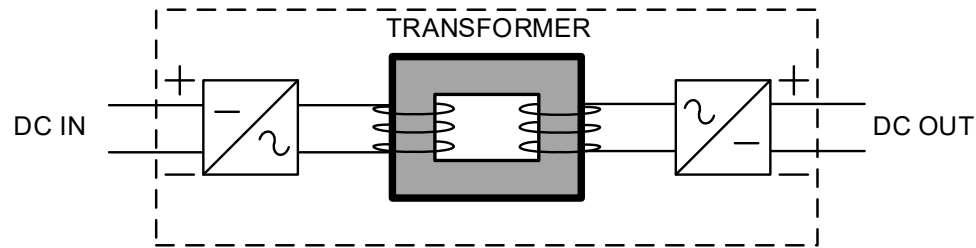
1. Cross-connections introduce vulnerabilities associated with configuration errors and acts of mal operations.
2. Diodes do not significantly limit the fault current to a failed consumer, nor the associated voltage dip experienced at the power supply terminals.
3. Diodes have a low tolerance for overcurrent and can be damaged by the fault current before the overcurrent protection operates.
4. Diodes do not provide galvanic isolation.
5. How load and fault current splits between two diode-connected dc power supplies depends on a number of circuit variables and can vary from half through each diode to all through one and none through the other.
6. dc power supplies can be configured for load sharing, but this is not typical in marine applications.
7. Diode failure may go unnoticed (hidden failure). Subsequent failures may have effects exceeding the worst-case failure design intent.

A.2.4 dc TO dc CONVERTERS

A.2.4.1 dc to dc convertors are an increasingly popular way of providing a dual power supply in a form that does provide galvanic isolation. Galvanic isolation means there is no direct current path from the source to the load. dc to dc convertors are essentially an inverter and rectifier coupled by a transformer as shown in Appendix A - Figure 3. Features of dc to dc convertors include:

- Fault current limiting (although this may be a disadvantage if redundancy depends on selectivity of over current protection – Converters are available which are designed to operate over current protection).
- Ability to change voltage between input and output.

- Electrical noise associated with switching of the inverter.
- The transformer provides the galvanic isolation (earth fault isolation).



Appendix A - Figure 3 dc to dc Converter

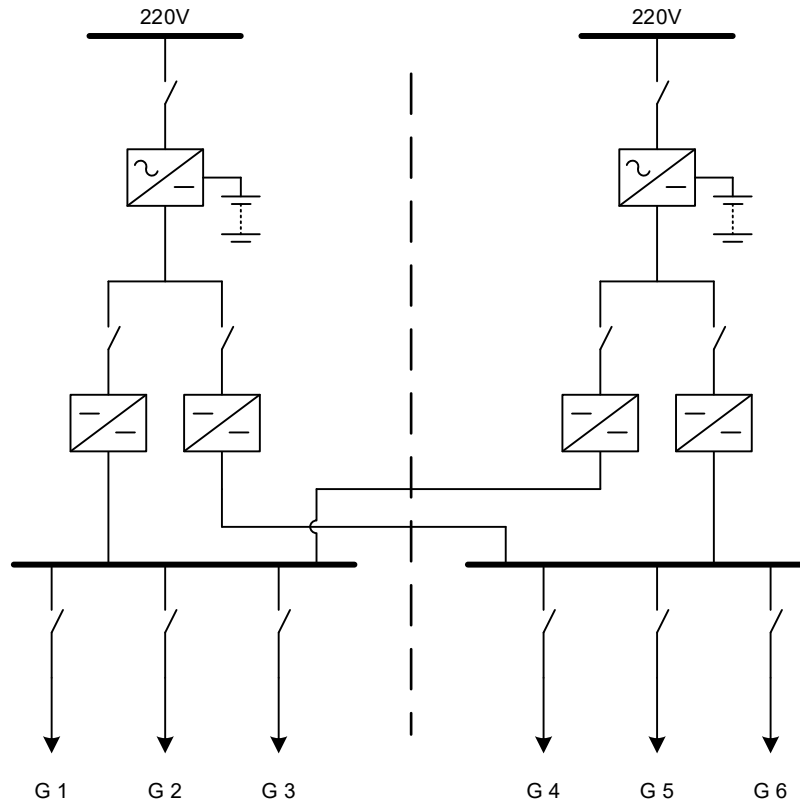
A.2.5 **BACKUP CONTROL SUPPLIES BY WAY OF DC/DC CONVERTERS**

A.2.5.1 dc to dc convertors generally offer a higher degree of integrity to fault transfer than arrangements based on diodes, but the presence of the necessary attributes should be established in systems using such devices. Refer to Appendix A - Figure 4.

- dc to dc convertors usually (but not always) have galvanic isolation between input and output which is typically provided by a switched mode power supply with toroidal transformer between the input and output stages.
- There may be sufficient impedance between input and output to reduce the voltage dip at the input 24Vdc power supply to acceptable levels.
- The design of the dc to dc converter may inherently limit the possibility for an overvoltage to propagate from input to output or vice versa due to the effects of transformer saturation etc.

A.2.5.2 However, the possibility of other fault paths through the device should be considered by review of the internal design. The low fault current capability of the dc to dc converter may limit the possibility for a voltage dip to be passed to the 24Vdc supplies upstream but may also make convertors unsuitable for operating overcurrent protection selectively. That is to say, that if several consumers are fed from one dc to dc converter by an arrangement of fuses or miniature circuit breakers it may be difficult to arrange selectivity to isolate the fault to the affected sub-circuit.

A.2.5.3 Although a design using dc to dc convertors in appears to solve some of the problems associated with designs based on diodes, the potential for hidden failures still exists and using one redundancy group to supply another does not restore fault tolerance and thus cannot be relied up to provide higher availability for work.



Appendix A - Figure 4 Dual Supplies Provided by dc to dc Converters (still cross connected – not preferred)

A.2.6 MITIGATING THE RISKS OF CROSS-CONNECTIONS

A.2.6.1 Mitigating risk associated with cross-connections is highly dependent on the skill of the system designers and the FMEA team in correctly identifying all the relevant failure modes and then designing and testing effective protective functions to address them all. This can be a resource intensive process and carries the risk of being overlooked or inadequately addressed.

A.2.6.2 Thus, there are at least two possible approaches to developing a DP redundancy concept.

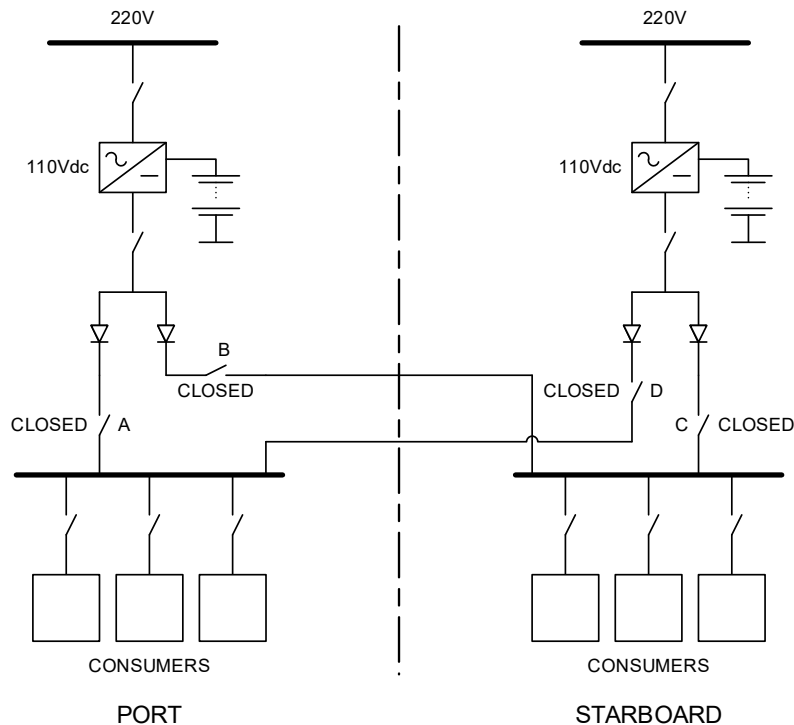
- Create a strongly coupled design with many cross-connections and commit to the resource intensive process to properly analyse and mitigate the risks.
- Employ good practices in the development of the redundancy concept (adhere to the seven pillars espoused in the MTS design philosophy guidance document) and reduce the number of cross-connections to as low a level as practical. This reduces the risk of unforeseen failure effects, the burden of identifying them and the risk of not identifying them.

A.2.6.3 The MTS LIFE Concept (Low Impact Failure Effect) Promotes the concept of reducing the number of cross-connections within the same redundant group to limit the amount of main machinery that could be lost as the result of single failure. This does not improve the post failure DP capability but offers a degree of protection against hidden lack of capacity in surviving equipment.

- A.2.6.4 Failure effects which propagate between redundant DP equipment groups through cross-connections associated with dual power supplies and auto changeovers are known causes of DP incidents. The failure modes which create these effects are not necessarily of high probability but when they do occur the effects are often severe and difficult to recover from.
- A.2.6.5 The threats posed by these failure modes are often overlooked in superficial DP system FMEAs and there may be a large number of DP vessels in service which are vulnerable to these types of failures. Some charterers specifically target these features during on-hire surveys to reduce their exposure to DP incidents.
- A.2.6.6 Cross-connections in control system power supplies are generally installed with the best of intentions or in the belief that they are required to satisfy certain class rule requirements. Where such requirements exist, it is usually possible to comply without creating cross-connections which have the potential to defeat the DP redundancy concept.
- A.2.6.7 Installing non-critical redundancy in the form of additional power supplies in the same redundant DP group may be cheaper than cross-connections when the overall cost of purchase, installation, commissioning and testing are considered.
- A.2.6.8 The fewer cross-connections between redundant DP equipment groups the fewer possible paths exist for fault transfer by failure mode, foreseen or otherwise. Reliance on protective functions is reduced as is the burden of maintaining and testing such protective functions periodically.

A.2.7 CROSS-CONNECTIONS CREATED BY DIODES

- A.2.7.1 Appendix A - Figure 5 shows a simple power supply arrangement in which two 110Vdc distribution board are fed by two sources of supply. One supply is from a local source and the other from a source in another redundancy group. The system is normally configured with all circuit breakers closed. There can be significant variations on this design including the number and locations of circuit breakers or fuses for overcurrent protection.



Appendix A - Figure 5 Simple Dual Supply Arrangement Using Diodes

A.2.7.2 Failure modes to be considered include:

- Low or zero voltage at one power supply.
- High voltage at one power supply.
- Short circuit or earth fault on a power supply.
- Short circuit or earth fault on a consumer.
- Short circuit or earth fault on a distribution board.
- Open circuit on a conductor or diode (potential hidden failure).
- Short circuit across a diode (potential hidden failure).
- Flat battery (insufficient capacity to deliver fault current).
- The effects of fire and flooding.

A.2.7.3 Note: *The list of failure modes above is the minimum that should be used to analyse such a system, but cross-connections are able to couple all sorts of common mode failures such as excessive electrical noise, spikes, thermal conduction in fires etc.*

Note: For a discussion of earth fault related failure effects see Section B.3.

A.2.7.4 Failure effects:

- Low or zero voltage at one power supply: This is the failure mode the cross-connections are intended to protect against. If one supply fails to low voltage the other supply will continue to power all consumers.
- Short circuit or earth fault on a power supply: This failure mode is the reason that the cross-connection must be made using diodes and not directly cross connected. In the case of connections without diodes, a fault with a power supply would be back fed from the other power supply, disabling both power supplies. All consumers would fail.
- High voltage at one power supply: This failure mode has the potential to destroy all consumers. Over voltage protection at the power supplies or wide voltage tolerance in the consumers is required to prevent the redundancy concept being defeated.
- Short circuit or earth fault on a consumer: A fault in any consumer will cause fault current to flow. Depending on how that fault current splits, there may be a significant voltage dip on both distributions. This may cause all consumers to malfunction if they cannot ride-through the voltage dip
- Short circuit or earth fault on a distribution board: A fault on a consumer should be cleared by the circuit breaker immediately upstream. A fault on the distribution board has to be cleared by one circuit breaker in each power supply. The same concerns relating to potential voltage dips apply.
- Open circuit on a conductor or diode (potential hidden failure): In some locations, this can become a hidden failure with the potential to defeat the redundancy concept. If the supply within the same redundancy group loses connection to the distribution board then all consumers are being supplied from one redundancy group. A subsequent failure in the surviving power supply connection will lead to loss of power in all consumers.
- Short circuit across a diode (potential hidden failure): This type of failure removes the protection against a fault in one power supply being back fed by the other.

- Flat or disconnected battery: The power supplies may rely on the current capability of the batteries to deliver sufficient fault current to operate the overcurrent protection selectively. If both batteries are allowed to go flat (hidden failure) it may not be possible to clear the fault and all consumers will be lost when both power supplies go into current limitation.
- The effects of fire and flooding: In DP class 3 designs the possibility of multiple faults must be considered. In the example in Appendix A - Figure 5 a fire in the port redundancy group could apply short circuit faults to both cross-connecting lines. The effect of this is that it would not be possible to clear a fault from the starboard distribution board, resulting in the loss of both DP redundancy groups. At least one major classification society has revised its DP rules to indicate that control power supply lines should not cross the A60 watertight boundaries between redundant equipment groups.

A.2.7.5 **Configuration errors**: It is possible to defeat the redundancy concept by leaving the circuit breakers from either main supply to the local distribution board open.

A.2.7.6 **Protection coordination**: The fault tolerance of this system relies on the proper coordination of certain overcurrent devices. If the upstream and downstream coordination is inadequate the circuit breakers at the dc power supply outputs may operate isolating all consumers. Fuses may be more reliable than miniature circuit breakers for this purpose. The level of analysis and testing applied to proving the coordination of protection on low voltage supplies can be insufficient to prove fault tolerance. Questions are being raised in industry about circuit breaker aging and how the effects can be verified. In some cases, ac components are used in dc systems, but no dc characteristics exists to allow the selectivity to be assessed.

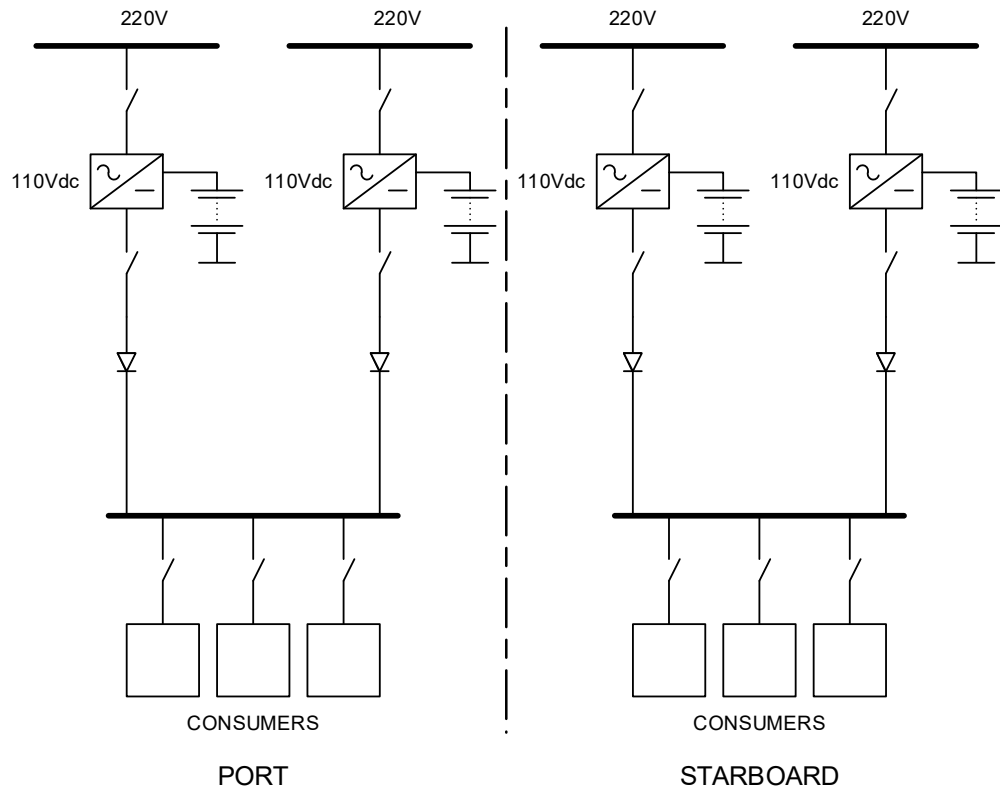
A.2.8 DUAL SUPPLIES - MITIGATION OF FAILURE EFFECTS

A.2.8.1 Deciding how to mitigate the undesirable effects of the failure modes listed in A.2.7.2 can be strongly influenced by the burden of reaching a satisfactory level of confidence in the original design. With the provision of monitoring, careful protection coordination, analysis, failure testing and periodic testing it may be possible to conclude that the system is fully fault tolerant. Alternatively, it may be concluded that time and money is better spent engineering out the risks by removing the cross-connections.

A.2.8.2 In Appendix A - Figure 5, removing the cross-connections is as simple as opening circuit breakers B and D. This does however reintroduce the concerns that the crossovers were designed to address in the first place which is that losing three generators and/or three thrusters due to failure of a low reliability component is not a desirable consequence of a reasonably probable failure. It also introduces another issue associated with the ability of the surviving equipment to accept the load transfer. If the frequency with which the vessel experiences a failure equal to its worst-case failure design intent is increased, then it becomes increasingly important that the surviving generators and thrusters can accept the load transfer as they may be required to do so more often.

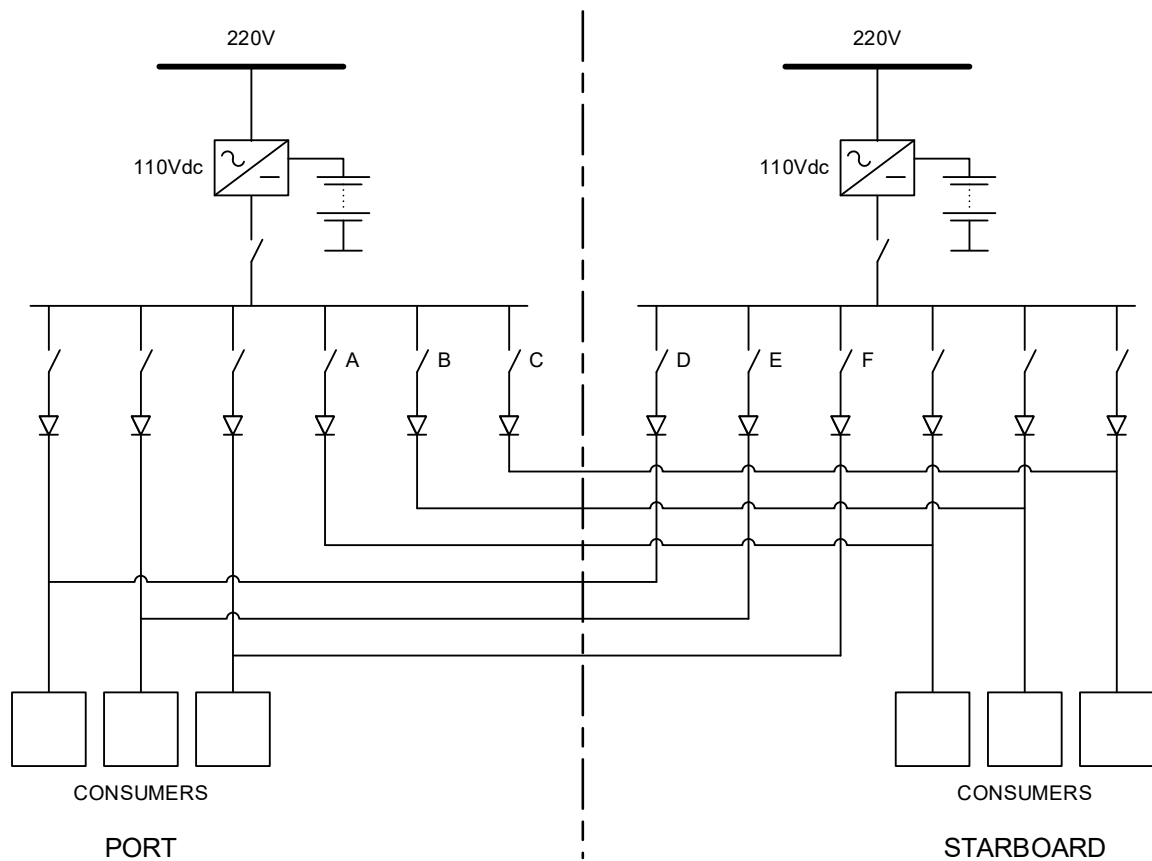
A.2.8.3 It is possible to address both risks to some degree as shown in Appendix A - Figure 6. In this arrangement, the cross-connections have been removed and a second charger has been added to address the issue of poor reliability. Some designers extend this concept even further and make each engine and generator autonomous and independent with its own control power supplies backed up by a supply from the permanent magnet generator so that it only requires external power to start. This is the design methodology that is encouraged by the Low Impact Failure Effect (LIFE) concept and MTS 'Seven Pillars'.

A.2.8.4 When charterers are performing on-hire or suitability surveys, there may be little time to conclude upon the fault tolerance of a system using cross-connections, particularly if verification of fault tolerance is poorly documented. Charterers are seeking to reduce the risk of a DP incident associated with fault transfer while the vessel is on hire to them. When isolation of the cross-connections is the preferred solution without adding additional power supplies then it becomes increasingly important to have confidence in the performance of all machinery that may be called upon to accept load transfer. Tests should be carried out to confirm this. Such tests may be part of annual DP trials or referenced from the configuration section of the ASOG.



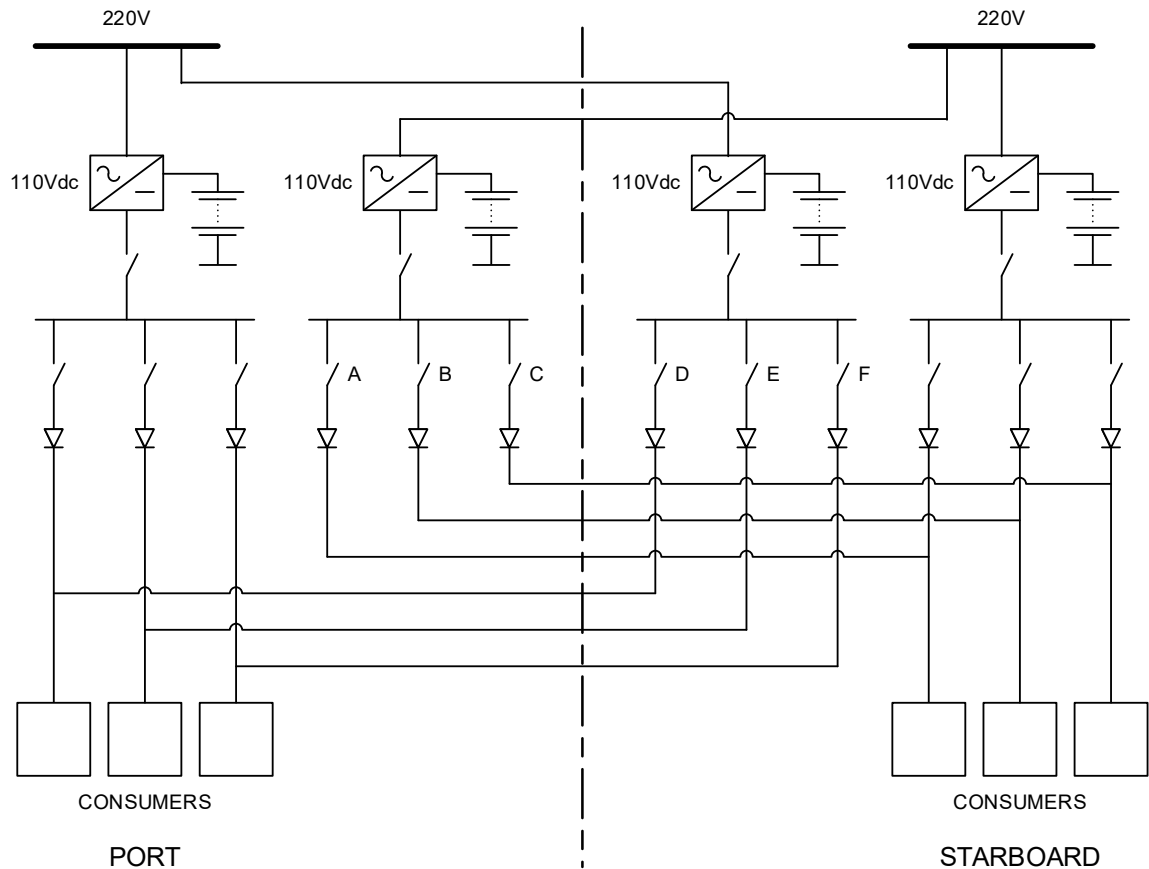
Appendix A - Figure 6 Control Power Supplies without Cross-connections

A.2.8.5 Appendix A - Figure 7 shows an alternative arrangement where each individual consumer has dual supplies rather than just the distribution board. There are variations in the failure effects for such designs but concerns about fault propagation remain the same. The cross-connections can be isolated by opening circuit breakers A to F.



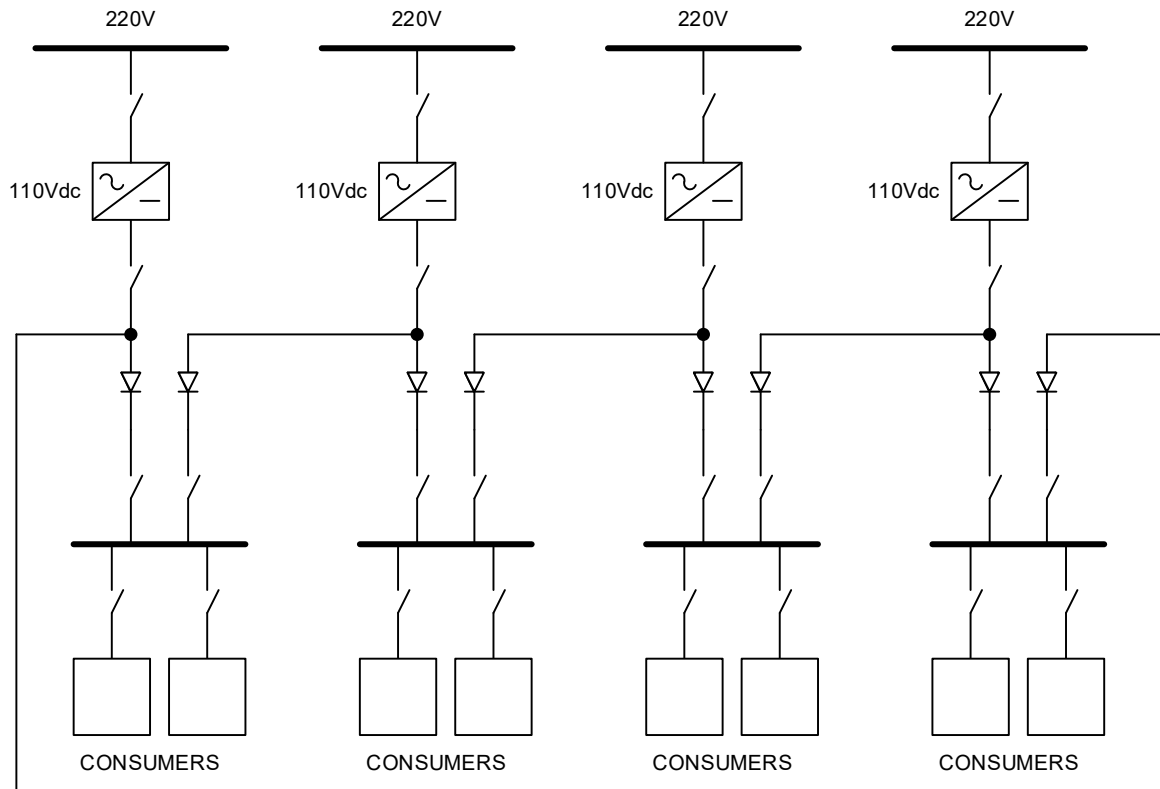
Appendix A - Figure 7 Individual Supplies

- A.2.8.6 To overcome the problem of having to pull back and re-terminate so many cables, some vessel owner faced with this problem have elected to separate the distribution boards as shown in Appendix A - Figure 8. This resolves the issues with technical failures on DP class 2 designs but not the issues associated with the effects of fire and flooding in DP class 3 designs. Never-the-less, it is a way of engineering out many of the risks associated with technical failures if not a full solution for DP Class 3.



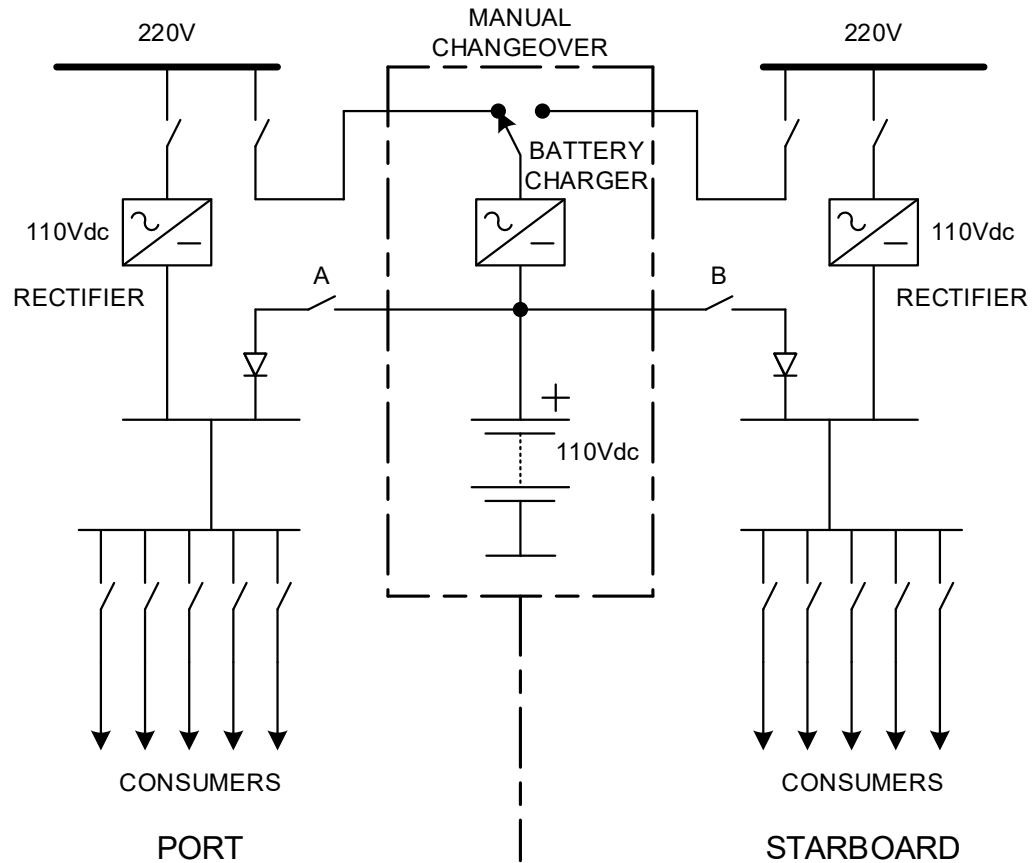
Appendix A - Figure 8 Separating Main and Backup Supplies

A.2.8.7 Up to this point, the discussion has focused on the traditional DP redundancy concept with a two-way split. Multi-split designs such as three-way and four-way splits are becoming increasingly popular as a way of reducing the impact of failure effects and obtaining a higher post failure DP capability with the same size of propulsion plant. Appendix A - Figure 9 shows an alternative arrangement of cross connected control supplies that takes advantage of the fact that there are multiple sources of control power. This arrangement removes the concern about faults causing voltage dips on more than one distribution board. In this design the voltage on the distribution board's remote supply (outside the DP redundancy group) is maintained by an adjacent supply while the local supply delivers the fault current. In this way only the faulted distribution board experiences a voltage dip. It also removes the concerns about protection coordination as both the local and the remote (backup) supply can be lost without exceeding the worst-case failure design intent. Other failure modes may succeed in propagating by way of the cross-connections if not adequately addressed. Such failure modes could include overvoltage and excess electrical noise. This design is an improvement on the two-way split but still has more issues to be resolved than fully isolated systems. The common point would be regarded as a distribution and the fuse on both supplies must be in the same zone as the distribution, or an additional fuse must be installed.



Appendix A - Figure 9 Multi Split Systems

- A.2.8.8 Where isolation is the preferred strategy to address vulnerabilities due to cross-connections, further analysis should be undertaken to ensure that such isolations do not introduce other unintended risks. Care must be taken when isolating cross-connections to ensure that there is a full understanding of the consequences of doing so and that other risks are not being introduced as a result.
- A.2.8.9 As an example, Appendix A - Figure 10 shows the 110Vdc control power supplies for a pair of switchboards. In this design, each switchboard has its own rectifier but shares a common battery bank. The battery connections form a common point. It may be possible to remove this common point by opening one of the battery supply circuit breakers (A or B) therefore associating the battery with only one redundant group. While isolation removes the potential fault propagation path it should be confirmed that this does not deprive one switchboard of its ride-through capability. If the purpose of the battery is to allow the switchboard control and protection to function correctly when clearing a short circuit fault on the ac distribution, then the switchboard without the battery may not perform that task correctly. Without the battery the rectifier will have no power while the short circuit is present because the system voltage drops to zero. Protection relays will have no power and it may not be possible to clear the fault selectively or at all. Exactly what happens depends on the detailed design of the protection scheme but failure to clear a fault from a main switchboard may lead to an undesirable situation. Any design change should be based on a full and documented understanding of how the system works and how it fails. In the example provided above, a better solution would have been to ensure that each switchboard has its own battery bank.



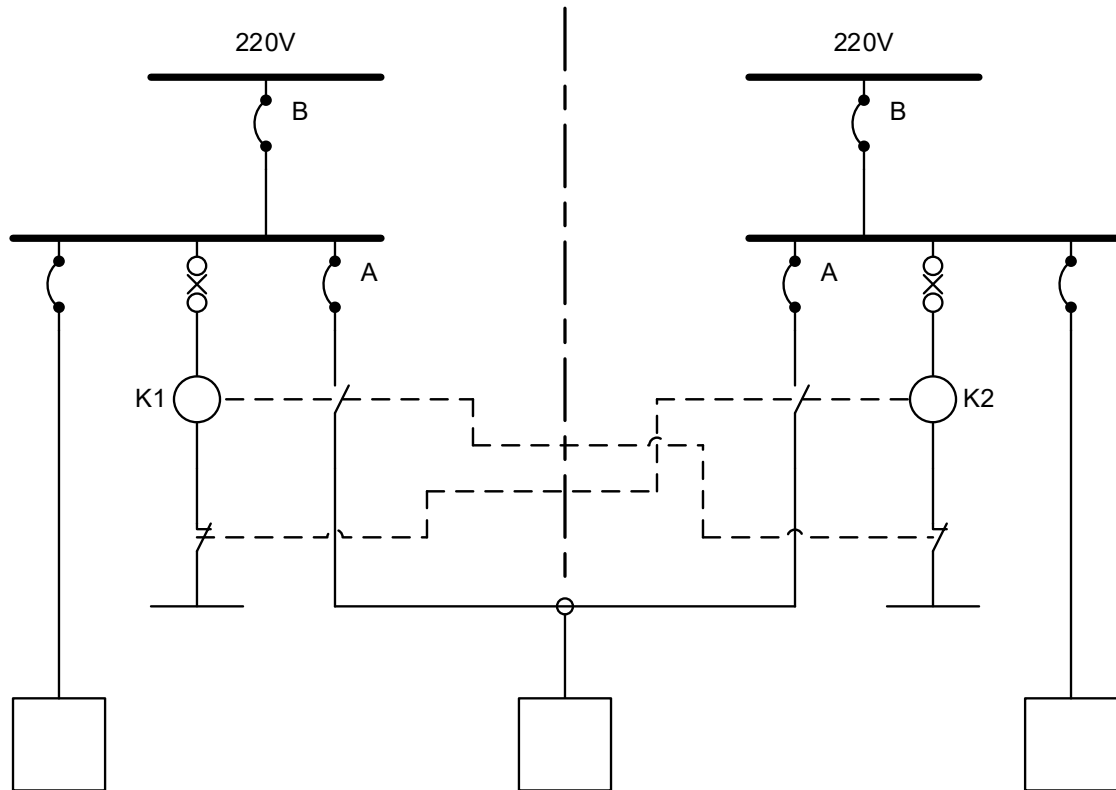
Appendix A - Figure 10 Common Battery Bank

A.2.9 CROSS-CONNECTIONS CREATED BY AUTO CHANGEOVERS

A.2.9.1

Auto-changeovers are typically used to provide a main and backup ac supply. Changeovers are generally not instantaneous so the consumer must have ride through capability or stop and restart of the consumer is an acceptable mode of operation. Appendix A - Figure 11 shows a simple auto changeover of a type typical of that found on DP vessels (can be used for ac or dc). The changeover consists of two double-pole dry contact relays. In each relay, one 'Normally Closed' and one 'Normally Open' contact are arranged to connect the power to the consumer and disconnect the relay coil on the opposite relay. Features of this arrangement are:

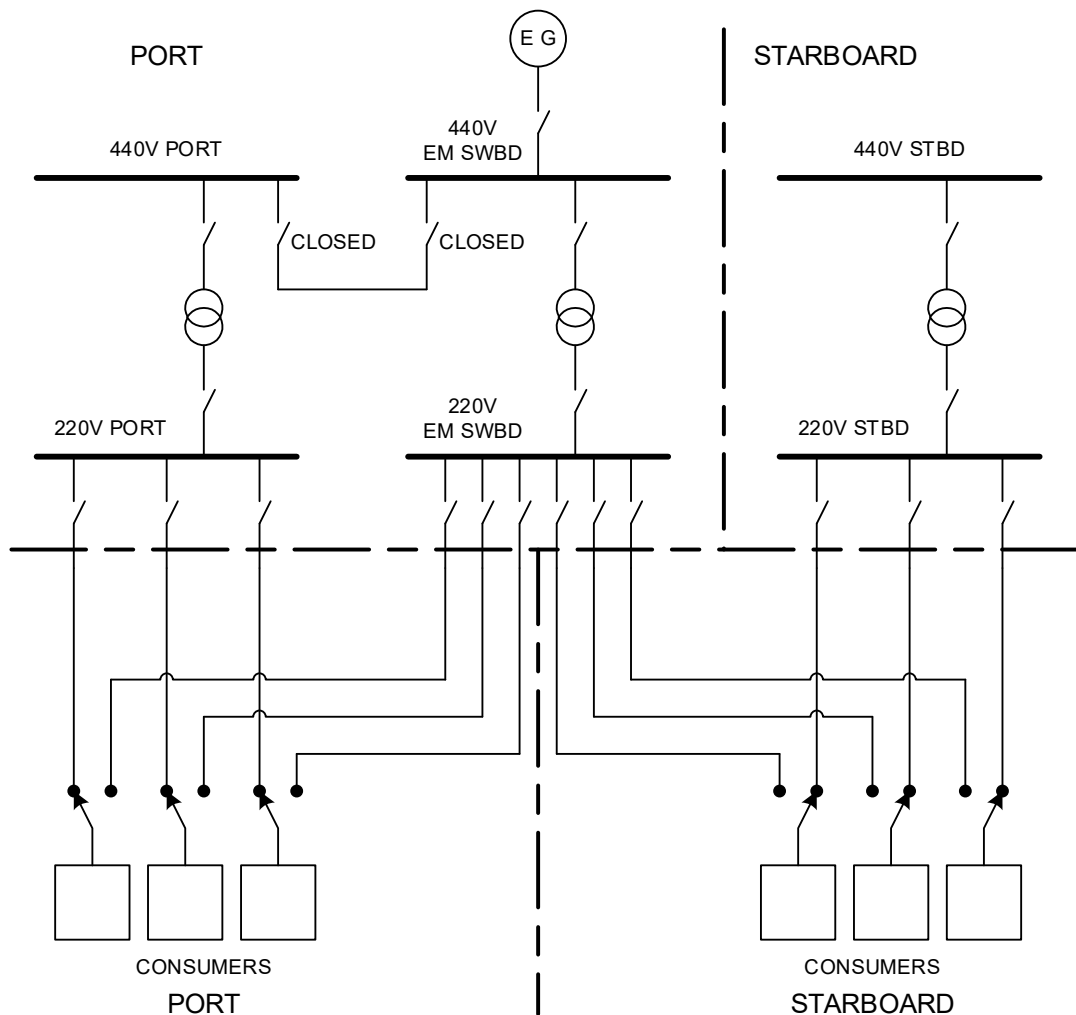
- Whichever source of 220V power is energised first becomes the main supply. This can encourage configurations errors following maintenance and repair etc. (e.g. failure to change supply back).
- A fault in the consumer will be cleared by the upstream overcurrent protection causing a voltage dip on that supply. The auto changeover will then operate and connect the faulty consumer to the other 220V supply at which point the upstream overcurrent protection on that circuit will operate creating a voltage dip on the other supply. If these distribution boards supply other sensitive consumers in each redundancy group then malfunction may occur in both redundancy groups.
- Clearing the faulty consumer requires the overcurrent protection on both feeds to operate. If the selectivity between the protection for the consumer (A) and the next circuit breaker upstream (B) for the overall supply is inadequate there is a risk that all three consumers are lost not just the faulty changeover unit.



Appendix A - Figure 11 Auto Changeover

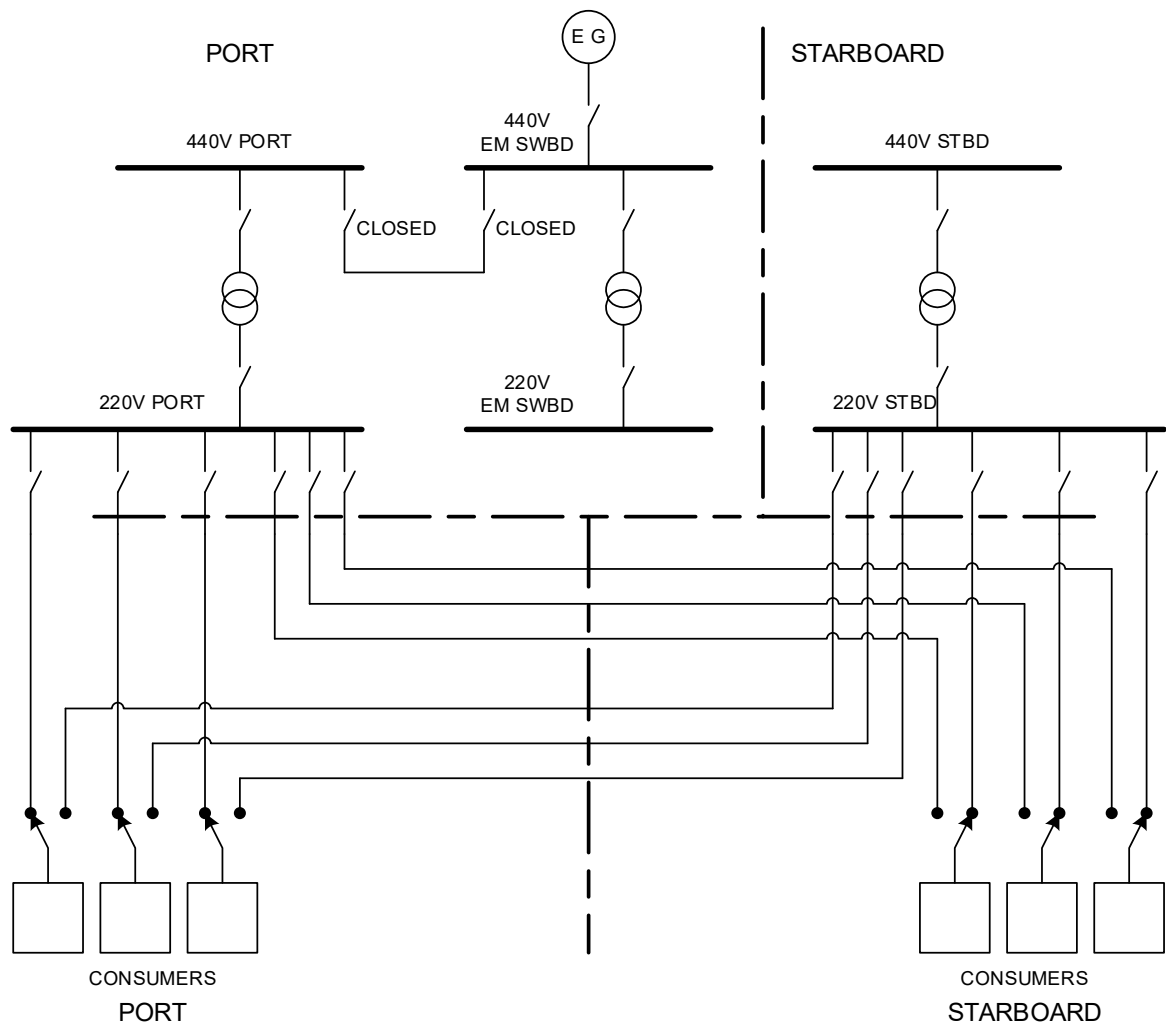
- A.2.9.2 Backup power supplies from the emergency switchboard are a common and useful way of providing an alternative source of power to essential consumers such as:
- UPSs
 - dc power supplies
 - Engine pre-lube pumps
 - Fuel booster pumps.
- A.2.9.3 Typically, the normal source of supply for these consumers is from the same redundancy group as the equipment they serve.
- A.2.9.4 Providing an alternative supply to UPSs is often essential to ensure the vessel's power plant can be black-started using only the stored energy in the emergency generator's starting system. In addition to providing a useful maintenance facility, the emergency supply provides the ability to keep UPS consumers supplied and engines pre-lubricated. It also provides some defence against a blackout of unusually long duration which might otherwise drain the batteries. Such events are less likely to occur in a well-designed DP system but unforeseen failure modes, common cause failures and combinations of hidden failures and subsequent failures can have such effects.

A.2.9.5 A common point is created in the redundancy concept by bringing feeders for consumers in each redundant group to the emergency switchboard. As with any common point it is necessary to evaluate the risk that a failure effect may propagate by way of this common point to affect the operation of more than one redundant group. In Appendix A - Figure 12 a number of consumers in each redundant group have a backup supply from the 220V emergency switchboard by way of an auto changeover. The normal supply is the local supply from within the same redundant DP equipment group. The emergency switchboard is powered from the port 440V power system. If the auto changeovers have no intelligence to prevent fault transfer, then a fault on a starboard consumer may cause it to connect to the supply from the emergency switchboard which will have to clear the fault again. Because the emergency switchboard is powered from the port power system both redundant DP groups have now experienced a disturbance. If the consumers in the DP redundancy groups can ride through that disturbance, then position will be maintained. If they cannot ride through the disturbance, then position may be lost. This scenario is possible whether the vessel operates with open or closed busties at the main power distribution level. That is to say isolated or common main power systems. Thus, the ride through capability and the magnitude and duration of the disturbance to the power systems become important factors in determining the risk of fault transfer in such a design. Only some class notations require that DP systems have their fault-ride through capability verified by testing in a realistic manner.



Appendix A - Figure 12 LV Distribution System - Backup Supplies from Emergency Switchboard

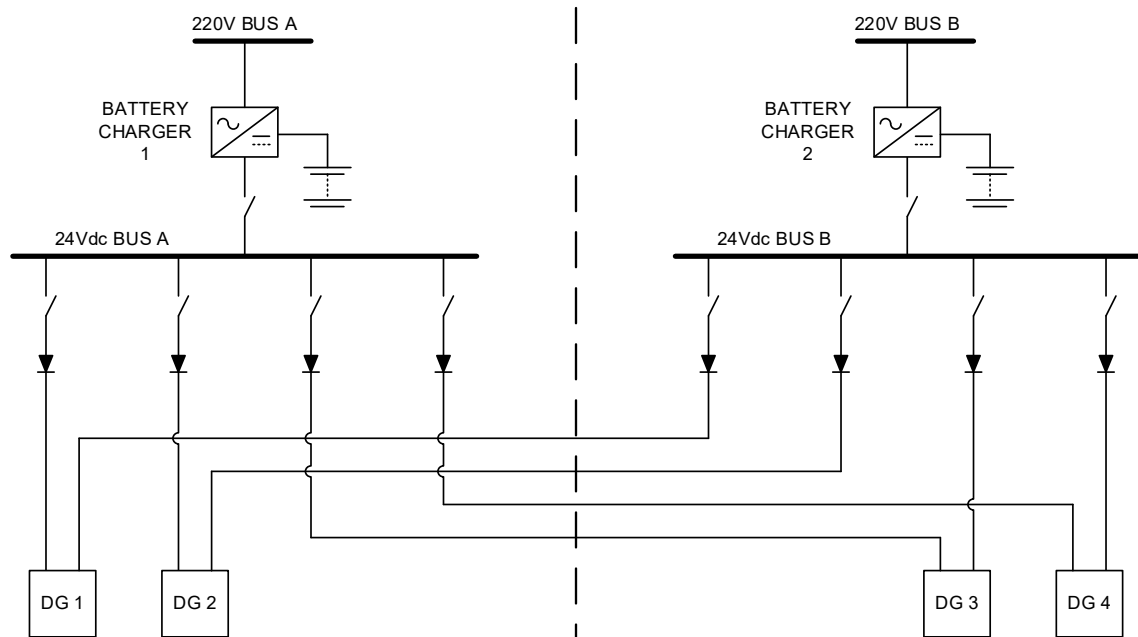
- A.2.9.6 In the example in Appendix A - Figure 13, the feeder circuit breaker will trip with no intentional delay. The consumers are 220V, and of relatively low power, thus, the cable and transformer impedance will limit the magnitude of the voltage dip and therefore the disturbance that could be transferred to the port power system is likely to be relatively small and consumers are likely to be able to ride through such a disturbance. This nature of the voltage dip can be predicted using standard power system modelling techniques. At 220V distribution level several circuit breakers would have to fail to trip before hidden failure of a protective device could defeat the redundancy concept.
- A.2.9.7 However, in some designs, the auto changeover is at 440V or 690V level and designed for much higher power consumers including thrusters. In these conditions the transient disturbance may be enough to cause malfunction in both redundant DP groups. High voltage changeovers exist at 6.6kV and 11kV for generators, thruster motors and other drives. These are able to create very significant disturbances. Designs for this type of changeover tend to have some intelligence to prevent fault transfer but this should not be assumed.



Appendix A - Figure 13 LV Distribution System - Backup Supplies from Other Redundant DP Group

A.2.10 CROSS-CONNECTIONS FOR RELIABILITY AND MAINTENANCE

- A.2.10.1 This TECHOP discusses all types of cross-connections but focuses on a particular subset that are often created with the intent of improving reliability or to allow functionality to be maintained after failure or during maintenance.
- A.2.10.2 Reliability is a highly desirable attribute in any system. Fault tolerant DP systems based on redundancy depend upon each redundant system being sufficiently reliable in its own right. Following a failure in one redundant group, the probability of experiencing a second failure in the surviving redundant group should be low enough to ensure there is ample time to suspend the DP operation in progress in a safe manner.
- A.2.10.3 DP systems are constructed from a wide variety of subsystems and equipment, all of which must function reliably to allow the DP vessel to conduct its industrial mission efficiently and effectively. Even if a DP vessel is fully fault tolerant it will not be able to conduct its industrial mission effectively if redundancy is lost frequently because the equipment is unreliable or the next failure may lead to a potential loss of position, In such cases, the vessel may be forced to suspend operations frequently to affect repairs and restore fault tolerance.
- A.2.10.4 There are several ways to improve overall mission reliability:
- Specify high quality components (Fault Resistant).
 - Operate equipment well within its design limits (over-engineered – low stress).
 - Provide non-critical redundancy over and above that required for single fault tolerance.
- A.2.10.5 Cross-connections can be created with the intention of minimising the impact of certain failures on main machinery. For example, many engine speed governors require a 24Vdc supply as shown in Appendix A - Figure 14. 24Vdc battery rectifier supplies may be considered to be less reliable than the diesel engine they support and therefore it seems appropriate to provide each governor with more than one supply. It is at this point that a cross-connection may be introduced by providing one of the two supplies from one redundant group and the second from a different redundant group. Typically, these two supplies would be coupled together at each governor by diodes. The intention being that all engines will continue to run if one control power supply fails. The DP vessel will no longer be fully fault tolerant after failure of one supply but the effect of a more probable failure (control power supply failure to no output) has been reduced in severity from loss of entire redundant group to loss of no generators this should allow the work in progress to be terminated more confidently than with the DP system in a severely degraded state.



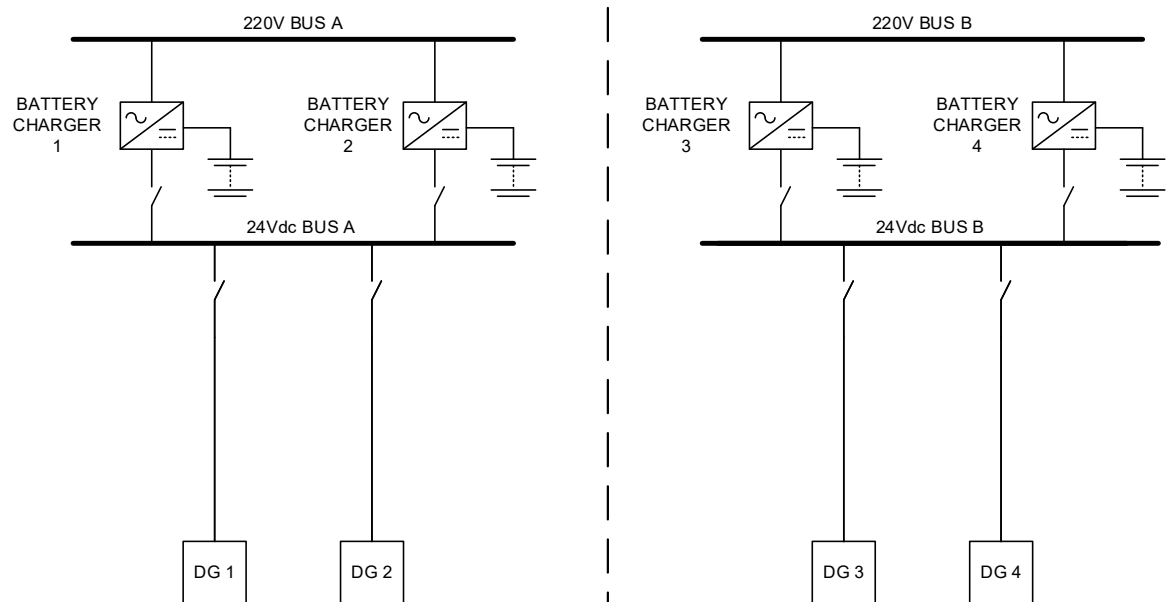
Appendix A - Figure 14 Dual Diode Connected Supplies to Engine Governors

- A.2.10.6 By limiting the number of high probability failures that can cause loss of multiple generators, the risk of being exposed to loss of position because surviving machinery is not capable of its nominal capacity is also reduced.
- A.2.10.7 Unfortunately, the cross-connection has introduced a path, by way of which, several failure modes may propagate to affect the operation of both redundant groups leading to blackout and loss of position with potentially catastrophic results for the vessel and its industrial mission.
- A.2.10.8 In this example, the faults that are capable of affecting both supplies, and therefore all engines, include:
- Over voltage of one of the two supplies destroying all the governors.
 - A short circuit fault in any one governor causing a voltage dip on both supplies which causes all governors to malfunction.
- A.2.10.9 The design with the cross-connections has also introduced several potential hidden failures that might result in all generators operating for an extended period from a single control supply. Blackout may follow the eventual failure of the surviving supply.
- A.2.10.10 Because the faults that could lead to blackout, (short circuit and overvoltage), are less probable than failure to no output, it can be demonstrated that the cross connected power supply is more reliable than the individual supplies, in terms of its ability to keep all the generators in operation. However:
- There will be no benefit in terms of the ability to carry out its industrial mission as work may still have to be suspended.
 - If one of these less probable propagating faults does occur the consequences are severe.
 - The cross connected design may not comply with the rules and/ or requirements of stakeholders and may be identified as such at an inconvenient time.

A.2.10.11 Even if time and effort was expended to engineer out the propagating faults using protective devices, it is possible to achieve the required level of reliability by other means that do not incur such severe penalties. As control power supplies are relatively inexpensive it may make economic sense to install an additional power supply within each redundant group. The cost may be offset by not fitting the cable providing the cross-connections.

A.2.10.12 In the alternative arrangement without cross-connections shown in Appendix A - Figure 15:

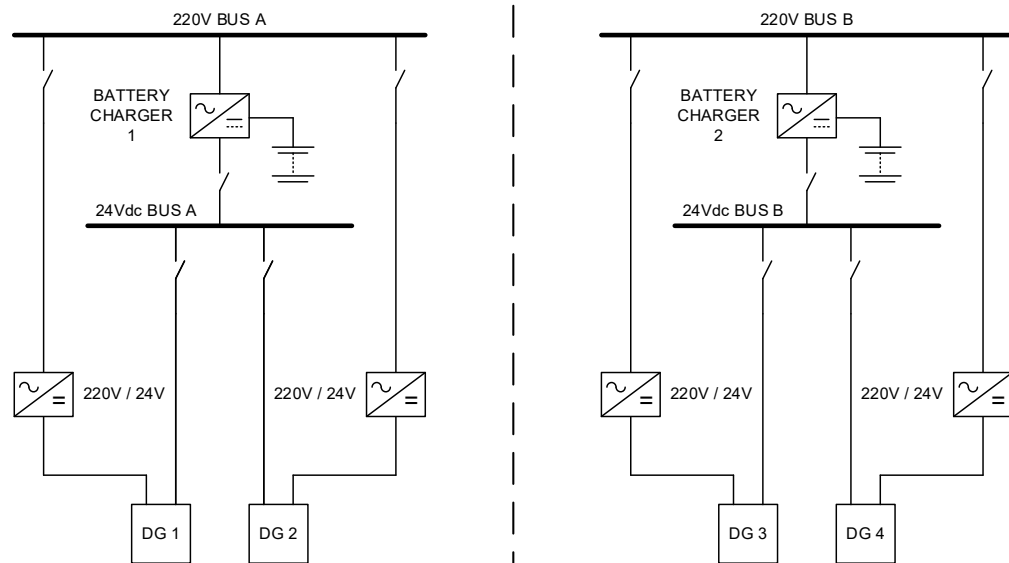
- High probability failure modes do not cause loss of any generators (unless a common battery bank is used - popular in some designs).
- Low probability failure modes would only cause loss of one redundant group and not blackout.
- Failure modes in one redundant group cannot propagate to the other.
- Loss of one of the four 24Vdc chargers by failure or for maintenance does not remove the vessel's fault tolerance and it can continue carrying out work.



Appendix A - Figure 15 Design with Additional Supplies and No Cross-connections

A.2.10.13 Having more 24Vdc battery chargers does increase the probability of experiencing a battery charger failure but this disadvantage is offset by the fact that the consequences are less severe, and the vessel should have higher availability for work (lower vessel non-productive time).

A.2.10.14 Some class rules for main class notations (not DP) require dual supplies or emergency backup supplies for propulsion and steering systems (some of these may originate from SOLAS requirements for non-redundant equipment). Where such requirements exist, it may be possible to seek exemption on the basis that DP redundancy is based on multiple power trains each capable of providing steering and propulsion duty. Where this is not possible, the risks associated with the fault propagation paths introduced by these cross-connections must be properly documented and mitigated.



Appendix A - Figure 16 Generator Controls with Dual Supplies

A.2.10.15 Variations on the supply arrangement are possible and Appendix A - Figure 16 shows a scheme that provides dual supplies to the generators controls without crossing the main redundant group boundaries but without the expense of eight separate supplies. It introduces some a commonality between the two generators in the same redundant group and therefore another possibility for losing two generators at the same time. This can cause a significant step load on the system which may be undesirable, but such design choices can be considered in the overall design philosophy and the risks mitigated by appropriate protection and detection.

A.3 TOOLS FOR EVALUATION

A.3.1 REDUNDANCY VERIFICATION TABLES

A.3.1.1 There are various means to identify and record cross-connections between redundant DP equipment groups. The tables and sketches in the examples which follow are intended to provide a graphical means to highlight any cross-connection in the control power supplies which could allow faults to propagate from one redundant group to another with the potential for effects of a severity exceeding that of the worst-case failure design intent for the DP system.

A.3.2 CONTROL POWER CONSUMERS AND SOURCES

A.3.2.1 The tables are filled, and colour coded as follows:

- Consumers such as generators, thruster and switchboards are entered into columns associated with the DP redundancy group to which they belong (e.g., DG1 & DG2 in the port redundancy group and DG3 & DG4 in the starboard redundancy group).
- The primary, secondary and tertiary (where fitted) sources of power are listed below each consumer (e.g., DG1 has a primary supply from DC1, a secondary supply from DC4 and tertiary supply from the Permanent Magnet Generator (PMG) of DG1 itself).
- Sources of power are colour coded according to their primary source of power thus DC1 is coded RED and DC4 is coded GREEN.
- A cross-connection is indicated by the presence of colour from one redundancy group in the column for another (e.g. – GREEN DC4 appears in the column for the port redundancy group).

Appendix A - Table 1 Control Power Consumer and Source

Control Power Consumers & Source				
Generators	DG1	DG2	DG3	DG4
Primary source	DC1	dc 1	DC4	DC4
Secondary source	DC4	DC4	DC1	dc 1
PMG or VT	PMG1	PMG2	PMG3	PMG4

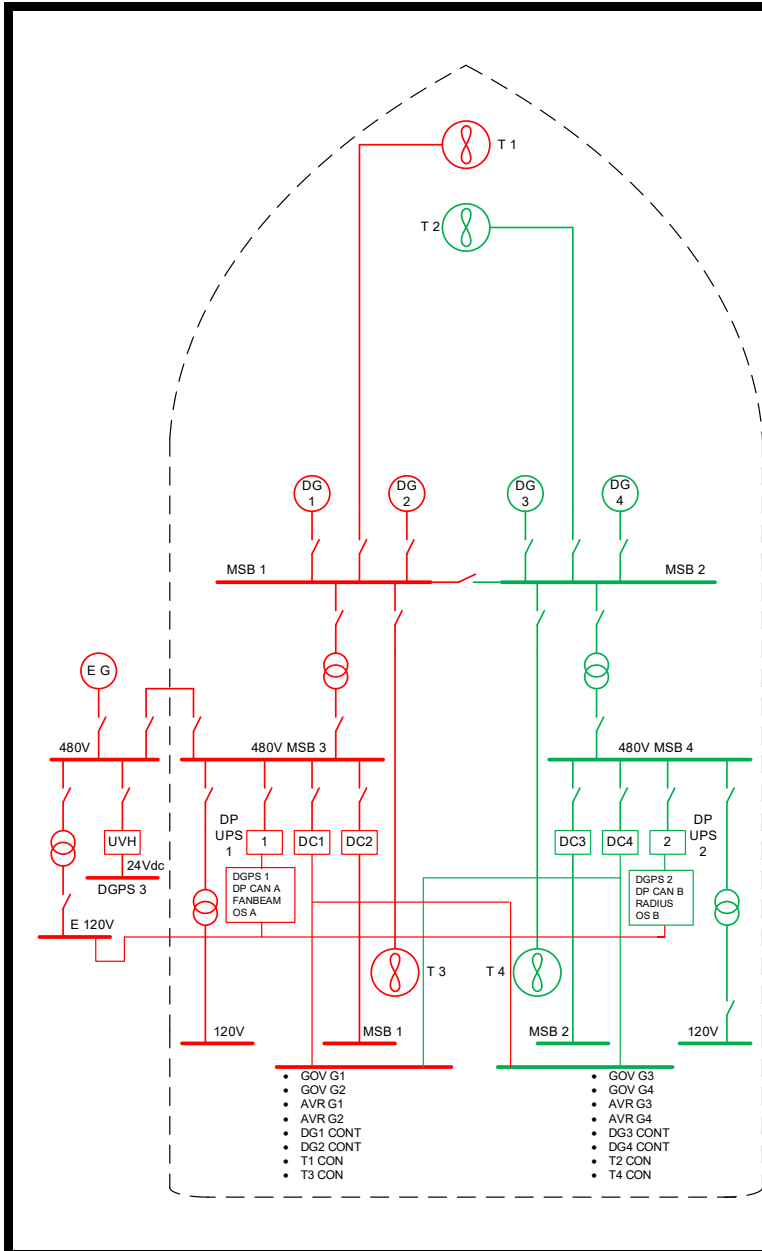
A.3.3 CONTROL POWER SOURCES AND THEIR SUPPLIES

A.3.3.1 Control power sources are treated in much the same way as consumers e.g. DP UPS 2 has a primary supply from MSB4 which is in the Starboard Redundancy group and a secondary supply from the emergency switchboard which is powered from the port redundancy group. This represents a cross-connection at DP UPS 2 shown by the presence of RED in the starboard redundancy group.

Appendix A - Table 2 DP UPS Arrangement

DP UPSs	DP UPS 1	DP UPS 2
Primary Source	MSB3	MSB4
Secondary Source	E SWBD 120V	

Appendix A - Table 3 Control Power ac & dc Distribution (Two-way Split) - Example

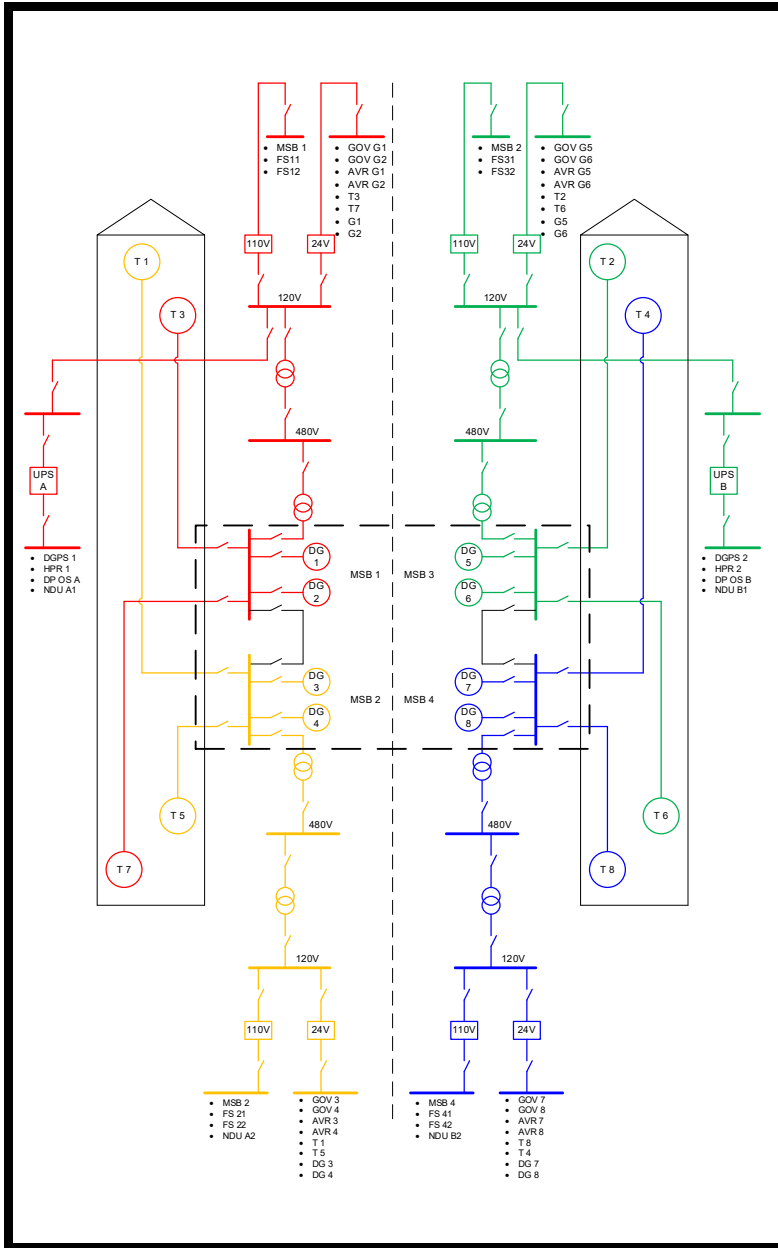


Control Power ac & dc Distribution (Two-way Split)

	Port Redundancy Group		Stbd Redundancy Group	
Control Power Consumers & Source				
Generators	DG1	DG2	DG3	DG4
Primary source	DC1	dc 1	DC4	DC4
Secondary source	DC4	DC4	DC1	dc 1
PMG or VT	PMG1	PMG2	PMG3	PMG4
Thrusters	T1	T3	T2	T4
Primary Source	DC1	DC1	DC4	DC4
Secondary Source	DC4	DC4	DC1	DC1
Main Switchboard	MSB1		MSB2	
Primary Source	DC2	DC2	DC3	DC3
Secondary Source	N/A	N/A	N/A	N/A
Aux Switchboards	MSB3	ESWB	MSB4	
Primary Source	N/A	N/A	N/A	N/A
Secondary Source	N/A	N/A	N/A	N/A

Supply to Control Power Source				
Battery Chargers	DC1	DC2	DC3	DC4
Primary Source	MSB3	MSB3	MSB4	MSB4
Secondary Source	N/A	N/A	N/A	N/A
DP UPSs	DP UPS 1		DP UPS 2	
Primary Source	MSB3		MSB4	
Secondary Source	ESWBD 120V			
VMS/PMS UPS	PMS1	VMS1	PMS2	VMS2
Primary Source	N/A	N/A	N/A	N/A
Secondary Source	N/A	N/A	N/A	N/A

Appendix A - Table 4 Control Power ac & dc Distribution (Four-way Split) - Example



Control Power ac & dc Distribution (Four-way Split)								
	Port FWD	Port AFT	Stbd FWD	Stbd AFT				
Control Power Consumers & Source								
Generators	DG1	DG2	DG3	DG4	DG5	DG6	DG7	DG8
Primary source	DC1	DC1	DC2	DC2	DC3	DC3	DC4	DC4
Secondary source	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
PMG or VT	No	No	No	No	No	No	No	No
Thrusters	T1	T2	T3	T4	T5	T6	T7	T8
Primary Source	DC1	DC1	DC2	DC2	DC3	DC3	DC4	DC4
Secondary Source	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Main Switchboard	MSB1		MSB2		MSB3		MSB4	
Primary Source	DC5	DC5	DG6	DC6	DC7	DC7	DC8	DC8
Secondary Source	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Aux Switchboards	ASB1	ASB5	ASB2	ASB6	ASB3	ASB7	ASB4	ASB8
Primary Source	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Secondary Source	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Supply to Control Power Source								
Battery Chargers	DC1	DC5	DC2	DC6	DC3	DC7	DC4	DC8
Primary Source	ASB5	ASB5	ASB6	ASB6	ASB7	ASB7	ASB8	ASB8
Secondary Source	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
DP UPSs	UPS A				UPS B			
Primary Source	ASB 5				ASB 7			
Secondary Source	N/A				N/A			
VMS/PMS UPS	UPS1		UPS2		UPS3		UPS4	
Primary Source	ASB1	ASB2	ASB3	ASB4	ASB5	ASB6	ASB7	ASB8
Secondary Source	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

A.3.4 INFORMATION RECORD FOR VESSEL

A.3.4.1 Three blank forms have been provided to suit DP redundancy concepts with:

- Two-way split
- Three-way split
- Four-way split

A.3.4.2 It may be necessary to adapt these forms to suit a particular redundancy concept.

Appendix A - Table 5 Control Power ac & dc Distribution (Two-way Split)

Control Power ac & dc Distribution (Two-way Split)					
		Port	Stbd		
Control Power Consumers & Source					
Generators					
Primary source					
Secondary source					
PMG or VT					
Thrusters					
Primary Source					
Secondary Source					
Main Switchboard					
Primary Source					
Secondary Source					
Aux Switchboards					
Primary Source					
Secondary Source					
Supply to Control Power Source					
Battery Chargers					
Primary Source					
Secondary Source					
DP UPSs					
Primary Source					
Secondary Source					
VMS/PMS UPS					
Primary Source					
Secondary Source					

Appendix A - Table 6 Control Power ac & dc Distribution (Three-way Split)

Control Power ac & dc Distribution (Three-way Split)						
	Port	Centre	Starboard			
Control Power Consumers & Source						
Generators						
Primary source						
Secondary source						
PMG or VT						
Thrusters						
Primary Source						
Secondary Source						
Main Switchboard						
Primary Source						
Secondary Source						
Aux Switchboards						
Primary Source						
Secondary Source						
Supply to Control Power Source						
Battery Chargers						
Primary Source						
Secondary Source						
DP UPSs						
Primary Source						
Secondary Source						
VMS/PMS UPS						
Primary Source						
Secondary Source						

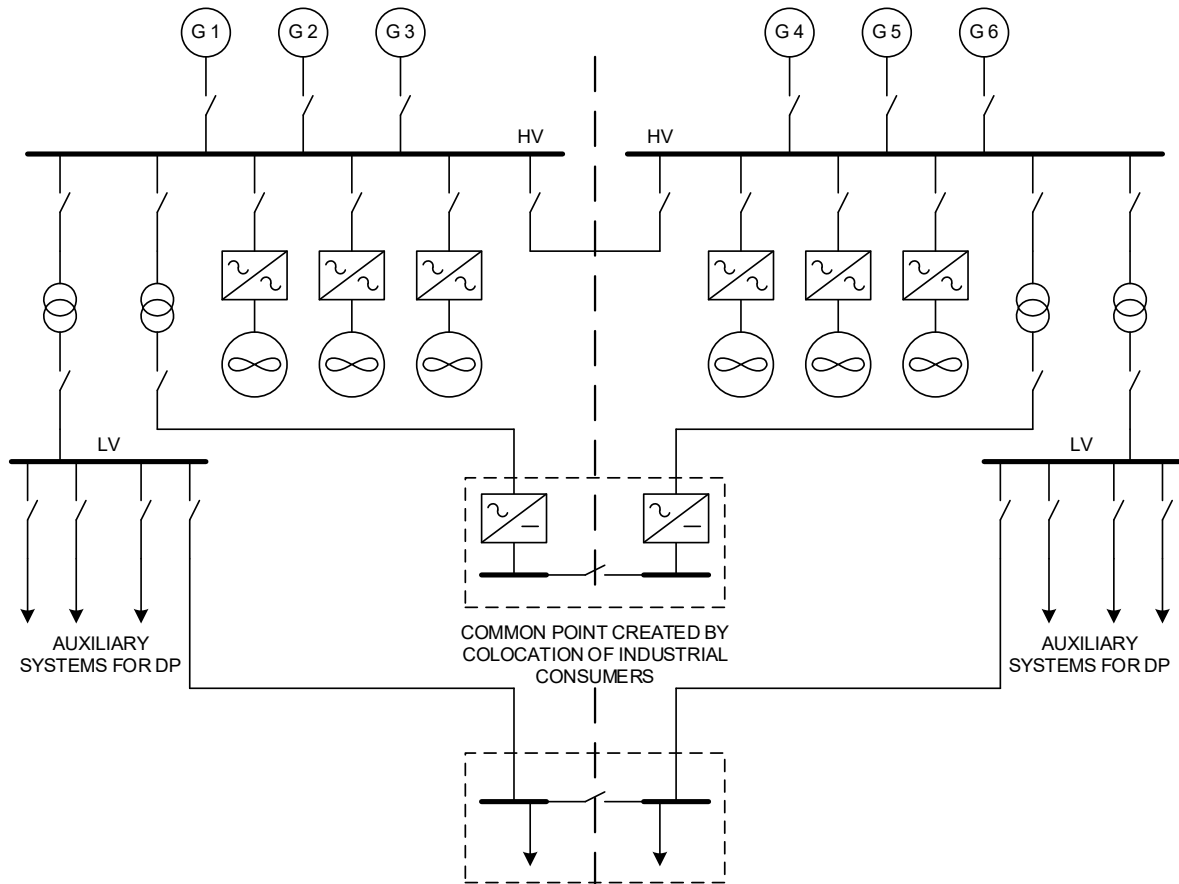
Appendix A - Table 7 Control Power ac & dc Distribution (Four-way Split)

Control Power ac & dc Distribution (Four-way Split)									
		Port	Port	Stbd	Stbd				
Control Power Consumers & Source									
Generators									
Primary source									
Secondary source									
PMG or VT									
Thrusters									
Primary Source									
Secondary Source									
Main Switchboard									
Primary Source									
Secondary Source									
Aux Switchboards									
Primary Source									
Secondary Source									
Supply to Control Power Source									
Battery Chargers									
Primary Source									
Secondary Source									
DP UPSs									
Primary Source									
Secondary Source									
VMS/PMS UPS									
Primary Source									
Secondary Source									

A.4 CLOSED BUSTIES

A.4.1 DIESEL ELECTRIC POWER PLANT

- A.4.1.1 Appendix A - Figure 17 shows a typical diesel electric DP power plant. Operating the power plant of a DP vessel as a single power system provides flexibility that can be exploited to good advantage when it is appropriate to do so.
- A.4.1.2 The tie-line represents a very significant common point and fault propagation path it is necessary to provide a comprehensive range of protective functions to prevent faults affecting more than one redundant DP equipment group.
- A.4.1.3 Protective functions are not usually sufficient on their own to create a fault tolerant design because by the time the protective function has identified the fault and opened the circuit breaker or bustie circuit breaker to isolate it, more than one redundant group will have experienced a significant disturbance. Thus, in addition to protection, all DP related equipment exposed to failure effects must have sufficient fault ride-through capability to maintain or resume operation once the fault has been removed. Fault ride through capability is a performance criterion that can be specified in the design and proven by testing.



Appendix A - Figure 17 Typical Diesel Electric DP Power Plant

- A.4.1.4 The following failure effects may propagate by way of a three-phase tie-line between redundant parts of a three-phase ac power system. Effects may occur singly or in combination.
- Phase to phase voltage dip associated with short circuit fault (in the tie line or in either power system).
 - Phase to ground voltage dip or rise associated with an earth fault (in the tie line or in either power system).
 - Over current associated with short circuit, overload or synchronisation failure conditions (crash sync, connection of stopped generator).
 - Line current imbalance caused by single phasing or broken conductor somewhere in the distribution system.
 - Severe harmonic distortion caused by failure of power electronic devices or harmonic cancellation facilities.
 - Severe active power import or export associated with load sharing failures.
 - Severe reactive power import or export associated with reactive power sharing failures.
 - Over frequency associated with speed control failures or severe load rejection.
 - Under frequency associated with overload condition, poor load acceptance or fuel / combustion air starvation.
 - Over voltage associated with voltage control systems failure or AVR overshoot following fault clearance.
 - Under voltage associated with severe overload condition.
 - Heat may be conducted through copper cables.
- A.4.1.5 Depending upon the sophistication of the protection system it may be possible to isolate the faulty generator or power consumer responsible for creating the failure effect. If this is possible it can prevent complete loss of one redundant group which may occur if the only protection action is to open the busties. Note that some DP notations require that there are two independent protection functions to deal with every potential failure. Thus, if one protection system is faulty or fails to clear the fault the other should operate.
- A.4.1.6 Phase to phase voltage dip associated with short circuit fault (tie line or either power systems): This type of fault is cleared by the overcurrent protection scheme either at a generator, in a power consumer or by the bus-bar protection. This type of protection is relatively reliable but depends on the generators to be able to deliver large amounts of fault current in order to operate the overcurrent protection scheme selectively. Thus, the generators must have an excitation system capable of maintaining excitation during periods of low bus voltage. Permanent magnet exciters, compounding CTs and auxiliary windings are methods used to provide this excitation support facility. Overcurrent protection may be based on time grading, differential or directional protection methods.
- A.4.1.7 Fault ride-through capability must be provided in:
- Control systems
 - Variable speed drives
 - Motor starters.

NOTE 1: *large asynchronous motors must be re-accelerated after the fault is cleared and this may result in another overcurrent condition.*

NOTE 2: *It is important to recognise that fault ride-through capability should be identified as a critical equipment design requirement and must be specified in all relevant equipment. Failure to emphasise the need for this attribute could result in sub-optimal performance and failure to meet expectations.*

- A.4.1.8 Greatest confidence in the ability of the power plant to survive this type of fault is provided by exploring the limiting conditions and power plant configurations using a mathematical model validated by testing to supplement the usual short circuit calculation required by class. Such modelling work is already a class requirement for some DP notations. Such modelling work followed by verification testing should be leveraged to build confidence in fault ride through capability even if it is not a class requirement.
- A.4.1.9 Phase to ground voltage dip or rise associated with an earth fault (tie line or either power systems): On HV power distribution systems which are not earth referenced or referenced by way of neutral earthing resistors the line to earth voltage may increase significantly during an earth fault. This effect should be considered in the rating of the HV cables used in the distribution system. In large power distribution schemes, the earth fault current may be large enough to require automatic isolation of earth faults. Time grading is typically used for earth fault protection but can be incorporated into directional and differential overcurrent schemes if they are sufficiently sensitive to detect the earth fault currents which can be of the order of a few tens of amps. Core balance current transformers are used to detect the presence of earth fault currents but deviation of the neutral point from zero voltage is an alternative method. Modelling of earth fault conditions should form part of the work used to prove fault ride through described above.
- A.4.1.10 Over current associated with short circuit, overload or synchronisation failure conditions: The voltage dips discussed above are created by large fault currents causing a voltage drop across the generators' internal impedance. Overcurrent conditions large enough to operate the overload protection may also occur because the plant becomes overloaded either through uncontrolled application of load or sudden loss of generating capacity. The power management system and thruster drives are usually programmed to relieve any overload by phase-back based on monitoring the power consumed and/or bus frequency. Low bus frequency is a more secure indicator of power plant malfunction as it does not depend on assumed figures for generator capacity. Generators which are starved of fuel or combustion air will act as though overloaded but will never reach their rated power and so never trigger load shedding measures based solely on available power. Large current fluctuations can also occur when a synchronous generator is pulled out of synchronism by a severe mechanical fault or when a generator is connected to the power system without proper synchronisation. Mathematical modelling is currently one of the few ways to have confidence the power plant can survive such a shock. Mechanical damage to the generator / engine couplings and end windings is off concern during such events.
- A.4.1.11 Line current imbalance caused by single phasing or broken conductor somewhere in the distribution system: Three phase synchronous generators have limitations on the amount of current imbalance they can tolerate between each of their three phases. Even a relatively small imbalance can give rise to overheating. Certain types of distribution faults can give rise to unbalanced line currents. Power system providers often fit current imbalance protection to the generators. It is important to ensure that this is made selective with the source of the imbalance otherwise multiple generators may trip.

- A.4.1.12 Severe harmonic distortion caused by failure of power electronic devices or harmonic cancellation facilities: Large non-linear power electronic drives create undesirable harmonic distortion of voltage and current waveforms. These distortions have the potential to cause malfunction and overheating of various systems. Various measures are employed to control their levels including filters, phase shifting transformers and drives with active rectifiers. Failure of these measures can result in high levels of harmonic distortion affecting more than one redundant DP equipment group by way of the closed busties. Harmonic distortion studies are required by class to prove levels remain within acceptable limits when the plant is intact but similar studies including a scan for resonance points should also be carried out for failure scenarios and failure of harmonic cancelation features in particular.
- A.4.1.13 Severe active power import or export associated with load sharing failures: Diesel electric power plants based on synchronous generators are designed in such a way that each generator carries an equal share of the total system load. Some form of load sharing system is required which may include operating the generators in speed droop or isochronous load sharing lines or compensated speed droop performed by using the power management system to adjust the governor speed set points. When any of these systems fail it may result in a severe load sharing imbalance. This may prevent the full power of the plant being available to the DP control system. At worst it may result in multiple generators tripping and loss of position. Protection functions are required to isolate redundant power systems or otherwise isolate the source of the imbalance before this occurs.
- A.4.1.14 Severe reactive power import or export associated with reactive power sharing failures: Reactive power must be shared between generators in a similar way to active power. The automatic voltage regulator in each generator is responsible for controlling terminal voltage and reactive power sharing. Load sharing lines and external trimming by power management systems are possible but less popular than for speed control and load sharing. When any of these measures fails it may result in a severe reactive sharing imbalance. This may prevent the full power of the plant being available to the DP control system. At worst it may result in multiple generators tripping and loss of position. Protection functions are required to isolate redundant power system or otherwise isolate the source of the imbalance before this occurs.
- A.4.1.15 Over frequency associated with speed control failures or severe load rejection: in addition to a severe load sharing imbalance a speed control failure on a generator may drive the common bus frequency up so far that multiple generators trip on over frequency or over speed. As over speed and over frequency protection is not selective and may trip healthy generators first it is essential that some other form of identifying the source of the fault is provided. Advanced protection systems for generators are available from various vendors to provide this function. Over frequency may also result from a severe load rejection (loss of load) this might happen because a large industrial consumer or a number of thrusters trip at high load due to a single fault. The design of the power plant must ensure that generators can survive the maximum load rejection. As the bus frequency rises, all the asynchronous motors driving fans, pumps and compressors will attempt to accelerate to the new bus frequency. This causes an increase in power consumption which may have a damping effect. Such phenomena are best modelled and tested to ensure plant stability.

- A.4.1.16 Under frequency associated with overload condition, poor load acceptance or fuel / combustion air starvation: A severe overload will cause the bus frequency to fall. Variable speed drives used for thrusters and industrial drives are typically configured with an internal load shedding function designed to shed load on detection of falling bus frequency. Other protection systems may be programmed to divide the power plant to isolate the source of the overload to one side or the other. Shedding industrial load is a legitimate way of making power available for thrust but shedding thrust load leads to a loss of position unless that load is used for thruster bias. The relatively poor load acceptance of modern engines complying with the latest emissions requirements means that carrying a spinning reserve is no guarantee that the plant can survive the effect of multiple generators tripping because of a common fault. This poor step load performance issue makes effective, fast frequency-based load shedding systems even more necessary.
- A.4.1.17 Over voltage associated with voltage control systems failure or AVR overshoot following fault clearance: Severe AVR failure to full excitation can occur for a number of reasons including failure of the voltage sensing line from the generator VT. In addition to the reactive power export condition thus created, there is a possibility that the bus voltage may be driven to levels at which the overvoltage protection may operate tripping multiple generators. Generator overvoltage is not selective, but time grading can be used on the bustie circuit breaker protection to divide the plant and isolate the source of the overvoltage to one redundant group or the other. During the time when a short circuit fault exists, the AVRs will be providing maximum excitation to operate the overcurrent protection and isolate the fault. Once the fault has cleared, all connected service transformers will simultaneously re-energise and this may result in a voltage overshoot. The design of the power plant should be such that it can ride through such failure effects.
- A.4.1.18 Under voltage associated with severe overload condition: AVRs are only capable of regulating voltage independently of frequency over a limited range and are programmed to maintain a constant flux in the machine. Therefore, they will ramp down the voltage on falling frequency. Ultimately, the control range will be exceeded and the voltage drop over the generators internal impedance will dominate leading to brown out and blackout when the generators trip.

APPENDIX B COMMONALITY

FIGURES

Appendix B - Figure 1	Typical Diesel Electric DP Power	2
Appendix B - Figure 2	Auto Changeover	3
Appendix B - Figure 3	Thruster with Dual Supplies	6
Appendix B - Figure 4	Dual Fed Consumer	7
Appendix B - Figure 5	Isolation of Load Sharing Lines	9
Appendix B - Figure 6	Cross-connections Spanning the A60 WT Divide	10
Appendix B - Figure 7	Cross-connections Spanning the Redundancy Groups	11
Appendix B - Figure 8	Control Power Crossing Boundaries	12
Appendix B - Figure 9	Effects of Fire on Supplies from Bus VTs	13
Appendix B - Figure 10	Main Bustie Controls and Interlocks	14
Appendix B - Figure 11	Un-Earthed and Earth-Referenced dc Power Supplies	16
Appendix B - Figure 12	Multiple Earth Faults Create Unpredictable Behaviour	17
Appendix B - Figure 13	Effects Exceeding WCFDI	18
Appendix B - Figure 14	Division of Remote-Controlled Valve Systems	21
Appendix B - Figure 15	Typical Vessel Management System Network	23

B.1 ADDRESSING COMMONALITY

B.1.1 GENERAL

B.1.1.1 The term ‘commonality’ is a general one, but in this context, it is used to describe elements of the DP system that are common to more than one (or all) redundant equipment groups. It has some similarity with cross-connections, but that term is reserved for discussion of control power or other services where there is an intention to provide an alternative or backup supply from a different redundancy group. Typical examples of commonality include:

- Consumers associated with more than one redundancy group – Typically thrusters.
- Networks connecting redundant equipment groups.
- Co-location – fire and flooding.
- Auto changeovers – between redundancy groups.
- Common marine auxiliary systems.
- The steel hull of the DP vessel - effects of ground faults.

B.1.2 NEW BUILDS AND VESSELS IN OPERATION

B.1.2.1 Vulnerabilities in DP operations can typically be addressed by considering their impact on:

- Design
- Operations
- People

B.1.2.2 Barriers to the consequences of the associated the risk may be developed within each of these spaces.

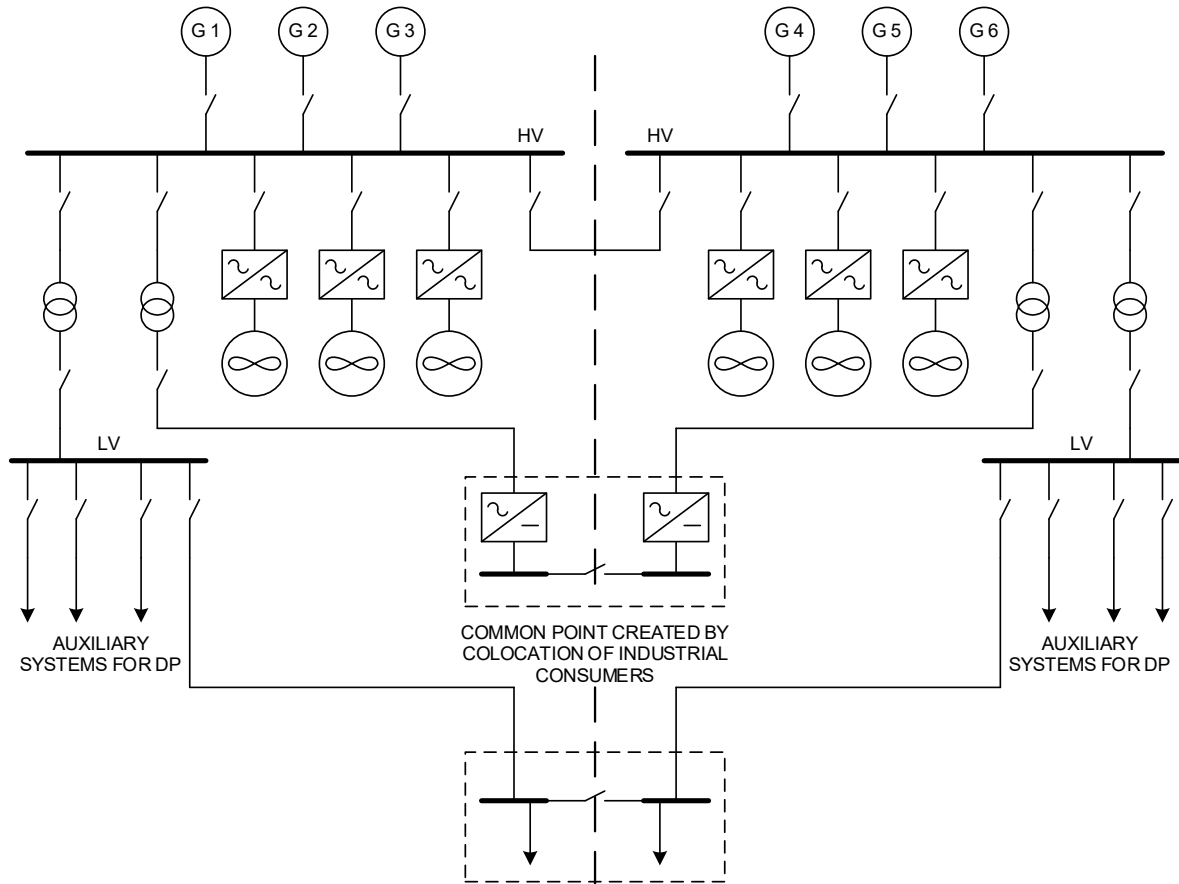
B.1.2.3 **Design:** From a practical perspective the approach taken would vary for new buildings and vessels in operation. In the case of a new building there is greater opportunity to influence the design and remove cross-connections and replace them with non-critical redundancy which is an effective way to reduce exposure to non-productive time.

B.1.2.4 **Operations and People:** In the case of vessels in service, there may be more limited opportunities to effect design changes and even where such are contemplated it may not be economically viable to carry these out until the next opportunity which could be a scheduled dry-docking or periodic survey. In this case, the approach may focus on mitigation of the risks through procedures and improved training and awareness. Validated post failure capability should always be used to establish criteria to carry out operations identified as CAM. Such post failure capability may be impacted by isolation of cross-connections.

B.1.2.5 Fault propagation paths can also be created by the colocation of equipment supplied from redundant power distribution systems. In DP Class 3 designs, these connections are made by considering the effects of fire and flooding in a common compartment.

B.1.2.6 Colocation or proximity can also create inadvertent coupling. Antenna locations may conflict causing ‘bleed-over’ in transmissions and other forms of interference. Unforeseen failure effects include receiving equipment failing to the transmit condition and blocking out reception in redundant antennas nearby,

B.1.2.7 Appendix B - Figure 1 also shows how colocation of non-DP related consumers can create a cross-connection between power distribution systems when the effects of fire and flooding are considered. Fault current contribution from the LV power system to an HV fault may assist the ride through of LV consumers but the same may not be true when the fault occurs in a common space containing LV consumers from different redundant groups.



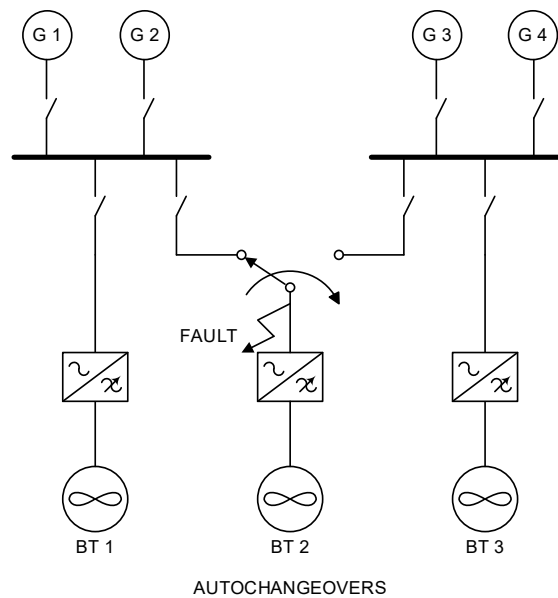
Appendix B - Figure 1 Typical Diesel Electric DP Power

B.1.3 AUTO CHANGEOVERS – BETWEEN REDUNDANT GROUPS

B.1.3.1 Equipment intended to provide redundancy should be available immediately and with a minimum of operator intervention. This requirement was established in IMO MSC645. There is wide variation in the interpretation of this requirement by the different classification societies and it even varies from one DP notation to another within the same classification society. The highest integrity is achieved by basing redundancy on running machinery as this reduces exposure to hidden failures associated with standby redundancy. Note that although it reduces the risk of hidden failures it does not remove them entirely because lack of capacity or other performance attributes in running machinery can also remain hidden until called upon to take up the load of the faulty system. Thus, it is essential to augment redundant systems with adequate alarms, monitoring and periodic testing to further reduce this risk.

B.1.3.2 Automatic changeovers like the one shown in Appendix B - Figure 2 may be used to provide an alternate source of ac power to equipment at various voltage levels. Typical applications include:

- Backup supplies to UPSs and battery chargers (often from the emergency switchboard).
- Backup supplies to thrusters and engine control systems.
- Provision of dual main power supplies to transferable thrusters.
- Transferable generators which can connect to more than one redundant equipment group.



Appendix B - Figure 2 Auto Changeover

- B.1.3.3 The risks associated with using auto changeovers as part of a DP redundancy concept relate to the following:
- The potential for hidden failure.
 - The potential for fault transfer.
 - The changeover creates a common point.
 - Transient position excursions.
- B.1.3.4 **The potential for hidden failure:** The auto changeover may not operate when required and thus the expected post failure capability will not be available when required. Alarms which monitor both supplies can help reduce the risk, as can periodic testing.
- B.1.3.5 **The potential for fault transfer:** Several scenarios must be considered. A fault downstream of the auto changeover may cause the upstream overcurrent protection to operate. This may in turn cause a significant voltage dip on the distribution system supplying the fault. If the nature of the auto changeover is such that it is designed to operate on loss of one supply, then it will make no difference whether this occurred because of a fault upstream or downstream of the changeover. The changeover will operate and apply the fault to the other redundant group. The overcurrent protection will operate on that side but now the consumers in the other redundant group(s) have to ride through the voltage dip without malfunction. In many DP systems the voltage dip ride through of consumers is not tested or even proven by analysis. This is particularly true in design where the power plant is operated as two or more independent power systems (busties open). However, the use of an auto changeover of this type may introduce the need for this attribute to be analysed and tested.
- B.1.3.6 Providing the auto changeover with greater intelligence can help to reduce the risk. In particular, including the ability to determine the location of the fault and lock-out the changeover if the fault is downstream. Other options include disabling the changeover during operations in CAM and accepting a lower post failure DP capability and operating the vessel within it.

- B.1.3.7 **The changeover creates a common point:** Even if the auto changeover is of a more robust design and should not transfer a fault the fact that the presence of the auto changeover over brings power feeds from redundant groups into close proximity creates a risk. In HV designs there may be the potential for flashover. In DP equipment class 3 designs the effects of fire or flooding could create a fault path. This risk can be mitigated to some extent by arranging the changeover function to take place at the source and not at the common point. Such designs can make use of the vessel management systems to carry out the monitoring and switching operation. In such designs only one feed to the common point is ever live at one time. Concerns relating to the potential for hidden failures and the need for intelligence in the design remain valid.
- B.1.3.8 **Transient position excursions:** A particular case is the design of vessels with a single stern tunnel thruster which rely on reallocating thrust to push pull propellers / rudders in certain failure conditions or which depend upon the single stern thruster changing over to another source of power to provide sway forces at the stern of the vessel following failure of a redundancy group. Studies and experience confirm that there may be very significant position excursions while thrust is reallocated during transients.
- B.1.3.9 **DP Class 3 considerations:** Such designs are best avoided for DP class 3 as the cross-connections are permanently live, the effects of fire and flooding can create multiple faults. Protection coordination studies typically assume a single fault and selectively may depend on a defined fault current path from power source to fault. It is for this reason that multiple simultaneous or near-sequential faults may introduce unpredictability into the protection scheme response.
- B.1.3.10 **Emergency generator and auto changeover as a mitigation of flat batteries:** Emergency generators are required to connect within 45s. Although many would be capable of connecting in a shorter time, the practice on DP vessels is to hold off connection of the emergency generator to give the main power generation system an opportunity to restore power through the automatic blackout recovery system.
- B.1.3.11 **Using an auto changeover to provide emergency power to UPSs:** The ride through capability provided by UPS batteries is an essential part of many DP redundancy concept and blackout recovery systems. UPS batteries should be tested periodically to ensure they are capable of sustaining the load for at least 30 minutes. Predicting the lifetime of UPS batteries can be problematic as cells may go open circuit with little warning. Periodic testing and replacement within manufacturer's recommendations is generally accepted as mitigation.

B.1.4 AUTO CHANGEOVERS - MITIGATION OF FAILURE EFFECTS

- B.1.4.1 Potential fault propagation paths are more cost effectively eliminated at the basic design stage. Arrangements such as that shown in Appendix B - Figure 2 are common in vessel designs where three bow thrusters and their control systems must be powered from a redundancy concept with a two-way split. An alternative is to create a redundancy concept with a three-way split. It is generally too late and too costly to implement such a radical design revision once the contact for the vessel has been agreed.

B.1.4.2 The method of mitigating the risks associated with the original design depends on whether the auto changeover can be disabled without adversely affecting vessel performance or whether the changeover function must be retained.

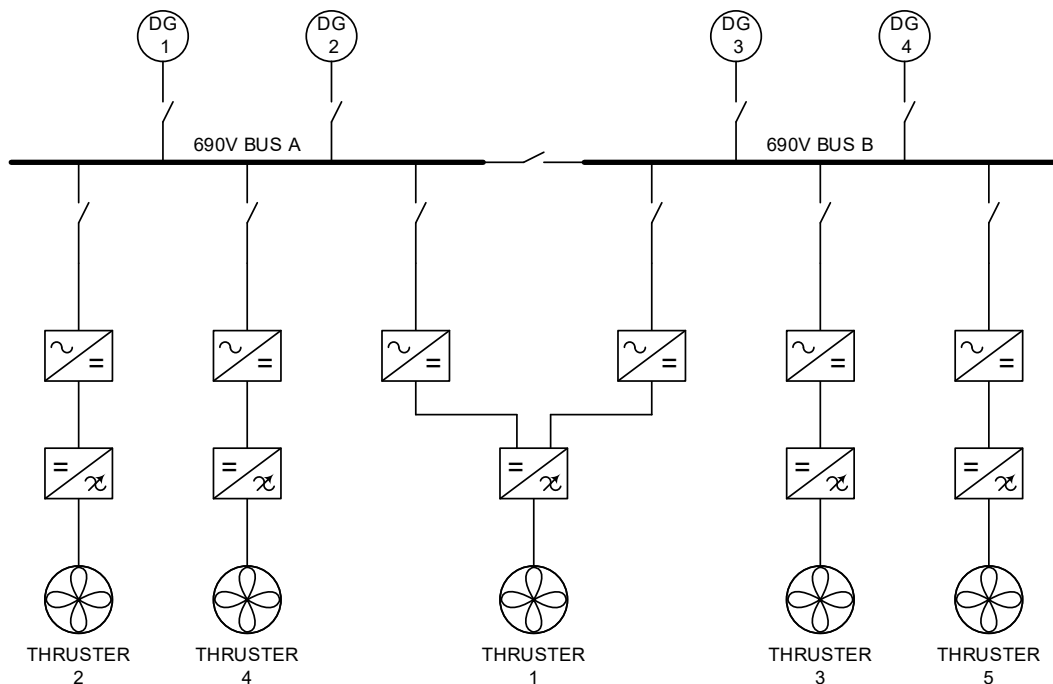
- **Disabling Transfer:** Disabling the auto changeover is generally a matter of pulling the control fuse on the backup supply (K2). In cases where there is limited time to prove fault tolerance this may be the preferred option but may require a reduction in the vessel's post failure DP capability. If the backup supply is only providing non-critical redundancy (e.g. alternative supply to a UPS) then disabling it may have no impact on post failure capability. An additional level of security is achieved by isolating the alternative power supply feeder at source which eliminates the possibility of a flashover in high voltage changeovers or multiple faults caused by the effects of fire and flooding in DP class 3 designs. Disabling the auto changeover for CAM and reinstating it for TAM may be a possible solution.
- **Preventing Fault Transfer:** If disabling the transfer is not an acceptable option then it becomes necessary to prove that it is not a potential single point failure. This process should have been part of the DP system FMEA but is often overlooked in superficial analyses.
 - **Interlock:** Adding interlocks to prevent the changeover operating if the transferable consumer is faulty.
 - **Ride Through capability:** Proving that the power system is sufficiently robust to ensure there is no malfunction of other consumers, while the faulty consumer is being cleared from the distribution. (This may form part of the overall fault ride through verification process for vessels that undergo short circuit and earth fault testing). It may be possible to arrange specific ride through testing for this circuit supported by appropriate mathematical modelling.
 - **Hidden failure:** It must always be accepted that an auto changeover may fail to operate on demand. It is for this reason that some DP notations do not accept changeover and standby equipment as contributing to post failure DP capability although they may be active. Confidence in the readiness of the changeover can be improved by monitoring the power supplies and the control supplies and initiating an alarm if any supply voltage is lost. Periodically testing the changeover provides additional confirmation of readiness.
- **Spurious operations:** Unexpected operations of the transfer mechanism should not lead to a critical situation provided it cannot occur if the changeover consumer is faulty. The power system to which the consumer is connecting must be capable of accepting the load.
- **DP class 3 issues:** In DP class 3 designs, a fire or flood in the space where the transferable consumer is located may apply faults to both power sources even without the changeover operating. This is because both feeds into that space are live at all times. This problem can be overcome by arranging the switching to occur at the supply end or at both supply and consumer ends of the feeders.

B.1.4.3 These hypothetical examples are intended to illustrate the mechanism by which earth faults which accumulate in floating power and control systems have the potential to create unpredictable failure effects. Much more insidious examples have occurred in switchboard and engine control panel wiring, causing all engines to stop on a vessel with four apparently independent insulated dc power systems.

B.1.5 DUAL FEEDS

B.1.5.1 **Dual fed thrusters:** These are now increasingly common in some hull forms. Where the supplies to a dual fed variable speed drive are taken from different redundancy groups the thruster effectively forms a common point even when the main busties are open. Typically, each switchboard feeds an ac to dc converter which in turn feeds a common dc link which supplies an inverter as shown in Appendix B - Figure 3. Some classification societies have rules on these arrangements but in general it is necessary to prove that failures at this common point cannot propagate back to affect the operations of both main switchboards and the consumers they supply. In some designs the fault will propagate back to both switchboards and thus it is necessary to prove that both power systems can ride through the effects. Fault ride through testing as described in TECHOP (D-07 - Rev1 - Jan21) 'A METHOD FOR PROVING THE FAULT RIDE-THROUGH CAPABILITY OF DP VESSELS WITH HV POWER PLANT' is one possible method of doing this. Some classification societies require this type of testing to be proven on DP class 3 vessels that have this thruster arrangement, including those that normally operate with their busties open. There is no technical reason to exclude DP class 2 vessels from the requirements to prove similar system by testing, but alternative verification methods may be accepted by class (not all regulatory bodies or stakeholders share this view).

B.1.5.2 In some designs there may be a defined phase shift between the two ac to dc supplies to the converters to create harmonic cancellation effects. It may be necessary for the DP redundancy concept to consider the impact of losing one of these supplies on the power output of the thruster and on the total harmonic distortion experienced by each power system. In some designs, the output of the thruster is affected by opening the busties due to load sharing issues between the line end converters. Any such restriction on thrust output should be reflected in the consequence analysers.



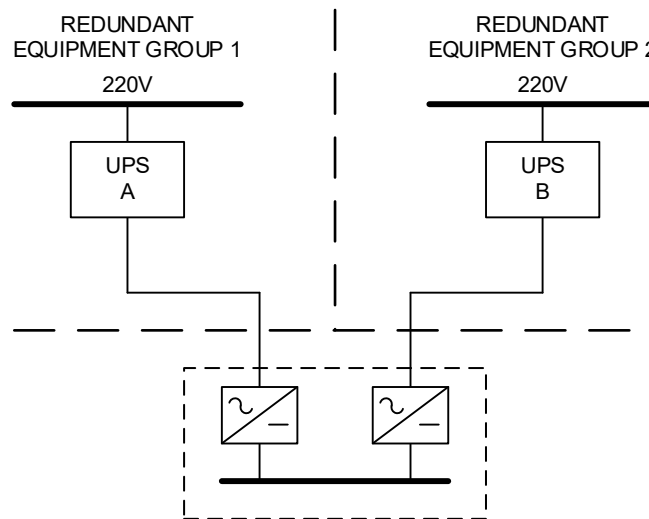
Appendix B - Figure 3 Thruster with Dual Supplies

B.1.6 DUAL AC SUPPLIES TO CONSUMERS WITH AC/DC POWER SUPPLIES

B.1.6.1 A popular method of providing dual UPS supplies to important consumers is to fit each consumer with dual ac to dc power supplies and tie the dc supplies together as shown in Appendix B - Figure 4 which could be a field station or operator's station in the vessel control system. Typically, the UPS operates at 110V or 220V and the internal circuits of the field station or operator station are supplied at 24Vdc. It is reasonable to want to improve the reliability of the field station by providing dual supplies, but care must be taken not to create a common point with failure effects that can cause malfunction in other parts of the vessel control system. This situation can arise if the second supply is taken from a UPS within a different redundant DP group. If the second supply is taken from the same redundant group, then fewer if any additional concerns are introduced. Thus, the issue of concern here is the potential effect of a failure at the dual fed consumer on the rest of the system, not the perceived improvement in consumer availability.

B.1.6.2 If the second UPS supply originates in another redundant group, introducing cross-connections, then certain attributes must be established including:

- A fault within the field station or operator station at the 24Vdc level must not be able to propagate back to affect the output of more than one UPS particularly if these UPSs supply other essential equipment in their own redundant groups that could malfunction.
- An overvoltage at either UPS may damage all of the dual fed consumers with effects exceeding the worst-case failure design intent. Therefore, it has to be demonstrated that such an external overvoltage cannot propagate into the interior of the field station to cause a malfunction.
- In the case of DP class 3 designs, the fault can be created externally to the field station directly on the UPS supplies by the effects of fire and flooding. This occurs when UPS outputs are taken across A60 / WT boundaries for various reasons. For example, dual supplies to PMS field stations.



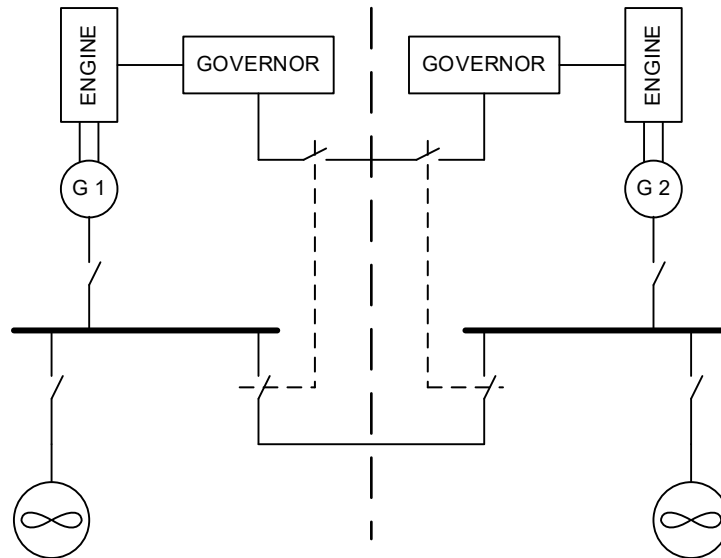
Appendix B - Figure 4 Dual Fed Consumer

- B.1.6.3 Fault ride though testing on relevant UPSs and other equipment should be considered essential in such designs. Engagement with multiple stakeholders may be necessary. Even when such tests are successful the risk is not entirely removed as some types of UPS use internal switching mechanisms to connect the output to the input to supply fault current to operate overcurrent protection. This represents a protective function which must be periodically tested to have confidence it will operate on demand.
- B.1.6.4 Note: Overvoltage or off-frequency from a UPS is not a high probability failure mode in most designs and some will have internal protection to shut them down if such conditions are detected. However, there is also a possibility that wiring faults allow input voltage to be coupled to the output and these may be very different voltage levels in some designs. So, there can be a credible risk that must be considered and eliminated. UPS consumers have a voltage rating. In some cases, this rating may have a very large range intended to allow connections to various supply standards. This may provide some degree of protection against over-voltage conditions.
- B.1.6.5 Fuses specially designed to protect electronic equipment have a better reputation for reliability and efficacy than miniature circuit breakers and may be able to interrupt the fault current so quickly that the voltage dip is well within the ride through capability of ac to dc power supplies. It may however be more difficult to arrange selectivity with such devices.
- B.1.6.6 Note: *The existence of 'Type Approval' for any piece of equipment may add confidence that the equipment meets certain standards in terms of suitability for the marine environment, but it does not necessarily guarantee 'fault tolerance' or 'fail safe' properties. Without knowing the extent of the analysis and testing that was carried out as part of the approval process it could be inappropriate to assume that all necessary failure modes have been considered.*

B.1.7 LOAD SHARING LINES

- B.1.7.1 Load sharing lines are used to connect the speed control systems of generators operating in parallel. It is one of several methods of load sharing which include:
- Speed droop (no connections between generators)
 - Pseudo isochronous (PMS trimming connects generators)
 - Isochronous (load sharing lines connects generators).
- B.1.7.2 Loads sharing lines are not generally fitted to improve reliability but as part of a control scheme designed to maintain constant frequency over the full load range. This method of load sharing provides a significant improvement in power plant stability compared to generators with traditional locomotive style electro-hydraulic governors operating in speed droop. Since the advent of digital governors, the relative merits and advantages are less clear and speed droop with fewer failure modes may offer perfectly satisfactory power plant response negating the need for load sharing lines or PMS trimming. Experience of at least one DP vessel owner who operates a large fleet of DP power plants in speed droop mode confirms there are no obvious disadvantages.
- B.1.7.3 Load sharing line failures continue to be responsible for DP incidents and attempts to improve reliability include:
- Adding a second (redundant) analogue or digital load sharing line.
 - Arranging for the governors to revert to speed droop on loss of communication.
 - Arranging to open the busties and load sharing lines on detection of a significant power sharing imbalance.

- B.1.7.4 In some designs, the action of opening the busties physically disconnects and terminates the analogue or digital load sharing line. In other designs the action of the opening the busties provides an input to a controller to indicate which groups of diesel engines are operating in parallel. Thus, the action of opening the busties may not remove all cross-connections in such designs and thus potential propagation paths for failure effects remain. Short circuits, earth faults, over voltages and noise, for example, may still be coupled across to affect the other redundant equipment group. In DP Class 3 designs it is necessary to isolate the load sharing lines on both sides of the A60 watertight divide. One possible way is shown in Appendix B - Figure 5.



Appendix B - Figure 5 Isolation of Load Sharing Lines

- B.1.7.5 It is vitally important that the failure modes and effects of load sharing be analysed and proven by testing. Analogue load sharing lines should as a minimum be subject to open circuit, short circuit and wire break testing. Digital load sharing lines may also be tested to determine their response to uncontrolled data transmission or 'jabber' on one node.
- B.1.7.6 Isochronous load sharing systems have a speed control loop for each generator (typically PID control) and a load balancing loop created by connecting the governors of all online generators together. In a working system the generators share equal load with a small deviation above or below average load depending on the relative error between speed set point and bus frequency. This is negligible in a working system. The effect of failing the load balance loop to a generator is that, in addition to not sharing the load information, it does not balance out the error between the speed set point and the actual bus frequency and the integral part of the speed controller integrates the error in an attempt to satisfy the set point. The effect is that faulty generator either trips on reverse power or imports load from all of the other online generators. In general, all generator governors need to be connected to each other for the load balance to work correctly and any break in communication causes groups to develop a power skew which may become severe. In more sophisticated systems the break is detected and the governors transfer to load sharing by droop mode or an alternative load sharing line.

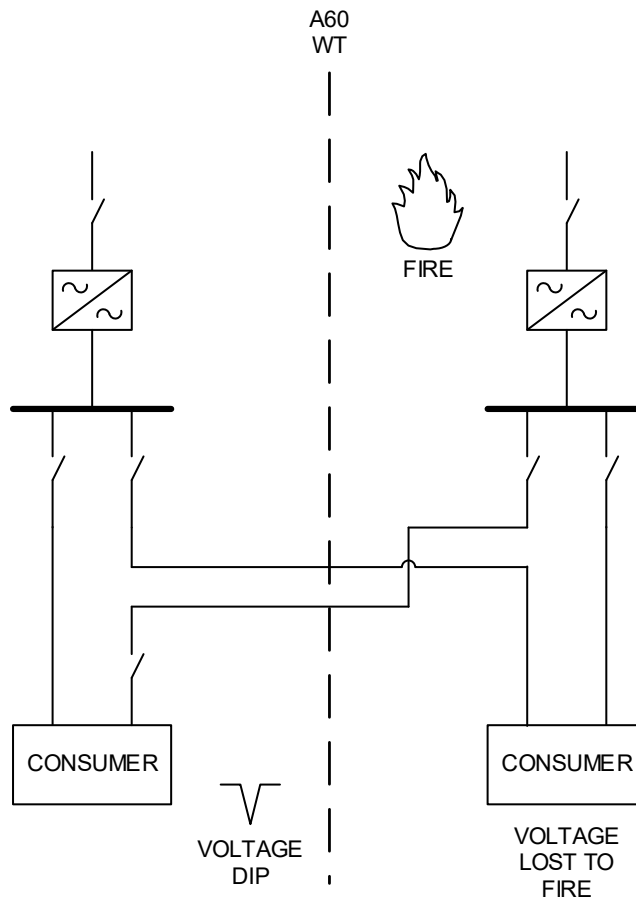
B.2 COMMONALITY IN DP CLASS 3 DESIGNS

B.2.1 BACKUP CONTROL STATIONS

B.2.1.1 There are particular issues related to the effects of fire and flooding. The backup DP system usually a simplex DP system in a location, sometimes with no view or a different view of the DP operation, with fewer communication facilities. The back-up DP system should only be required if there is a fire at the main DP station. Position control must be engaged in the event of fire which makes it vulnerable to hidden failure of the transfer mechanism. The design should ensure the main DP system is not entirely dependent on UPS power after a fire which disables the main DP control station. The transfer mechanism and any shared signals sources must not propagate faults in either direction between main and backup DP control stations.

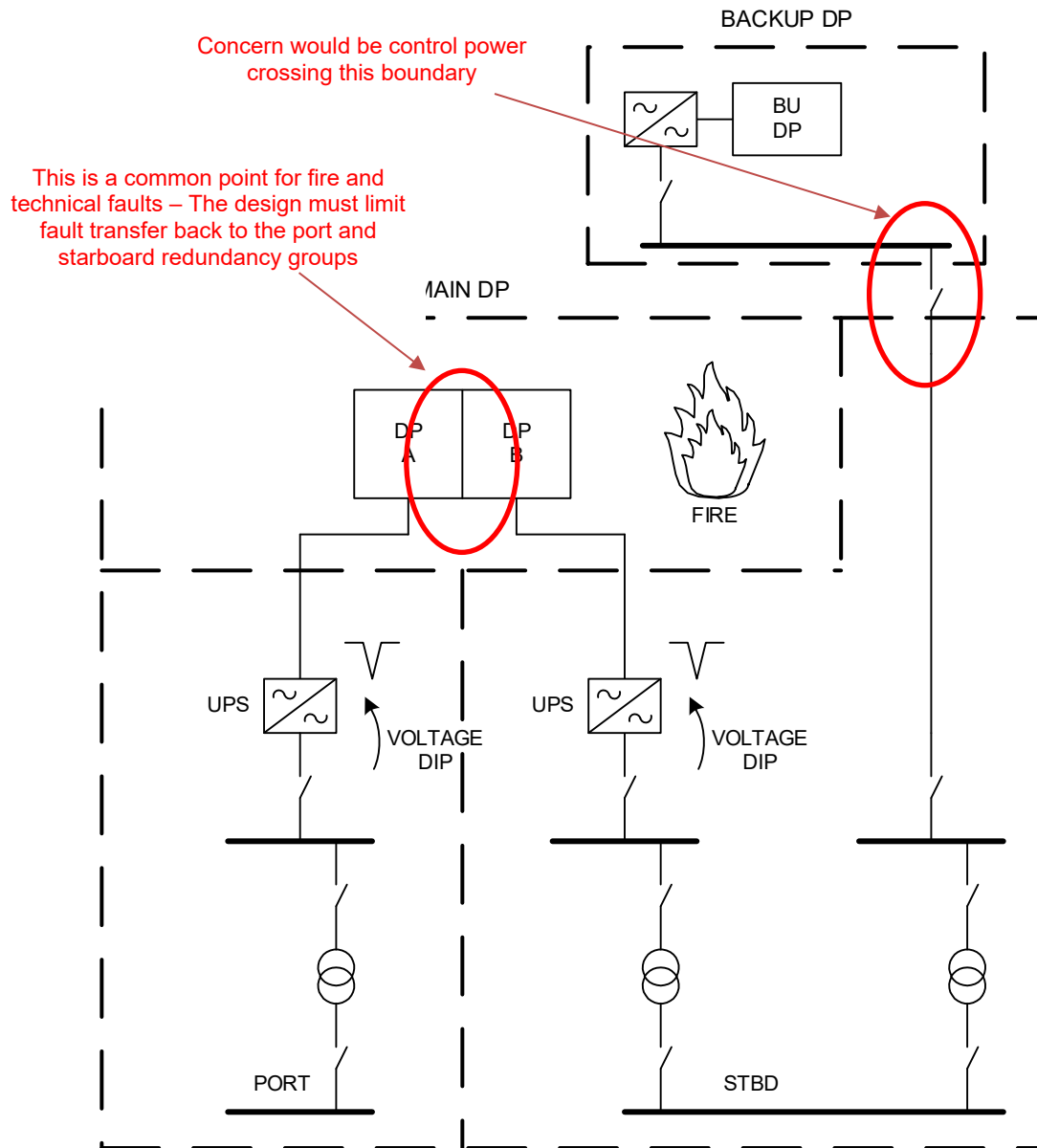
B.2.2 FIRE PROTECTION AND WATERTIGHT BOUNDARIES

B.2.2.1 Control power lines which cross the A60 and watertight boundaries between redundant DP class 3 equipment groups are vulnerable to the effects of faults created by fire and flooding. Fire and flooding are capable of causing multiple sequential and simultaneous faults which may defeat protection coordination schemes designed to isolate a single fault. Such faults may also extend voltage dips beyond the time associated with the clearance of a single fault. As such it may be prudent to avoid designs that require control power to cross A60 / WT boundaries as shown in Appendix B - Figure 6 .



Appendix B - Figure 6 Cross-connections Spanning the A60 WT Divide

- B.2.2.2 Some commonality is difficult to avoid. Appendix B - Figure 7 shows the control power supplies crossing an A60 boundary but although a fire at the main DP control station could cause short circuit on both UPSs it should only affect equipment for the main DP control station. The UPSs and the 440V / 220V transformers should limit any transients being coupled back to the port and starboard power systems and even if it did it should not affect the operations of the back-up DP control systems which is on a dedicated UPS.

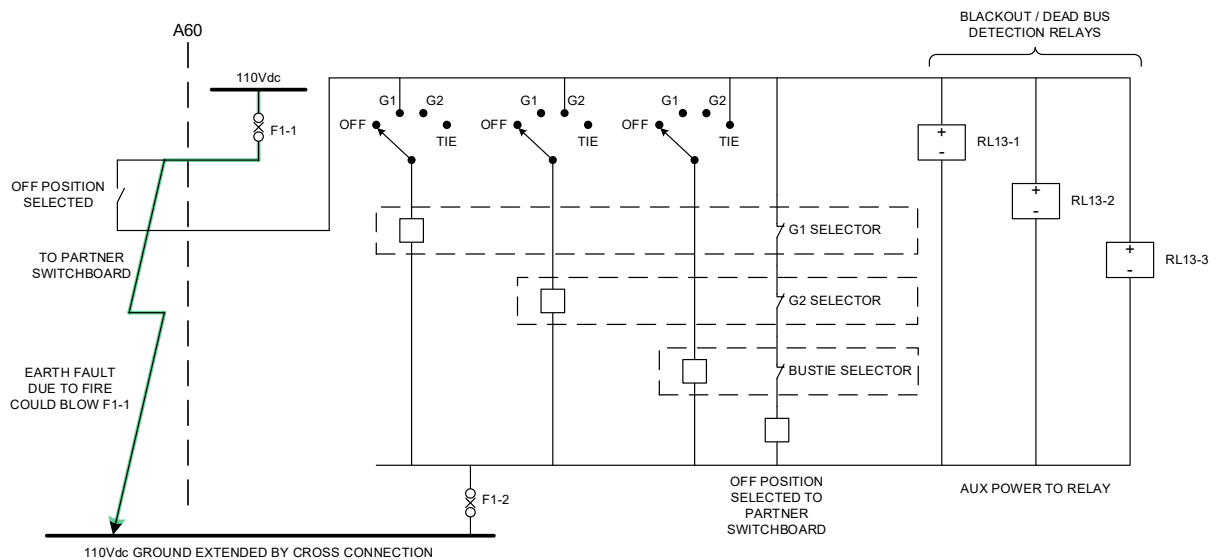


Appendix B - Figure 7 Cross-connections Spanning the Redundancy Groups

B.2.3 SWITCHBOARD CONTROL POWER AND SYNCHRONISING LINES

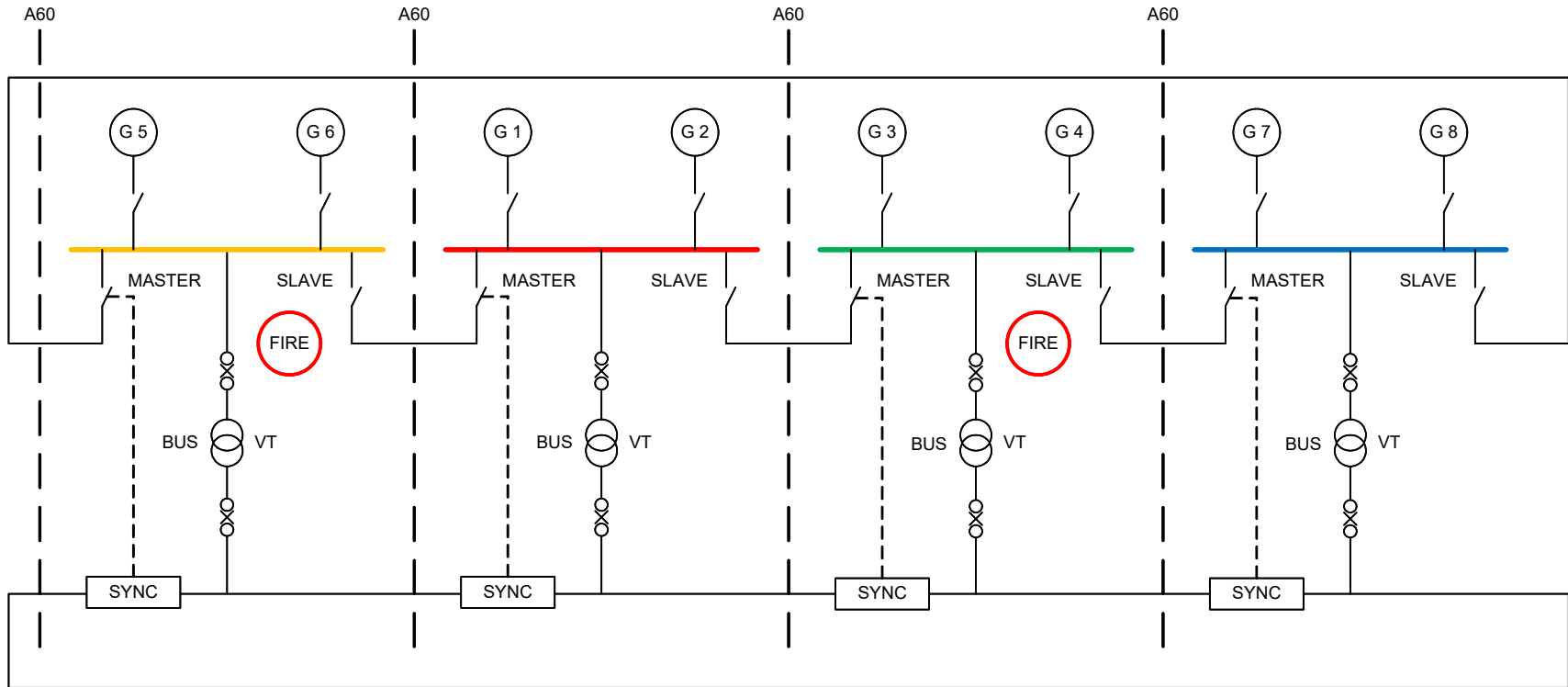
- B.2.3.1 Control power for switchboards is typically 110Vdc and 24Vdc. It is used for a variety of functions including switchgear controls, relay logic, interlocks, protection relays, governors and AVRs. Failures or intermittency in these types of supplies can be highly disruptive causing engines to stop, circuit breakers to trip and so on.

- B.2.3.2 In fire situations, multiple faults may occur on any or all lines which cross the boundaries, including open circuits, short circuit, earth faults and various combinations of these. Higher voltages could be coupled across to low voltage control circuits by fire and flood damage. This is potentially a very difficult failure scenario to analyse reliably and therefore there are good reasons to design out such cross-connections. Many can be replaced with alternative system designs which require no cross-connections. These may also be more economical to implement when the cost of installing and commissioning cables is considered. Appendix B - Figure 8 shows one example where a control fuse in one switchboard room can be blown by a fire or flood in the other. This may cause a voltage dip on the control power supply causing malfunction in other consumers. Such problems may be even more likely when miniature circuit breakers are used for protection.

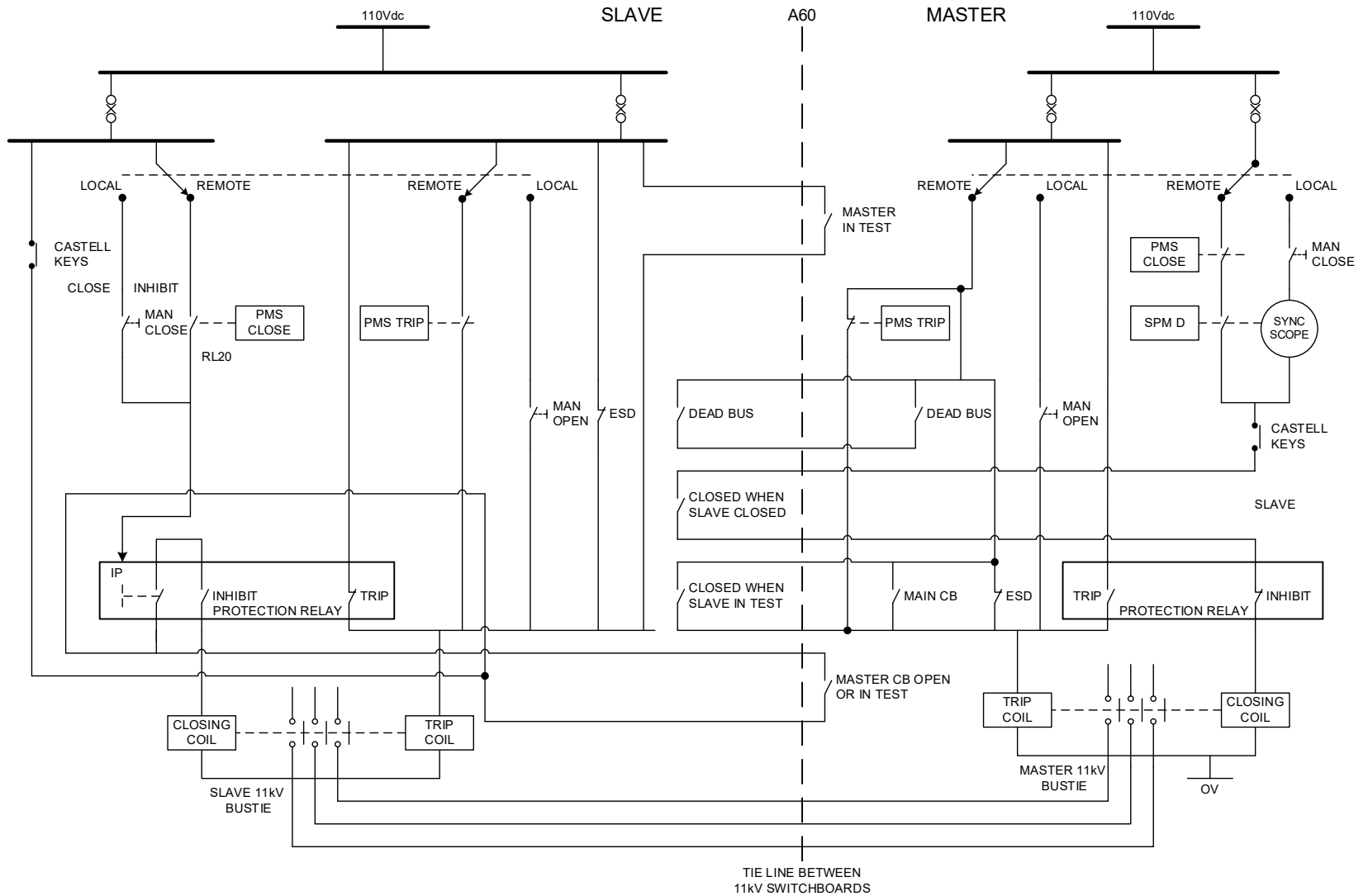


Appendix B - Figure 8 Control Power Crossing Boundaries

- B.2.3.3 Bus voltage transformers are another example of a control and protection component that often crosses A60 / WT boundaries. In Appendix B - Figure 9, a fire in any switchboard room has the potential to blow a control fuse in the adjacent switchboard because of the common synchronising lines causing malfunction in other consumers using the voltage signals from the VT.
- B.2.3.4 Appendix B - Figure 10 shows the cross-connections in a typical master slave bustie arrangement. All of these may be subject to the effects of fire or flooding causing various combinations of faults in both redundant DP groups.
- B.2.3.5 An additional consideration with DP class 3 designs is that heat may be conducted through copper cables: This particular fault propagation path is not often considered in the failure modes. On vessels with DP equipment class 3 notation, the cable is usually isolated by circuit breakers on both sides of the A60 bulkhead and its ability to damage redundant equipment should be limited.



Appendix B - Figure 9 Effects of Fire on Supplies from Bus VTs



Appendix B - Figure 10 Main Bustie Controls and Interlocks

B.3 GROUND FAULTS – PROPAGATION THROUGH SHIP’S HULL

B.3.1 GROUNDING EARTHING STRATEGIES

B.3.1.1 **Power system earth / ground reference:** The terms earth and ground are equivalent in electrical engineering and commonly in use in Europe and North America respectively. The term earth fault or ground fault is used to mean an unintentional connection to something that is at the potential of the earth by way of an electrical fault.

B.3.1.2 All power distribution systems are referenced to the potential of the earth to some degree by stray capacitance or other impedances such as insulation resistance and capacitance. Some systems are intentionally referenced by various means or may become earth referenced by faults. A marine power system may be intentionally referenced to the potential of the ship’s hull by various means or left ‘un-earthed’. The term ‘un-earthed’ or ‘insulated’ is used to mean there is no intentional earth reference (connection point).

B.3.1.3 **Alternating current systems:** In marine applications the ac system’s ‘neutral’ may be treated in the following ways:

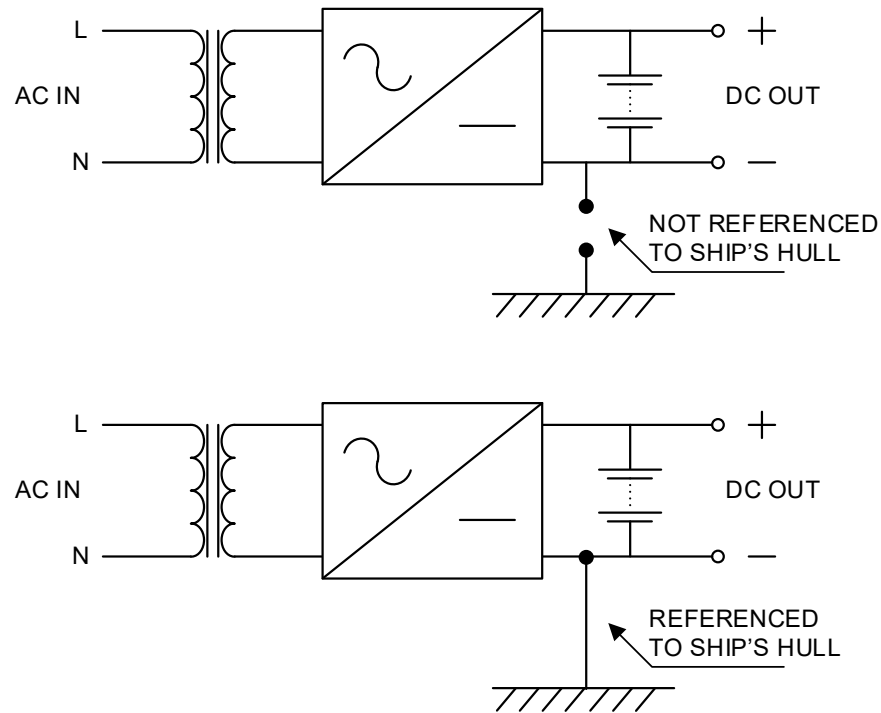
- Un-earthed (insulated) - Not connected to the ship’s hull (other than through cable and winding impedance to earth).
- High resistance earthing – Generator star point connected to the ship’s hull through a high resistance (high resistance earthing, for alarm or automatic isolation). Typically, 100s of Ohms or more.
- Low resistance earthing – Generator star point connected to the ship’s hull through a low resistance or directly connected to the ship’s hull. Typically, $< 1\Omega$.
- Transformer earthing – zigzag or broken delta transformer - Distribution system referenced through a transformer which has an earth referenced winding.

Note: *Some special schemes are employed for tankers and warships.*

B.3.1.4 **Direct current systems:** Refer to Appendix B - Figure 11. Marine dc systems (24Vdc, 110Vdc) are typically referenced in the following ways:

- Un-earthed (insulated) – Not connected to the ship’s hull (or connected through a high resistance for fault detection and alarm). – Sometimes referred to as a ‘Floating’ power system in some literature.
- Earth referenced – Typically, the negative rail of the distribution system is connected to the ship’s hull at the charger / rectifier. In some designs the return conductor (negative supply rail) is the ship’s steel hull. This is uncommon in DP vessel designs.

B.3.1.5 Equipment manufacturers may stipulate the way they wish the power supplies for their equipment to be earth referenced. Problems may arise at the interfaces between one manufacturer’s scope of supply and another if different earthing methods are specified. These need to be resolved. Specifications for how to implement protective earthing, the earthing of screens for signal cables and those for power cables are also important to ensure predictable behaviour and failure effects.

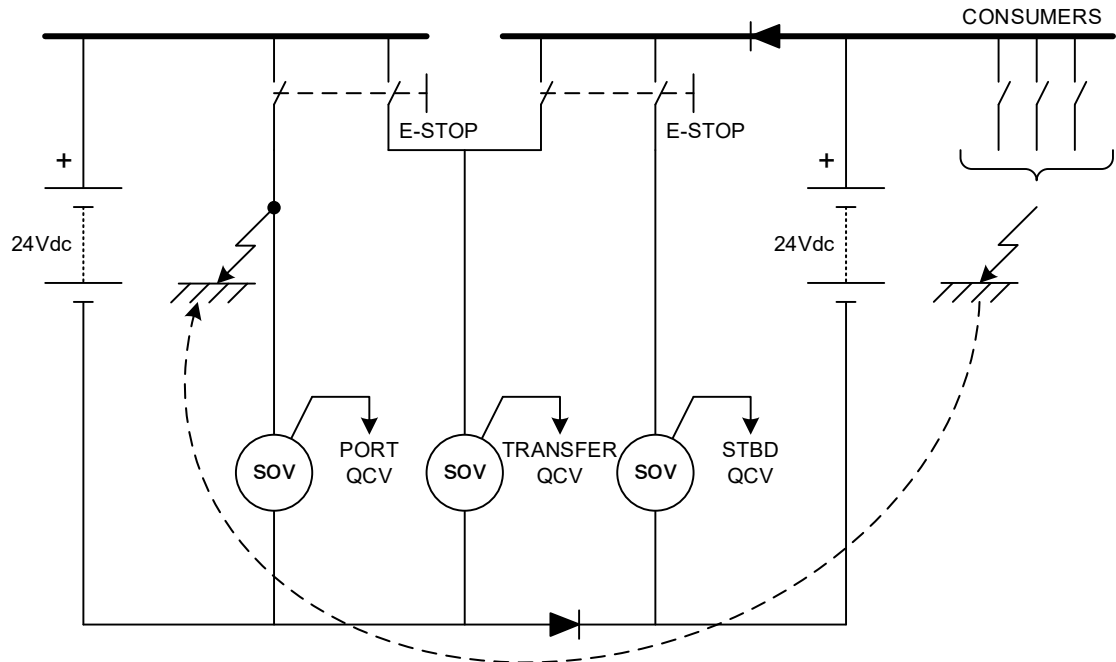


Appendix B - Figure 11 Un-Earthened and Earth-Referenced dc Power Supplies

B.3.2 COMMONALITY CREATED BY GROUND FAULTS

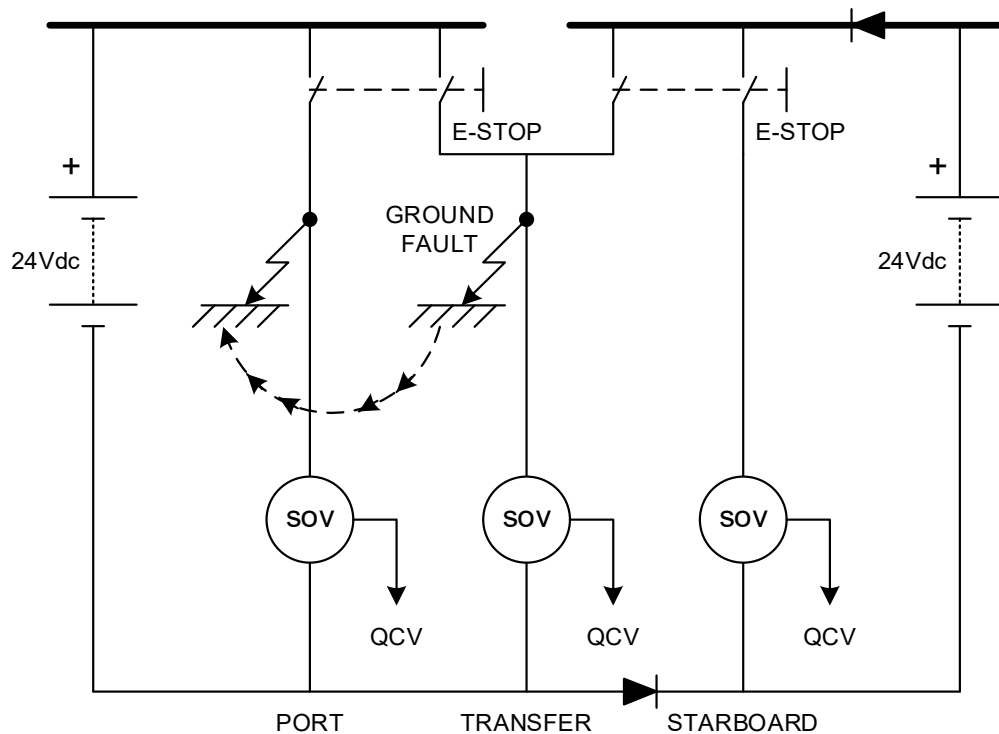
- B.3.2.1 Insulated dc distribution systems are popular on merchant ships and DP vessel's alike because they permit continued operation in the presence of an earth fault. Earth faults are relatively common on marine power systems particularly where the distribution systems supply consumers on deck or in machinery spaces subject to heat, vibration, salt corrosion, accumulations of bilge water and so on.
- B.3.2.2 Unfortunately, the earth fault detection systems on dc power distributions tend to be unsophisticated and an earth fault anywhere on the system initiates a common alarm. Where redundant dc power systems are coupled together through diodes, an earth fault on one system is also registered on the other system. It is for this reason that locating and clearing earth faults can be a time consuming and tedious process requiring one consumer at a time to be energised and isolated to determine whether it is the source of the fault. Furthermore, it may be difficult to perform this type of trouble shooting without causing down time or disruption to the vessel's industrial mission. As a result, earth faults may be present on marine power distribution systems for extended periods of time. This creates the possibility for multiple earth faults to accumulate in different parts of the power distribution system.
- B.3.2.3 Appendix B - Figure 12 and Appendix B - Figure 13 are much simplified extracts from an electric emergency stop system used to operate the fuel quick closing valves on a DP vessel with a port and starboard fuel tank which has a cross connecting fuel transfer line between the two tanks that may need to be isolated at the same time as one of the tanks is isolated.
- B.3.2.4 The example vessel has port and starboard 24Vdc power systems which are floating with respect to the vessel's hull. The design allows the operator to close the tank suction and transfer valves from a single emergency stop push button. To provide this facility, the port and starboard dc power system are connected through diodes in this part of the control system.

- B.3.2.5 In Appendix B - Figure 12, an earth fault occurs on the control line for a solenoid valve. This may be due to insulation failure associated with abrasion of the cable etc. or insulation failure within the solenoid itself. Initially, this does nothing more than raise an alarm. Sometime later an earth fault develops on the supply side of another consumer on the starboard power distribution system. This completes a circuit through the vessel's hull which operates the port quick closing valve. If the earth fault on the starboard systems was associated with a fire or flooding event the redundancy concept could be defeated as both redundant groups are now affected.



Appendix B - Figure 12 Multiple Earth Faults Create Unpredictable Behaviour

- B.3.2.6 In Appendix B - Figure 13, earthfaults have accumulated on the transfer valve solenoid and the port suction solenoid valves. When the starboard emergency stop is operated the transfer valve and the port quick closing valve also operate and the vessel blacks out due to fuel starvation in the surviving systems.



Appendix B - Figure 13 Effects Exceeding WCFDI

B.3.3 MITIGATION OF GROUND FAULTS

- B.3.3.1 Earth faults will occur in marine power systems. Using insulated power systems prevents one earth fault from causing disruption or a significant voltage dip but a second fault may become a short circuit or may introduce unpredictable system behaviours or failure response depending on location. Diligently clearing earth faults from insulated power distribution systems may be hampered by the operational disruption caused by identifying the fault location.
- B.3.3.2 Earth referenced power supplies are preferred by some DP vessel operators because they improve the predictability of failure effects. An earth fault on the negative rail becomes another reference point with generally limited effect on system performance. An earth fault on the positive rail becomes a short circuit which is cleared by the over current protection. Generally, this means that if an earth fault occurs, a fuse or miniature circuit breaker operates, positively identifying the fault location and clearing it from the systems. Some functionality is lost and other consumers must be able to ride through the voltage dip or resume operation to prevent significant disruption but provided redundant power distribution systems are not tied together, any disruption should be limited to one redundant DP equipment group.

B.4 MARINE AUXILIARY SERVICES

B.4.1 GENERAL

B.4.1.1 Cross-connections in marine auxiliary systems are allowed in some DP notations and there may be no separation of pipework in some designs. Such designs can be vulnerable to common mode failures associated with contamination, leakage or aeration of the fluids they transport. Such vulnerabilities are usually managed with rigid enforcement of procedural barriers. Full separation of marine auxiliary systems is desirable. Cross-connections for maintenance purposes can be accepted with mitigation measures in place.

B.4.2 VENTILATION

B.4.2.1 Common ventilation systems for compartment cooling and supply of combustion air are vulnerable to contamination from smoke or dust generated by activities associated with the vessel's industrial mission. Common ventilation of redundant spaces should be avoided and intakes well separated. The provision of effective air filters offers further protection provided these are periodically maintained.

B.4.2.2 Suitable HEMP process should be used as the basis to create robust and secure methods of establishing a confirmed fire. Systems should be developed which are not prone to false activation. Some DP vessel owners chose to operate the, ESD and F&G system in 'manual' mode to provide a further barrier to loss of position.

B.4.2.3 Control equipment can be sensitive to overheating associated with ventilation failure and the location of such equipment and the ventilation systems serving those spaces should be segregated along the lines of the DP redundancy concept.

B.4.3 FUEL OIL

B.4.3.1 The risks of contamination, aeration and leaks support the need for full separation of fuel systems along the lines of the division in the DP redundancy concept. Effective fuel management processes can help reduce the risks of cross contamination. Valves that allow the fuel supply system to be made common can be accepted provided they remain closed. Water contamination from fuel oil coolers may be a risk in some designs.

B.4.3.2 Fuel quick closing valves and their control system sometimes form a common point connecting redundant fuel systems which needs attention to ensure failures in the control equipment cannot affect more than one redundant group.

B.4.4 LUBRICATING OIL

B.4.4.1 There are generally fewer opportunities for cross-connections to affect more than one redundant group in typical DP vessel designs because it is unusual for more than one element of main machinery to share a lubrication system with another. In some designs, configuration errors in the clean oil supply system could result in one generator sump being overfilled and another being emptied. Effective workplace procedures are generally accepted as providing sufficient mitigation.

B.4.5 SEAWATER COOLING

B.4.5.1 This is one particular auxiliary system where commonality between redundant groups is accepted as offering some benefits. In designs with two sources of seawater supply it is not uncommon to operate the entire power plant from a single source and keep the other source clean and ready for use. In more recent designs however, the trend has been to provide each redundant group with two sources of seawater and this is recommended. Differential pressure alarms on sea strainers, flow switches and pressure switches / transducers can help to improve robustness and detect the onset of cooling water problems. Alarms to initiate operator intervention should be regularly tested and crew should be familiar with procedures for changing over seawater supplies.

B.4.6 FRESHWATER COOLING

B.4.6.1 Unlike seawater cooling systems the capacity of freshwater cooling system is limited to the capacity of the system and its header tanks. The risk of leakage and loss of coolant associated with pressurisation of the system by jacket water leaks in engines supports the need for freshwater cooling systems to be split along the lines of the redundancy concept as a minimum. MTS design philosophy guidance recommends providing individual coolant circuits for each generator and thruster.

B.4.7 COMPRESSED AIR

B.4.7.1 Compressed air system is used for a number of services and several systems may be provided for different purposes.

- Starting air – engines.
- Control air - engines, thrusters, brakes, seals, cooling water valves, fire dampers.
- Service air – maintenance.
- Rig & bulk air – industrial.

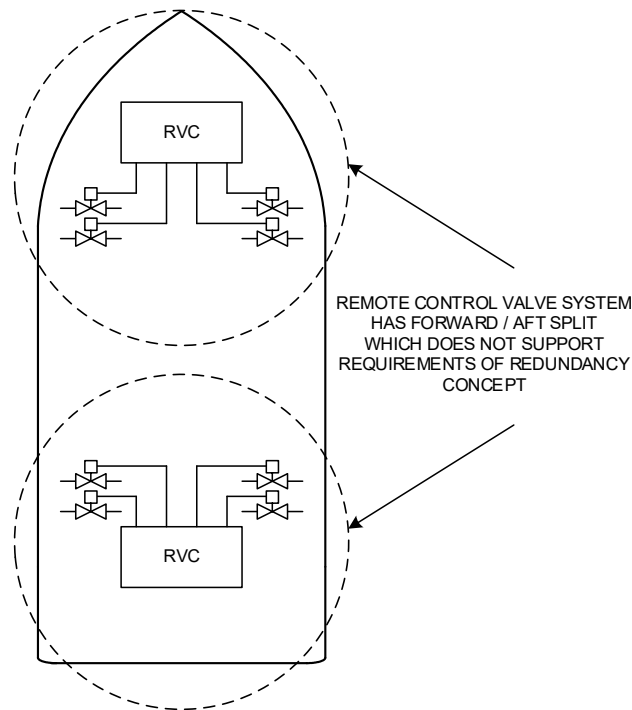
B.4.7.2 Classification societies approach to the acceptance of design of compressed air systems for control purpose in DP vessels is that they may be arranged as a common system provided its failure has no immediate effect on DP. Control air systems often serve a large number of equipment items intended to provide redundancy but failure to low pressure does not usually produce an unacceptable effect in modern designs. However, although the effect on DP may not be immediate, the loss of functionality may be unacceptable, particularly if it affects the ability to fight fires effectively. The consequences of such a decision could be that DP operations should be terminated. Complete segregation of control air system along the lines of the DP redundancy concept is recommended.

B.4.8 REMOTE VALVE CONTROL

B.4.8.1 Remote valve control systems are often provided as part of ballast control systems and can be overlooked in the DP redundancy concept. Although the system may be divided this is not to provide redundancy, rather it is for the convenience of reducing pipe and cable runs. Often the split is 'fore and aft' not 'port and starboard' as required for DP as shown in Appendix B - Figure 14. In some designs, generator cooling water valves are controlled from the remote valve control system. The following concerns arise.

- All valves may close as the result of single failure in the valve power supply (electric, pneumatic or hydraulic) leading to overheating and blackout.
- Even where 'fail as set' valves are chosen there is a possibility that the common control systems may drive valves closed.

B.4.8.2 Remote control valves associated with the DP system should be subject to same design philosophy and analysis as all other parts of the DP system and arranged to fail in a manner that does not exceed the worst-case failure design intent. Note that in some cases the classification society may require a particular valve failure response. In cases where this is 'fail to the closed position' which is sometimes a requirements for hull isolation valves it is particularly important to ensure there are no failure modes that can cause power or control signal to be lost to DP related cooling water valves in more than one redundant group.



Appendix B - Figure 14 Division of Remote-Controlled Valve Systems

B.4.9 FIRE DAMPER CONTROLS

- B.4.9.1 Automatic fire dampers for engine rooms and other machinery spaces can also be designed with different failure responses in the same way as remotely controlled valves can. Where the engines draw their combustion air from within a common engine room, as is permitted for DP equipment class 2, it is essential to ensure that no single failure of the fire damper control system or the power source for the dampers (electric or pneumatic) can cause all fire dampers to close. Where fire dampers are designed to fail to the closed position it is particularly important to segregate exhaust and supply dampers into functional and redundant groups such that no single failure can cause a restriction on the combustion and ventilation air supply. Even if the engines are not severely power limited when the fire dampers close, the rapid change in engine room pressure has been known to cause weather-tight doors to slam or fly open with potentially dangerous effects for personnel.
- B.4.9.2 From a DP perspective, dampers which fail 'as set' offer the best compromise but the failure response may be specified by the classification society for reasons other than station keeping integrity. Where there is more than one engine room, redundant DP groups should have completely independent fire damper power and controls.

B.5 NETWORKS

B.5.1 DP VESSEL NETWORKS

B.5.1.1 A DP control system typically communicates via dual redundant Ethernet network to distributed thruster control hardware. If this redundant communication link fails, all automatic control of the thrusters is lost. Network storms and lack of throughput are well documented causal and contributory factors in DP loss of position incidents. It is therefore concluded that:

- Data communication links are one of the most critical elements of the DP system.
- A network with inadequate performance is a potential hidden failure.
- Protection is required against common cause failures such as network storms.
- Network storm protection and throughput must be proven periodically.

B.5.1.2 An offshore vessel can have multiple control systems of various types, these may include:

- Main DP control system (DPCS)
- Backup DP system
- Independent Joystick System (IJS)
- Thruster Control System (TCS)
- Power Management System (PMS)
- Emergency Shutdown System (ESD)
- Integrated Automation System (IAS)
- Fire detection and Fire & Gas detection (F&G)
- Networks for industrial mission systems.

B.5.1.3 Many of these systems use networks and some share the same network. These systems routinely use dual redundant Ethernet communication to send and receive data between connected nodes. These nodes may include field stations, operator stations, data recorders, printers, and controllers. Modern vessel network topology is typically based on 100 Megabits / second networks, running full duplex, and may also include additional protocols that utilise Ethernet technologies such as PROFINET and/or Modbus TCP.

Note:

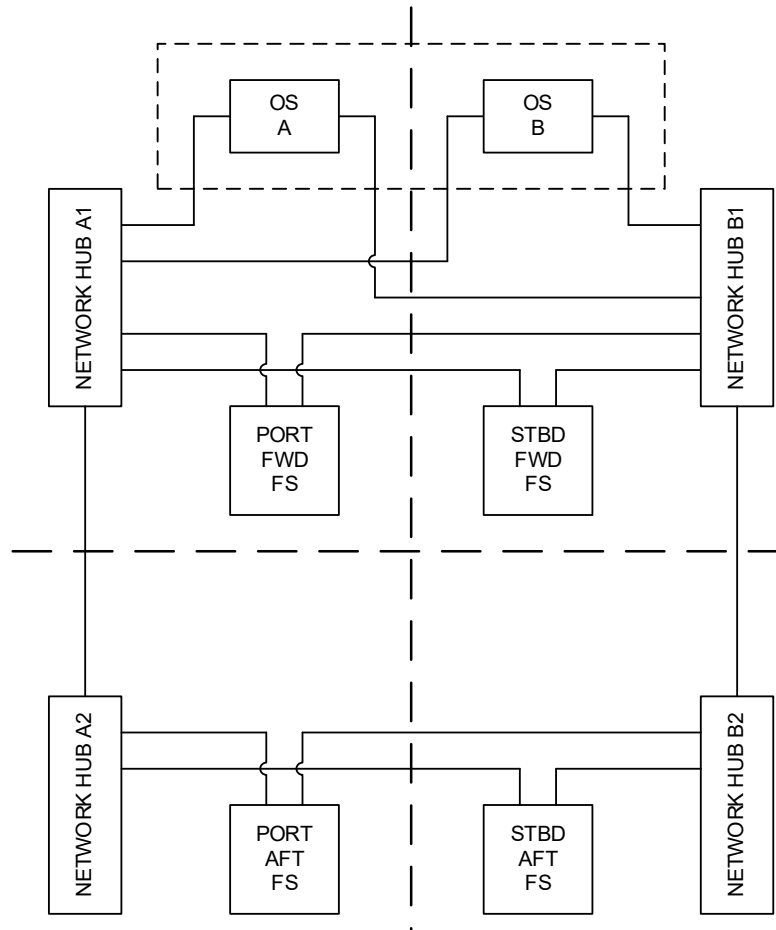
Although not so widely used, there are networks, other than ethernet, that have been used on DP vessels for DP and VMS. One such example is the Factory Interface Protocol (FIP). FIP is a type of deterministic field bus found in different topologies including dual ring, quad ring and dual star topology both dual star and dual ring topologies are known to have suffered from total communications failure. Failure mechanisms includes failure of offline Bus Arbiter to take over. Blocking of both channels by noise generated at a common point.

B.5.1.4 There have been designs where a single bi-directional ring topology has been used to create redundant network. Loss of communication incidents have been reported on such systems.

- B.5.1.5 Other failure mechanisms responsible for total communication failure in Ethernet based designs include simultaneous and spurious activation of flow control signals intended to allow slow data consumers time to process data on networks shared with high speed data sources. Such a feature is not required in networks where all consumers / producers of data are equally capable. The feature is retained for use with legacy equipment. A common mode failure within a field station that can set the flow control active on both networks can effectively halt all communication. In most modern vessel networks flow control can usually be turned off, but any such decisions should be taken in cooperation's and consultation with the network OEM. However, Information should be sought on whether Flow Control is active and what are the precautions in place to ensure that communications are not halted.

B.5.2 NETWORKS AS COMMONALITY

- B.5.2.1 Data communication networks in DP vessels are generally considered to be an unavoidable common point. Although there are redundant networks, all DP related control equipment is generally connected to both networks. Even designs where the DP control system connects to the thrusters by way of an analogue interface have networks within the DP control system that carry signals from shared references and sensors. Networks are also used for comparison alarms and voting purposes between controllers. A typical vessel management system network connecting fields stations to operator stations over a dual industrial Ethernet is shown in Appendix B - Figure 15.



Appendix B - Figure 15 Typical Vessel Management System Network

B.5.3 NETWORK FAILURES

- B.5.3.1 Redundant data communications networks require the same attributes of performance, protection and detection as any other element of the DP redundancy concept and should be subject to periodic checks to ensure their performance and integrity. Each network must be capable of:
- Rated performance.
 - Isolating any faults with the potential to affect both networks.
 - Have sufficient alarms and monitoring to allow the operator to know when redundancy has been lost.
- B.5.3.2 There have been a number of DP incidents related to network failure in DP vessels, some quite recently which have revealed unforeseen flaws in network design. These have all occurred at common points connecting the two networks.
- B.5.3.3 Mechanisms known to cause failure of redundant networks includes the following.
- Network storms
 - Jabber
 - Simultaneous activation of flow control
 - Failure of bus arbiters to take over.
- B.5.3.4 One such example is the 'flow control' function. Industry experience confirms that this function can be activated in both networks by a common fault in an operator or field station leading to total loss of both networks. In most designs, flow control is not necessary, and the risk can be eliminated by turning off the function.
- B.5.3.5 In some types of DP control system with an analogue interface to the thrusters, dual serial links using the RS485 protocol are used to interface information from thrusters and vessel sensors (such as the gyro ready signal) to each redundant controller. Such links have failed in service in such a way as to cause loss of vital information to all redundant DP controllers leading to loss of position. In the case of DP control systems with a digital interface to the thrusters this RS485 link still exists but may have very limited functionality. Never-the-less it represents a common point connecting redundant DP equipment groups. Consideration could be given to engineering out this link when it is practical to do so.
- B.5.3.6 A netstorm is a type of network failure. It is essentially an excessive amount of traffic, or more specifically, a flood of packets on the network. In a control system network scenario, the vastly increased number of packets can cause controllers to become overloaded, unable to handle their normal tasks – such as controlling a thruster (DP), monitoring shutdown conditions (ESD), or providing switchboard protection (PMS). Valid packets may never reach their intended destination.
- B.5.3.7 Causes of a netstorm can include one or more of the following:
- Software failure
 - Hardware failure
 - Human error
 - Inherited design issue
 - Network configuration error.

B.5.3.8 Netstorm could affect different control systems in the following ways:

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

B.6 NETWORK TESTING

B.6.1 OVERVIEW

- B.6.1.1 Networks are critical to DP functionality and performance. Annual testing carried out on DP vessels should include tests designed to demonstrate confidence in network performance and protective functions.
- B.6.1.2 The test methods and procedures being used to demonstrate throughput and network storm protection should have the capability (bandwidth) to fully exercise the network and those protective function upon which the redundancy / fault tolerance of the network relies. Packet injection and loop back tests can both provide useful information.
- B.6.1.3 Periodically operating the entire vessel from only one of the two networks, when it is safe to do so, may provide some confidence that each network is operational, but this may not test maximum performance or be representative of the highest traffic level that may occur when the DP system experiences a failure generating an avalanche of alarms. In many modern designs the available theoretical bandwidth is well above that required but unless it is tested periodically the actual performance is unknown.
- B.6.1.4 Networks have many protective functions but one that has been most important in relation to previous DP incidents is the network storm. Most commercially available systems installed on DP vessels have some form of net-storm protection. It is also important to know when protection is operating as this indicates that redundancy (and thus fault tolerance) has been lost. Alarm and network status pages on the vessel management systems can provide this information.
- B.6.1.5 Other protective functions or attributes exist within the network switches intended to limit the effects of electrical faults such as short circuits which may occur when copper conductors are used as the transmission medium. As these are inherently part of the transmission process, they are less likely to become hidden failures as loss of the galvanic isolation (for example) would be accompanied by failure of the transmission which should generate alarms for lost messages. This isolation has particular significance for DP class 3 designs where the effects of fire and flooding could impose electrical faults on connections to both networks and consideration can be given to the use of fibre optic links which are not susceptible to electrical faults or electromagnetically coupled interference.
- B.6.1.6 A useful indicator of the ability of a network ability to withstand a network storm (even with appropriate protection) is the 'spare time' figure for the distributed processors. OEMs should be consulted to provide an acceptable figure for spare time which should not be exceed. During a network storm the indicated spare time may increase but should stabilise at some point during the networks storm test.
- B.6.1.7 Spare time is the measure of available capacity on an operational controller; this value is displayed as a percentage and can be viewed on the DP/automation system's operator stations. A controller running at 70% capacity will show 30% spare time. DP and automation controllers are real-time computers, as such there are time constraints in place to guarantee data which has been input to the system is processed within a specified timeframe. This differs from a traditional PC - whereby tasks are queued and processed whenever CPU capacity allows.
- B.6.1.8 A typical minimum amount of spare time a controller should have during normal operations is generally considered to be 30% to 40%. With sufficient spare time available, the controller should be able to function correctly during a netstorm, executing protection to avoid becoming overloaded. OEMs should be consulted to confirm what spare time is considered appropriate.

- B.6.1.9 Significant Instability in the spare time figure during a netstorm test can be an indicator that the networks, and thus the DP system, will begin to exhibit unpredictable behaviours if the networks storm test continues. Continuing the test to the point where spare time is observed to stabilise provides confidence in the robustness of the communication networks and their protective functions. such an approach may be better than choosing an arbitrary test duration.

B.6.2 NETSTORM PROTECTION

- B.6.2.1 Many network switches will feature some form of netstorm control and rate limiting, with the ability to drop packets of various types when a specified traffic level is exceeded. This prevents a netstorm degrading network performance for essential / time - critical traffic. In a control system network, this first line of defence can stop the overload of a controller, and the system can maintain proper function.
- B.6.2.2 If a netstorm is detected by the DP control system software, then it may be possible that any hardware-based protection within the network switches has failed or is not present. The increased traffic level now poses a real threat to the DP control system, and to maintaining position.
- B.6.2.3 A DP control system should be able to detect a netstorm, warn the operator, and also attempt to limit the effects by disabling the affected network; all this while continuing operation on the redundant network.

B.6.3 THROUGHPUT

- B.6.3.1 Throughput is an important feature of a network, it is essentially the speed at which traffic moves from point A to point B, i.e. the net result. Throughput should not be confused with bandwidth - this defines the maximum speed at which a link can send or receive, i.e. the potential. Throughput testing should also be carried out periodically.

APPENDIX C EXTERNAL INTERFACES & INFLUENCES

FIGURES

Appendix C - Figure 1	Abandon Vessel Shutdown at Remote Locations	6
Appendix C - Figure 2	ESD Interface to Push Button Matrix	7
Appendix C - Figure 3	Simplified Schematic of a Monolithic Emergency Shutdown System (Propulsion Part)	9
Appendix C - Figure 4	Fail as Set Fire Dampers Driven Closed by ESD System Failure	10
Appendix C - Figure 5	Simplified Schematic of a Distributed Emergency Shutdown System (Propulsion Part)	12
Appendix C - Figure 6	Preferred Method - Loop Power Originates at ESD Field Station	13
Appendix C - Figure 7	Sending Loop Power from Switchboard End	14
Appendix C - Figure 8	Preferred Method - Line Monitoring Resistors Installed at Switch	15
Appendix C - Figure 9	Line Monitoring Resistors Installed at I/O Card	16
Appendix C - Figure 10	Common Ventilation Systems Defeats Redundancy	17
Appendix C - Figure 11	Fire - Fighting System with Ventilation and Engine Shutdown	22
Appendix C - Figure 12	Simplified Schematic of Water Mist System	23

C.1 EXTERNAL INTERFACES & INFLUENCES

C.1.1 OVERVIEW

C.1.1.1 The term 'DP system' is defined as all equipment necessary for maintaining position and heading. However, there are other systems that interface to the DP system in various ways. Some of these interfaces may be provided to improve station keeping performance, but many play no direct role in station keeping. However, such interfaces have the potential to cause a loss of position if they fail or malfunction.

C.1.1.2 Such interfaces may not receive the scrutiny they deserve during design and verification phases, usually due to:

- Mis-categorisation as 'not being part of the DP systems.
- Networks carrying no DP related data (true or not they introduce fault propagation paths).
- Often being retrofitted.
- The lack of a systems engineering approach in their implementation.
- A lack of understanding of the potential impacts due to failure or malfunction.
- A lack of testing of failure modes and their effects.
- Approval authority if applicable residing between different disciplines and potential for misalignment of understanding of impacts.
- Existing rules and guidelines are adequate to guide the development and testing of these interfaces. Problems arise because of misinterpretation, misapplication or non-application of these rules and guidelines.
- Reviewing the design of such systems and interfaces against the 'seven pillars' described in the MTS DP Vessel Design Philosophy Guidelines helps identify potential weaknesses or opportunities to increase robustness and predictability.

C.1.1.3 The term 'external influences' is often reserved for less tangible interfaces to the DP system which may often be external to the vessel such as the atmosphere drawn in for ventilation and engine combustion air. Other examples include the effects of radio interference and noise in the water column. All these influences have the potential to create external common cause failure modes in the DP system itself.

C.1.2 EXAMPLE EXTERNAL INTERFACES & INFLUENCES

C.1.2.1 Example external interfaces to the DP system include:

- External force compensation.
- Draught sensors.
- Emergency Shutdown Systems (ESD).
- Fire and Gas Systems (F&G).
- Power control interfaces for industrial equipment.
- Power and circuit breaker status for DP control system.
- Power distribution for industrial consumers.
- Power distribution for life support consumers.
- Fixed firefighting systems – water mist – CO₂.

- Communications equipment.
- Navigation equipment.
- Roll compensation.
- Anti-heeling systems.
- Group emergency stops.

C.1.2.2 Example external influences on the DP system include:

- The atmosphere & ionosphere, contamination of ventilation and combustion air.
- Environmental conditions, wind, wave, swell, sea current, temperature.
- The sea surrounding the hull.
- Sea life.
- uncompensated forces.

C.1.3 GENERAL REQUIREMENTS FOR EXTERNAL INTERFACES

C.1.3.1 The general requirements for an external interface can be categorised as below:

- If complete loss of the external interface can adversely affect station keeping, then it must be redundant. – That is to say no single failure should cause loss of the service provided by the interface.
- If a failure of the interface does not affect station keeping, but malfunction of the interface could have an adverse effect, the interface must be designed to fail safe.
- Some types of interface will need to be redundant and fail safe.
- Where redundancy is required it should be applied in a manner that supports the vessel's redundancy concept.
- Optionality for manual inputs to be provided if applicable (example external force compensation, pipe tension etc).
- Sensors, if any, to have optionality that provides use for monitoring without input as control.
- Any decision to use sensors / interface information for control should be supported by data obtained from implementation of a system's engineering approach which includes testing to prove failure modes and effects.
- Low level shutdowns of ESD and F&G systems should not automatically result in loss of thrust. They should trigger alarms and shutdown of equipment leading to loss of thrust should require manual intervention.

C.1.3.2 NOTE: Stakeholders may have additional requirements that may need to be addressed.

C.1.4 IDENTIFYING EXTERNAL INTERFACES

C.1.4.1 It should be possible to identify the external interfaces from the detailed design documents for the DP vessel or from a competently executed DP system FMEA. If the veracity of the FMEA is in doubt, consideration can be given to carrying out a DP FMEA Gap Analysis using MTS TECHOP (D-05 - Rev1 - Jan21) 'FMEA GAP ANALYSIS'.

C.1.5 ANALYSING EXTERNAL INTERFACES

C.1.5.1 Each application will present its own challenges:

- Identify failure modes that may propagate by way of these interfaces.
- Identify where redundant interfaces are required to provide continuity of essential information.
- Identify where a fail-safe design is required and the fail-safe philosophy to be applied with consideration to the overall redundancy concept.
- Identify where unnecessary or unacceptable cross-connections are introduced.
- Identify any lack of protective functions essential to ensure failsafe.
- Identify potential hidden failures.
- Identify any barriers that can be put in place such as adopting a manual control interface or isolating interfaces and cross-connections.
- Identify and mitigate opportunities for configuration errors and acts of maloperation.

C.1.5.2 *Note: Due consideration to be given to adopting manual control interface or isolating interfaces and cross-connections as the default unless adequate confidence can be demonstrated by implementation of a system's engineering approach including testing for failure modes and effects.*

C.1.6 IMPROVING EXTERNAL INTERFACES

C.1.6.1 In addition to the points listed above it may be beneficial to carry out a review of the design against the desirable attributes listed in the MTS DP Vessel Design Philosophy Guidelines which are:

- Autonomy
- Independence
- Segregation
- Differentiation
- Fault resistance
- Fault tolerance
- Fault ride through.

C.1.6.2 Not every system needs all of these attributes. A focused and systematic review of the design against these seven attributes may identify gaps, if any, as well as opportunities for improvement in the design.

C.1.6.3 In the context of this TECHOP, design for fault tolerance includes fail-safe philosophy.

C.1.6.4 Examples given in the sections which follow demonstrate how design issues have defeated DP redundancy concepts. Some of these design issues were identified during DP FMEA or proving trial but others only manifested themselves in service. The intent of inclusion of these examples in the TECHOP is to aid owners to conduct a review of their vessels for the presence of similar vulnerabilities.

C.2 FIRE & GAS AND EMERGENCY SHUTDOWN (ESD)

C.2.1 INTRODUCTION

- C.2.1.1 Vessels conducting industrial missions with a 'gas hazard' are fitted with emergency shutdown systems (ESD) (example, MODUs- a requirement of the MODU code). Vessels which operate alongside vessels with the potential for hydrocarbon release may also be fitted with an ESD system.
- C.2.1.2 The purpose of an ESD system is to prevent the escalation of the consequences of a hydrocarbon release and limit the severity and duration of such events. This is achieved by a combination of actions which includes cutting off the source of hydrocarbons and bringing equipment to a pre-defined safe condition. Isolation of sources of ignition is also performed on initiation of ESD.
- C.2.1.3 Nothing in this guidance intends to contradict or replace classification society rules or flag state requirements for emergency shutdown systems. Neither does it intend to provide guidance on best practice in the design of ESD system in terms of their efficacy in controlling the escalation of events following a hydrocarbon release or other fire hazard. Reference should be made to other sources for this information.
- C.2.1.4 Failing to consider the requirements of station keeping integrity in the design of such systems can lead to DP incidents which also represent a significant safety hazard. In general, the objective should be to develop a design that satisfies the requirements of ESD and station keeping. Information is presented on how the design of ESD systems has compromised station keeping integrity. The intent of this TECHOP is to provide guidance and awareness of these issues with a view to avoiding the same problems in future DP vessel designs and upgrades.

C.2.2 REQUIREMENTS

- C.2.2.1 Station keeping, ESD and F&G are all considered to be safety critical systems. The rules and guidelines acknowledge the necessity for the needs of one to be considered in the design of the other. IMO MSC 645 & 1580, 'Guidelines for Vessel (and Units) with Dynamic Positioning Systems', 1994 / 2017, states in Section 3.6 'Requirements for essential non-DP systems':
- C.2.2.2 *MSC 645 '3.6.1 For equipment classes 2 and 3, systems not directly part of the DP system but which, in the event of failure, could cause failure of the DP system, (e.g., common fire suppression systems, engine ventilation systems, shutdown systems, etc.), should also comply with relevant requirements of these guidelines.*
- C.2.2.3 *MSC 1580 'For equipment classes 2 and 3, systems not directly part of the DP system, but which in the event of failure could cause failure of the DP system (e.g. common fire suppression systems, engine ventilation, heating, ventilation and air conditioning (HVAC) systems, shutdown systems, etc.), should also comply with relevant requirements of these Guidelines.'*
- C.2.2.4 The statement above is generally interpreted to mean that it is acceptable to shut down the DP system in response to a genuine safety condition that requires such action to be taken but it is not acceptable for a single failure in the safety system itself to adversely affect station keeping.
- C.2.2.5 Similarly, the 2009 MODU Code allows for special consideration to be given to dynamically positioned vessels. Sections 6.5.2 and 6.5.4 of the code are particularly important from a DP FMEA perspective. In general, the classification society rules for ESD now reflect the special status afforded to DP vessels and different rules are applied to vessels that require power for station keeping.

C.2.2.6 Section 6.5.2 states:

In the case of units using dynamic positioning systems as a sole means of position keeping, special consideration may be given to the selective disconnection or shutdown of machinery and equipment associated with maintaining the operability of the dynamic positioning system in order to preserve the integrity of the well.

C.2.2.7 Section 6.5.4 states:

Shutdown systems that are provided to comply with paragraph 6.5.1 should be so designed that the risk of unintentional stoppages caused by malfunction in a shutdown system and the risk of inadvertent operation of a shutdown are minimized.

C.2.2.8 It is of paramount importance that while it is required for equipment to be shut down, in a real event, spurious or unintended shutdowns should not affect station keeping. Efforts should be made to review and validate each vessel's ESD and F&G system design to identify and mitigate such potential. This review should be carried out as part of the DP system FMEA and include a review of the cause and effects matrix.

C.2.3 TYPICAL IMPLEMENTATION AND PROBLEMS

C.2.3.1 The IMO MODU Code 2009 requires the provision of ESD systems in drilling units and the classification societies have various rules in relation to the design of such systems. The main ESD control station is usually on the bridge with another in the Engine Control Room (ECR) or some other command and control location. Remote ESD buttons may also be located at the helideck, lifeboat stations and other locations. In some designs, there is a single ESD level pushbutton that initiates a total shutdown of the unit including propulsion, emergency and support facilities. This is sometimes referred to as All Vessel Shutdown (AVS) or 'dead ship'. Different ESD levels are used to denote an all vessel shutdown. These differences arise because there is more than one standard for ESD systems. Depending on the standard used, ESD 0 or ESD 3 may both mean total shut down level.

C.2.3.2 In this guidance note, the example used is a DP vessel with a three-way split in its redundancy concept using the following convention:

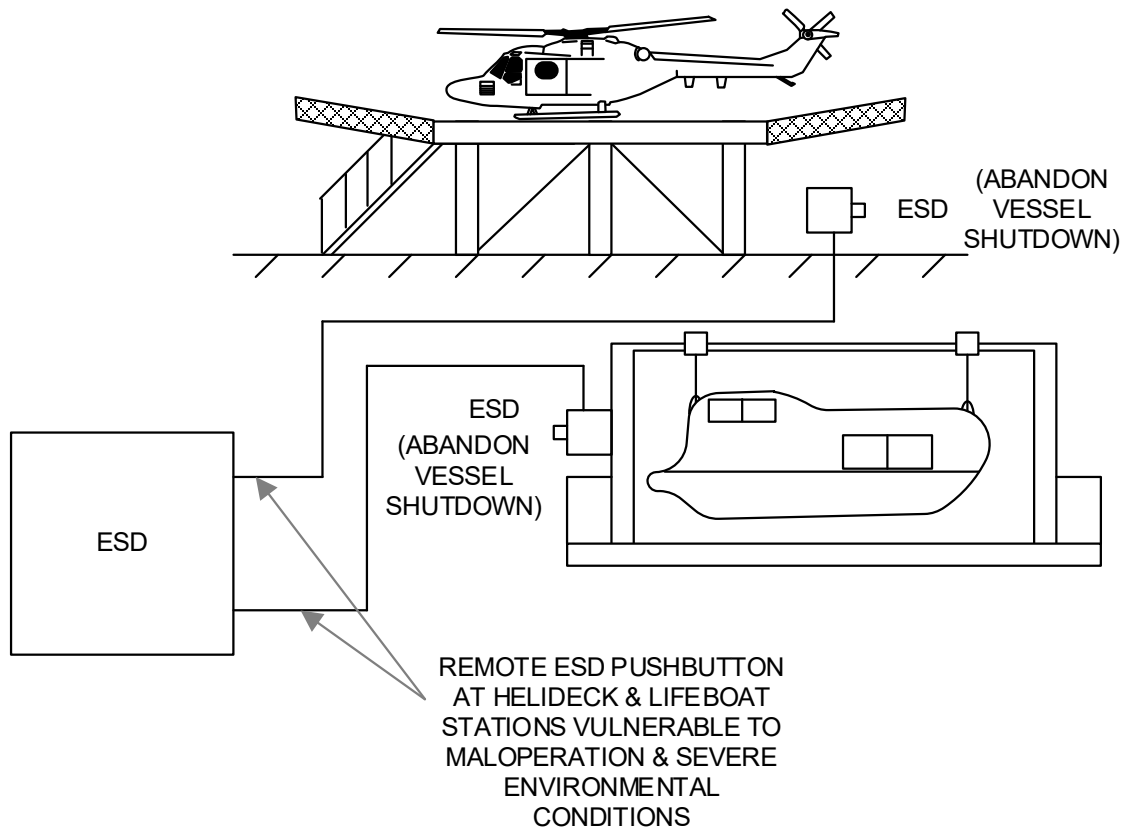
- ESD 0 Total shutdown.
- ESD 1 Emergency power system.
- ESD 2A Port power system.
- ESD 2B Centre power system.
- ESD 2C Starboard power system.
- ESD 3, 4 etc Accommodation or industrial spaces.

C.2.3.3 In some designs there is a 'cascade down' function which automatically activates all levels below the level that has been manually activated. For example, if ESD 0 (total shutdown) is operated then all levels below that are automatically activated. If ESD 1 (typically emergency power shutdown) is activated then ESD 2A, 2B and 2C and so on will be activated which is the entire main power generation system. This is equivalent to a blackout on a DP vessel and will lead to a loss of position. Therefore, even when there is some inhibit function (such as a bypass or lockout switch) on ESD 0, the cascade function may still cause a blackout if the ESD 1 function operates spuriously.

C.2.3.4 ESD and F&G system are generally required to have active redundancy. This is generally implemented to help ensure that the ESD system will operate on demand and not be in a failed state when required. Fail safe conditions are specified with reference to DP related equipment. Compliance with these requirements should ensure adequate integrity but incidents experienced in industry confirms that these arrangements have proven to be less robust than required in relation to ensuring the vessel is not shut down in response to a false or inadvertent shutdown activation.

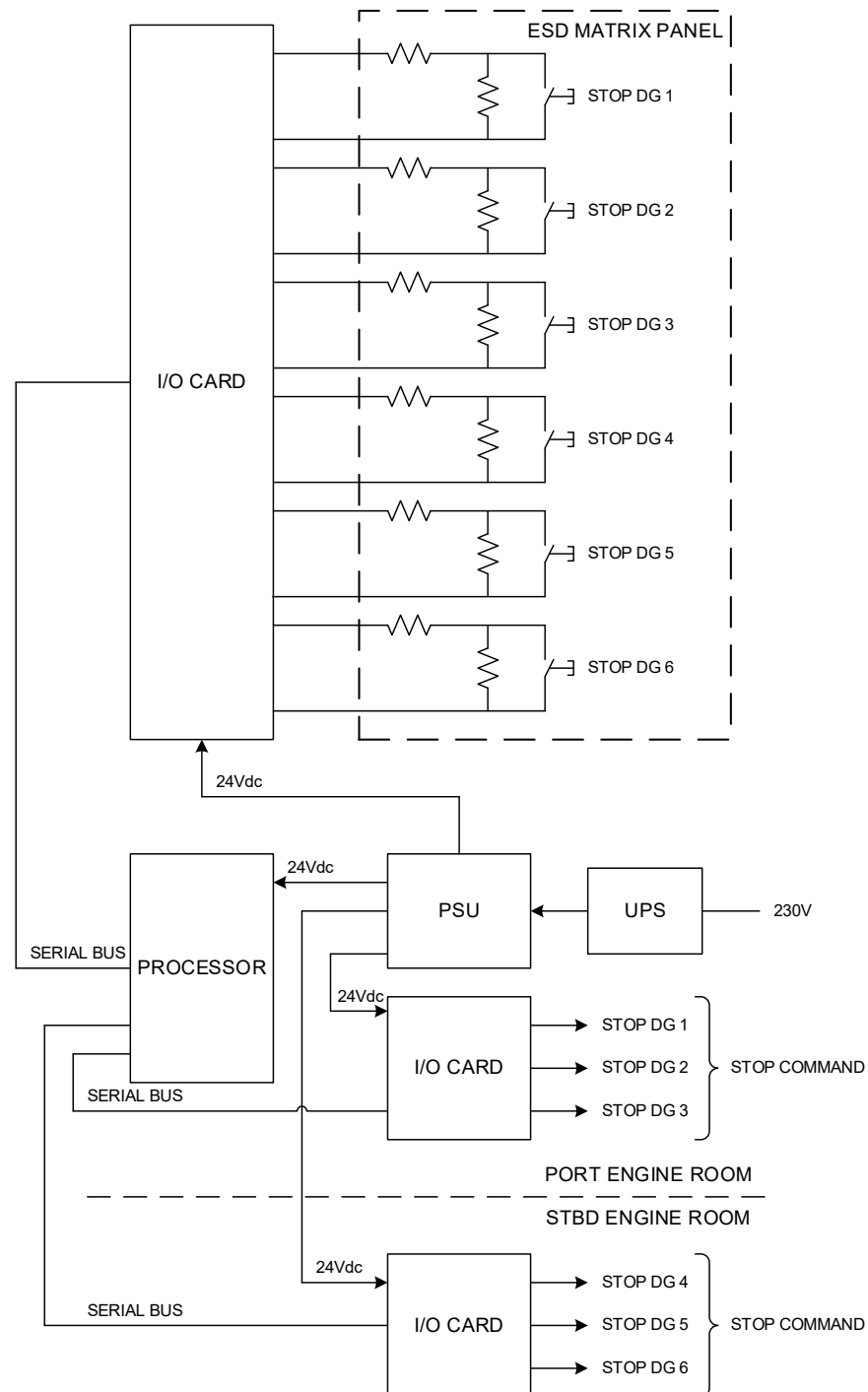
C.2.3.5 Typical scenarios include:

- Inadvertent operation of the total shutdown ESD buttons at remote locations such as those in Appendix C - Figure 1. These events have occurred even when clear signage and inhibit functions formed part of the barriers to a 'single inadvertent act'. This sometimes occurs because crew members, unfamiliar with the arrangement, mistake the control for some other service they require to operate. As loss of position on a DP MODU carries significant safety and environmental risks it is not evident that these 'remote' ESD buttons actually contribute to overall safety in their present form.
- There have been several cases where internal software and hardware faults have caused unintended activation of the total shutdown ESD level. Such faults have occurred even when there has been no single total shutdown level and where there has been an ESD inhibit function that was in the correct 'inhibit position' when the shutdown occurred. Appendix C - Figure 2 shows just such an example where care had been taken to ensure that the digital outputs used to shut down the generators were segregated. Unfortunately, the generators' stops were interfaced to one card. This commonality contributed to a condition where the processor believed all six pushbuttons had been operated and initiated a complete shutdown of the power plant.



Appendix C - Figure 1 Abandon Vessel Shutdown at Remote Locations

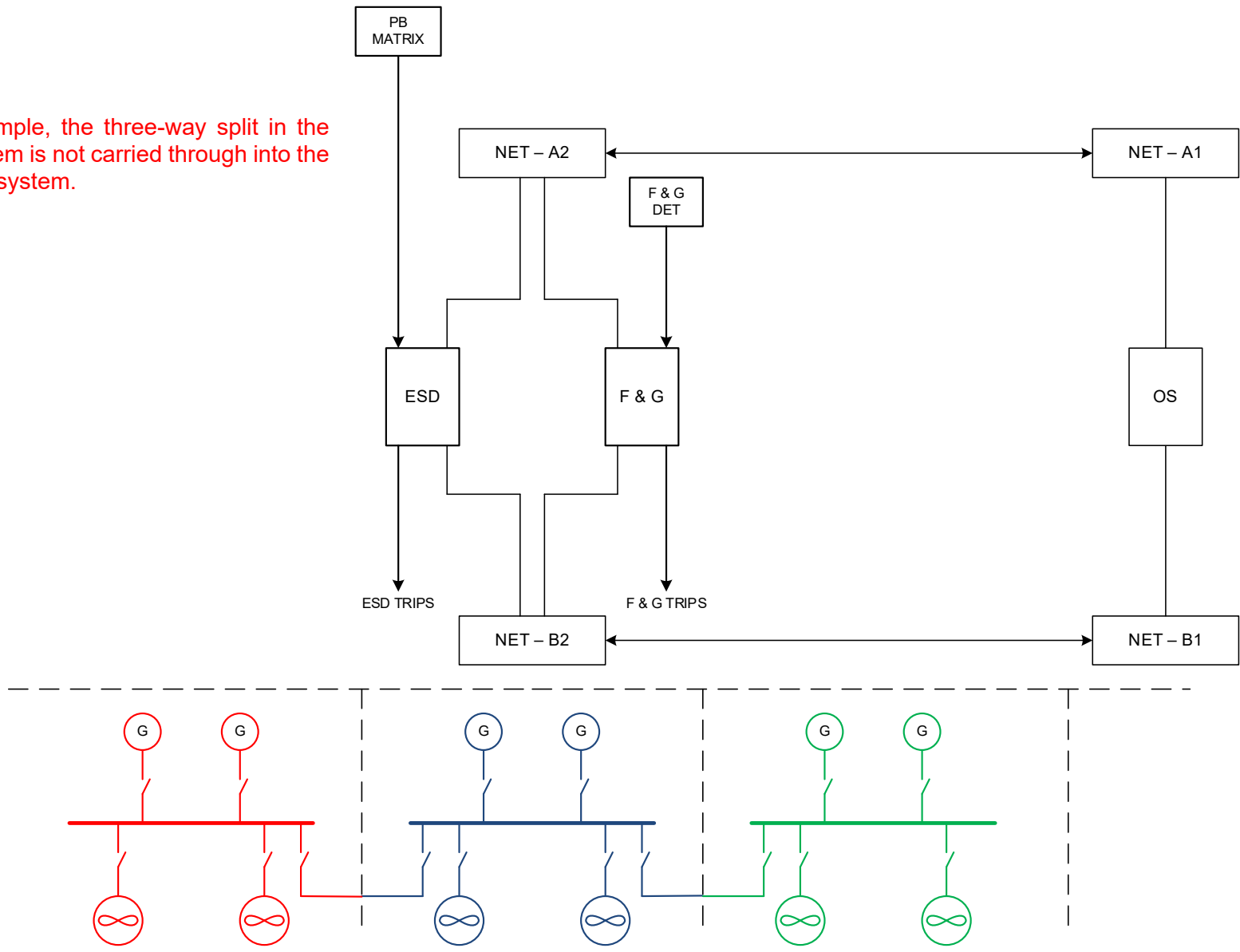
- C.2.3.6 Despite the fact that rules exist acknowledging the special circumstances of DP vessels, DP incidents associated with failure and malfunction of ESD and F&G systems continue to occur.
- C.2.3.7 Some vessel operators, as a barrier to spurious and unintended shutdowns, have relied upon the security of operating the ESD and F&G system entirely in manual mode. This was expected to provide a very high level of security but even this barrier has been defeated by software related problems as the manual inhibit function is simply another status input to the ESD controller and not a physical barrier to unintended shutdown initiation.



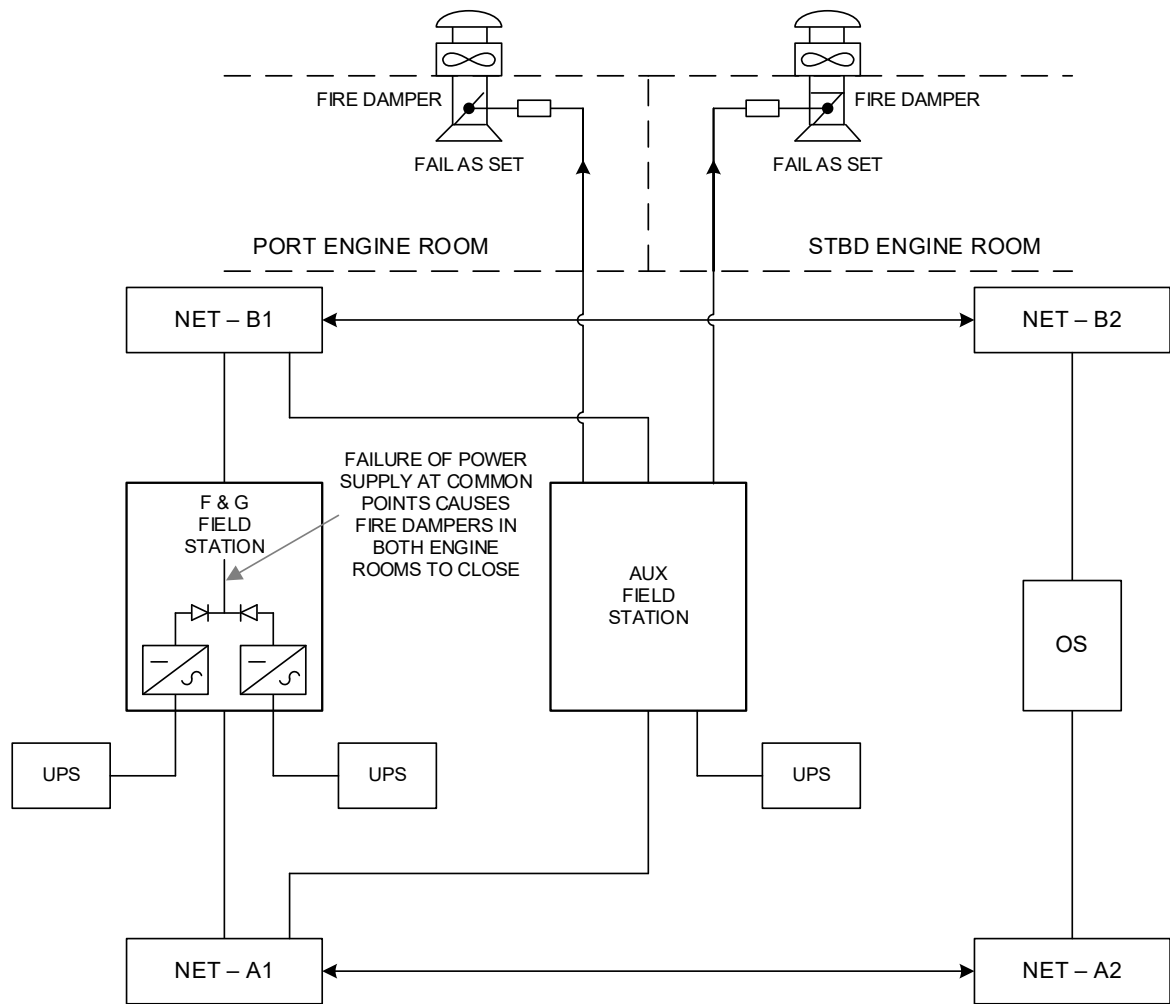
Appendix C - Figure 2 ESD Interface to Push Button Matrix

- C.2.3.8 A much-simplified schematic of an emergency shutdown system (propulsion part) is shown in Appendix C - Figure 3. Separate field stations for F&G and ESD communicate with a remote operator station over a dual redundant network. Each field station will usually have redundant processors and power supplies and be supplied from a UPS. Fire and gas detection is often provided by a specialist supplier and integrated by the automation system supplier. A hardwired interface from the ESD field station is provided for the ESD pushbutton matrix panel (several panels may exist in practice). In such designs, no attempt is made to provide any physical segregation of hardware along the lines of the DP redundancy concept. In practice there may be more than two field stations, but this is more to do with the amount of I/O required rather than to achieve segregation of systems which provide redundancy. Even when some distribution of hardware is part of the design it may be used to create a fore/aft split for the convenience of cabling rather than a split that matches the DP redundancy concept. In some examples, I/O for redundant systems is separated onto different I/O cards without achieving full hardware segregation. This is an improvement over designs which are vulnerable due to commonality in the I/O distribution but less robust than full hardware segregation.
- C.2.3.9 In the case of systems which are routinely operated in automatic mode, the severity of failure effects or acts of maloperation are often compounded by unacceptable levels of commonality in the design of the shutdown system. It is for this reason that the attribute of 'separation' along the lines of the divisions in the DP redundancy concept is promoted so strongly in MTS design philosophy. Separation helps to reduce the risk of unforeseen failure effects propagating from one redundant equipment group to another by way of that commonality. Appendix C - Figure 4 shows one such case where the F&G field station was redundant in terms of power supply and processors but had a common point connecting the internal dc supplies. When this common point was failed, all of the engine room fire dampers closed even though they were of 'fail as set design'. A 'fail-safe' condition to the closed position had been inadvertently programmed on loss of communications between the F&G field station and the auxiliary field station.

In this example, the three-way split in the power system is not carried through into the ESD, F&G system.



Appendix C - Figure 3 Simplified Schematic of a Monolithic Emergency Shutdown System (Propulsion Part)



Appendix C - Figure 4 Fail as Set Fire Dampers Driven Closed by ESD System Failure

C.2.4 SUGGESTED IMPLEMENTATION FOR ESD & F&G

C.2.4.1 The suggested design from a DP perspective is for the shutdown system to be split along the same lines as the overall DP redundancy concept with no single overall total shutdown function (e.g. ESD 0). Appendix C - Figure 5 shows how such a hypothetical design might be achieved. It is appreciated that such hardware segregation will need to be addressed in the software as well and there may be some challenges if not specified up front. The design philosophy's impacts on industrial mission systems should be assessed and addressed up front.

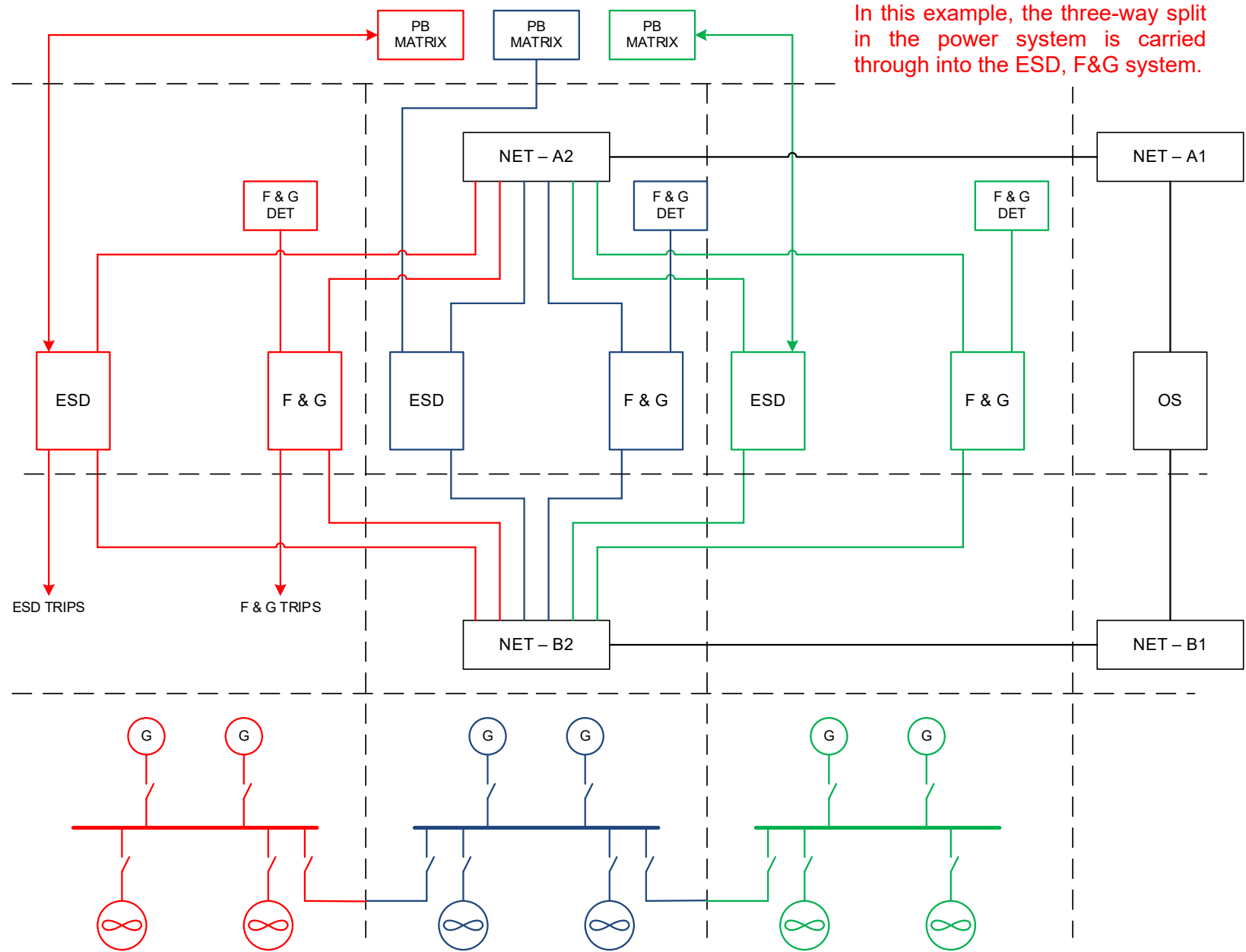
C.2.4.2 The following features can help to enhance robustness from a DP safety perspective:

- Use of normally de-energised contacts for shutdown of essential DP equipment (class requirement in most cases anyway).
- Line monitoring with alarm on cable faults or supply failure.
- Dual (or multiple) independent circuits to ESD push buttons (and dual buttons). Each push button circuit interfaces to a different FS or at least a different I/O card.
- Shutdown actuation should originate from separate field stations in a manner that aligns with the overall division of the DP systems into redundant equipment groups.

- Loop power for shutdowns should not originate from common points in a manner that makes cable route a potential single point failure for fire.
- Suitable voting on multiple circuits. Signals that initiate an alarm but not a shutdown if they disagree.
- Fail safe mode of ESD field stations should be to not shutdown on loss of power or communications.
- ESD pushbuttons should be provided with.
 - Cover
 - Signage
 - Key switch inhibit – where appropriate.
- Manually operated ‘inhibit function’ of robust design on all ESD 0 or ESD 1 (if there is a cascade to blackout).
- The indication that the inhibit function is in the ‘inhibit position’ should be based on confirmation that the function is active from the controller and not just the switch position.

C.2.4.3 Fire dampers for generator combustion air need not be closed as part of ventilation shutdowns if they are designed such that they only provide air to the engine and compartment ventilation can be shut down separately. ‘Rig savers’ or equivalent are used to provide individual engine protection on MODUs.

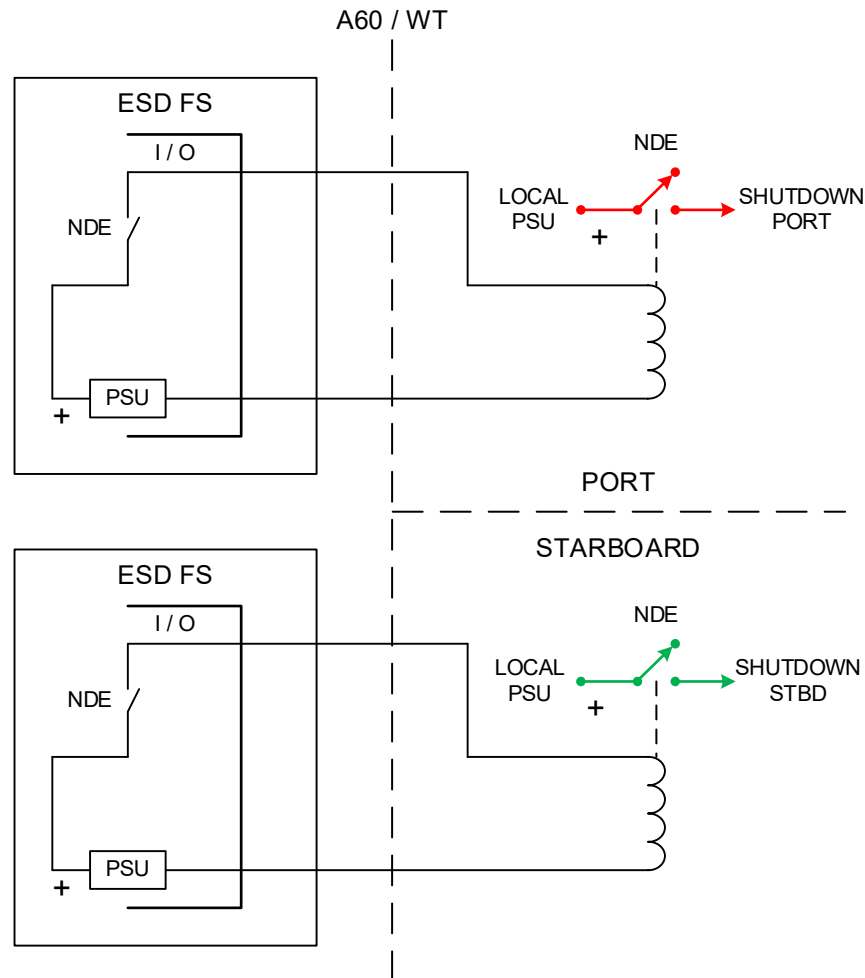
C.2.4.4 Fire dampers for combustion air may be of the normally de-energised type which implies that it takes power to close them and therefore they remain open on loss of that power.



Appendix C - Figure 5 Simplified Schematic of a Distributed Emergency Shutdown System (Propulsion Part)

C.2.5 SOURCES OF LOOP POWER

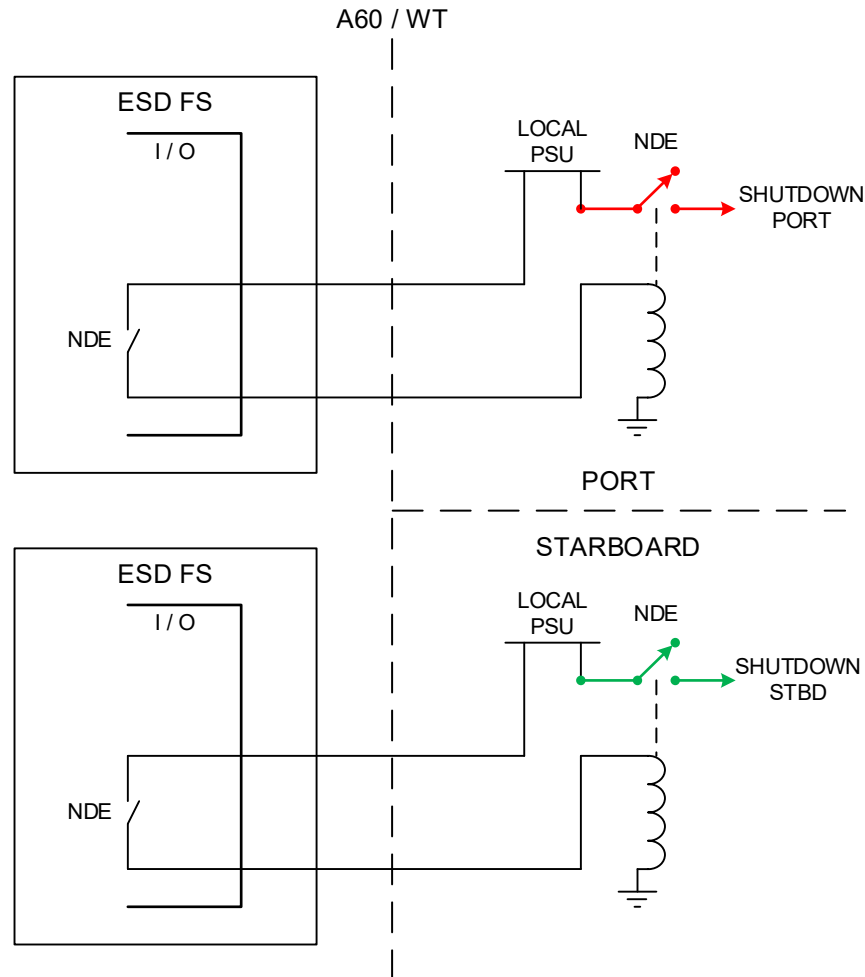
C.2.5.1 One issue which is often the subject of discussion at design reviews of shutdown systems relates to the source of loop power and the effect the choice has on effects of failures in common cable routes. This is normally done correctly by the major suppliers but should be checked. The example in Appendix C - Figure 6 below shows a DP equipment class 3 design where shutdown signals originate in a common compartment and a common cable route eventually separates at the A60/WT divide to the port and starboard switchboard rooms.



Appendix C - Figure 6 Preferred Method - Loop Power Originates at ESD Field Station

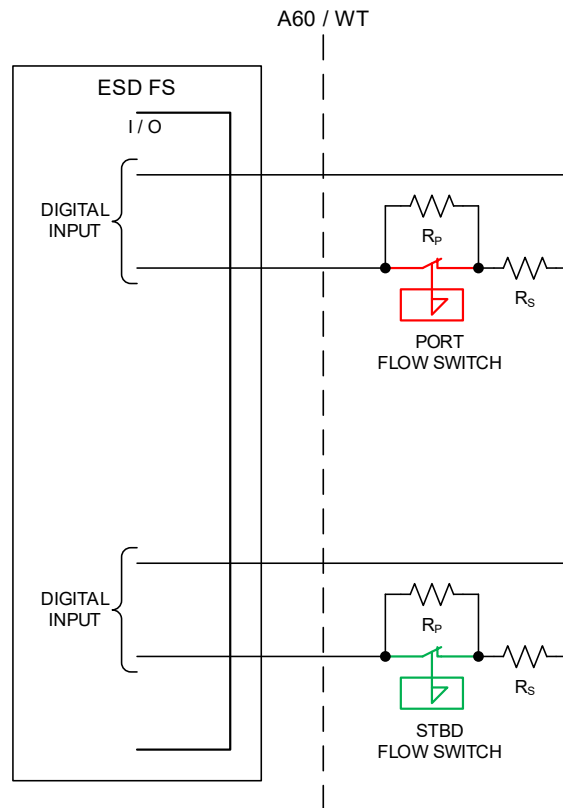
C.2.5.2 Although the shutdowns have been separated into two different field stations, the common cable route introduces some degree of commonality. However, by sending loop power from the field station any short circuit in the damaged cables will operate the fuses on the power supplies and no propulsion shutdown should result. The fire can then be dealt with by the measures appropriate to its location. Providing fire and watertight segregation of the shutdown system and its cables along the lines of the redundancy concept would also have enhanced the robustness of the design but this practice is not yet universal.

- C.2.5.3 Appendix C - Figure 7 illustrates the other possibility which is to send the loop power from the switchboard power supply into the common space containing the shutdown systems. In this case, fire damage in the common cable routes effectively completes the circuits and shuts down the port and starboard power systems. Although the example discussed here is related to the shutdown system, similar issues are encountered in other systems such as power management system and remote valve control or thruster emergency stops where cables from redundant equipment are brought to a common point.



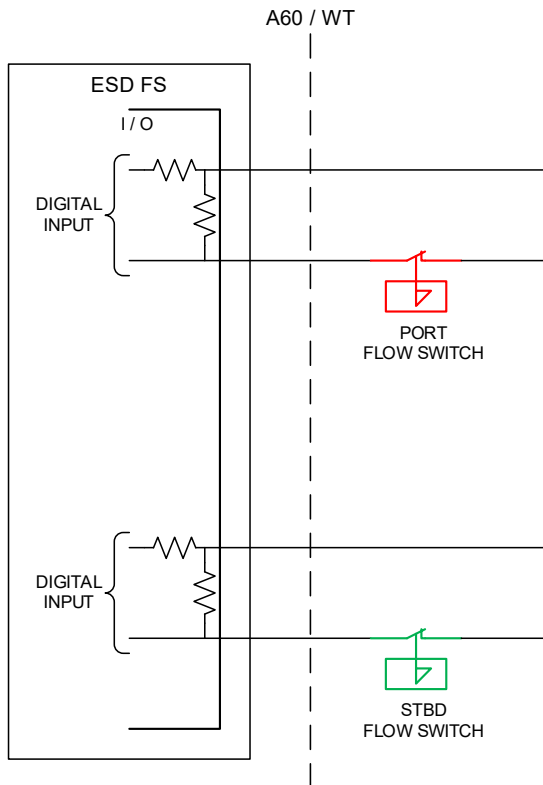
Appendix C - Figure 7 Sending Loop Power from Switchboard End

- C.2.5.4 **Line Monitoring:** Line monitoring is a popular method of reducing the risk that cable faults cause by fire, mechanical damage, insulation failure or broken conductors will initiate an unwanted control system response. The principle of operation is that the control system will only respond to a defined step change in loop current between two defined values and not to any other current level as might be caused by a short circuit or open circuit or earth fault. These defined values are created by a series and parallel resistance installed across the switch contacts. The change in current is measured by an analogue I/O card or a dedicated switch amplifier. Appendix C - Figure 8 shows a typical installation. The example shows flow switches but could equally apply to shutdown push buttons.



Appendix C - Figure 8 Preferred Method - Line Monitoring Resistors Installed at Switch

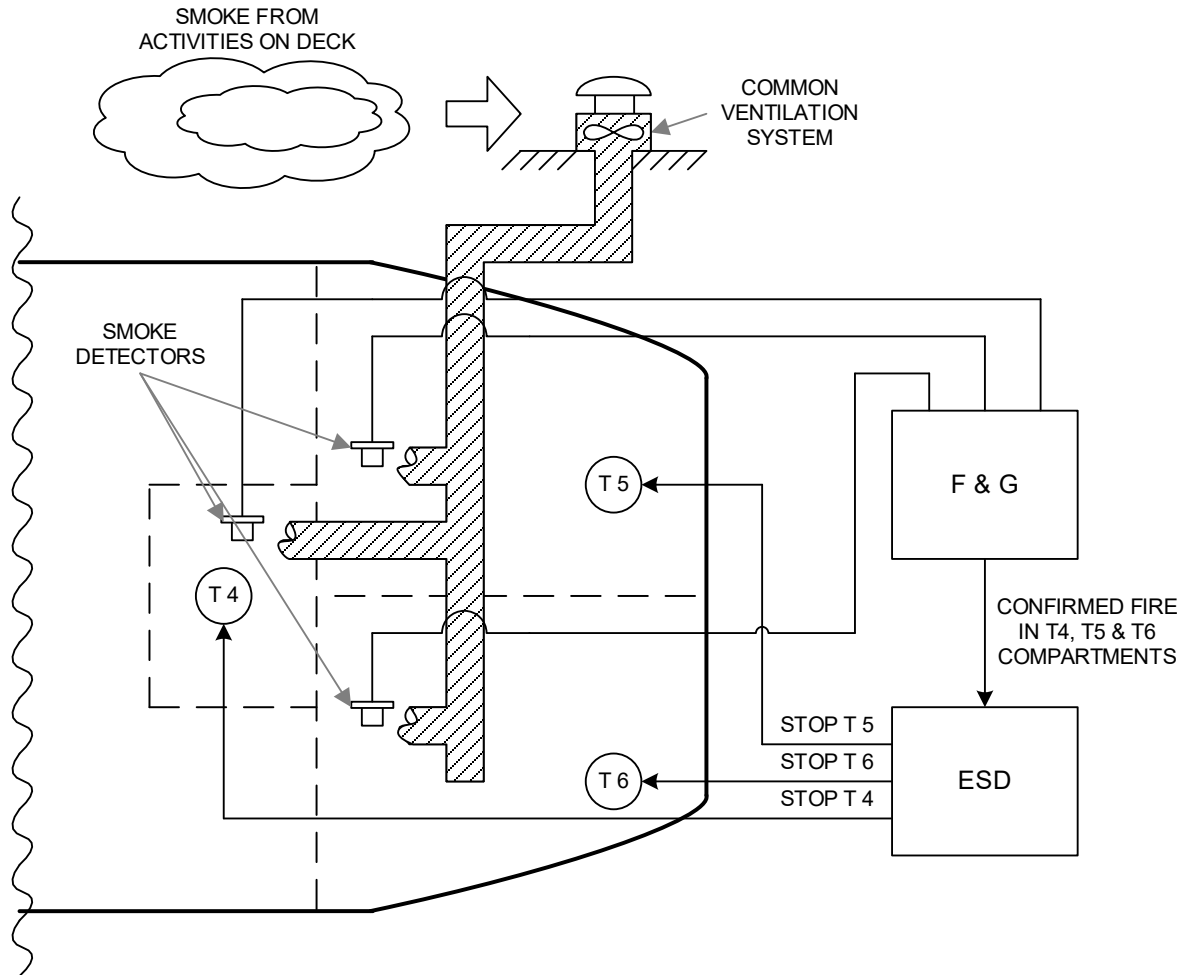
- C.2.5.5 Appendix C - Figure 9 shows an alternative location for the resistors which will work effectively as far as creating the desired current step is concerned but does not protect the cable run that crosses the A60/WT boundary. Why this alternative location would ever be chosen is unclear but when cables cross between one vendor's scope of supply and the other and one vendor has omitted to supply switches prepared with resistors, it may be a solution that allows the other vendor to commission the system with the required functionality. Unfortunately, the effect on the system's fault tolerance to fire damage is not addressed.



Appendix C - Figure 9 Line Monitoring Resistors Installed at I/O Card

C.2.6 CONFIRMATION OF FIRE DETECTION AND GAS INGRESS

- C.2.6.1 One of the most significant vulnerabilities in the application of ESD systems to DP vessels is the robustness of measures used to confirm the presence of gas or the occurrence of fire. Voting on multiple sensors is often used in the design of shutdown systems and this has the potential to enhance robustness. This potential may be overlooked, and lack of implementation precludes realisation of robustness.
- C.2.6.2 In DP equipment class 3 designs, the physical separation provided by the fire resistant and watertight bulkheads and deck heads is defined by the split in the DP redundancy concept and makes it possible to arrange ESD and F&G in a manner that supports the objective of providing a defined post worst case failure DP capability. Unfortunately, this objective can be defeated by:
- C.2.6.3 Commonality in ventilation systems that cross the A60/WT divisions
- C.2.6.4 Insufficient separation of air intakes and jalousies for compartments intended to provide redundancy.
- C.2.6.5 Appendix C - Figure 10 shows the compartment and ventilation arrangement for the aft thrusters in a DP equipment class 3 drillship. Although the thruster compartments are separated by A60 rated watertight bulkheads, all three are served by a common ventilation system. Smoke or dust drawn in from activities on deck contaminated the air in all three thruster compartments activating the smoke detectors. The cause and effects matrix for F&G detectors was written to shut down the thrusters on detection of a confirmed fire. Setting aside any operational barriers that could have been used to mitigate this risk the design has two main vulnerabilities:
- A common ventilation system connecting redundant DP equipment groups.
 - Lack of robustness in detecting a confirmed fire.



Appendix C - Figure 10 Common Ventilation Systems Defeats Redundancy

- C.2.6.6 In DP equipment class 2 designs it is even more difficult where collocation of DP related equipment is permitted by the rules. In such circumstances it is even more important to have a robust fire and gas detection strategy that can confidently distinguish between a real fire or gas release and conditions with the potential to mimic the same conditions.
- C.2.6.7 Gas detectors may be provided for flammable and toxic gas. In general, gas detectors have a better reputation for reliability in detection as they are designed to detect the presence of the hydrocarbon in the air. There is no direct equivalent for fire detectors and the existence of a fire is inferred from its effects including:
- Smoke
 - Heat
 - Light – IR/UV.

- C.2.6.8 Once it reaches a critical concentration, the risk of explosion from gas drawn into machinery or other spaces is such that it is reasonable to take immediate action to isolate sources of ignition. In DP class 2 designs this may mean accepting the consequences of a loss of position if gas is detected in a space containing more than one redundant group. Although gas detectors themselves have a good reputation for reliably reporting the presence of gas there are other vulnerabilities associated with the I/O cards and field stations which increase the risk of false indication. Thus, in any space containing elements of more than one redundant DP equipment group it would be prudent to have three gas detectors at the air intakes and confirm the presence of gas on two out of three detectors indicating the presence of hydrocarbons. Each detector would be interfaced to a separate I/O card in a redundant field station and different field stations if practical. Two out of three voting provides a reasonable compromise between a hidden failure preventing legitimate gas detection and a faulty detector or I/O channel causing a spurious shut down and loss of position.
- C.2.6.9 For fire detectors it is even more important to have a robust detection system. If an ESD is to be initiated by a confirmed fire using multiple detectors there should be some diversity in the detection method. It is prudent to initiate an alarm on any detector activating to initiate investigation by the fire team but reserve initiation of executive action by ESD only when fire risk confirmed by multiple and diverse detection methods. The need for diversity in fire detection is highlighted by the number of DP incidents associated with false activation of ESD by smoke or dust from activities on deck being drawn into several compartments or a common ventilation system serving redundant DP equipment groups.

C.2.7 INTERNAL EQUIPMENT FIRE DETECTORS

- C.2.7.1 The convertor cabinets for Variable Speed Drives (VSD) may be fitted with internal fire detectors designed to shut down the thruster drive if smoke is detected. This can introduce vulnerabilities similar to those that may be present in the ESD system. Typically, shutdown is based on a single smoke detector. The ventilation fans on the VSD cabinets normally draw their air supply from the machinery space. DP equipment class 2 designs with redundant equipment groups in the same compartment are particularly vulnerable to this. Failure effects exceeding the severity of the worst case failure design intent have resulted from something as simple as the smoke produced from a slipping V-Belt on a service air compressor in the same space.

C.3 OTHER EXTERNAL INTERFACES

C.3.1 EXTERNAL FORCE COMPENSATION

C.3.1.1 External force compensation describes the process whereby the external force acting on the DP vessel is measured and therefore known separately from the environmental force. This value is then included in the DP calculation and treated as a force feed forward. This feature is used to account, for example, for the impact of pipe tensions in pipe layers and hawser tension in shuttle tankers etc. on station keeping. Generally, the signals originate at load cells or other measuring devices and are often 4-20mA current loop signals. In some designs, the interface may be dual redundant.

C.3.1.2 Because the industrial mission equipment and load is often unavailable during DP FMEA proving trials and annual trials, the failure effects of these signals are seldom tested, nor the ability of the DP control system to reject erroneous readings. Because of the uncertainty and lack of predictability associated with these interfaces it is not unusual to require a manual force input mode during critical operations (CAM). Automatic correction may be acceptable in TAM. If the intent is to use this feature in automatic mode, the design of the interface should be subject to a system engineering approach validating redundancy and fail-safe response to failure by analysis and testing.

C.3.2 DRAUGHT SENSORS

C.3.2.1 A manual input of draft is typically sufficient for DP control systems. With the advent of Vessel Management Systems (VMS), automatic draught measurement and input into the DP system is not uncommon as a feature of some DP control systems. The signal may be provided by hardware and sensors that form part of the ballast or tank gauging systems. This can be mis-categorised as 'not part of the DP system'.

C.3.2.2 Industry experience has recorded instances of such installations being problematic. Loss of position has resulted when the DP control system received erroneous information directly from sensors about the draught of the vessel. This corrupted the mathematical model leading to a drive off.

C.3.2.3 Typically, there can be several draft sensors interfaced to the DP system at points around the vessel. The DP system will normally use the average of all sensors in its computation.

C.3.2.4 Model data such as mass and drag are tuned at pre-defined draughts during sea trials. Correct draught sensor signals are essential to the interpolation process of the mathematical model. The draught signal determines to some extent how much of the combined force acting on the vessel is assumed to be from tidal current and how much is from wind. If the wind and the current are from significantly different directions the thrust solution will be in error and the vessel will drive off.

C.3.2.5 On vessels with an integrated automation system, it is common practice for the draught sensors to be connected to a convenient field station. The DP control system then receives the draft information by way of the dual Ethernet connecting the automation system to the DP control system.

C.3.2.6 The following vulnerabilities have been identified and can be avoided in future designs:

- All sensors connected to the same field station.
- No logical bounds on signal value, thus out of range signals can have a severe effect (e.g. negative draught).
- No analysis of draught sensor arrangement or failure modes in FMEAs or testing at proving trials.
- No real justification for requiring an automatic input of draught.

C.3.3 POWER CONTROL FOR INDUSTRIALS CONSUMERS

- C.3.3.1 The vast majority of DP vessels are designed around diesel electric propulsion systems based on the power station concept. This design provides all power for dynamic positioning and for hotel and industrial consumers from a combined source that may be operated as a single power system or as two or more independent and isolated power systems. DP vessel with large industrial loads such as drilling, or pipe laying may have a dedicated power management system for the industrial consumers which is interfaced to the power management for the DP system so that functions such as load shedding may be prioritised.
- C.3.3.2 Some industrial consumers such as active heave drawworks may need to regenerate significant amounts of power either to the main power system or to dynamic braking resistors or a combination of both.
- C.3.3.3 Few if any of these vessels can operate with sufficient spinning reserve to prevent overload of the power plant following the worst-case failure therefore the redundancy concept depends on shedding away the industrial consumers in a controlled manner but rapidly when required.
- C.3.3.4 Information on the amount of power that can be safely drawn from and regenerated to the vessels power systems from the industrial consumer may be communicated over analogue or serial data links. As this link acts as part of a protective function it is important that it fails in a predicable manner and that there is no potential for effects exceeding the severity of the worst-case failure design intent.
- C.3.3.5 Typical issues to be considered include the failure modes of analogue 4-20mA loops used to indicate power available and power consumed for industrial consumers. These links typically fail out of range and provide an alarm but what condition should the PMS adopt? Whatever strategy is developed it should be robust, well explained, analysed in the DP system FMEA and proven at commissioning and trials.
- C.3.3.6 All such links should provide an unambiguous alarm on failure. Consideration should be given to providing redundancy and voting in these links to allow continued operation.
- C.3.3.7 Serial links may fail to the last valid data value. This may affect the DP system and industrial consumers.
- C.3.3.8 Some designers rely upon the frequency of the power waveform in a common power system operating in speed droop for load sharing to also indicate power plant loading. This is a very robust way of communicating power plant load which can also be used to trigger load shedding at defined levels. No control links are required to achieve this.
- C.3.3.9 In some drillship designs the drawworks is given priority for power over the thrusters when the active heave drawworks is operating in lock-to-bottom mode. There is variability in the configuration of this lock-to-bottom mode across vessels. It is essential to fully understand and document vessel specific information and ensure familiarisation of the crew. In some designs, priority for power is only transferred from the drawworks to the thrusters if the vessel is not holding position within a defined watch circle. The issue here is not the relative merits of this particular function but that it introduces additional control links to the DP system which need careful consideration regarding their failure modes and fail-safe condition. Additionally, power may not be available to thrusters without deliberate intervention.

C.3.4 POWER DISTRIBUTION FOR INDUSTRIAL AND HOTEL LOADS

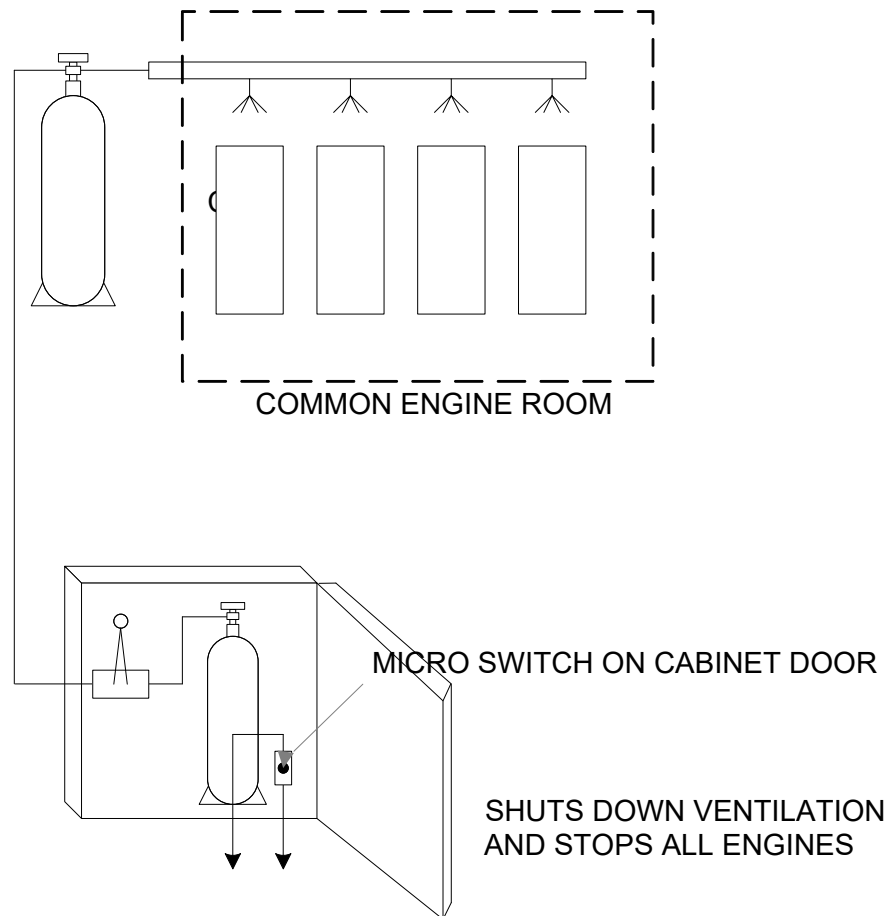
C.3.4.1 Power consumers not directly related to DP can also be considered to be an external interface with the potential for failure effects to adversely impact the operation of the DP system. It is relatively straight forward to divide up power and propulsion systems for DP along well-defined lines. The same is not always true of supplies from accommodation or industrial consumers and these often introduce unwanted asymmetries in the load or create common points between redundant equipment groups. Common points can be created by features such as dual supplies; auto-changeovers and colocation of non-DP related consumers within the same A60/WT zone in the case of DP equipment class 3 designs. In earlier rules for DP class 3 designs it was accepted that the influence of their failure on the DP system should be demonstrated by analysis but in more recent revisions, the presence of such features triggers similar requirements for analysis and testing that is more akin to that required to prove the fault tolerance and fault ride-through capability of a common power system even though the normal operating configuration is with the main busties open.

C.3.4.2 Methods that can be used to address these issues include:

- Where there is a need to provide a dual supply into a common compartment, determine whether it is necessary for both supplies to be live at the same time. – If not, it may be possible to isolate one supply or arrange for switching at the supply end (switchboard) rather than at the consumer. Issues related to transfer of fault should be addressed.
- Maintain the same split in industrial and hotel distributions as is provided for DP related consumers to as low a voltage distribution level as is practical. This will avoid issues of load asymmetry particularly when operating the power plants as independent power systems.
- Provide power to non-DP related loads from their own service transformers so that there is some impedance between DP and non-DP related consumers. This is particularly important for industrial power distributions on deck which may be subject to routine earth faults.
- A few DP applications may justify a separate industrial power plant. Some vessels have been built with this philosophy.

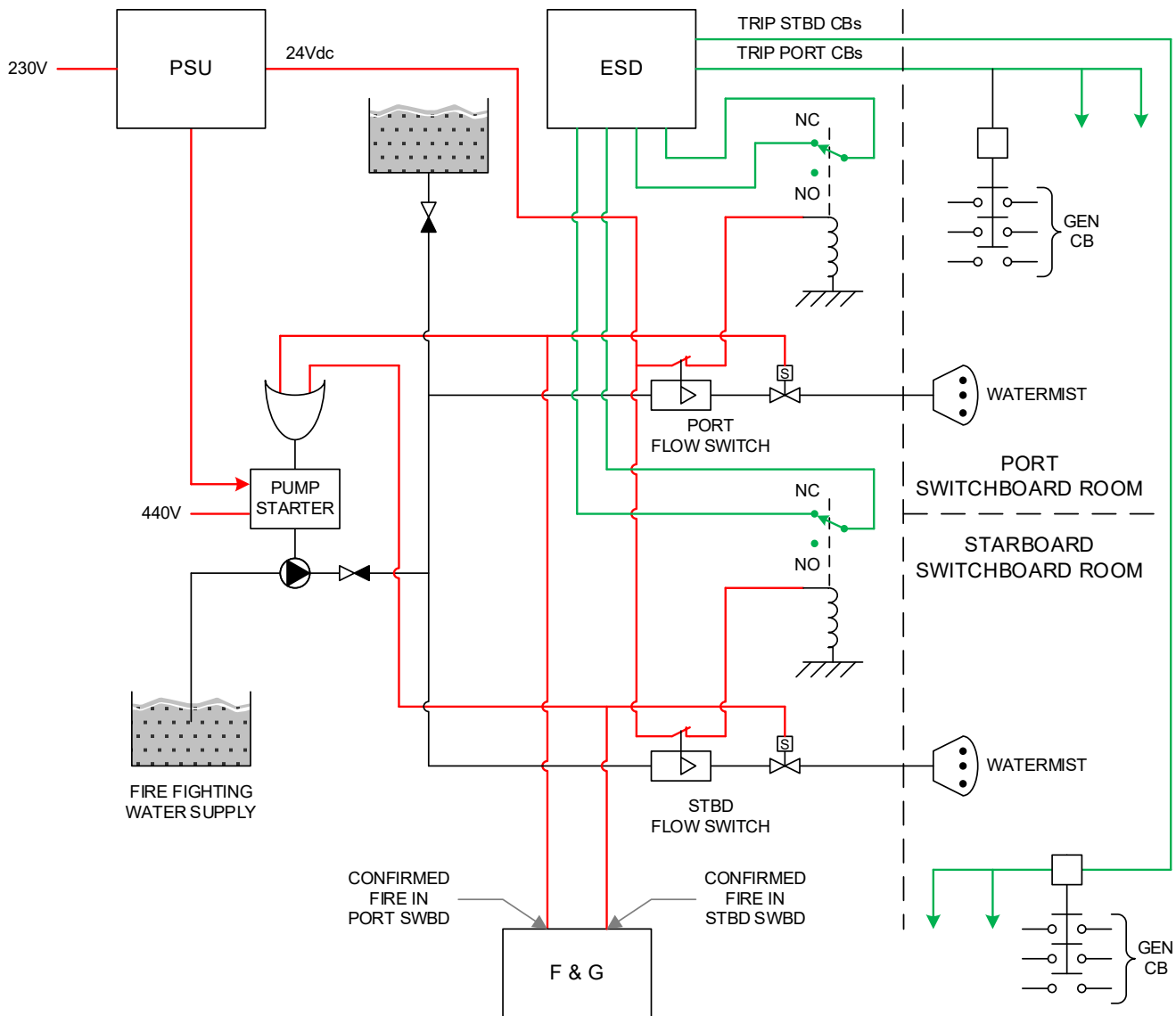
C.3.5 FIRE FIGHTING SYSTEMS

C.3.5.1 CO₂ systems and similar gaseous extinguishing mediums have a reputation for reliability and there are very few, if any reports of unscheduled release of fire-fighting agent on DP vessels. The fire-fighting system should be arranged to allow fires in one DP equipment group to be addressed without significant impact on other DP equipment groups. This is easier to achieve on DP class 3 vessels. The opportunities for the design of CO₂ systems to compromise DP redundancy concepts more often occurs in the conversion to commercial vessels for DP or repurposing of older vessels, particularly where some part of the original power plant is retained along with its fire-fighting installation. In such cases it is possible for unsuitable functionality to remain undetected. Examples such as that shown in Appendix C - Figure 11 include micro-switches intended to detect the opening of pilot cylinder cabinet doors. This feature has been used to stop fans, close fire dampers or even stop engines in preparation for the release of CO₂ into the common engine room space on DP equipment class 2 vessels.



Appendix C - Figure 11 Fire - Fighting System with Ventilation and Engine Shutdown

C.3.5.2 Water mist is a relatively recent addition to fire-fighting systems on DP vessels and has brought with it a number of problems associated with unacceptable commonality in the interface. Appendix C - Figure 12 shows a very simplified schematic intended to illustrate one particular design issue. In the example below, the F&G system was designed to initiate release of water mist in the engine room. At the same time, the ESD system was ordered to open the generator circuit breakers in the associated switchboard room. The command to open the circuit breakers originated at flow switches which detect the flow of water to the nozzle. Unfortunately, the design of the system was such that failure of the internal 24Vdc supply had a similar effect in so far as it caused the relays controlled by the flow switches to de-energise and indicate to the ESD system that the flow switch was active even though it had not changed state. Because all the relays changed state on loss of 24Vdc power the ESD system tripped all the generator circuit breakers and the vessel blacked out.



Appendix C - Figure 12 Simplified Schematic of Water Mist System

- C.3.5.3 Fire and watertight dampers: There are various designs of fire dampers including, variations on electrically operated and air operated designs. Watertight dampers are found in semi-submersible designs to limit the effects of down flooding. Motor operated versions tend to fail as set, but some units are effectively spring operated and motor power or air power is simply used to charge the actuating spring. These units tend to be 'trip to close'. Air operated dampers may fail to any condition depending on designs. The use of non-return valves to hold 'failed closed' dampers open is vulnerable to hidden failures of such valves. Local air receivers for each damper or group of dampers may improve this.
- C.3.5.4 In the case of ventilation dampers, the effect of closure is not usually immediate and as long as there is an alarm and a means of opening the damper again, before equipment overheats, the failure modes of these dampers are less significant. A great deal of modern power and propulsion machinery is water cooled which limits heat rejection to the machinery space and thus it takes a long time for the compartment temperature to rise to unacceptable levels.

C.3.5.5 For combustion air dampers there are reasons to select a 'fail as set' damper. Experience from trials suggests that closing fire dampers may not always create sufficient seal to power limit engines but it can create a very substantial drop in engine room pressure which has disadvantages related to:

- Malfunction of crank case differential pressure detectors leading to multiple engine shutdowns exceeding WCFDI.
- Has been implicated in a number of fatalities related to doors slamming open or closed.

C.3.5.6 MTS DP Vessel Design Philosophy Guidelines recommend 'Fail as Set' for combustion air dampers.

C.3.6 COMMUNICATIONS AND NAVIGATION EQUIPMENT

C.3.6.1 North speed correction: An interface to a navigation GPS may be provided on gyros for correcting the deviation associated with the vessel's north speed. If one navigation GPS signal is interfaced to all three DP gyros this represents a common point by which a faulty GPS signal could affect all three heading signals to DP. Such incidents have happened and most DP vessels owner isolate this facility on DP if it is provided.

C.3.6.2 Shut down thrusters above defined hull speed: Retractable azimuth thrusters may have limits on speed through the water in the extended position. In at least one vessel design a signal from the navigation GPS was used to provide a vessel speed signal to the thruster drive which would shut down the thruster when the limiting speed was exceeded. Failure of the power supply to the navigation GPS was found to cause all the retractable thrusters to stop with effects exceeding the severity of the worst case failure design intent. Clearly this is an example of unacceptable commonality.

C.3.6.3 Gyro repeater switches: The DP gyros are often used to supply heading information to other systems such as radars, ECDIS, bridge wing repeaters, entertainment/ communications systems and so on. A gyro switching device may be provided to allow different gyros to provide the signal to these services. These non-DP related heading consumers represent an external interface and the gyro switching unit represents a common point between redundant equipment groups that should be analysed in the DP FMEA.

C.3.7 ROLL STABILISATION

C.3.7.1 The characteristics of cycloidal thrusters allows them to be used for roll stabilisation in OSVs and other DP vessels because they can reverse thrust direction very quickly. The roll stabilisation function is active at the same time as DP and is usually a standalone control system which superimposes stabilisation commands upon those issued by the DP systems such that the resultant thrust vector satisfies both the requirements of DP and stabilisation. The roll stabilisation interface should be analysed in the DP FMEA from both a redundancy and fail-safe perspective.

C.3.8 GROUP EMERGENCY STOPS

C.3.8.1 Group emergency stops are fitted to many DP vessels and share some of the same problems as the more sophisticated or extensive ESD systems found on MODUs. Group emergency stop systems are provided to assist in firefighting and allow the operator to stop groups of consumers which may include DP related consumers such as:

- Ventilation fans.
- Electric fuel pumps.
- Hydraulic pumps for CPPs and azimuthing gear.
- Lubricating oil pumps.

-
- C.3.8.2 The design of the group emergency stop system should be aligned with the overall split in the DP redundancy concept be analysed in the DP system FMEA. Stop groups should not, in general, include consumers from more than one redundant DP equipment group such that it is possible to stop one group at a time without loss of position.
 - C.3.8.3 Classification societies may have particular requirements in relation to the nature of the control loops used. Typically, propulsion related equipment will usually be controlled by a normally open, Normally De-Energised (NDE) control loop with appropriate line monitoring for push buttons and power supply monitoring. A shunt trip coil is normally fitted to trip the consumer feeder circuit breaker on application of power. Normally Energised circuit should not normally be used to trip DP related consumers due to concerns about unreliability related to vibration of relay contacts and wire breaks.
 - C.3.8.4 External interfaces to the group energy stop system should also be considered. Smoke detectors may be interfaced to operate the group emergency stop system automatically in some designs. The nature of this interface should reflect and align with the overall split in the redundancy concept and fail to the safest conditions with appropriate alarms.
 - C.3.8.5 DP FMEA proving trials should confirm the effects of executive actions taken by group emergency stops and any fire detection systems that are interfaced to them.