TECHNICAL AND OPERATIONAL GUIDANCE (TECHOP)

TECHOP_ODP_13_(D) (CONTROL POWER SUPPLIES AND AUTO CHANGEOVERS)

NOVEMBER 2017

CONTENTS

SECTION		PAGE
1	**INTRODUCTION - TECHOP (TECHNICAL AND OPERATIONAL GUIDANCE)**	**4**
1.1	PREAMBLE	4
1.2	TECHOP_ODP	4
1.3	TECHOP_GEN	4
1.4	MTS DP GUIDANCE REVISION METHODOLOGY	5
2	**SCOPE AND IMPACT OF THIS TECHOP**	**6**
2.1	SCOPE	6
2.2	IMPACT ON PUBLISHED GUIDANCE	6
3	**CASE FOR ACTION**	**7**
3.1	DP INCIDENTS	7
3.2	EXAMPLE INCIDENTS	7
3.3	FAULT TOLERANT SYSTEMS BASED ON REDUNDANCY	8
3.4	CROSS CONNECTIONS IN CONTROL POWER SUPPLIES	9
3.5	FAILURE MODES OF DIODES	9
3.6	DC TO DC CONVERTERS	10
3.7	GROUNDING / EARTHING STRATEGIES	11
3.8	CROSS CONNECTIONS CREATED BY DUAL SUPPLIED DIODES	12
3.9	DUAL SUPPLIES - MITIGATION OF FAILURE EFFECTS	14
3.10	CROSS CONNECTIONS CREATED BY AUTO CHANGEOVERS	19
3.11	AUTO CHANGEOVERS - MITIGATION OF FAILURE EFFECTS	23
3.12	CROSS CONNECTIONS CREATED BY GROUND FAULTS	24
3.13	MITIGATION OF GROUND FAULTS	26
4	**SUGGESTED IMPLEMENTATION STRATEGY**	**27**
4.1	GENERAL	27
4.2	IDENTIFY OPPORTUNITIES FOR IMPROVEMENT	27
4.3	BUILDING CONFIDENCE	28
5	**MISCELLANEOUS**	**29**

FIGURES

Figure 3-1	Generalised DP Redundancy Concept	8
Figure 3-2	DC to DC Converter	11
Figure 3-3	Un-Earthed and Earth-Referenced DC Power Supplies	12
Figure 3-4	Simple Dual Supply Arrangement Using Diodes	12
Figure 3-5	Control Power Supplies without Cross Connections	15
Figure 3-6	Individual Supplies	16
Figure 3-7	Separating Main and Backup Supplies	16
Figure 3-8	Multi Split Systems	17
Figure 3-9	Common Battery Bank	18
Figure 3-10	Auto Changeover	19
Figure 3-11	LV Power Distribution System - Backup Supplies from Emergency Switchboard	20
Figure 3-12	LV Power Distribution System - Backup Supplies from Other Redundant DP Group	22
Figure 3-13	Multiple Earth Faults Create Unpredictable Behaviour	25
Figure 3-14	Effects Exceeding WCFDI	25

1 INTRODUCTION - TECHOP (TECHNICAL AND OPERATIONAL GUIDANCE)

1.1 PREAMBLE

1.1.1 Guidance documents on DP, Design and Operations, were published by the MTS DP Technical Committee in 2011 and 2010, subsequent engagement has occurred with:

- Classification Societies (DNV, ABS).
- United States Coast Guard (USCG).
- Marine Safety Forum (MSF).

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.
- 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 two categories.

- TECHOP_ODP.
- TECHOP_GEN.

1.2 TECHOP_ODP

1.2.1 Technical Guidance Notes provided to address guidance contained within the Operations, Design or People (Future development planned by the MTS DP Technical Committee) documents will be contained within this category.

1.2.2 The TECHOP will be identified by the following:

TECHOP_ODP_SNO_CATEGORY (DESIGN (D), OPERATIONS (O), PEOPLE (P))

- EG 1 TECHOP_ODP_01_(O)_(HIGH LEVEL PHILOSOPHY).
- EG 2 TECHOP_ODP_02_(D)_(BLACKOUT RECOVERY).

1.3 TECHOP_GEN

1.3.1 MTS DP TECHNICAL COMMITTEE intends to publish topical white papers. These topical white papers will be identified by the following:

TECHOP_GEN_SNO_DESCRIPTION.

- EG 1 TECHOP_GEN_01-WHITE PAPER ON DP INCIDENTS.
- EG 2 TECHOP_GEN_02-WHITE PAPER ON SHORT CIRCUIT TESTING.

1.4 MTS DP GUIDANCE REVISION METHODOLOGY

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

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

1.4.3 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 AND IMPACT OF THIS TECHOP

2.1 SCOPE

2.1.1 TECHOP_ODP_13_(D)_(Control Power Supplies and Auto Changeovers) is intended to highlight the vulnerabilities that are introduced into DP redundancy concepts by cross connections in control power supplies including dual supplies and auto changeovers. Possible methods of eliminating or reducing the associated risk are suggested. See also:

- TECHOP_ODP_10_(D)_(EXTERNAL INTERFACES)
- TECHOP_ODP_11_(D)_(CROSS CONNECTIONS)

2.2 IMPACT ON PUBLISHED GUIDANCE

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

3 CASE FOR ACTION

3.1 DP INCIDENTS

3.1.1 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 which are not comprehensive and when addressed tend to 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 and there can be significant reluctance to allow failure effects to be proven by realistic testing. Many cross connections are installed with the intention of improving reliability. Although they may reduce the severity of the effects of higher probability failure modes, they rarely contribute to increased vessel availability because fault tolerance is lost as soon as power is provided by the backup supply. Responsible DP operators should bring the vessel to a safe position and suspend DP operations when fault tolerance is lost. Section 3.2 provides examples of failure effects associated with cross connections and auto changeovers that occurred in service or was revealed by DP FMEA proving trials.

3.2 EXAMPLE INCIDENTS

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 systems 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.

3.3 FAULT TOLERANT SYSTEMS BASED ON REDUNDANCY

3.3.1 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. 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. For this to occur as the result of a single failure 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 between redundant groups are the means by which failure effects propagate between redundant groups. Either the fault occurs in the cross connection itself or the failure effects propagate by way of the connection.

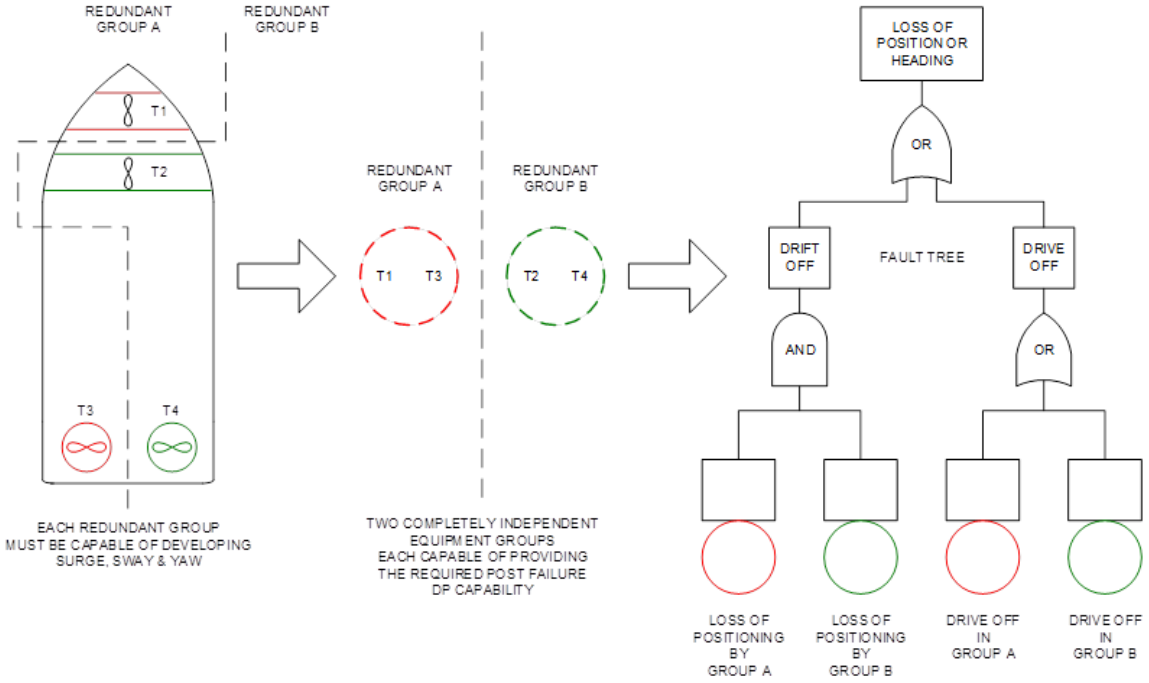

Figure 3-1 Generalised DP Redundancy Concept

3.4 CROSS CONNECTIONS IN CONTROL POWER SUPPLIES

3.4.1 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.
- **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.
- **Severity of failure effect**: The failure effects of losing a battery rectifier supply may equal the worst case failure design intent (WCFDI). See Section 3.8

3.4.2 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.

3.4.3 Most DP related equipment requires control power in some form or other and dc supplies are a popular way of fulfilling the requirements for clean power, fault ride-through capability and continuity of control power in a blackout. 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 but 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 should not be rationalised as a normal and acceptable occurrence.

3.4.4 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 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.

3.4.5 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. 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.

3.5 FAILURE MODES OF DIODES

3.5.1 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.

3.5.2 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.

3.5.3 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’.

3.5.4 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 more common than failure of the power electronic device itself.

3.5.5 Note:

- Cross connections introduce vulnerabilities associated with configuration errors and acts of mal-operations.
- Diodes do not significantly limit the fault current to a failed consumer nor the associated voltage dip experienced at the power supply terminals.
- Diodes have a low tolerance for overcurrent and can be damaged by the fault current before the overcurrent protection operates.
- Diodes do not provide galvanic isolation.
- 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.
- DC power supplies can be configured for load sharing but this is not typical in marine applications.
- Diode failure may go unnoticed (hidden failure). Subsequent failures may have effects exceeding the worst case failure design intent.

3.6 DC TO DC CONVERTERS

3.6.1 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 Figure 3-2. 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).
- 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).

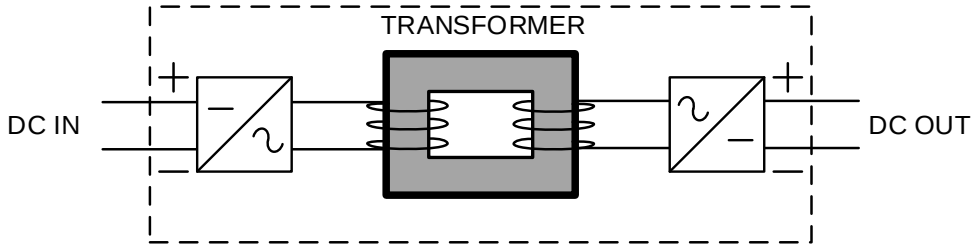

Figure 3-2 DC to DC Converter

3.7 GROUNDING / EARTHING STRATEGIES

3.7.1 **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.

3.7.2 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).

3.7.3 **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 < 1Ω.
- **Transformer earthing** – zig-zag 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.

3.7.4 **Direct current systems:** Refer to Figure 3-3**.** 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.

3.7.5 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.

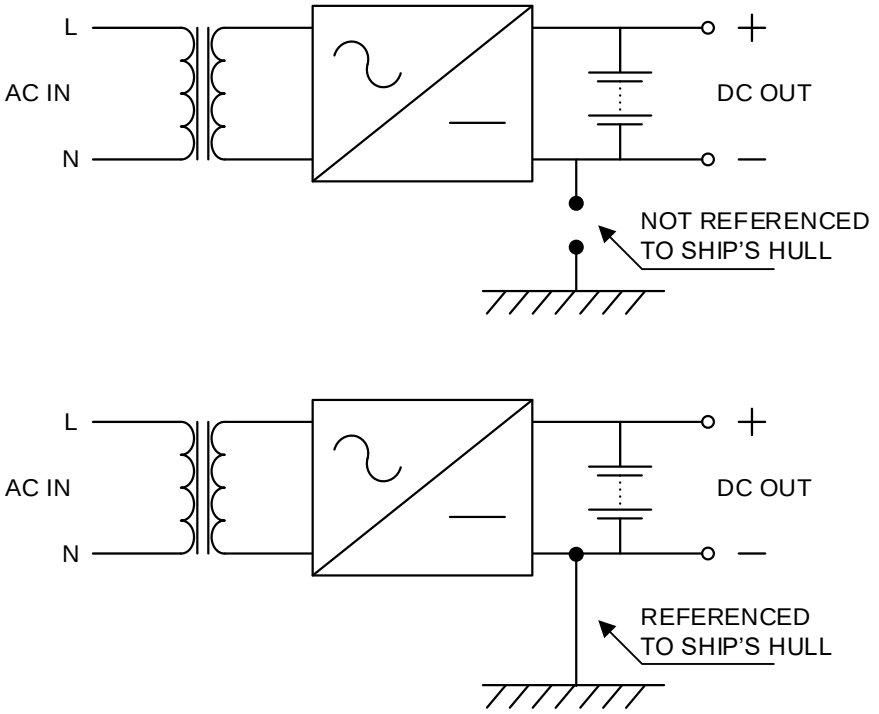

Figure 3-3 Un-Earthed and Earth-Referenced DC Power Supplies

3.8 CROSS CONNECTIONS CREATED BY DUAL SUPPLIED DIODES

3.8.1 Figure 3-4 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.

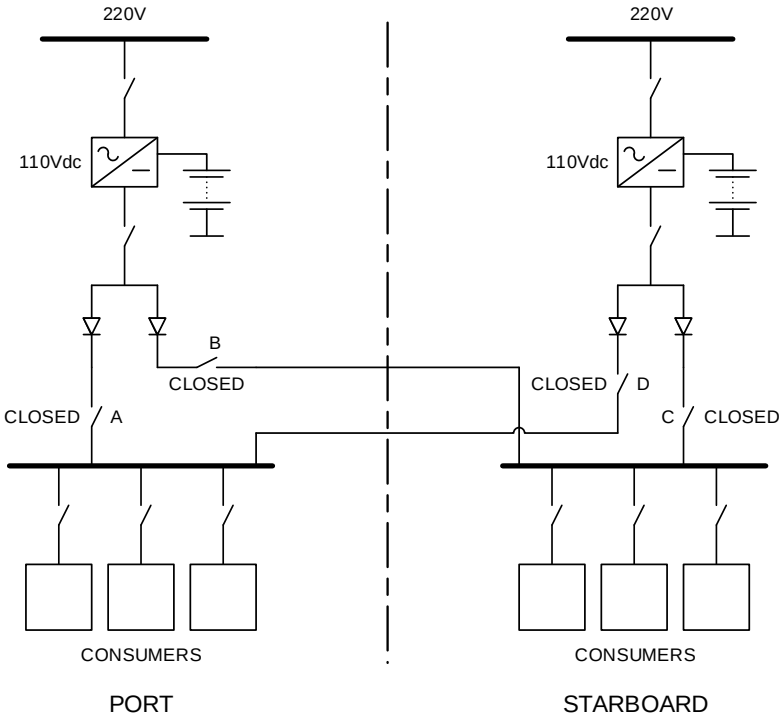

Figure 3-4 Simple Dual Supply Arrangement Using Diodes

3.8.2 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.

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 3.12.

3.8.3 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 Figure 3-4 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.

3.8.4 **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.

3.8.5 **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.

3.9 DUAL SUPPLIES - MITIGATION OF FAILURE EFFECTS

3.9.1 Deciding how to mitigate the undesirable effects of the failure modes listed in 3.8.2 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.

3.9.2 In Figure 3-4, 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.

3.9.3 It is possible to address both risks to some degree as shown in Figure 3-5. 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’.

3.9.4 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.

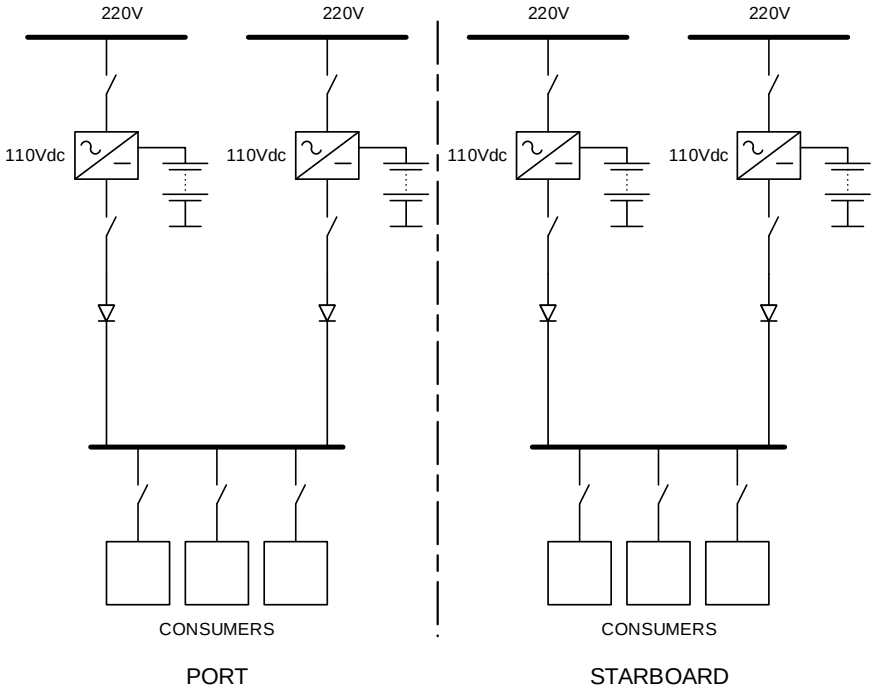

Figure 3-5 Control Power Supplies without Cross Connections

3.9.5 Figure 3-6 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.

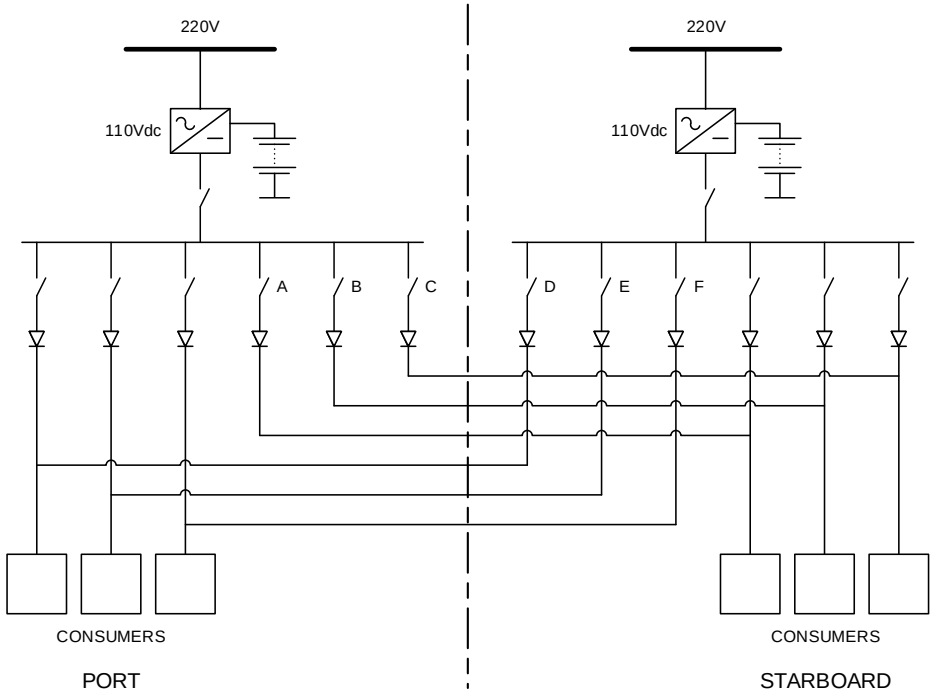

Figure 3-6 Individual Supplies

3.9.6 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 Figure 3-7. 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.

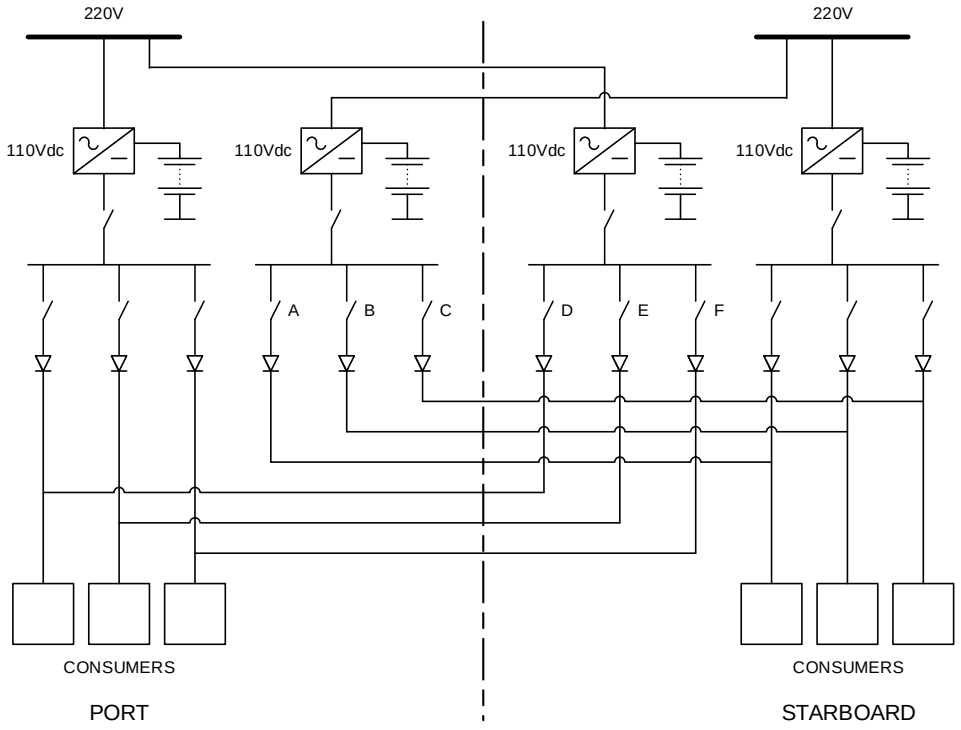

Figure 3-7 Separating Main and Backup Supplies

3.9.7 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. Figure 3-8 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.

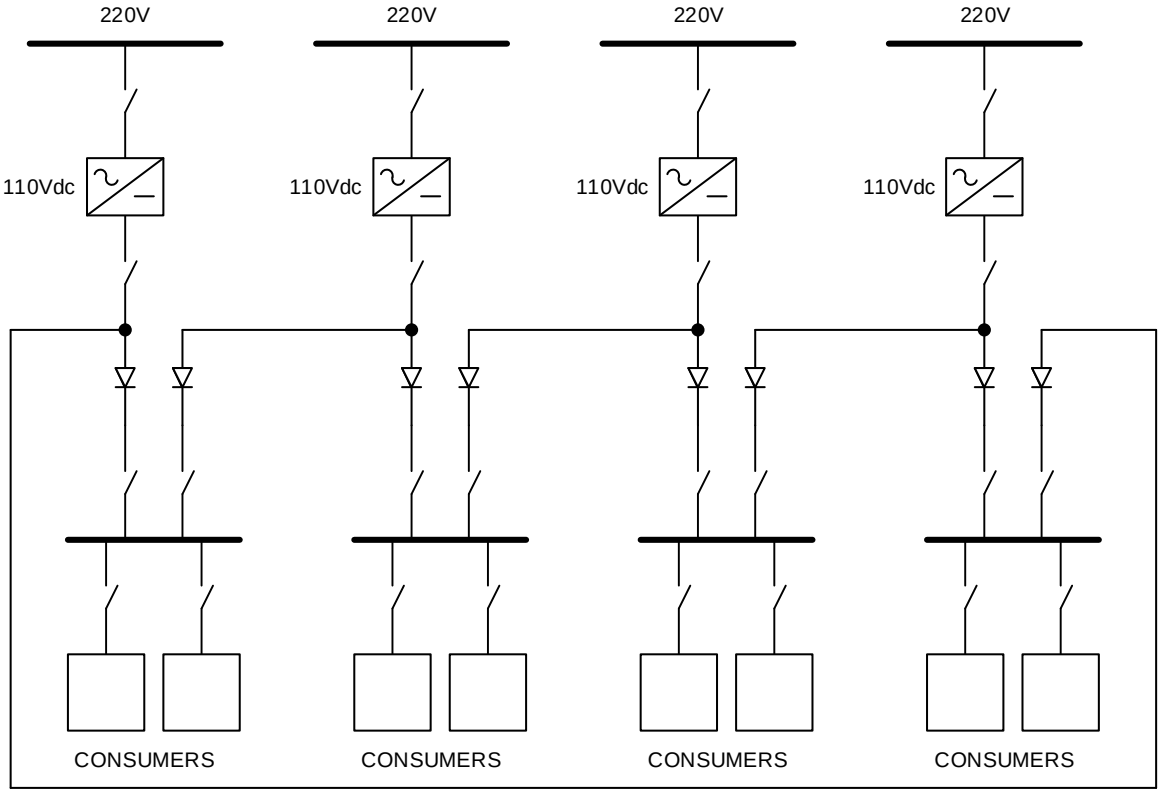

Figure 3-8 Multi Split Systems

3.9.8 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 risk are not being introduced as a result.

3.9.9 As an example, Figure 3-9 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.

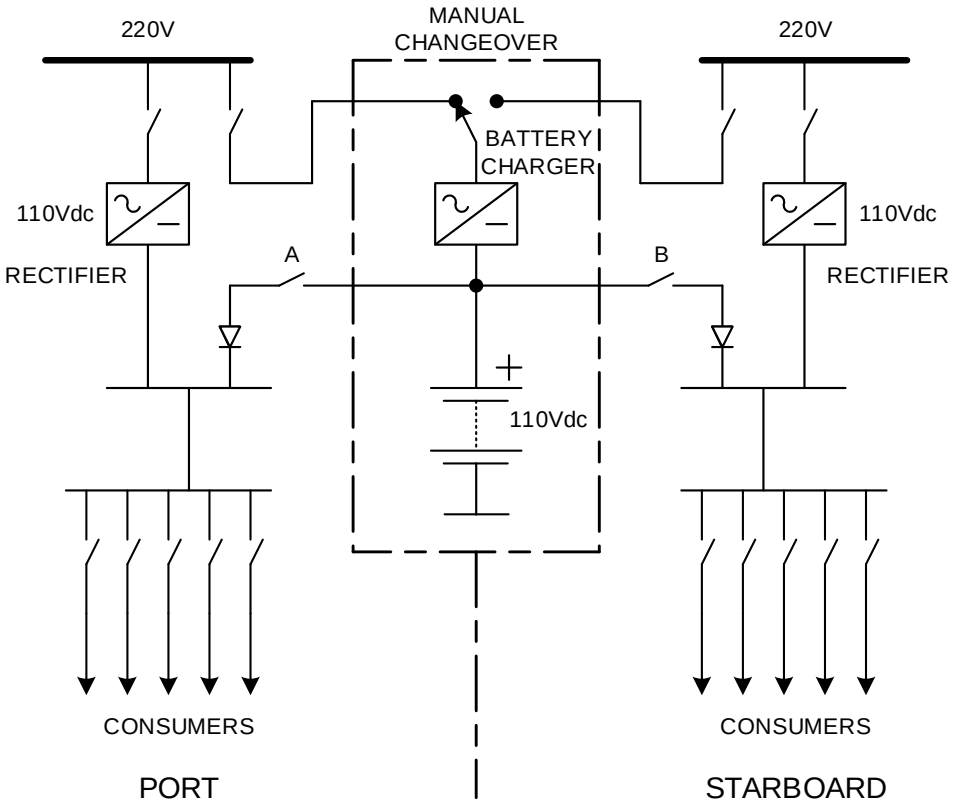

Figure 3-9 Common Battery Bank

3.10 CROSS CONNECTIONS CREATED BY AUTO CHANGEOVERS

3.10.1 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. Figure 3-10 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.

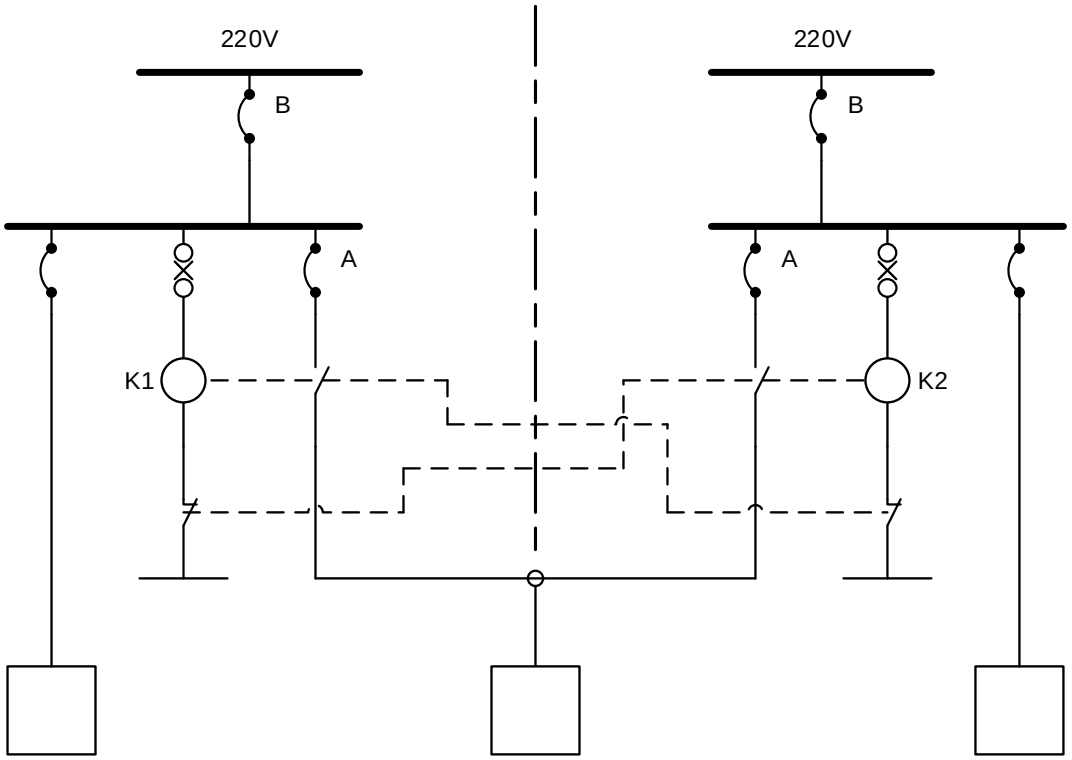

Figure 3-10 Auto Changeover

3.10.2 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

3.10.3 Typically, the normal source of supply for these consumers is from the same redundancy group as the equipment they serve.

3.10.4 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.

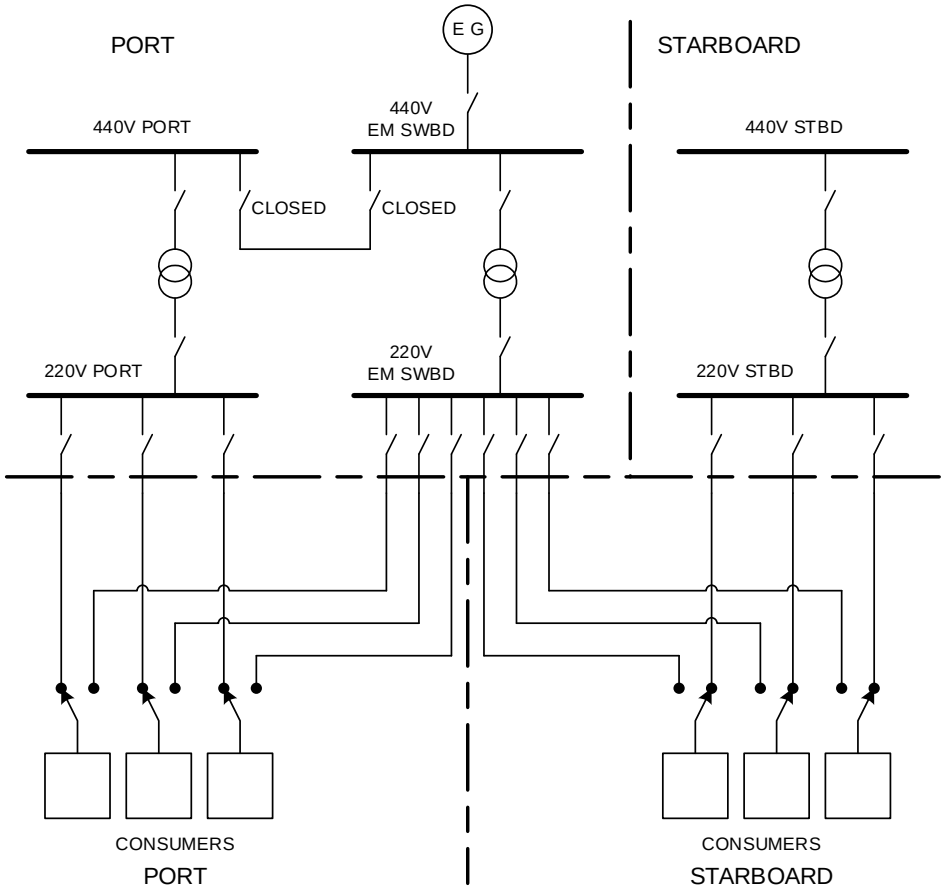

Figure 3-11 LV Power Distribution System - Backup Supplies from Emergency Switchboard

3.10.5 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 Figure 3-11, 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 many 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.

3.10.6 In the example in Figure 3-11, 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.

3.10.7 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.

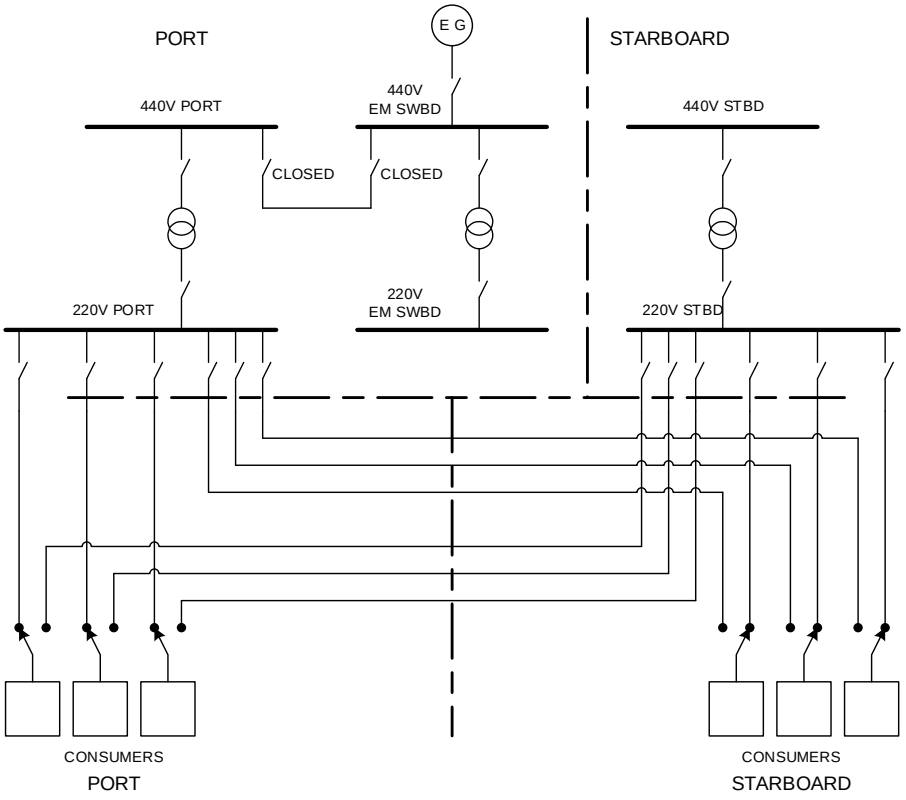

Figure 3-12 LV Power Distribution System - Backup Supplies from Other Redundant DP Group

3.10.8 Auto changeovers are also used to provide alternative supplies from other redundancy groups as shown in Figure 3-12. Similar arguments apply regarding the severity of any disturbance associated with fault transfer.

3.10.9 **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.

3.10.10 **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.

3.10.11 **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.

3.11 AUTO CHANGEOVERS - MITIGATION OF FAILURE EFFECTS

3.11.1 Potential fault propagation paths are more cost effectively eliminated at the basic design stage. Arrangements such as that shown in Figure 3-10 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.

3.11.2 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.

3.12 CROSS CONNECTIONS CREATED BY GROUND FAULTS

3.12.1 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 relativity 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.

3.12.2 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.

3.12.3 Figure 3-13 and Figure 3-14 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.

3.12.4 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.

3.12.5 In Figure 3-13, 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.

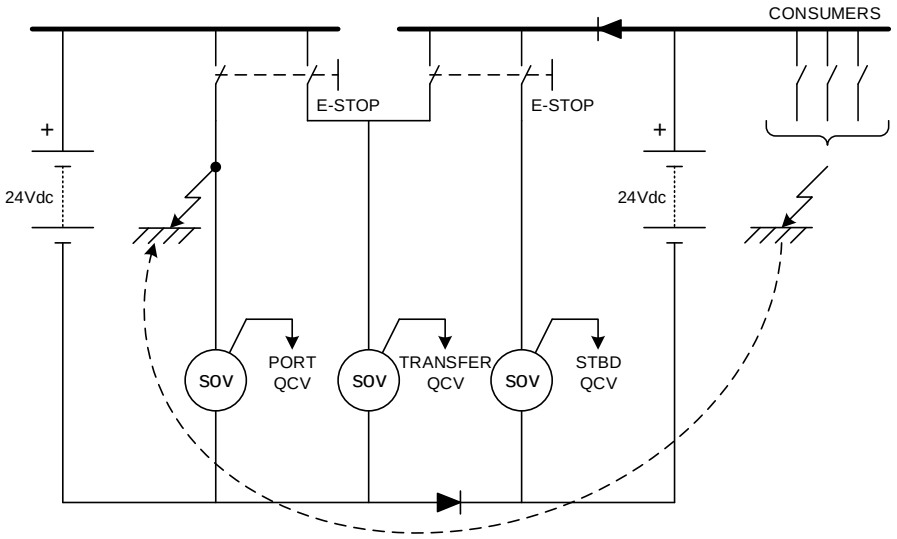

Figure 3-13 Multiple Earth Faults Create Unpredictable Behaviour

3.12.6 In Figure 3-14, 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 surving systems.

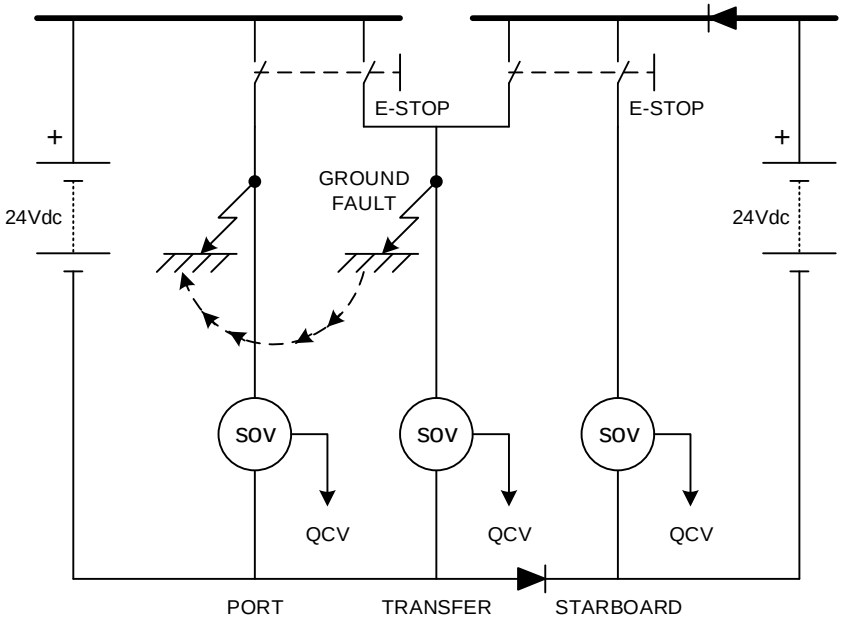

Figure 3-14 Effects Exceeding WCFDI

3.12.7 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.

3.13 MITIGATION OF GROUND FAULTS

3.13.1 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.

3.13.2 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 to 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.

4 SUGGESTED IMPLEMENTATION STRATEGY

4.1 GENERAL

4.1.1 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.

4.1.2 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.

4.1.3 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 requirement exists it is usually possible to comply without creating cross connections which have the potential to defeat the DP redundancy concept.

4.1.4 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.

4.1.5 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.

4.2 IDENTIFY OPPORTUNITIES FOR IMPROVEMENT

4.2.1 **Dual diode connected supplies:** Examine the possibility of isolating the feed from the opposite redundant group. Pay particular attention to load transfer to a surviving redundant group and install additional power supplies. If isolation is not possible then it may be necessary to carry out very comprehensive analysis, modelling and testing to satisfy all stakeholder expectations for the robustness of the DP system. Consider the merits of DC to DC convertors over diodes if cross connections are to remain.

4.2.2 **Auto changeovers**: At the design stage it may be possible to adopt a different redundancy concept obviating the need for changeovers. For vessels in service it may be possible just to lock the changeover in one position for critical DP operations. If the changeover function must be retained then all necessary precautions should be taken to ensure it cannot transfer a fault from one redundant DP group to the other.

4.2.3 **Ground faults**: Ground faults in insulated power systems have greater potential to cause unpredictable behaviour. Investigate the benefits of employing earthed referenced power supplies. If insulated power systems must be retained, it is important that earth faults in station keeping related power systems are promptly cleared from the power distribution system.

4.2.4 Any modification to the DP system should be notified to class and may be the subject of an addendum to the FMEA to be confirmed by proving trials.

4.3 BUILDING CONFIDENCE

4.3.1 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.

4.3.2 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.

5 MISCELLANEOUS

Stakeholders	Impacted	Remarks
MTS DP Committee	✓	To track and incorporate in next rev of MTS DP Operations Guidance Document Part 2 Appendix 1. Communicate to DNV, USCG, Upload in MTS website part.
USCG	X	MTS to communicate- FR notice impacted when Rev is available.
DNV GL	✓	MTS to Communicate- DNV RP E 306 & 307 impacted.
ABS	✓	ABS Guide for Dynamic Positioning Systems
Equipment vendor community	X	MTS to engage with suppliers.
Consultant community	X	MTS members to cascade/ promulgate.
Training institutions	X	MTS members to cascade/ promulgate.
Vessel Owners/Operators	✓	Establish effective means to disseminate information to Vessel Management and Vessel Operational Teams.
Vessel Management/Operational teams	✓	Establish effective means to disseminate information to Vessel Operational Teams.