TECHNICAL AND OPERATIONAL GUIDANCE (TECHOP)

TECHOP_ODP_11_(D) (CROSS_CONNECTIONS)

18 MAY 2015

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	FAULT TOLERANT SYSTEMS BASED ON REDUNDANCY	7
3.2	CROSS CONNECTIONS	7
3.3	EXAMPLE INCIDENTS	8
3.4	STAKEHOLDER REQUIREMENTS	9
3.5	FAULT PROPAGATION PATHS	9
3.6	CROSS CONNECTIONS FOR RELIABILITY AND MAINTENANCE	10
3.7	BACKUP CONTROL SUPPLIES BY WAY OF DC/DC CONVERTERS.	13
3.8	CLOSED BUSTIES	14
3.9	AUTO CHANGEOVERS – BETWEEN REDUNDANT GROUPS	19
3.10	DUAL AC SUPPLIES TO CONSUMERS WITH AC/DC POWER SUPPLIES	22
3.11	LOAD SHARING LINES	23
3.12	SWITCHBOARD CONTROL POWER AND SYNCHRONISING LINES	25
3.13	MARINE AUXILIARY SERVICES	27
3.14	NETWORKS IN DP CONTROL AND VESSEL MANAGEMENT SYSTEMS	29
3.15	INFLUENCE OF CAM AND TAM	31
4	**SUGGESTED IMPLEMENTATION STRATEGY**	**32**
4.1	GENERAL	32
4.2	NEW BUILDS AND VESSELS IN OPERATION	32
4.3	IDENTIFYING CROSS CONNECTIONS	33
5	**MISCELLANEOUS**	**34**

FIGURES

Figure 3-1	Dual Diode Connected Supplies to Engine Governors	11
Figure 3-2	Design with Additional Supplies and No Cross Connections	12
Figure 3-3	Generator Controls with Dual Supplies	13
Figure 3-4	DC to DC Converter	13
Figure 3-5	Dual Supplies Provided by DC to DC Converters (still cross connected – not preferred)	14
Figure 3-6	Typical Diesel Electric DP Power Plant	15
Figure 3-7	Auto Changeover	20
Figure 3-8	Thruster with Dual Supplies	22
Figure 3-9	Dual Fed Consumer	23
Figure 3-10	Isolation of Load Sharing Lines	24
Figure 3-11	Control Power Crossing Boundaries	25
Figure 3-12	Effects of Fire on Supplies from Bus VTs	26
Figure 3-13	Main Bustie Controls and Interlocks	26
Figure 3-14	Division of Remote Controlled Valve Systems	29
Figure 3-15	Typical Vessel Management System Network	30

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_11_(D)_(CROSS_CONNECTIONS). This TECHOP addresses cross connections between redundant groups in the DP system. Evidence from DP incident data confirm that cross connections in all parts of the DP system continue to be a very significant factor in DP incidents and are often the reason that failure effects exceed anticipated consequences and sometimes the worst case failure design intent.

2.1.2 All parts of the DP system are vulnerable and all types of cross connections are considered but particular focus is placed on those cross connections which are often introduced to allow functionality to be maintained after a failure but which do not restore fault tolerance and which cannot therefore reduce vulnerability to non-productive time.

2.1.3 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 introducing vulnerabilities in fault resistance, fault tolerance and fault ride-through.

2.1.4 Another misconception that is prevalent is that opening bustie breakers at the highest voltage 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.

2.1.5 Galvanic isolation is often used to demonstrate a means of avoiding fault transfer. This has proven to be inadequate in a number of installations as credible protection against fault transfer.

2.1.6 Note: Figures provided in this TECHOP are intended to illustrate the problems associated with cross connections. They are not intended to represent practical or good examples of how such connections could be created.

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 FAULT TOLERANT SYSTEMS BASED ON REDUNDANCY

3.1.1 DP vessels of Equipment Class 2 and 3 are required to be single fault tolerant in respect of defined failure criteria. Fault tolerance is created by providing at least two redundant systems each capable of developing the necessary surge, sway and yaw forces to maintain position and heading.

3.1.2 Loss of position may occur in several ways:

- Drift off – Insufficient thrust following a failure.
- Drive off – Thrust exceeds that required 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 from set-point.
- Force off – The vessel has insufficient thrust in the intact condition to maintain position in the prevailing environmental conditions.

3.2 CROSS CONNECTIONS

3.2.1 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 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.

3.2.2 The term ‘cross connections’ is most commonly used to describe tangible connections. The concept can be extended to include less obvious connections such as software functions, the seawater that surrounds the hull, the air that is drawn for ventilation and combustion and the fuel that is provided to the engines. Safety systems that span redundant groups such as CO2 and water mist systems can also be thought of in this way. Most of the above are also the subject of another TECHOP on ‘External Interfaces’ to the DP system.

3.2.3 Cross connections 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.

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

3.2.5 Coupling of interference from power cables to control cables is generally controlled by good installation practice such as the cable segregation requirements in classification society rules.

3.2.6 Typical cross connections include:

- Backup dc supplies by way of diodes or dc/dc converters.
- Auto changeovers.
- Load sharing lines.
- Common control air service.
- Busties.
- Networks in DP & PMS control systems.

- Vessel management networks.
- Violating principle of redundancy – example: All UPS input supplies on one MCC.

3.3 EXAMPLE INCIDENTS

1. A large crane / pipe play vessel had a common 24Vdc distribution system for all engine governors with multiple sources of supply – This designs 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.
2. 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.
3. A DP class 2 construction vessel has two 110Vdc supplies for switchboard controls that are connected by diode 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.
4. 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 220V on to the 24Vdc supply. All thruster controllers were damaged.
5. A pipe laying vessel suffered an internal fault on a generator which should have been tripped by the generator's differential protection. However
6. 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 out.
7. A DP class 3 diving 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.
8. 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.
9. 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.
10. 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.

11. 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.
12. 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.

3.4 STAKEHOLDER REQUIREMENTS

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

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

3.5 FAULT PROPAGATION PATHS

3.5.1 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).

3.5.2 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 mal-operation.
- Switchboard control, power and synchronising lines.

3.5.3 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.

3.6 CROSS CONNECTIONS FOR RELIABILITY AND MAINTENANCE

3.6.1 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.

3.6.2 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.

3.6.3 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.

3.6.4 There are several ways to improve overall mission reliability:

- Specify high quality components.
- Operate equipment well within its design limits (over-engineered).
- Provide non-critical redundancy over and above that required for single fault tolerance.

3.6.5 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 Figure 3-1. 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.

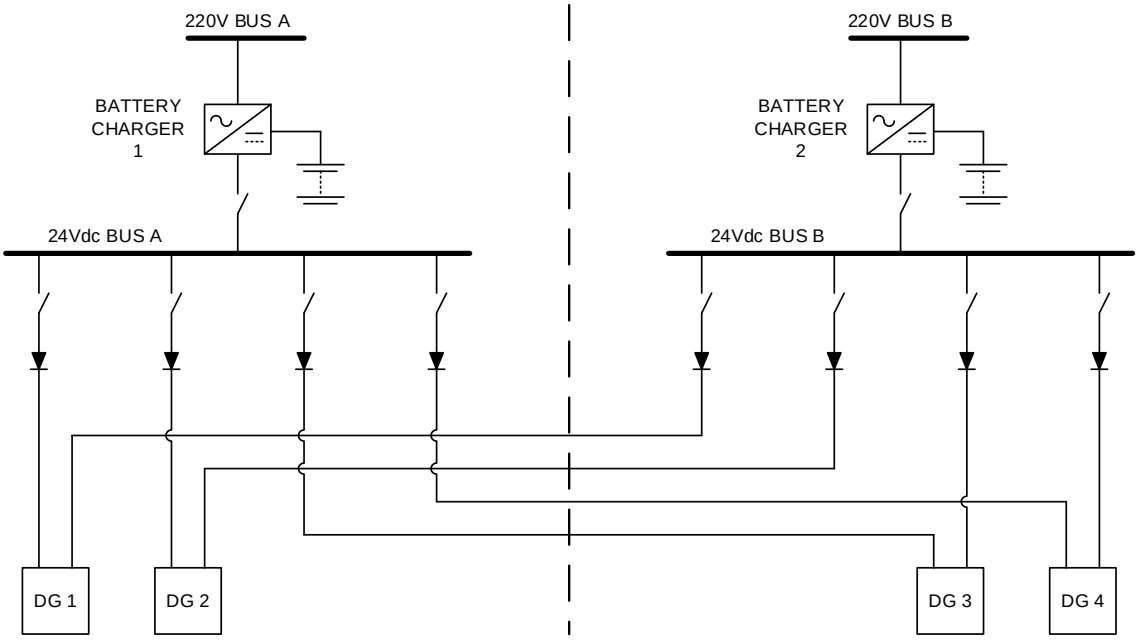

Figure 3-1 Dual Diode Connected Supplies to Engine Governors

3.6.6 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.

3.6.7 Unfortunately, the cross connection described in 3.5.5 and 3.5.6 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.

3.6.8 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.

3.6.9 The design with 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.

3.6.10 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.

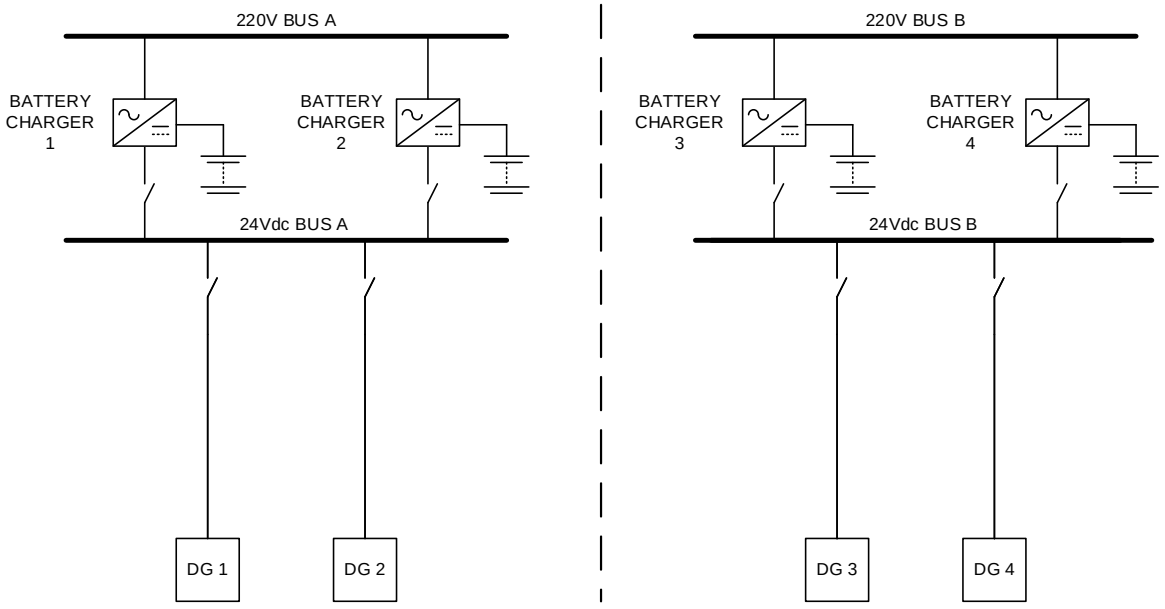

Figure 3-2 Design with Additional Supplies and No Cross Connections

3.6.11 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.

3.6.12 In the alternative arrangement without cross connections shown in Figure 3-2:

- 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.

3.6.13 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).

3.6.14 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.

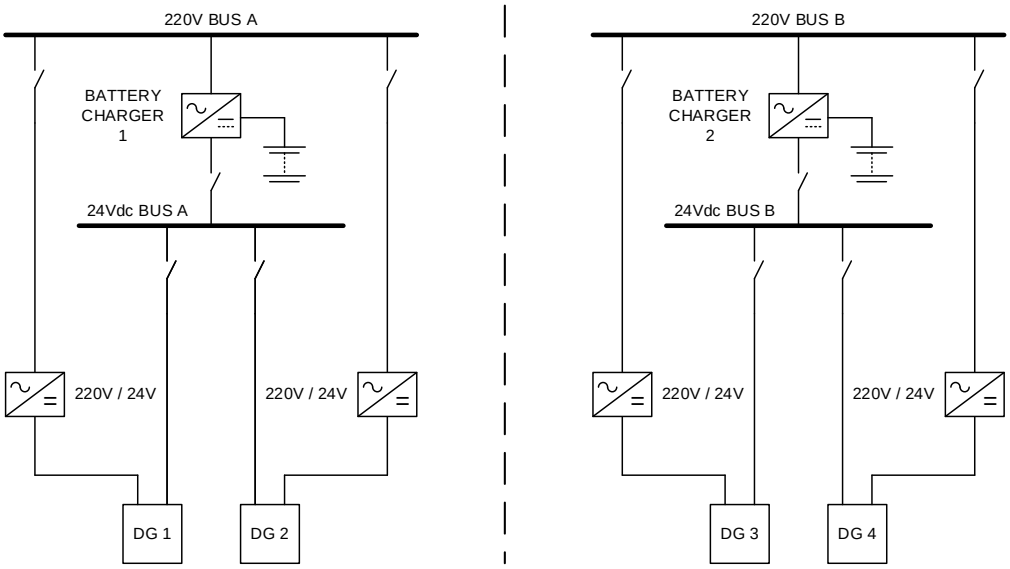

Figure 3-3 Generator Controls with Dual Supplies

3.6.14.1 Variations on the supply arrangement are possible and Figure 3-3 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.

3.7 BACKUP CONTROL SUPPLIES BY WAY OF DC/DC CONVERTERS.

3.7.1 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 Figure 3-3

- 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.

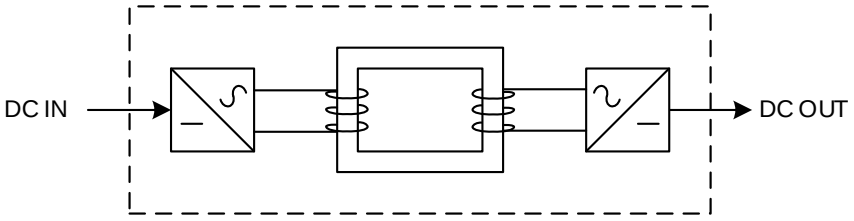

Figure 3-4 DC to DC Converter

3.7.2 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.

3.7.3 Although a design using DC to DC convertors in Figure 3-3 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.

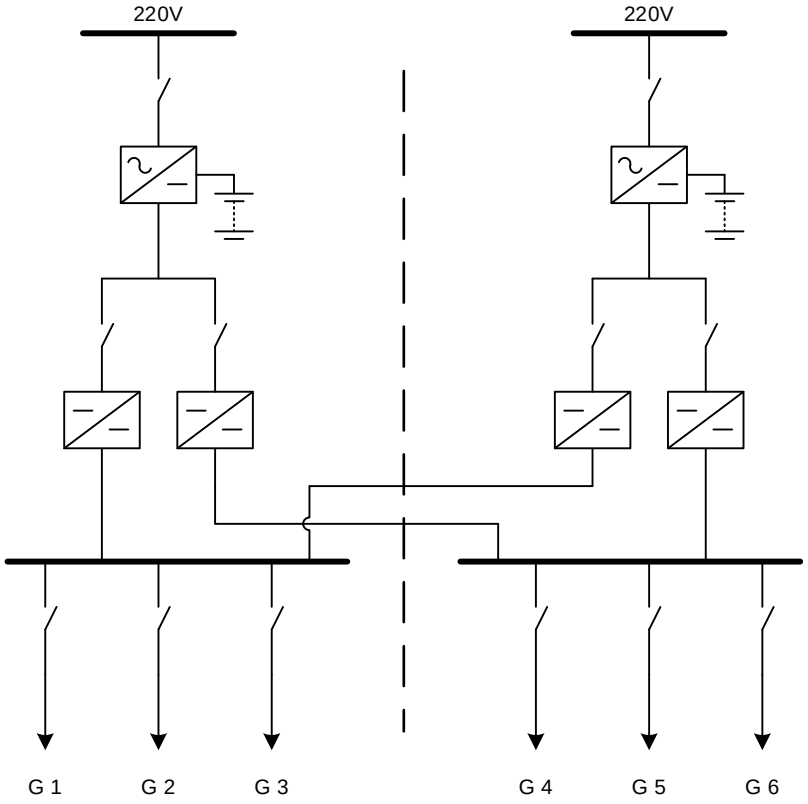

Figure 3-5 Dual Supplies Provided by DC to DC Converters (still cross connected – not preferred)

3.8 CLOSED BUSTIES

3.8.1 Figure 3-4 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. As 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. 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 though capability is a performance criteria that can be specified in the design and proven by testing.

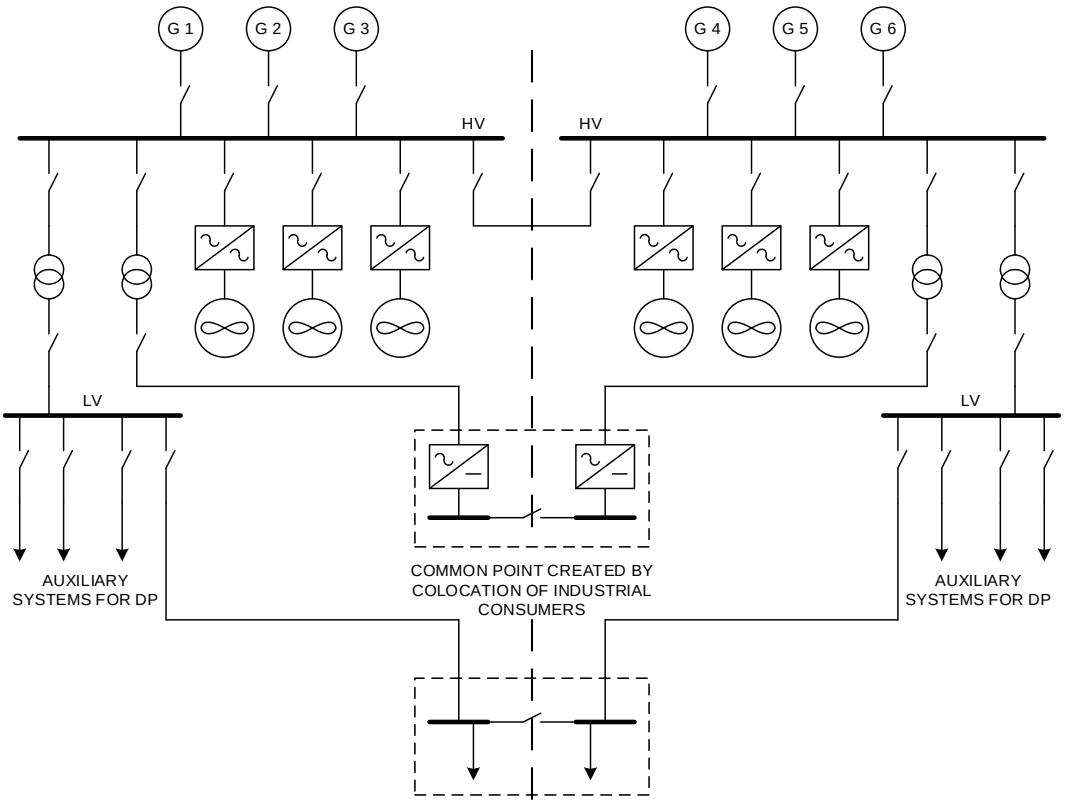

Figure 3-6 Typical Diesel Electric DP Power Plant

3.8.2 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.

3.8.3 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.

3.8.4 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.

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.

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.

3.8.5 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.

3.8.6 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 plat can survive such a shock. Mechanical damage to the generator / engine couplings and end windings is off concern during such events.

3.8.7 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.

3.8.8 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.

3.8.9 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.

3.8.10 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.

3.8.11 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.

3.8.12 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.

3.8.13 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 though such failure effects.

3.8.14 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.

3.8.15 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.

3.8.16 Figure 3-5 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.

3.9 AUTO CHANGEOVERS – BETWEEN REDUNDANT GROUPS

3.9.1 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.

3.9.2 Automatic changeovers like the one shown in Figure 3-6 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.

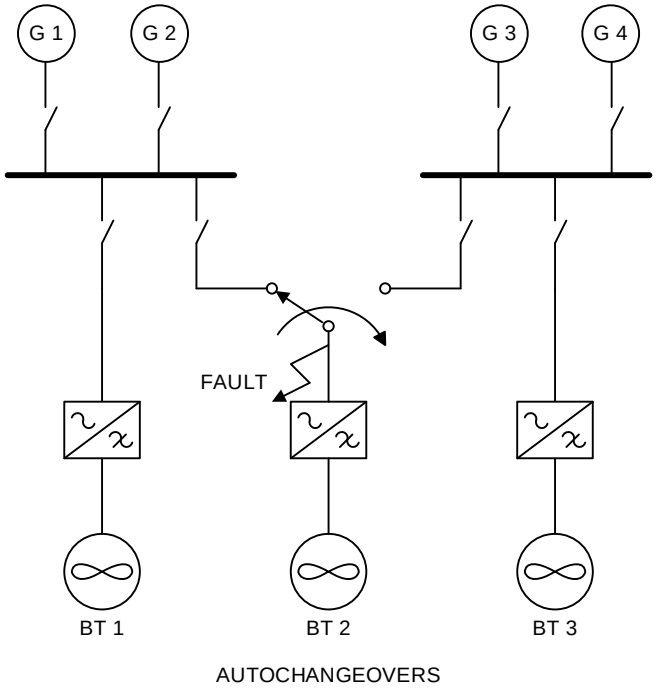

Figure 3-7 Auto Changeover

3.9.3 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.

3.9.4 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.

3.9.5 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 though 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.

3.9.6 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.

3.9.7 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.

3.9.8 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.

3.9.9 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 convertor which in turn feeds a common DC link which supplies an inverter as shown in Figure 3-8. 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 descried in TECHOP_ODP_(D)_09 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).

3.9.10 In some designs there may be a defined phase shift between the two ac to dc supplies to the convertors 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 convertors. Any such restriction on thrust output should be reflected in the consequence analysers.

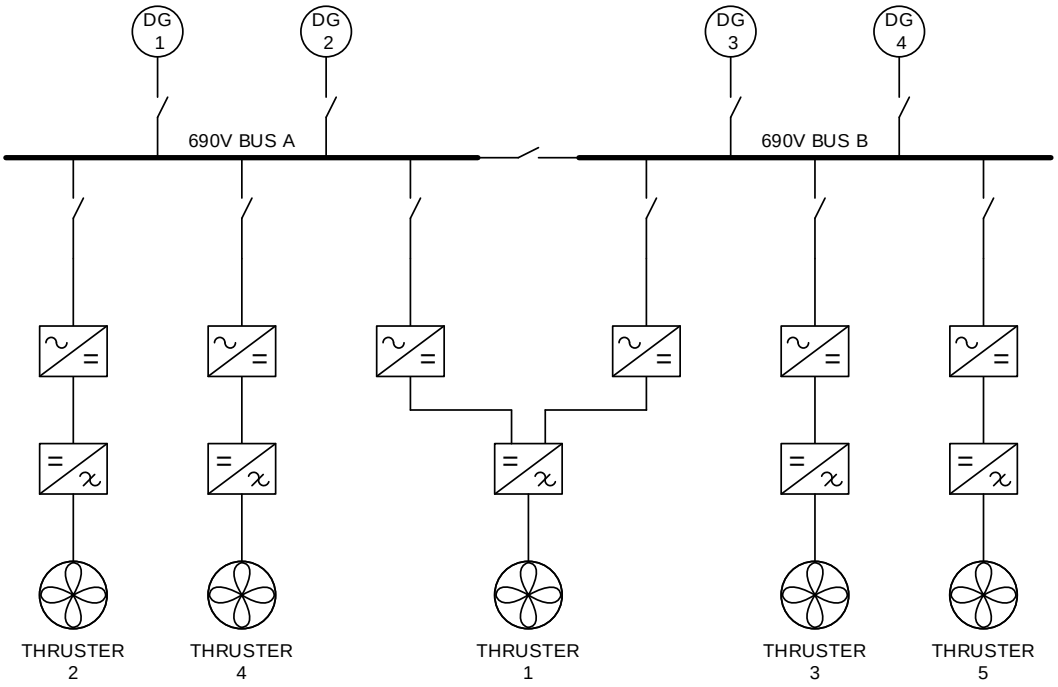

Figure 3-8 Thruster with Dual Supplies

3.10 DUAL AC SUPPLIES TO CONSUMERS WITH AC/DC POWER SUPPLIES

3.10.1 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 Figure 3-7 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.

3.10.2 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.

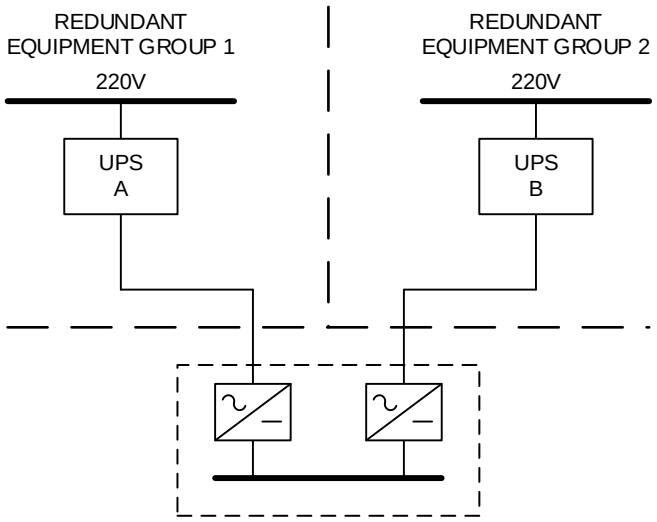

Figure 3-9 Dual Fed Consumer

3.10.3 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.

3.10.4 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.

3.10.5 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.

3.10.6 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 guaranteed ‘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.

3.11 LOAD SHARING LINES

3.11.1 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)

3.11.2 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.

3.11.3 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.

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 Figure 3-10.

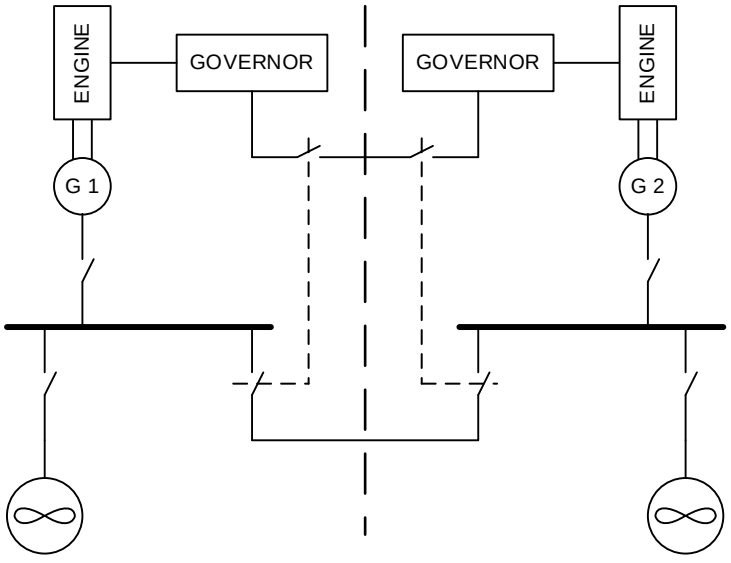

Figure 3-10 Isolation of Load Sharing Lines

3.11.4 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.

3.11.5 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.

3.12 SWITCHBOARD CONTROL POWER AND SYNCHRONISING LINES

3.12.1 Control Power

3.12.1.1 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.

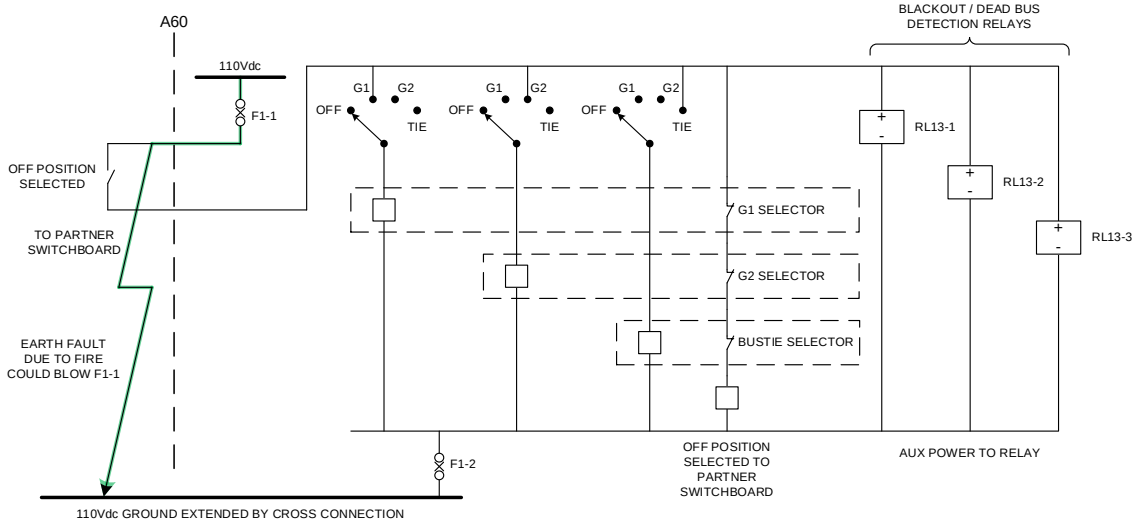

Figure 3-11 Control Power Crossing Boundaries

3.12.1.2 In DP class 3 designs it is necessary to consider the effects of fire and flooding on any such control or power lines crossing the A60 WT divide between redundant DP equipment groups. 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 of which 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. Figure 3-9 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.

3.12.1.3 Some classification societies have gone so far as to recommend against such cross connections in their rules for DP class 3 vessels.

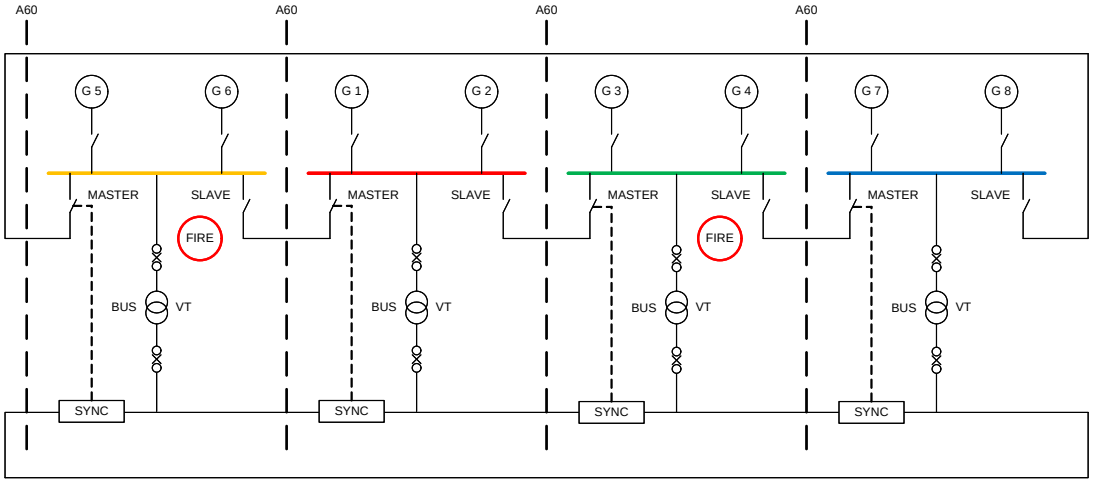

Figure 3-12 Effects of Fire on Supplies from Bus VTs

3.12.1.4 Bus voltage transformers are another example of a control and protection component that often crosses A60 / WT boundaries. In Figure 3-12 above, 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.

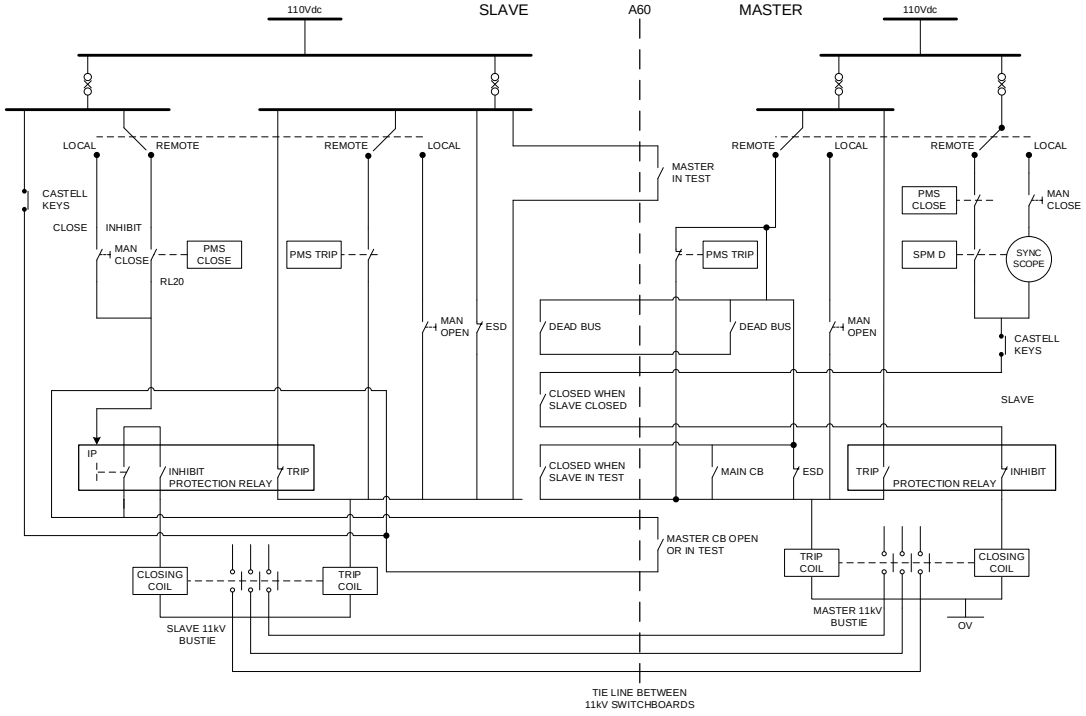

Figure 3-13 Main Bustie Controls and Interlocks

3.12.1.5 Figure 3-13 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.

3.13 MARINE AUXILIARY SERVICES

3.13.1 General

3.13.2 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.

3.13.3 Ventilation

3.13.4 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.

3.13.5 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.

3.13.6 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.

3.13.7 Fuel oil

3.13.8 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.

3.13.9 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.

3.13.10 Lubricating oil

3.13.11 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.

3.13.12 Seawater cooling

3.13.13 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.

3.13.14 Freshwater cooling

3.13.15 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.

3.13.16 Compressed air

3.13.17 Compressed air system are used for a number of services and several systems may be provided for different purpose

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

3.13.18 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.

3.13.19 Remote valve control

3.13.20 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 Figure 3-9. 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.

3.13.21 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 are 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.

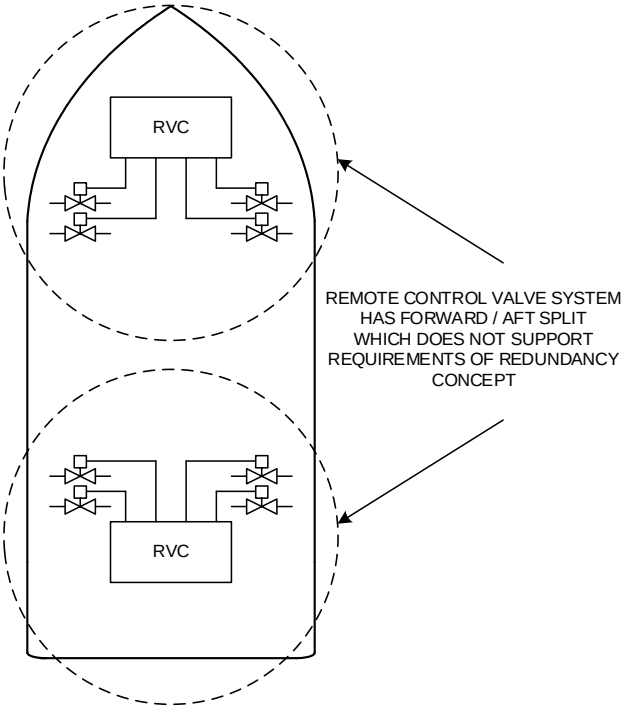

Figure 3-14 Division of Remote Controlled Valve Systems

3.13.22 Fire damper controls

3.13.22.1 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.

3.13.22.2 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.

3.14 NETWORKS IN DP CONTROL AND VESSEL MANAGEMENT SYSTEMS

3.14.1 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 Figure 3-10

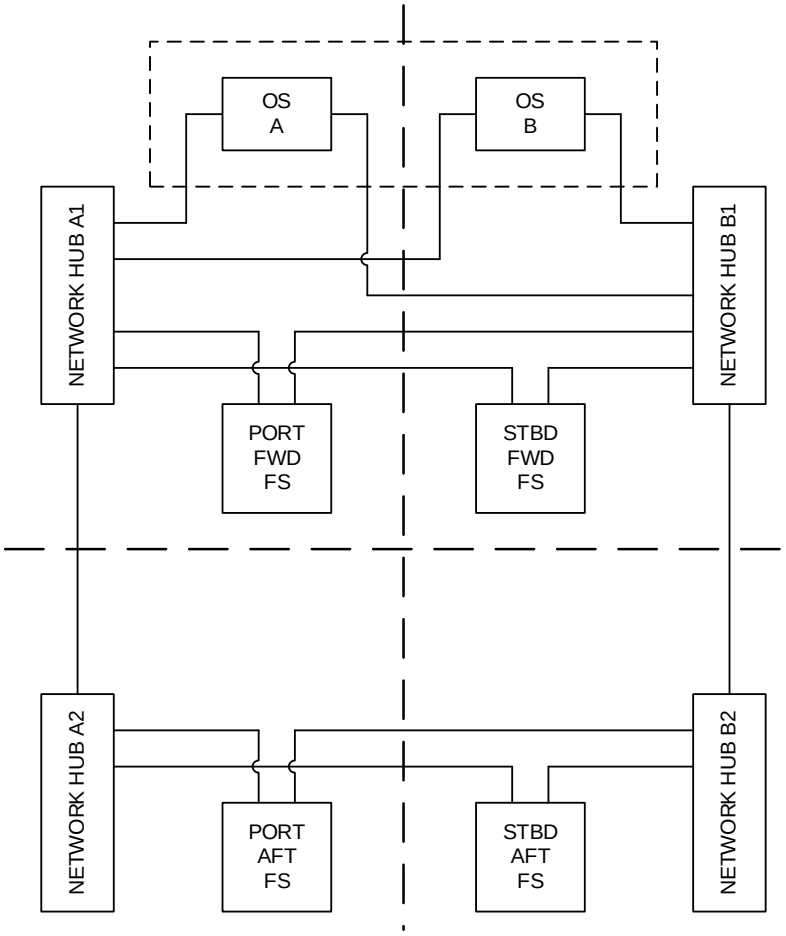

Figure 3-15 Typical Vessel Management System Network

3.14.2 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. 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.

3.14.3 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.

3.14.4 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.

3.14.5 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.

3.14.6 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.

3.14.7 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.

3.14.8 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.

3.15 INFLUENCE OF CAM AND TAM

3.15.1 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 protective functions would also be part of that process.

3.15.2 In Task Appropriate Mode (TAM) the consequences of a loss of position are known, limited, acceptable and do not include risk to life or the environment. Essentially, there may be a defined commercial risk associated with failure to complete the work on time or the need for remedial work. In this mode of operation greater flexibility may be considered including the use of cross connections and reliance on protective functions.

4 SUGGESTED IMPLEMENTATION STRATEGY

4.1 GENERAL

4.1.1 The preceding discussion has identified the risks and limitations associated with certain type of cross-connections between the redundant equipment groups in a DP system. Some cross connections provide more benefits than others but very rarely do cross connections reduce exposure to non-productive time following a failure as they can be used to restore functionality but not fault tolerance.

4.1.2 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.

4.1.3 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.

4.1.4 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.

4.2 NEW BUILDS AND VESSELS IN OPERATION

4.2.1 Vulnerabilities in DP operations can typically be addressed by considering their impact on:

- Design
- Operations
- People

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

4.2.3 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.

4.2.4 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.

4.3 IDENTIFYING CROSS CONNECTIONS

4.3.1 It should be possible to identify the cross connections in a DP system from a competently executed DP System FMEA.

- Identify failure modes that may propagate.
- Identify any lack of protective functions.
- Identify potential hidden failures.
- Identify any barriers that can be put in place such as isolation of cross connections.
- Identify cross connections created by colocation of equipment.

4.3.2 Undue reliance on FMEAs to identify cross-connection and their impacts is cautioned against as there is wide variation in the quality of FMEAs for DP vessels. MTS TECHOP_ODP_04_(D)_(FMEA GAP ANALYSIS) can be used to ascertain whether or not the FMEA is likely to have covered the important issues.

4.3.3 DNV Recommend Practice for ‘FMEA of Redundant Systems’, RP D102 is an FMEA methodology specifically designed to identify common points and cross connections.

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	✓	MTS to Communicate- DNV RP E 306 & 307 impacted
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