Return to Session Directory


**DYNAMIC POSITIONING CONFERENCE**
**October 9-10, 2007**

**DP Innovation**

---

# A Novel Solution to Common Mode Failures in DP Class 2 Power Plant

**Dr. Steven Cargill**

***Noble Denton Consultants, Ltd.***

---

## Abstract

This paper presents an overview of Transocean's Advanced Generator Protection (AGP) scheme and Advanced Thruster Control and Protection (ATCP) initiative and explains how this innovative combination of model based generator protection and grid inter-connector technology has produced a novel solution to well known common mode failures found in many DP Class 2 power plants. Such failures continue to cause DP incidents and are associated with faults in various systems including power management, power distribution and generator controls. The paper begins with a review of these failure mechanisms and discusses the advantages of the new arrangement in relation to earlier solutions. The information presented is based on experience gained from DP system FMEAs and proving trials on vessels equipped with these new technologies.


## Propulsions System Redundancy for DP

The vast majority of medium and large dynamically positioned vessels in service today have Diesel electric propulsion systems based on the power station concept. Thrusters with fixed pitch propellers driven by frequency converters to provide variable propeller speed are also the norm for this type of vessel. A typical propulsion system arrangement is shown in Figure 1.

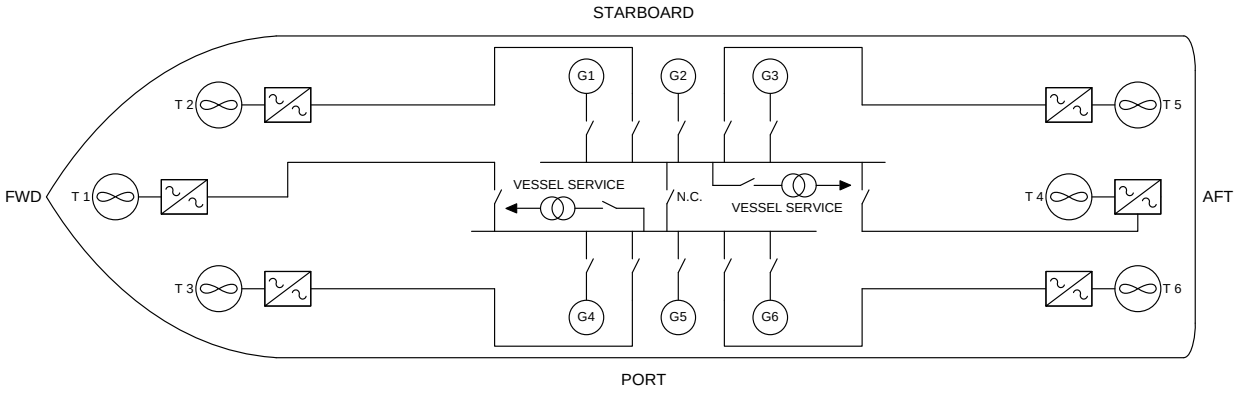


**Figure 1 Conventional Propulsion System Arrangement**

Although this arrangement offers many advantages in terms of plant flexibility and efficiency it does present a number of challenges for designers seeking to comply with the requirements of DP Class 2 and DP Class 3.

In simple terms, DP Class 2 requires that the propulsion and control systems are tolerant of single failures of active components and that the vessel can maintain position and heading following this type of failure. For DP Class 3 the requirements for station keeping integrity include tolerance of faults in any component (active or passive) and the ability to withstand a fire or flood in any one compartment of the vessel.

Under the rules for DP Class 2, vessels may be designed with a single power system provided it can be divided into two or more subsystems to isolate any fault which may develop. Isolation of faults must be fully automatic and sufficient propulsion machinery and control functions must remain available to maintain position and heading. The maximum amount of propulsion machinery that can be lost as the result of a single fault is often referred to as the Worst Case Failure Design Intent (WCFDI).

Failure Modes and Effects Analysis (FMEA) is performed during the design process to identify faults that have the potential to destabilise the plant. Where such faults are found, recommendations are made to mitigate the risk, which may require a change of design or provision of additional protection functions to identify and isolate the fault. The FMEA considers all parts of the dynamic positioning system to ensure that there is sufficient redundancy and separation in the provision of power generation and thrust. The arrangement of auxiliary services such as cooling water, compressed air, ventilation and fuel oil are also examined to ensure that the failure effect described by the Worst Case Failure Design Intent is not exceeded. The desktop analysis is confirmed by FMEA proving trials when the vessel is complete.

## History of Common Mode Failures

In any power system where redundancy is provided by synchronous generators operating in parallel, there is a risk that all connected generators may react adversely to an electrical or control system fault in one generator or indeed to a fault elsewhere in the power distribution system which causes a severe voltage transient. The operation of power consumers such as thruster drives, pumps, compressors and fans can also be disrupted by the effects of severe electrical faults.

The term Common Mode Failure (CMF) is sometimes used to describe plant failures in which several apparently separate and redundant elements, all react adversely to a fault in one of the redundant elements, or elsewhere in the plant. The stability of an ac power generation system is at risk if any of its fundamental operating parameters, voltage, current and frequency exceeds safe working limits. As electrical power systems are very well protected, plant failure is likely to follow the operation of safety systems in response to unsafe conditions created by the original fault rather than the direct effects of equipment failure. One of the fundamental problems for designers of fault tolerant power systems, is how to balance the need to ensure personnel safety and protect equipment while maintaining continuity of power to thrusters. The design and function of traditional generator protection schemes is biased in favour of safety and equipment protection and may not provide complete protection against certain common mode failures which could lead to blackout and loss of position in a DP vessel.

The typical range of Common Mode Failures which designers consider when developing a fault tolerant power generation system includes:-

Primary fault conditions

1. Over and under frequency
2. Over and under voltage
3. Over load – rating of engine exceeded
4. Over current – rating of alternator exceeded

Secondary fault conditions (these would give rise to primary fault conditions but protective functions may intervene first)

1. Severe active power sharing imbalance
2. Severe reactive power sharing imbalance

3. Excessive regeneration of power

The challenge for any designer of fault tolerant power systems or related protection equipment is to quickly and reliably identify the cause of the fault and isolate it to the equipment in which it has occurred. Difficulty in identifying the source of the failure effect arises from the need to determine whether the observed effect is caused by a fault in the generator or whether the generator is simply reacting to a fault elsewhere in another generator or load.

For example: A generator may shed load because there is a fault within the engine or because load is reducing or because its share of the load is being taken by another generator with a fuel control fault.

There are two failure scenarios in parallel generator operation which pose particular challenges:-

1. Severe load sharing imbalance between generators leading to multiple generators being tripped by their reverse power protection. This can be caused by an engine governor failing to the 'excess fuel' condition. In very severe cases the power system frequency may be raised to the point where several or all generators trip on over-frequency.

2. Severe reactive power sharing imbalance between generators leading to multiple generators tripping on their field failure protection. This condition can be caused by an AVR failing to full excitation. In very severe cases the power system voltage may rise to the point where several or all generators trip on over voltage.

Although almost all Diesel electric power systems using parallel generators are vulnerable to these failure modes very few vessels were provided with specific protection against them and it is only within the last few years that reliable and effective protective functions have been developed.

The first generation of Diesel electric vessels based on the power station concept used variable pitch thrusters driven by large asynchronous motors operating at poor power factor. The poor efficiency of variable pitch thrusters provided a significant base load. Many of these vessels also had relatively small generators in relation to the system load. These features provide a degree of intrinsic immunity to the failure scenarios discussed above because a faulty generator is not capable of carrying the entire system kW or kVAr demand. This is one of the conditions required for these failure modes to succeed. Ironically, advances in technology have not improved the situation as the introduction of thrusters with fixed pitch propellers driven by variable frequency drives has reduced base loads and improved power factor. Similarly, the demand for more and more powerful offshore construction vessels has seen the power rating of generators rise in relation to the number of generators and propulsion load such that a faulty generator is capable of carrying the entire system load.

One fact that was not widely realised was that load shedding functions in power management systems which were programmed to shed thruster load in response to the overload of a single generator actually exacerbated these failure modes by reducing system load to the point where the faulty generator could force the healthy ones to trip. The intention was to prevent cascade failure of heavily loaded generators if one generator tripped but this undesirable interaction was overlooked. This is further evidence, if such is needed, of the care that must be taken to understand the interaction of protective functions with power system faults when designing any fault tolerant propulsion system.

## Previous Solutions

Early attempts at providing protection against these failure modes were based on voting systems which monitored the kW and kVAr condition of all connected generators. A central monitoring system attempted to diagnose the faulty generator by identifying and tripping the set which was reacting in opposition to all the others. As with any system based on voting, these systems would only work with three or more generators thus there was no protection if the vessel was operating with only two generators online. Another disadvantage of these systems was that because all monitoring and tripping functions were located within a centralised control system, they introduced another layer of commonality between generators which were supposed to be separate and mutually redundant. In at least two cases, blackouts have been caused by failures or design flaws in such protection systems. In one case, the designers failed to consider that two out of three generators could shed load because they shared a common fuel system and a common control power supply. Thus, in the case of a fuel supply problem or a control power failure, the generator taking load was not the faulty set. The actual fault was that two generators were suffering from fuel starvation causing the single healthy generator to carry the entire system load. In this case, tripping the highly loaded generator made the failure effect significantly worse. Failure of load sharing lines connecting engine governors in isochronous load sharing systems can also cause severe load sharing imbalance when no one generator is faulty. Again tripping a heavily loaded generator is not the correct response to this fault and will only make a blackout more likely.

## Advanced Generator Protection

When engineers at Transocean Engineering in Houston had an opportunity to upgrade the power plant on one of their 5$^{th}$ generation semi-submersibles they decided upon a complete review of the generator protection systems with a view to improving the response to common mode failures.

The result of this review was a system called Advanced Generator Protection (AGP), designed by Transocean and developed by engineers at Aspin Kemp Associates. AGP is not just a bolt on protection system designed to cover a few extra failure modes, but a complete philosophy about how fault tolerant power systems should be managed and protected to ensure continuity of power supply.

Transocean engineers realised at an early stage that so called ‘true-isochronous’ or ‘pseudo-isochronous’ speed control and load sharing schemes were actually masking the onset of generator fuel control problems until they reached a critical level. They also concluded that isochronous control provides little performance advantage over modern digital engine governors load sharing through speed droop. In droop mode, the speed of generators operating in parallel is allowed to fall slightly with increasing load. Thus a straight-line frequency against load characteristic is created in which no-load and full load are defined by the upper and lower limits of the steady state plant operating frequency. This characteristic resides within the electronic governor and is used to regulate fuel admission over the entire load range.

Generators operating in parallel under droop control share load naturally at the point at which their speed / load characteristics intersect. Figure 2 shows how this control mode operates in practice. In this example, identical generators G1 and G2 have a speed (frequency) droop of 3Hz (5%) from no-load to full load and are arranged to run at 60Hz at full load. The system frequency and relative loading of each generator can be obtained diagrammatically by reversing the power scale for G2 such that the two speed / load characteristics intersect. For simplicity, the two generators are operating in parallel with a system load equal to the rating of one generator; thus, when both generators have the same speed / load characteristic each generator carries 50% of the load as shown by the solid lines in Figure 2. If a speed offset is applied to either characteristic, the proportion of the total load being carried by each generator changes as shown by the intersection of the dashed line for G2 and the solid line for G1. In the new case, a +2Hz speed bias has been applied to G2 which now carried carries 84% of the system load. G1 carries the remaining 16%. Note that the system frequency has now risen from 61.5Hz, for equal load sharing, to

62.5Hz for the asymmetric case. Increasing the speed bias on G2 by a further 1Hz would cause G2 to carry the entire system load at a frequency of 63Hz and any further increase would push G1 into reverse power with risk of it tripping on its reverse power protection. An external speed bias is used in pseudo-isochronous load sharing systems to correct for errors in the governors. Significant differences in speed / load characteristics were a feature of the older generation of electro-hydraulic governors, particularly when worn, but this is not a problem with modern digital governors. No trimming of the external speed bias is performed during the normal operation of power plants utilising AGP other than for synchronising and asymmetric load sharing for engine conditioning. Additional protective functions are active at this time.

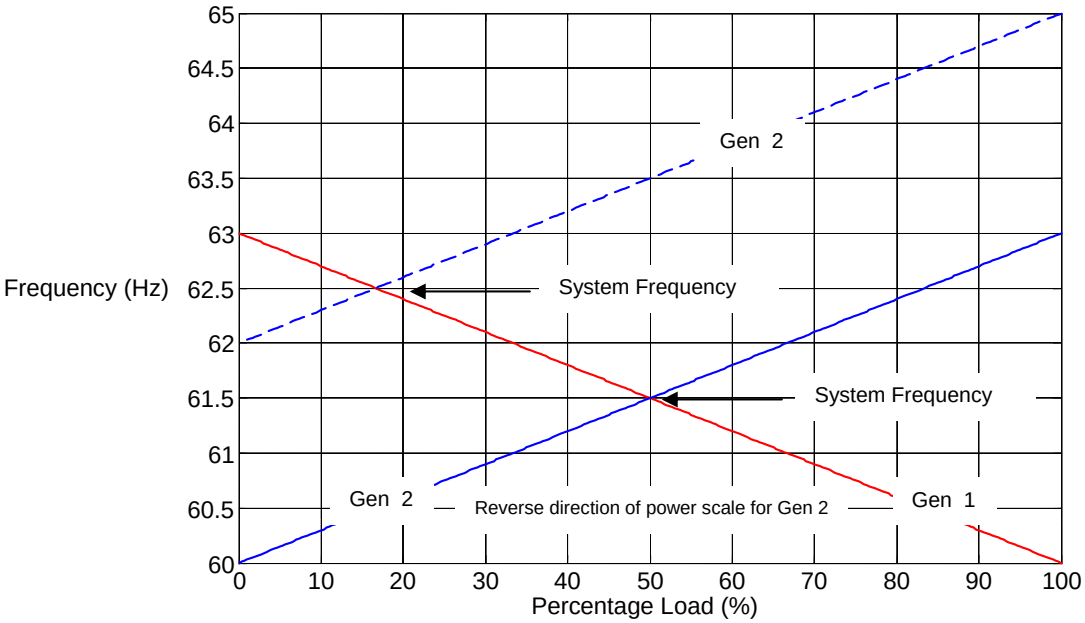


**Figure 2- Generator Load Sharing by Droop**

The most important advantage to be obtained from adopting droop mode for speed control and load sharing is that it allows the power system frequency to be used to indicate overall plant loading and form the basis of protection functions which can identify a faulty generator without having to compare its performance to those of other online generators. Thus a faulty protection system can only trip the generator which it is monitoring and not multiple generators as is the case with centralised voting systems.

Droop mode has another advantage from an FMEA perspective in that it requires no load sharing lines between governors or external common control systems and so introduces no additional commonality between generators which are supposed to be independent.

With parallel generators operating in droop mode under the control of accurate digital governors, creating protection against fuel control failure becomes deceptively simple. Any generator that follows its droop characteristic is healthy and any generator that deviates from its droop characteristic is not. A faulty generator should be tripped if it risks destabilising the plant or brought to the attention of the engineers by way of an alarm in less severe cases. Figure 3 shows how it is possible to determine which generator has failed to excess fuel even when there are only two generators online.

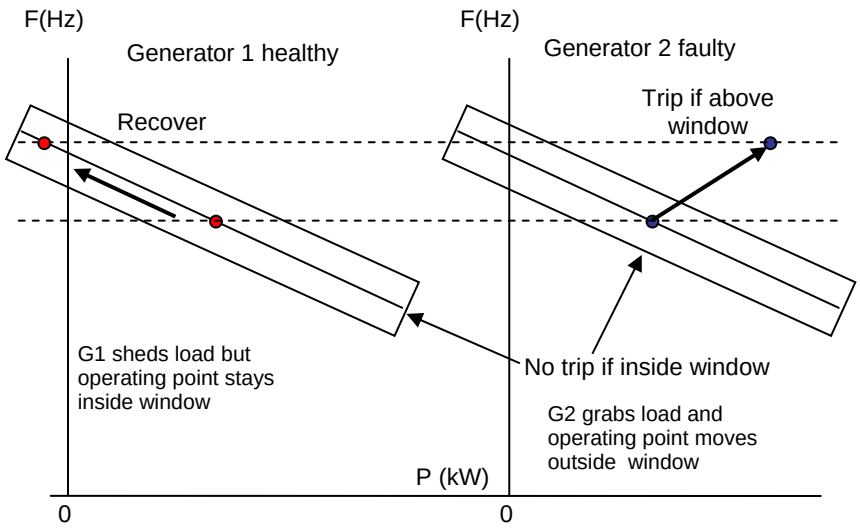


**Figure 3-Identification of Faulty Generator**

In this much simplified example of the protection philosophy a simple window is created around the droop characteristic which is recreated within the Programmable Logic Controller (PLC) used to form the protection hardware (One PLC per generator). The PLC monitors the generator's load and frequency to determine whether it is operating within the window and therefore healthy. When the governor on G2 fails to full fuel in the example above it picks up more and more load from G1 pushing it back along its droop characteristic towards its reverse power tripping point. This also has the effect of raising the power system frequency. In a plant with a conventional protection scheme, the outcome would be blackout when G1 trips on reverse power and G2 trips on over speed.

In a plant with AGP, the protection PLC on G2 is able to identify that it is faulty because the generator's operating point has moved off it droop characteristic and out of the window. This is the only way that G2 can acquire load from G1 if the frequency has gone up for the same system load. All that is required to correct the fault and save the plant from blackout is for the AGP PLC on G2 to trip the faulty generator before G1 trips on reverse power (if indeed it has been driven that far) As the time delay on a reverse power trip is set at around 10s there is plenty time to trip the faulty generator which must include a suitable delay to accommodate the effects of power system dynamics.

A very similar philosophy can be applied to AVR faults in which one AVR fails to full excitation. As marine power systems typically operate in droop mode for voltage control and reactive power sharing no special adaptation is required to implement this protection philosophy on most power systems.

Transocean have since developed and refined AGP to act as a complete backup to traditional generator protection schemes and included a much larger range of protection functions than described here. Every installation has a fully Class approved generator protection relay in addition to the AGP system. In future applications of AGP, the functionality may be absorbed into the vessel management system rather than standalone hardware.

## Other Common Mode Failures

Governor and AVR faults are not the only power generation problems capable of disabling a Diesel electric propulsion system. Short circuit faults occurring anywhere on the main power distribution system will create very significant dips in the power system voltage. In the case of vessels which operate a common power system, this voltage dip will be experienced by all connected consumers. All essential consumers must be capable of riding through this voltage dip without interruption.

Some early variable speed thruster drives did not have sufficient voltage dip ride-through capability and there have been several cases in which all thrusters stopped and would not restart because of an unrelated electrical fault on the main power distribution system.

Voltage source thruster drives were particularly susceptible to voltage dips because of the high speed under voltage protection on their DC Links. This protection is required because their rectifier sections are not capable of withstanding the current transients associated with charging their dc link capacitors banks from low voltage. Typically, the DC link is charged by an auxiliary supply by way of a current limiting resistor. To protect the drive against power supply outages, the drive controller is programmed to trip the main circuit breaker if the DC link voltage falls below 60% for as little as a few microseconds.

Thruster drives are not the only consumers which react adversely to voltage dips, the main power contacts of motor starters can open causing pumps, compressors and fans to stop. This occurs because the ac coils of motor starters are powered directly from the power distribution. Typical effects include thrusters tripping, or dropping out of DP, when their hydraulic pumps stop and engines overheating rapidly on loss of jacket water cooling.

The ride-through capability of drives has improved significantly since early installations and the fragility of LV systems can be addressed by using auto-restart functions, dc coils for contactors and delayed under-voltage release functions on motor control centres and service transformer feeders. Although it is not difficult to create a severe voltage dip on a power distribution system, there is a risk of severe equipment damage if the test goes wrong. Large amounts of energy could also be released. Consequently, the voltage dip ride-though capability of actual vessel installations is seldom proven in practice.

## Advanced Thruster Control and Protection

When the opportunity arose to develop propulsion systems for a new generation of DP drillships and semi-submersibles, Transocean decided to look again at the issue of voltage dip ride-through and how conventional power plants were designed.

In conventional power plants, the only way to have a high degree of confidence that a fault in one power system will not be transferred to the other is to design the vessel with two or more independent power systems. Most DP Diesel electric vessels can be operated this way but this mode of operation is not always popular with vessel owners or crews. This is particularly true when the power plant has not been specifically designed with the independent power system configuration as the primary mode of operation.

Operating with smaller power systems can lead to more frequent partial blackouts, restricts the flexibility of generator assignment and encourages low load running leading to maintenance problems. Such problems bring their own risks to station keeping integrity and it can be argued that the increased risk from these issues outweighs the benefits of greater fault isolation.

Transocean engineers considered whether there was a 'third way' that would provide the flexibility of a common power system with the fault isolation qualities of independent power systems. The result of these deliberations was the development of the Siemens' Siplink based power system in which each thruster has a true dual supply from two independent power systems as shown in Figure 4.

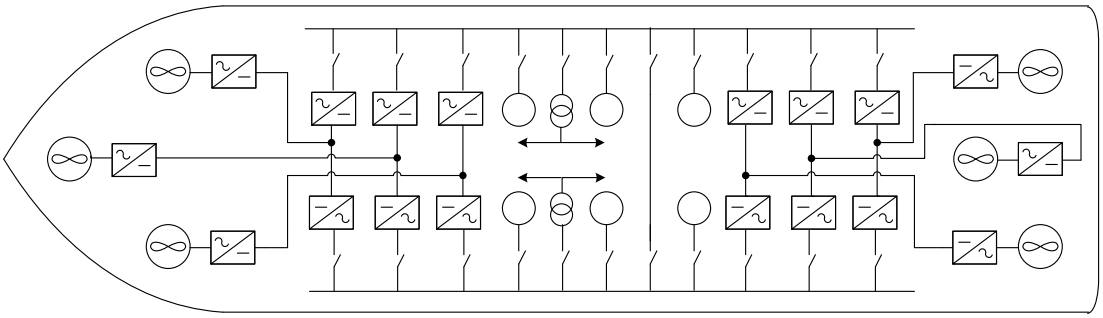

**Figure 4-Arrangement of Siplink Based Propulsion System**

As is the case with AGP, the Siplink based power system or Advanced Thruster Control and Protection (ATCP) initiative is not simply an add-on to a conventional power system to mitigate one particular disadvantage or another but a completely new approach to the design of fault tolerant power systems that provides a raft of other advantages in addition to improved fault isolation.

Central to the power system design is the Siemens' Siplink developed by Integral Drive Systems of Switzerland. This adaptation of grid interconnector technology allows two separate power systems to be connected together and transfer power either to and from each other or to a load at their common point by way of bi-directional ac to dc converters.

Although it can be argued that each Siplink forms a common point between the two power systems the ac/dc converters have inherently high impedance provided by the reactance of the drive transformers and the line reactors within the Siplinks. Thus, faults occurring at the common point created by the dc bus will affect both power systems but to a much lesser degree than in a more conventional power plant operating

as a common power system with closed busties. It could be argued that, there is no 'transfer of fault' (as required by DP rules and guidelines), if the level of disturbance is so small that it has no effect on the generators or consumers. In addition to the passive protection provided by the relatively high impedance, each Siplink has a range of protective functions designed to shutdown a faulty unit before a serious fault develops. Siplink based power systems can also be operated in common power system mode in which case fault tolerance is dependent on the ride-through and restart capabilities of HV and LV consumers as in a conventional plant.

Providing each thruster with a true dual supply means that all thrusters remain available following a partial blackout. There are advantages in terms of the amount of thrust that can be developed by having more thrusters operating at low load than a few operating at high load as is the case with conventional propulsion systems designs following loss of one main switchboard.

Mathematical modelling of the power system's response to fault conditions has been carried out but there has also been an opportunity to witness failure effects in service when two Siplink line reactors with manufacturing defects suffered phase to phase short circuits during sea trials. In both cases all generators and all healthy thrusters remained on line. The 480V power system was unaffected and the faulty ac/dc converter was successfully isolated by the protection scheme.

## Autonomous Operation

One of the main design goals in developing the new generation of propulsion systems was to make each redundant element of the DP system as independent as possible. Each thruster is served by a Main Siplink and an Auxiliary Siplink as shown in Figure 5. The Main Siplink supplies the thruster motor (or motors) and the Auxiliary Siplink supplies all the auxiliary services required by the thruster including, cooling water, ventilation and hydraulic power. Autonomy is not, however, limited to self contained auxiliary services. Each thruster drive control system has all the intelligence necessary to start the thruster and make it ready for DP control. Each Auxiliary Siplink has a battery bank which provides power to the control system and the converters during a blackout so that the Main and Auxiliary Siplinks can be made ready independently of the main generators. To further reduce dependence on external control systems the Siplinks are programmed to auto start and reconnect in the event of a blackout.

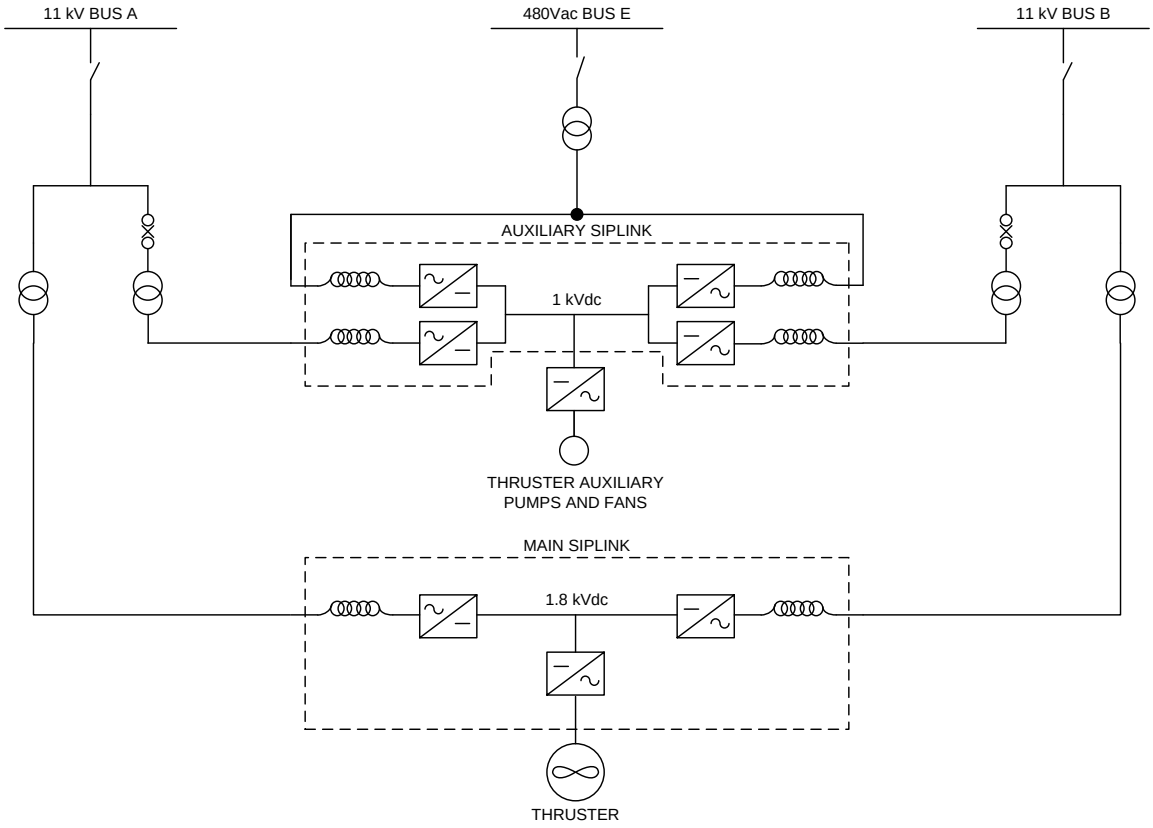


**Figure 5-Arrangement of Main and Auxiliary Siplinks**

From an FMEA perspective this emphasis on thruster autonomy makes it relatively easy to prove the independence of the thrusters as there are very few common points between them which could allow failure effects to propagate. Thruster independence also ensures a predictable failure response when the vessel is operating with some thrusters shut down. This is not always the case in more conventional designs in which a different combination of thrusters may fail in response to different subsystem failures.

## Blackout Recovery

Most designers of propulsion systems for DP vessels agree that a good blackout recovery system is an essential part of even the most robust redundancy concept. In the Siplink based power system the emphasis is on optimising the speed and reliability of recovery. During the start up process, the Siplink battery bank is used to run the ac/dc converters in reverse to pre-magnetise the drive transformers so that there is no large inrush current when they connect to the main power system as there would be in a conventional plant. Such inrush currents are capable of tripping generators during automatic blackout recovery and normal practice is to have the Power Management System delay thruster connection until the power system is sufficiently robust to cope with the inrush transient. This means waiting until two or three generators are online which can waste valuable time. By eliminating the inrush current and making the thrusters ready in parallel with the generators instead of sequentially, the process of stopping the drift off and recovering position can start as soon as the first thruster and generator have connected. With this arrangement, blackout recovery times are largely determined by the connection time of the generators. FMEA proving trials confirm that recovery times are now measured in tens of seconds rather than minutes.

## Conclusions

Common mode failures in DP Class 2 power plant have been a persistent source of DP incidents on Diesel electric vessels. In particular the consequences of governor failures, AVR failures and the voltage dip associated with power system faults have proved difficult to eliminate in a way that does not introduce further commonality between redundant elements. The unique combination of Transocean's Advanced Generator Protection with a Siplink based power system arrangement addresses these issues and brings with it a number of other benefits including fast and reliable load shedding and rapid blackout recovery. The combined package represents a very significant improvement in station keeping integrity over conventional power plant designs.