DYNAMIC POSITIONING CONFERENCE
October 11 - 12, 2022

POWER 2 SESSION

Closing the Station Keeping Integrity Gap Between DP Power Plant Configurations using Open and Closed Busties

By

Steven Cargill & Bolshoy Bhattacharya - Noble Denton marine services

Ed Bourgeau and Jason Aspin - AKA

Michael Hensley - ABS

Aleks Karlsen - DNV

Ari Andrade Do Nascimento - Petrobras

Suman Muddusetti - Shell

Contents

Abstract

Industry experience has shown that variations in the fault tolerance of DP systems (of DP classes 2 & 3) are so large that a well-designed power plant configured with closed busties, which has been verified and validated by comprehensive analysis and testing, can have better station keeping integrity than designs using open busties. However, this approach to verification and validation is far from universal.

As such, there is still a widely held view that, DP vessels operating with split power systems (isolated power systems) will have higher station keeping integrity than those using configurations based on closed busties (a common power system). Recent loss of position incidents on DP vessels operating in configurations based on open busties have demonstrated that such confidence is misplaced.

The gross inefficiencies of isolated (split) power plant configurations means that configuring the power plant of marine assets as several small, isolated power systems (open busties) comes with significant penalties which include being unable to satisfy corporate and societal expectations for reductions in Green House Gas (GHG) emissions.

In her testimony [1] to the US Senate Committee on Energy and Natural Resources on May 17, 2011, Nancy Leveson (Professor of Aeronautics and Astronautics at MIT) referred to a practice believed to be unique to the oil and gas industry in which certain process safety incidents were categorized (labelled) as low probability when it would have been more correct to categorize them as low frequency. That is to say:

- These events ‘do not occur frequently’, for a reason.
- A change in conditions or circumstances could make such an event highly probable.

In order to ensure that blackouts on DP vessels operating with closed busties are actually low frequency events it is essential that vessels intending to operate in this configuration (to achieve mission objectives including GHG emissions reductions) demonstrate that the gap in station keeping integrity between closed bus and open bus configurations has been closed (this goal has to be achieved universally and not just by a few vessel operators with specialist knowledge).

This paper discusses failure modes, effects and other challenges involved in ensuring that redundant DP power systems, operated as a common power system, have the attributes of fault tolerance, predictability, reliability, and resilience needed to exhibit equivalent (or better) station keeping integrity to DP power plant operating with open busties. In addition to elements of Design, the paper will discuss the imperative to adopt an integrated and ‘systems thinking’ approach which incorporates the other equally important elements of Operations, Process and People.

Some of the failure modes that are not universally addressed in current DP power plant designs based on closed busties include:

- Generator fuel control and excitation failures
- Fault ride through capability
- Crash synchronizing of generators and busties
- Inadvertent connection of stopped generators
- Intermittent ground faults, transient phenomena, and arcing faults.
- Logical links dependencies in software
- Vertical dependencies within redundant groups associated with common mode of failure.
- Misconfiguration

Notes:

1. *The above list is not intended to be exhaustive. There are significantly more failure modes, but these are the examples that are discussed in the sections that follow.*

2. *It is emphasized that the effects of failure modes associated with physical and logical links (other than through the busties) and effects associated with failures and other abnormal conditions in vertical dependencies may manifest themselves also on open bus systems which have not effectively addressed physical and logical cross connections and common points.*

3. *The operational risk profile is agnostic to the DP equipment class. Due consideration of the need for comprehensive verification and validation should be applied to DP vessels carrying out a particular activity irrespective of whether they operate in an open or closed bus configuration.*

Advances in mathematical modelling (and the ease with which models of power systems can be created and used) can assist in addressing these gaps and must play a much more significant role in the verification and validation process. It is emphasized that modeling is complementary to testing and not a replacement for comprehensive validation testing.

Abbreviations

ABS	American Bureau of Shipping
AC	Alternating Current
ASOG	Activity Specific Operating Guidelines
BESS	Battery Energy Storage Systems
CAM	Critical Activity Mode
CAMO	Critical Activity Mode of Operation
Closed Busties	A DP power plant configuration in which otherwise redundant or independent power systems are connected to create a common power system
DC	Direct Current
DNV	Det Norske Veritas AS
DP	Dynamic Positioning
DPCS	DP Control System
ESD	Emergency Shut Down
ESS	Energy Storage Systems
F&G	Fire and Gas
FMEA	Failure Modes & Effects Analysis
FMECA	Failure Modes, Effects & Criticality Analysis
GHG	Greenhouse Gas
HV	High Voltage
IMO	International Maritime Organization
JDP	Joint Development Project
LV	Low Voltage
MIT	Massachusetts Institute of Technology
MODU	Mobile Offshore Drilling Unit
MTS	Marine Technology Society
OEM	Original Equipment Manufacturer
PMS	Power Management System
PWM	Pulse Width Modulation
STPA	System Theoretic Process Analysis
TAGOS	Thruster and Generator Operating Strategy
UPS	Uninterruptible Power Supply or Uninterruptible Power Source
WCFDI	Worst Case Failure Design Intent
WSOG	Well Specific Operating Guidelines

Introduction

Station Keeping Integrity is a subjective and qualitative term used widely in the DP community to describe the reliability, robustness, and resilience of a DP system. That is to say its ability to:

- Operate predictably and consistently on DP without suffering
    - Loss of redundancy
    - Loss of position and / or heading
      for an acceptable period of time,
- Resist the effects of failures and recover from their effects(4).
- Be resilient to the effects of hidden failures and human performance issues.

Note 4: *The basic recovery requirement is to be able to safely terminate the DP operation in progress, but some DP notations require automatic blackout recovery.*

Attempts to apply quantitative risk assessment (QRA) to DP operations have generally been thwarted by lack of data and the enormous diversity of equipment, designs, the quality of verification and validation processes to which they are subjected and inspection repair & maintenance throughout the operational phase of the vessel's lifecycle. Attempts to impose requirements for DP station keeping reliability are generally limited to stating that it must be no worse than a mooring system [2]. To address this objective, in lieu of QRAs, the DP community has focused on ensuring that diesel electric DP systems are single fault tolerant with sufficient DP capability and endurance in their failed state (worst case) to safely suspend operations. Proving this is true for systems using closed bus configurations requires considerably more effort and expertise than for systems configured with open busties, and this is the origin of the gap.

The DP community has long been divided over the subject of operating DP power plant as a common power system with closed busties. Operating the power plant as two or more isolated systems with open busties was seen as a relatively low burden path to acceptable levels of station keeping integrity. Although vessel owners recognized the benefits of reduced fuel consumption and maintenance that the closed busties configuration enables, responsible and knowledgeable end user charterers were (and still are) wary of the magnitude of the technical challenges involved in developing and operating a fully fault tolerant power system and in verifying and validating that fault tolerance on an ongoing basis.

In the last few years, two factors have shifted opinion in favour of using configurations based on closed busties as a preferred operating configuration for CAM (where there is confidence in both the design, and the verification and validation process). These factors are:

- Reductions in Greenhouse Gas (GHG) – GHG emissions are at the forefront of energy company policy. Corporate and societal expectations have begun to exert pressure to achieve such objectives in addition to maintaining focus on safety and station keeping integrity.
- Incidents with Open Busties - Evaluation of recent incidents recorded by one of the co-authors to this paper(5), which involved DP vessel's operating with open busties, suggests that there is an over reliance (and misplaced emphasis in IMO MSC 645 & 1580(6)) on power plant configuration as an assumed route to station keeping integrity.

  Notes:

  5. *Requirement to respect anonymity prevents further disclosure.*
  6. *At the time IMO MSC 645 was written, physical separation of redundant power system was the only dependable route to higher station keeping integrity. Advancements in technology offer a greater number of options but the emphasis on physical separation was retained in IMO MSC 1580.*

The traditional relative merits of the two bustie configurations are often characterised thus:

- Power plant operating with open busties is more vulnerable to a partial blackout(7) but less vulnerable to total blackout.
- Power plant operating with closed busties is less prone to partial blackout but more vulnerable to total blackout.

  Note 7: *Frequent partial blackouts are not without risk because the failure effect is large, and the surviving machinery has to rapidly accept the station keeping power demand. Thus, proving the performance of redundant equipment is equally important in vessels operating with open busties.*

Requirements for equivalent power system integrity (of closed busties to open busties) are expressed within Section 3.2.4 of the IMO Guidelines for Vessels and Units with dynamic Positioning Systems, IMO MSC.1 Circ 1580, 16th June 2017 and its predecessor IMO MSC.1 Circ 645. For DP class 3 systems this is expressed as:

'3.2.4 For equipment class 3, the power system should be divisible into two or more systems so that, in the event of failure of one system, at least one other system will remain in operation and provide sufficient power for station keeping. The divided power system should be located in different spaces separated by A-60 class divisions. Where the power systems are located below the operational waterline, the separation should also be watertight. ***Bus-tie breakers should be open during equipment class 3 operations unless equivalent integrity of power operation can be accepted*** *according to paragraph 3.1.4.'*

In theory, an open bustie circuit breaker should prevent all forms of directly coupled fault propagation in a power system but a closed bustie is only one of many possible fault propagation paths in a practical DP system. The overall risk picture is influenced by other factors such as those listed below:

- Hidden limitations in equipment capacity (e.g., poor performance in surviving equipment)
- Internal and external common cause failures (e.g., engine load acceptance, harmonic distortion which increases with subdivision of power plant)
- Common points not subjected to verification and validation (e.g., industrial mission equipment)
- Software in common control systems (e.g., PMS & DPCS)
- Safety systems not divided along the lines of the DP redundancy concept (e.g., ESD, F&G)
- Networks connecting all redundant equipment groups (e.g., digital / analogue load sharing, vessel control systems, safety systems)
- Misconfiguration & human factors (e.g., human performance).

Classification societies have introduced specific rules, notations and qualifiers for DP systems designs intending to operate with closed bustie. Initially these were additional rules within existing notations:

- Rules for closed busties in DP class 3 require features such as redundant / independent protection systems, self-diagnostics, (and other methods for detecting hidden failures), realistic power system testing and mathematical modelling.
- Rules for DP class 2 tended to have less stringent design and verification requirements in line with the concept of DP Equipment Class being chosen on the basis of the consequences of losing station(8).

In many theatres of operation, DP class 2 vessels perform all the same roles as their DP class 3 counterparts although DP class 3 has become an expectation for MODUs.

Note 8: *Decisions by charterers and/or the flag administrations to dictate some level of fault tolerance and fault ride through testing (beyond what is prescribed in established DP notations) has led to the development of the Class notations listed below. These optional notations have been accepted by charterers as confirmation of higher system attributes, integrity, and testing.*

The role of the classification societies

The classification societies provide rules and verification services and play a leading and essential role in defining minimum standards and more recently a range of optional notations and qualifiers to satisfy industry demand. Classification societies ensure that DP vessels are designed and built-in compliance with the rules for assigned notations and qualifiers. The classification societies offer notations that they believe align with the three IMO DP Equipment Classes (and some that deliberately do not for defined reasons). However, responsibility for ensuring the vessel has an acceptable level of station keeping integrity, for its intend industrial mission, lies with the vessel owner and the charterer. The ability of different notations and qualifiers does help introduce transparency into the design process and allow 'knowledgeable' stakeholders to understand any compromises that are being introduced. Typical special DP notations and qualifiers include:

Table 1 Special DP Class Notations and Qualifiers – See References [3] and [4] for full details

ABS	Enhanced System Notation (EHS)	EHS-E	Electrical
		EHS-P	Power System and Thrusters
		EHS-C	Control
		EHS-F	Fire and flooding
DNV	DYNPOS(E) & DYNPOS(ER) (Enhanced Reliability DP notations)	CB	Closed Busties
		CBT	Closed Busties Tested
		CBS	Closed Busties Simulation
	DPS & DYNPOS	CB	Closed Busties
		CBT	Closed Busties Tested
		CBS	Closed Busties Simulation

In broad terms, modern verification and validation requirements for DP power plant configured with closed busties tend to be much more stringent than for open busties and demands the use of more advanced verification and validation tools and processes. This increased effort tends to spill over into the whole design and is not limited to the power plant. When properly executed this increased focus will produce a higher level of station keeping integrity.

As mentioned above, the classification societies have responded to industry demand by introducing additional qualifiers to provided different levels of DP system specification and verification which ultimately translate to different levels of station keeping integrity (although no attempt is made to quantify this). What is clear however, is that a significant number of vessels initially fail in their attempts to achieve the qualifiers that offer the highest station keeping integrity. Thus, it seems likely that those that do not undertake the more rigorous testing regime are at higher risk of harbouring defects that can defeat the DP system's redundancy concept.

Visualizing the station keeping integrity gap

Figure 1 attempts to depict the relative station keeping gaps created by the differences in Equipment Class, bustie configuration and the realities of practical verification and validation. The reasons for each gap are shown above the column but essentially:

- **DP Equipment Classes** - The equipment classes differ from each other in terms of their single failure criteria:
    - DP1 - not single fault tolerant
    - DP2 – single fault tolerant for failure of active components (fire, flooding and passive (9) components not considered)
    - DP3 - no exception in the definitions of single failures.
- **Ideal V Reality** – The reason for the difference between an ideal system and reality is that there are fault propagation paths in all DP systems where the station keeping integrity relies on protective functions and mitigation measures. However, poor design, verification and validation are capable of significantly reducing the confidence level in the station keeping integrity of DP vessels in the real world. Additionally, throughout the DP vessel's life cycle, lack of management may lead to divergence from the designed integrity level.
- **Open and Closed busties** - The difference between open and closed bus is that there is at least one more fault propagation path and several more failure modes, where fault tolerance relies very heavily on a comprehensive range of verified and validated protection functions which is also in need of periodic reverification.

The station keeping gap that has to be closed (the target) for a DP class 3 vessels configured with closed busties is shown by the orange area.

Note 9: *Some DP notations define a list of passive components that must be considered to fail. IMO MSC.1/Circ. 1580 states that for equipment class 2: "Common static components may be accepted in systems which will not immediately affect position keeping capabilities upon failure". DP2 notations may also have less comprehensive testing requirement and accept mitigation of the common causes of a particular failure mode rather than complete mitigation of all possible causes (example – AVR sensing failure detection rather than protection against over excitation as required for DP3 closed busties. Adding additional notations or qualifiers may increase the requirements also for DP-2 notations).*

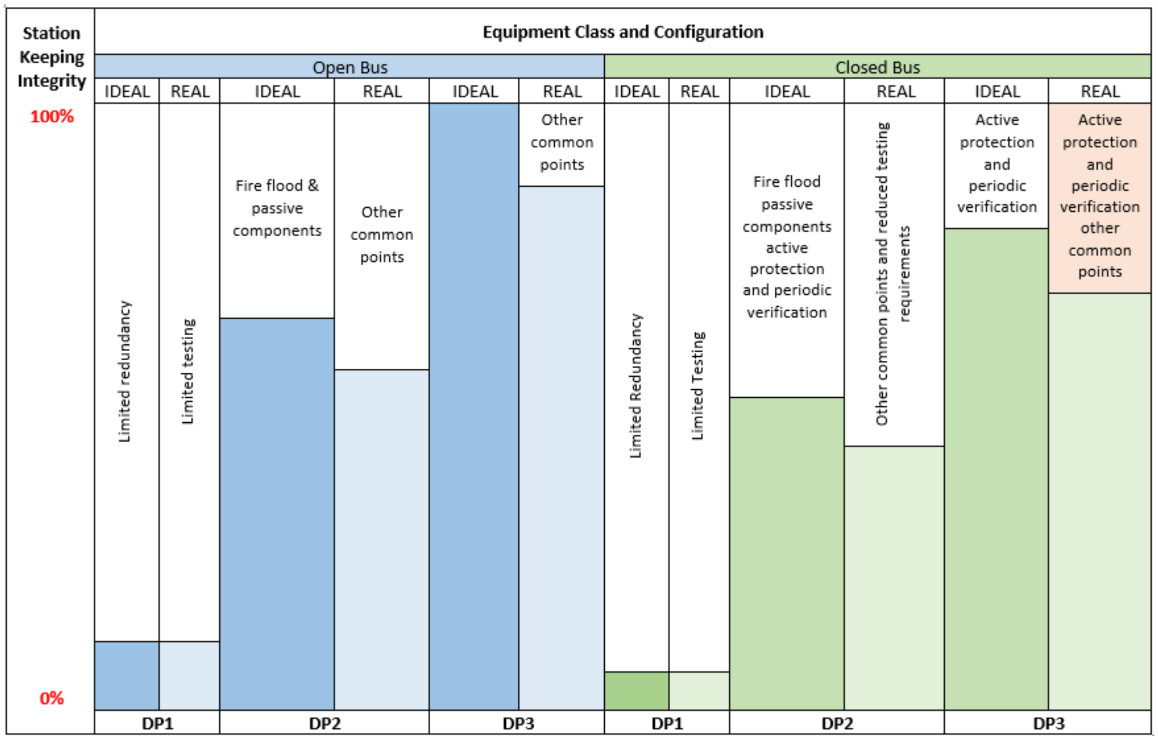


Figure 1 The station keeping gap created by the equipment classes, reality and bustie configurations

Closing the station keeping integrity gap

In practical terms, it appears that the gap between closed bus and open bus configurations has narrowed because DP incidents, related to power systems, have also occurred on vessels operating in open bus configurations. Evidence therefore suggests that the station keeping integrity of DP vessels operating with open busties is arguably, not as good as it is intended to be. There are many aspects of the DP system design that are not influenced by power plant configuration. If conscious efforts are expended to reduce the existing (and detrimental!) variability in the verification and validation process, a comprehensively proven closed bus power plant design can further improve station keeping integrity (actual and perceived) when compared to a poorly verified and validated power plant operated in an open bus configuration.

However, making an argument that the integrity gap has closed because open bus power plant does not actually have the integrity attributed to it is not one that generally finds favour amongst risk holders and classification societies. What is sought are assurances that the integrity of a power plant operating with closed busties is equivalent to that of an idealised open busties power plant design. Achieving this in an acceptable manner requires:

- Addressing the closed bus power system's vulnerability to total blackout to a level equivalent to a comprehensively proven system based on open busties.
- Reduced reliance on experiential knowledge to develop fault tolerant systems.
  Note: *The sentiment expressed in the latter bullet point can also be expressed as 'Not learning one Blackout at a Time!'*

Achieving and sustaining this level of integrity, over the life cycle requires attention to the well-established themes of:

- Design
- Operations
- People
  and
- Process.

The influence of these themes on the station keeping integrity of power systems operating with closed busties is examined in the sections that follow.

Design

Design rules for DP vessels

Classification society rules facilitate the design of fault tolerant DP power systems operating with closed busties, but they do not dictate the approach that should be taken to developing the power system. Designers are free to develop any system that meets the rule requirements. However, the effort needed to verify some designs is much greater than others. Much of the burden of verification is placed on the designer to provide and/or commission engineering studies to support the conclusions of the DP system FMEA. It is often at this point that highly complex, and heavily integrated designs fail to achieve their full potential. Essentially, the verification and validation effort needed to prove such complex and integrated designs exceeds the capabilities of the current verification toolbox (including the DP system FMEA process). If such designs are developed to achieve identified benefits, the verification and validation process must be developed in parallel with the design from the outset. A well-documented design is fundamental in executing an effective verification and validation process.

In recognition of the reliance on active protective functions, some DP notations and qualifiers require that there be two independent protective functions for each failure mode that can propagate by way of the closed busties. There will also be greater requirement for testing and self-diagnostic functions to detect hidden failures. All these requirements can be found by reference to the relevant rule set. Active protection requires periodic verification if confidence in its ability to mitigate the effects of faults is to be maintained. Designing low burden test methods reduces pressure to curtail periodic reverification for operational reasons.

Vulnerabilities

Alternating Current (AC) power systems dominate the high-power end of the DP vessel fleet as Direct Current (DC) systems continue to gain favour in the logistics and construction vessel fleet. DC power distribution offers several beneficial properties in terms of their ability to control fault propagation but modifying and testing traditional AC power systems is likely to be the route to closed bus operations for many DP vessels.

The common point created by tying the switchboards together makes AC power systems vulnerable to a list of well-known and less well-known (and less well understood) failure modes including:

- Generator fuel control and excitation failures
- Lack of fault ride through capability
- Crash synchronizing of generators and busties
- Inadvertent connection of stopped generators
- Intermittent ground faults, transient phenomena and arcing faults
- Logical links dependencies in software
- Vertical dependencies within redundant groups associated with common mode of failure.

Creating a fault tolerant alternating current power system requires a holistic approach to design, verification, and validation. It is not something that is easily 'bolted-on' afterwards. A range of ready-made protection systems has been available for some time, from established control and power system manufacturers which address some, but not all of these failure modes. Specifying one of these protection systems is therefore only one small part of the process of creating a fully fault tolerant closed bus AC power system. The challenges posed by these failure modes are discussed in more detail in the sections that follow.

Generator fuel control and excitation failures

In AC power systems all the generators run in synchronism with one another and are held naturally in synchronism (within limits) by a synchronising torque. The frequency, voltage (some designs) and phase angle of incoming generators is matched closely to the grid before connection, and they pull into synchronism on connection with very little disturbance. Generators operating in parallel share the active and reactive power under the control of various types of load sharing systems. Faults in generators and their active and reactive power sharing systems are capable of rapidly destabilising the power system leading to loss of multiple generators. Failures to full fuel (Figure 2) or full excitation (Figure 3) are examples of failures which continue to be responsible for full and partial blackouts. Speed / Voltage droop mode is the simplest form of sharing active / reactive power. Operating in droop mode eliminates several failure modes present in many other commonly used methods. It also removes the need to compare the performance of generators to determine which is the bad actor. Protection systems which address these failure modes are available from established manufacturers (and all can be made to function effectively), but robust verification and validation is essential to ensuring the system provides comprehensive protection. Consideration should be given to verifying the protection scheme and its settings and parameters by mathematical modelling validated by secondary injection of simulated fault waveforms into the entire switchboard protection.

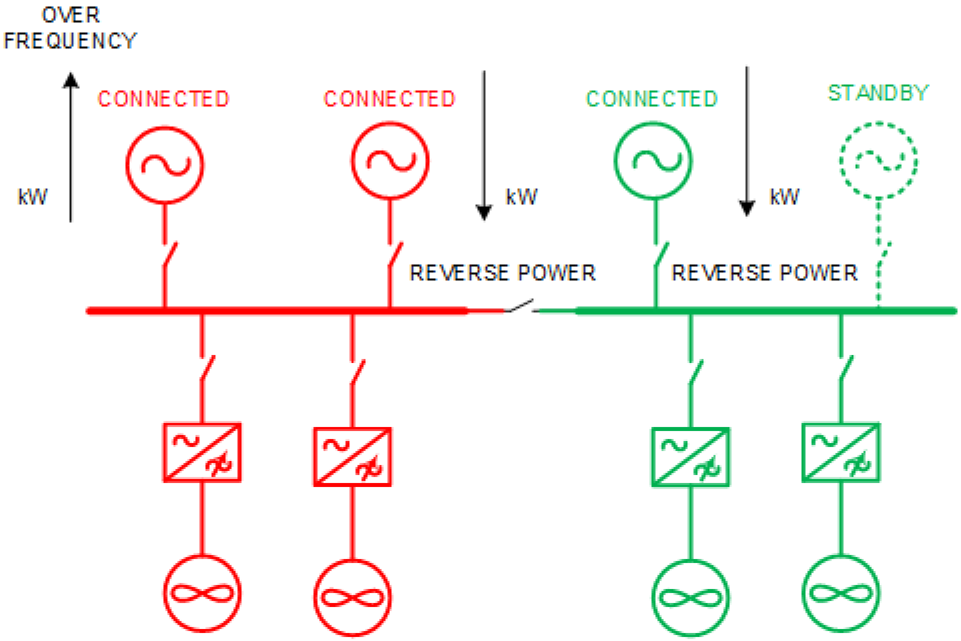


Figure 2 Blackout resulting from failure to full fuel in port side generator

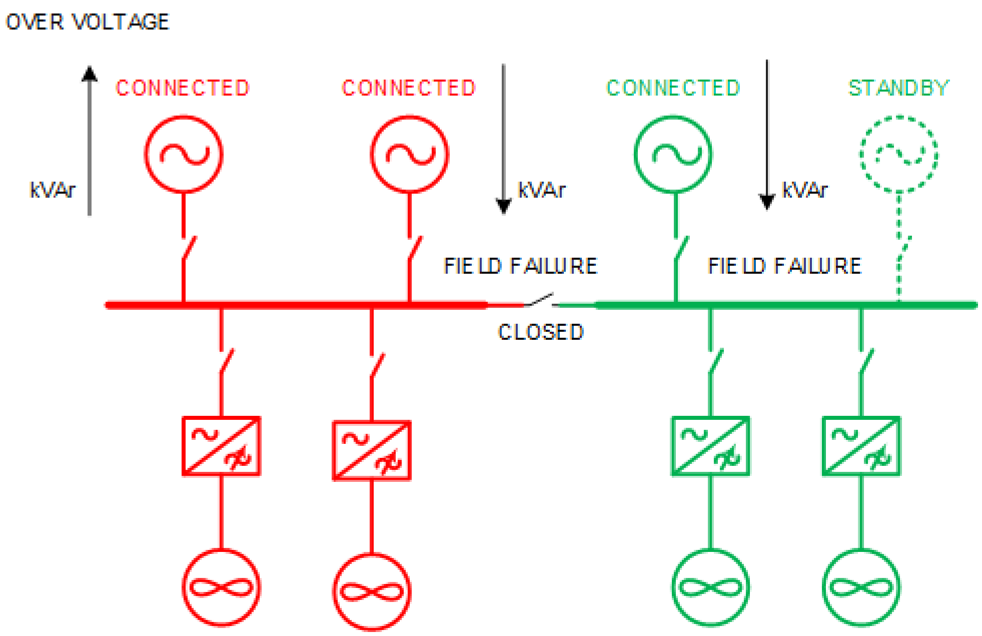


Figure 3 Blackout resulting from failure to full excitation in port side generator

Fault ride through capability

Fault ride through capability is the term used to describe the ability of generators and power consumers to automatically continue in operation (without stopping and restarting) following the occurrence of a severe voltage and/or frequency excursion in the power distribution system associated with clearing a fault (typically a short circuit fault). It is most commonly associated with thruster variable speed drives and motor control centres for auxiliary systems. Control power distribution systems typically include battery storage specifically for this purpose. Until more recently, using battery energy storage to provide ride through for large power convertors was limited to a few specialist designs but that has changes in recent years (See sections on ESS). Fault ride through capability for voltage source PWM drives may depend on engaging a dedicated ride through mode in the drive such as kinetic buffering (power is returned from the rotating propellor to maintain the DC link voltage in the drives and prevents multiple (all) thrusters tripping on low DC link voltage. Propellor speed at the time of the fault may limit the effectiveness of this strategy which may require augmentation with other functions(10). In the case of motor control centres, AC contactors (which are the most popular form of motor control) are known to drop out during voltage dips of even a few cycles duration. Various strategies to keep them energised include providing UPS power to the coils, mechanically latching contactors are another option, as is holding the run signal energised all the time. In the latter case the contactor may drop out and pull back in again when the voltage returns – Classification society views may differ on whether this constitutes a restart. However, one risk that is common to all strategies is the power distribution to all auxiliary systems trips on over current when motors reaccelerate after the fault has been cleared.

The MTS DP committee has published guidance on Methods for Proving the Fault Ride-Through Capability of DP Vessels with HV Power Plant [5]. Figure 4 is a real live short circuit test record taken from that guidance which shows the voltage dip that the power system consumers are expected to ride through without malfunction. In addition to the voltage dip the power system must survive the overvoltage during recovery and the current surge associated with reaccelerating motors for auxiliary systems which were feeding the fault prior to recovery.

Note 10: *Fault tide though functions can be present in more than one system and care must be taken not to create conflicting interactions. Examples of technical personnel from one manufacturer disabling functions in another manufacturers control system have been observed.*

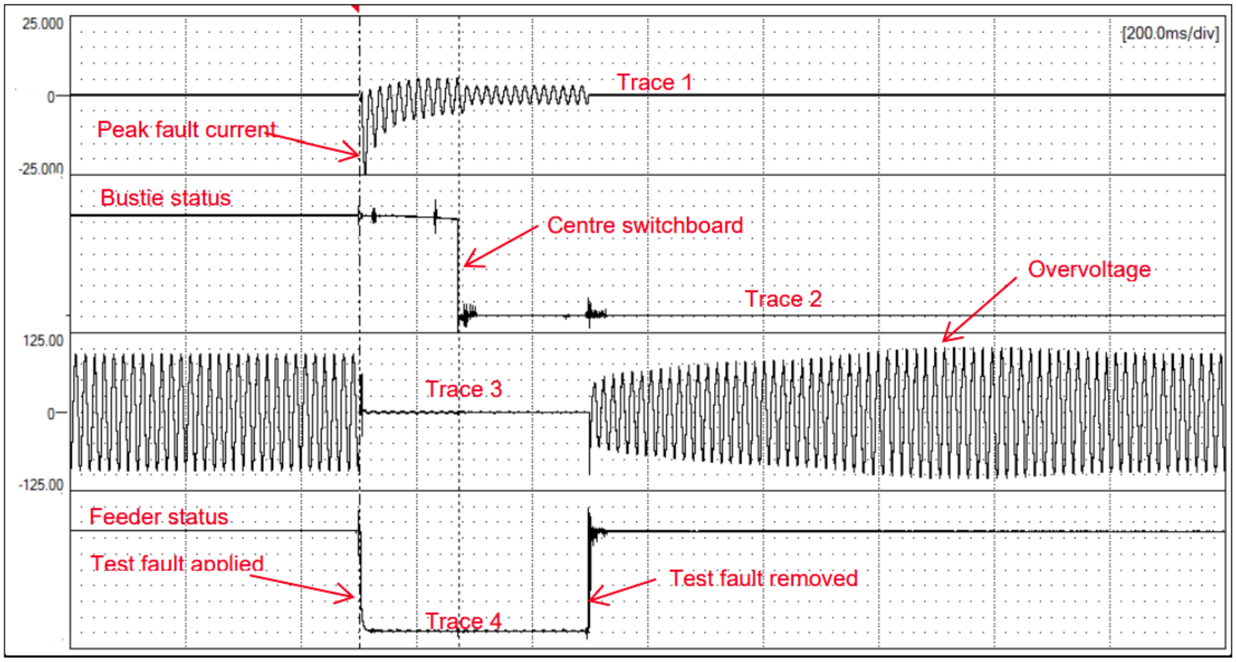


Figure 4 Live short circuit test on DP MODU – Courtesy MTS DP committee

Crash synchronizing of generators and busties

Figure 5 shows the synchronised connection of an incoming generator. Crash synchronisation (crash sync) or mal synchronisation are the terms used to describe the connection of a generator to a power system (or the connection of two power systems) when the power frequency waveforms to be connected together are significantly misaligned. Consequences range from an incoming generator tripping on reverse power to wild voltage and frequency fluctuations leading to loss of generators and thrusters exceeding the worst-case failure design intent. In some cases, generators may suffer mechanical damage including (but not limited to) broken couplings between engine and generator. There is no comprehensive protection again crash synchronisation as it has to be accepted that a generator circuit breaker may inadvertently fail to the closed position or close at the wrong point on the power frequency waveform. This is a rare failure mode but examples where this is known to have happened includes cases where the circuit breaker mechanism become ‘sticky’ through prolonged lack of use or inadequate maintenance.

Much can be done to reduce the likelihood of experiencing a crash sync by careful design of the circuit breaker control circuit. Redundancy in synchronising checks (i.e., two checks in series) can help protect against synchroniser error. The range of checks carried out by synchronisers can be extended although care must be taken to ensure the availability of a standby generator is not compromised by making the synchronising checks so onerous that a generator can only connect during periods of high power plant stability. However, these measures are not comprehensive and ultimately it is necessary to adequately demonstrate through effective verification and validation that the power plant is capable of surviving a crash synchronisation without incurring loss of position.

Power systems operating with open busties are not immune to crash synchronisation if there is only a single busties circuit breaker between redundant switchboards or the circuit breaker control system for dual bustie designs is based on a ‘leader-follower’ type design in which there is no dedicated synchronising check on the ‘follower’ circuit breaker.

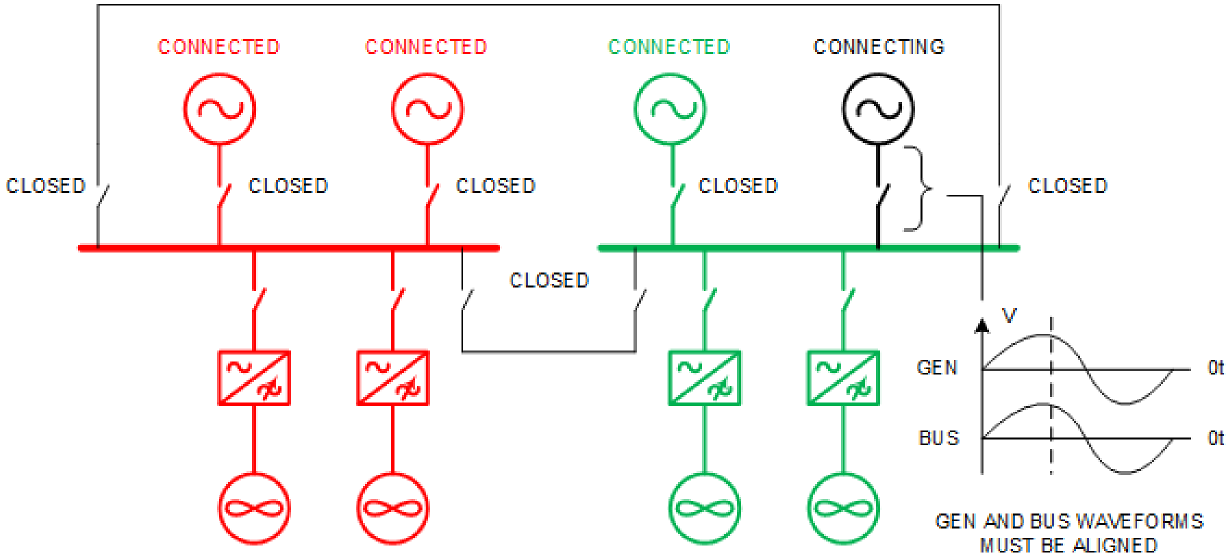


Figure 5 Crash Synchronization

Inadvertent connection of stopped generators

Inadvertent connection can occur for many reasons. One example relates to the mechanical 'on' function present in many circuit breakers which can be operated by a 'reach rod' from the front panel. Engineers carrying out repairs or maintenance on generators may need to simulate circuit breaker closure and this can often be simulated by switching the circuit breaker into a 'Test Position'. In this position the main stabs are disengaged but the control circuits remain powered up. The circuit breaker can then be opened and closed without risk of power system disruption. However, if the circuit breaker is not in test position (but the engineer believes it is) the mechanical 'on' function will generally not prevent the circuit breaker connecting the stopped generator. Administrative controls such as isolating the bus with the generator under test, lock and key access to reach rods may play their part in reducing exposure to this risk but ultimately, it is necessary to adequately demonstrate through effective verification and validation that a closed bus power system can withstand the effects of an inadvertent energisation without malfunction.

Intermittent ground faults, transient phenomena, and arcing faults

Although transient phenomena can be considered as a variation on a steady failure modes, repetition and variation in power system parameters (voltage, frequency and current) can cause very different effects with more onerous outcomes and consequences. It is beyond the capability of the DP system FMEA process, as it is currently practiced, to predict the effects of such phenomena. DP FMEA practitioners can make reference to these types of failures, but the effects must be obtained by commissioning a specific electrical engineering study from a source that has the requisite expertise in this field and the necessary tools to identify and conclude on such failure modes. The effects of intermittent faults in power system rarely feature in FMEAs for DP power systems. In fact, most closed bus FMEAs rarely consider that an AC power system is actually a polyphase power distributions system and failure modes can include various faults in one or more phases or combinations of same.

Although intermittent and transient phenomena are only addressed at a superficial level in contemporary DP systems FMEAs, the effects of such phenomena on power system performance and reliability are well understood in other power related industries [6]. In particular, the electrical utility companies are well aware of the effects of lightning strikes, arcing faults and intermittent faults. The effects of intermittent ground faults on the line to ground voltages in an isolated three-phase power distribution system are capable of generating common mode overvoltages that can cause the main bus to fail and destroy control voltage consumers in the entire power plant. Arcing faults are capable of creating a strike-restrike phenomenon that raise the line to ground voltage every time a restrike occurs as shown in Figure 6. Theoretically, there is no limit to the voltage that can be generated by this phenomenon but in practice this failure mode can cause a situation where over stressed components will fail in multiple redundant DP equipment groups creating a blackout or loss of multiple thrusters exceeding the severity of the Worst-Case Failure Design Intent (WCFDI). In 2015 DNV introduced new requirements to their rules for ships electrical systems intended to address and mitigate the effects of such faults.

RU-Ship Pt4 Ch8 Section 7.1.3 Overvoltage Protection states (July 2022):

'The following measures shall be installed to protect against overvoltage:

- *Overvoltage protection shall be arranged for lower-voltage systems supplied through transformers from high-voltage systems.*
- For high voltage distribution systems with insulated or high resistance earthed neutral, protection against transient Overvoltages caused by intermittent earth faults shall be installed. Unless equivalent protection with other arrangement can be achieved, overvoltage arresters shall be installed on the cable side of circuit breakers installed in the main switchboard.

Although this rule applies to all vessel types with the relevant power systems designs, it is not necessary to have such specific requirement in the DP system rules because eliminating or mitigating such failure modes is part of the requirement to ensure that '*no single failure will lead to a loss of position'* The specific rule requirements apply to systems with isolated and high resistance grounding systems. Prior to the introduction of these new requirements, it was generally accepted, within the DP community at least, that the damping effect of a properly designed high resistance grounding system would prevent voltage escalation to damaging levels, but events have proven that this cannot be assumed and should be proven. DP system FMEAs should refer to this failure mode and commission mathematical modelling of the response to intermittent ground faults. When necessary, these studies should form part of the verification and validation process for closed bus power systems with the relevant grounding types. An internet search for information on the effects of intermittent ground faults will return several papers on the subject which include guidance on developing models that are in the public domain.

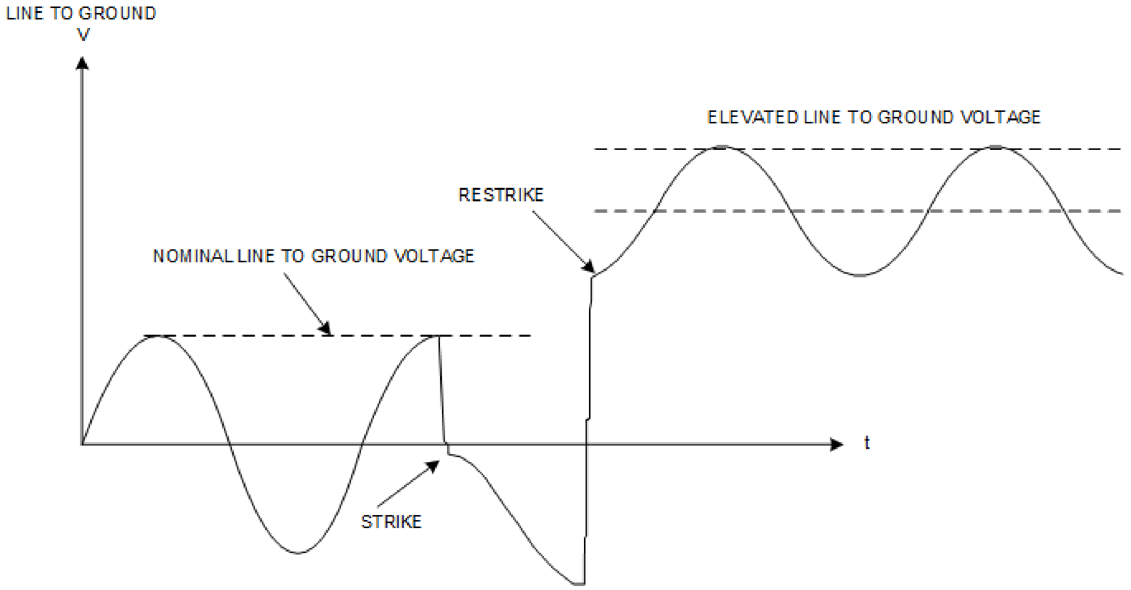


Figure 6 Line to ground voltage elevated to failure point by strike – restrike phenomena of intermittent fault [6].

Logical links & dependencies in software

Established guidance on the development of DP system FMEAs is hardware-focused and specifically excludes requirements for ‘FMEA of software’. However, it is difficult to arrive at any positive conclusion about the fault tolerance of a DP system without at least considering the functionality that software provides, particularly when it acts as a protective function upon which the DP system relies for its fault tolerance. In response to a high-profile DP incident in Norway (in which conflicting functionality led to a loss of position incident with economic consequences and high potential for risk to life and the environment) a Joint Development Project (JDP) hosted by DNV Maritime has brought together a large group of stakeholders from across the DP community to develop a parallel and complementary approach to the DP FMEA processes intended to close the gap created by limitations imposed by such a hardware focus. The approach taken by the JDP recognises that identifying the existence of such conflicts is the first step to preventing them causing DP incidents. A methodology has been developed which is intended to encourage designers, OEMs and other relevant stakeholders to provide information with the transparency to allow potential conflicts to be identified and mitigated at the design stage.

Vertical dependencies within redundant groups associated with common mode of failure or malfunction

The DP system FMEA process is currently not used to its full potential, but this is largely related to factors such as competence of practitioners, over reliance on FMEA practitioners to be subject matter experts in a diverse range of disciplines and under resourcing of FMEAs associated with a dysfunctional business model. However, even if all these issues were to be resolved DP FMEA would still have limitations that restrict its ability to identify potential causes of loss of position incidents. At a fundamental level this limitation arises from the recognition that abnormal or unsafe conditions can occur for reasons other than failures. A properly executed DP system FMEA is highly focused on dependencies between redundant DP equipment groups and fault propagation originating at common points and propagating to adjacent redundancy groups (or propagating from one redundancy group to another by way of a common point between them). However, abnormal conditions can arise in a common controller (such as the DP control, vessel control or power management system) or within each redundancy groups when hierarchical controllers exhibit unsafe control actions in response to some process model flaw or common stimuli (which may lead to a drive off). No failure (as the term is understood for DP FMEA)(11) is necessary for these unsafe control actions to occur although they can also occur in response to these types of failures. This additional focus on failures or abnormal conditions within a single redundancy group has led to the concept of Horizontal and Vertical dependencies as shown in Figure 7. Analysis methodologies such as System Theoretic Process Analysis [7] (STPA) do not have the inherent limitations of FMEA. These methodologies have an overhead burden that makes them less favourable for application to the more mundane aspects of DP system verification and validation, but they can be applied to specific aspects of the DP system to overcome the limitations of FMEA.

Some DP FMEA practitioners have tried to address these inherent limitations by extending the definitions of 'failures' to include unsafe control actions without having to identify a cause but it may be more effective and rigorous to apply a method such as STPA when it would be beneficial to do so. The concept of System Theory to which STPA owns its origins is also at the root of the methodology being developed in the JDP on DP System Integration.

Note 11: *FMEA practice assumes that there was, in the beginning, an intact state in which a system was operating as designed. At some subsequent point in time, a failure occurs, and the effects of that failure are observed to propagate through the system. STPA does not rely on a failure occurring for the system to malfunction. The system may exhibit undesirable behaviour without anything having to fail. This effect could be referred to as a design flaw in so far as the behaviour exhibited by the system is not desirable nor intended.*

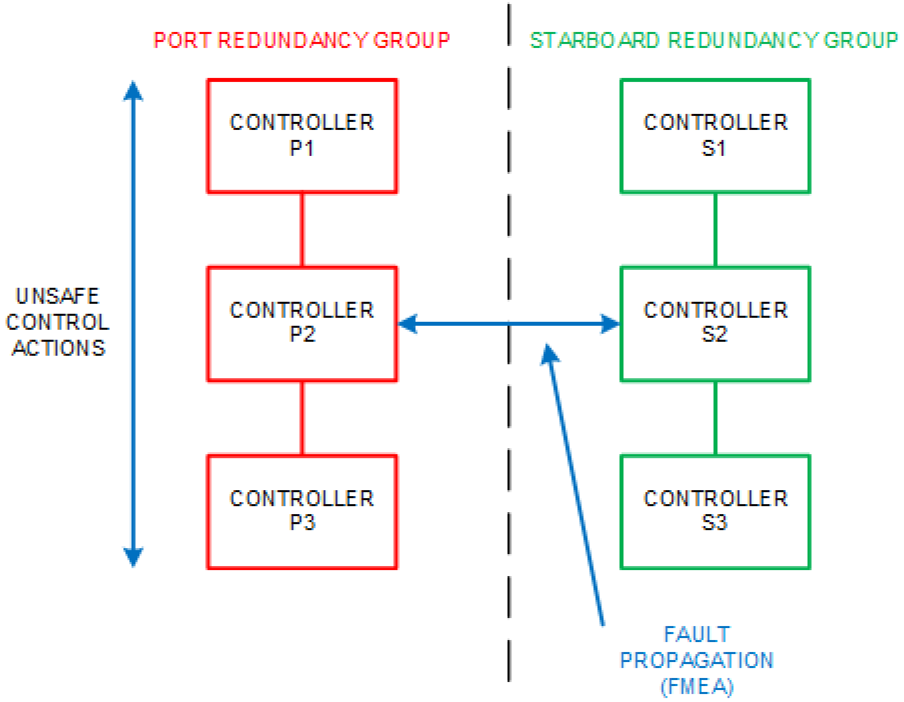


Figure 7 Horizontal and Vertical Dependencies

Alarm Management Systems

Alarm Management aims to produce an alarm system that really acts as an aiding tool to the operation. A poor alarm system will hugely affect the capability of the crew to recover the unit, especially when it fails outside the WCFDI. It is important to clearly warn the operator what failed and the consequences of the failure to station keeping, leading to the correct action and restoring the integrity level. IEC-62682 provides a robust framework to address all typical problems such as rationalization of alarms, logic and avalanche.

Energy Storage Systems

Energy storages systems can be applied to power systems for a variety of reasons, such as providing spinning reserve or peak shaving. They have a range of failure modes, but they can also act as a compensating provision used to mitigate failure effects in closed bus power systems. For the purpose of this discussion the concept of energy storage is limited to Battery Energy Storage Systems (BESS) which can provide a method to address some of the more challenging vulnerabilities of common power systems by effectively decoupling the thrusters (and other essential consumers) from the generators. Developments in battery technology permit power systems designers to provide large power consumers with fault ride through capability in the same way they provide control power consumers with fault ride through capability from UPSs and battery charger/rectifiers. Such is the amount of energy that can be stored in BESS that it is now practical to use them as spinning reserve in place of diesel generators and rely upon their power and capacity to suspend DP operations following worst case failure of the DP system.

A BESS typically consists of a large Lithium based battery bank coupled to a power electronic converter (invertor for AC connection, DC chopper for DC connection) which can act as a battery charger and / or electronic generators as circumstances dictate. BESS can’t provide ride through capability for thrusters in case of main bus disturbance if they are installed on the main bus although they may provide other functions such as spinning reserve and peak shaving. To provide ride through capability they must be embedded within the thruster drives system, as shown in Figure 8, so they can power the thrusters independently of whatever is happening on the main bus. Dimensioning BESS for such an embedded role has proven practical for MODUs with 6 or 8 identical azimuthing thrusters but the effort in translating the concept to project and construction vessels with a diverse set of azimuth thrusters tunnel thrusters, main propellers and rudders have proven to be challenging though not insurmountable if the benefits warrant the effort. MODUs and construction vessels have different risk profiles.

The use of BESS in logistics vessels is often to allow single generator plus single BESS configurations to be used within the 500m zone of fixed or floating assets. In some of today’s AC power plant designs, this is achieved by cross feeding mode through the DC link in the BESS with the AC side busties open. In many other AC power systems, achieving, single generator, plus single BESS mode involves closing the main busties between DP redundancy groups which introduces many other modes of failure and requires live short circuit testing to provide the necessary level of confidence for some end user charterers.

Cross feeding mode through the DC side and back on to the AC bus is not without its challenges. Using the DC link between redundant groups created by the BESS and its AC to DC to AC converters does not automatically eliminate the potential for fault propagation, although there are designs where the risk of fault propagation can be reduced to acceptable levels with minimum reliance on active protective functions.

The low voltage power systems on many existing logistics and light construction vessels are often not designed to be tested and alternatives to live short circuit testing have yet to find universal acceptance amongst charterers. Even in designs which are suitable for live short circuit and ground fault testing ‘Test Anxiety’ may be so high as to hamper project progress and the verification and validation effort.

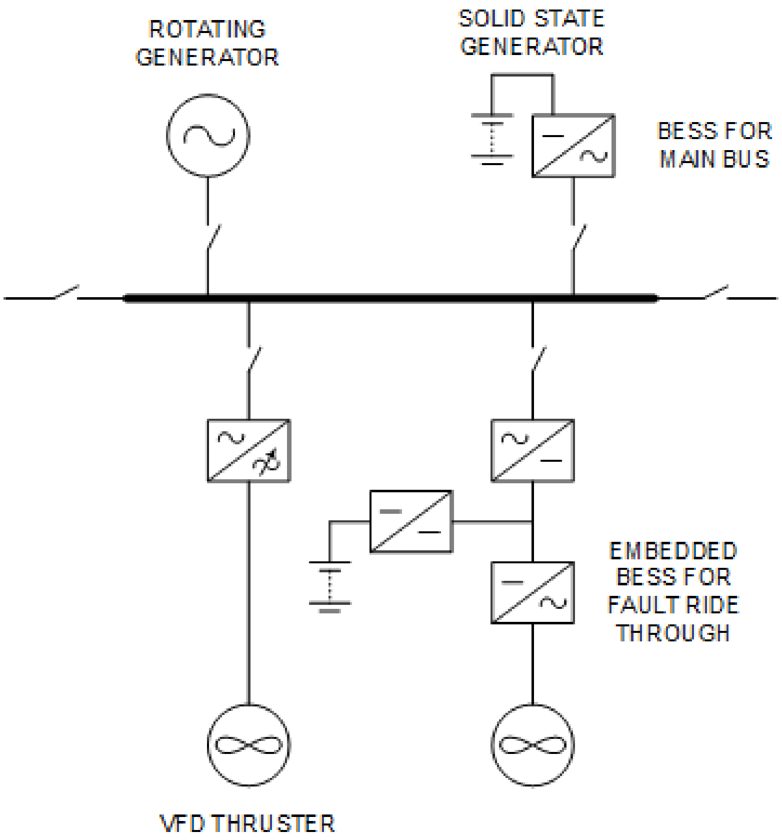


Figure 8 BESS embedded in thruster to provide fault ride through capability

Operations

Planning

DP operations planning for carrying out activities using a DP vessel configured with closed busties should not vary significantly from that used for configurations based on open busties provided the closed bus power system has undergone rigorous and comprehensive verification and validation and has the necessary reverification and revalidation processes in place to ensure it has equivalent station keeping integrity to an idealised DP power plant based on open busties. When this is the case, closed bus configuration can be used for all operations requiring the vessel to be configured for Critical Activity Mode of Operation (CAMO or CAM). However, charterers may consider it prudent and pragmatic to develop a more granular approach to operations planning that identifies activities that require the power plants robustness to be enhanced by connecting more (or all) generators and when it is acceptable to operate with the minimum number of generators required for redundancy. The outcome of this process is often referred to as a Thruster and Generator Operating Strategy (TAGOS). Activity Specific Operating Guidelines (ASOG) and Well Specific Operating Guidelines (WSOG) developed for this purpose may also prescribe the use of open busties for operations where the consequences of a loss of position are severe (particularly if the activities are of short duration where there is no detrimental long-term effect on other objectives such as GHG reduction) and/or there are fewer barriers or measures to control escalation (example – well control measures, heavy lift operations etc. or SIMOPS).

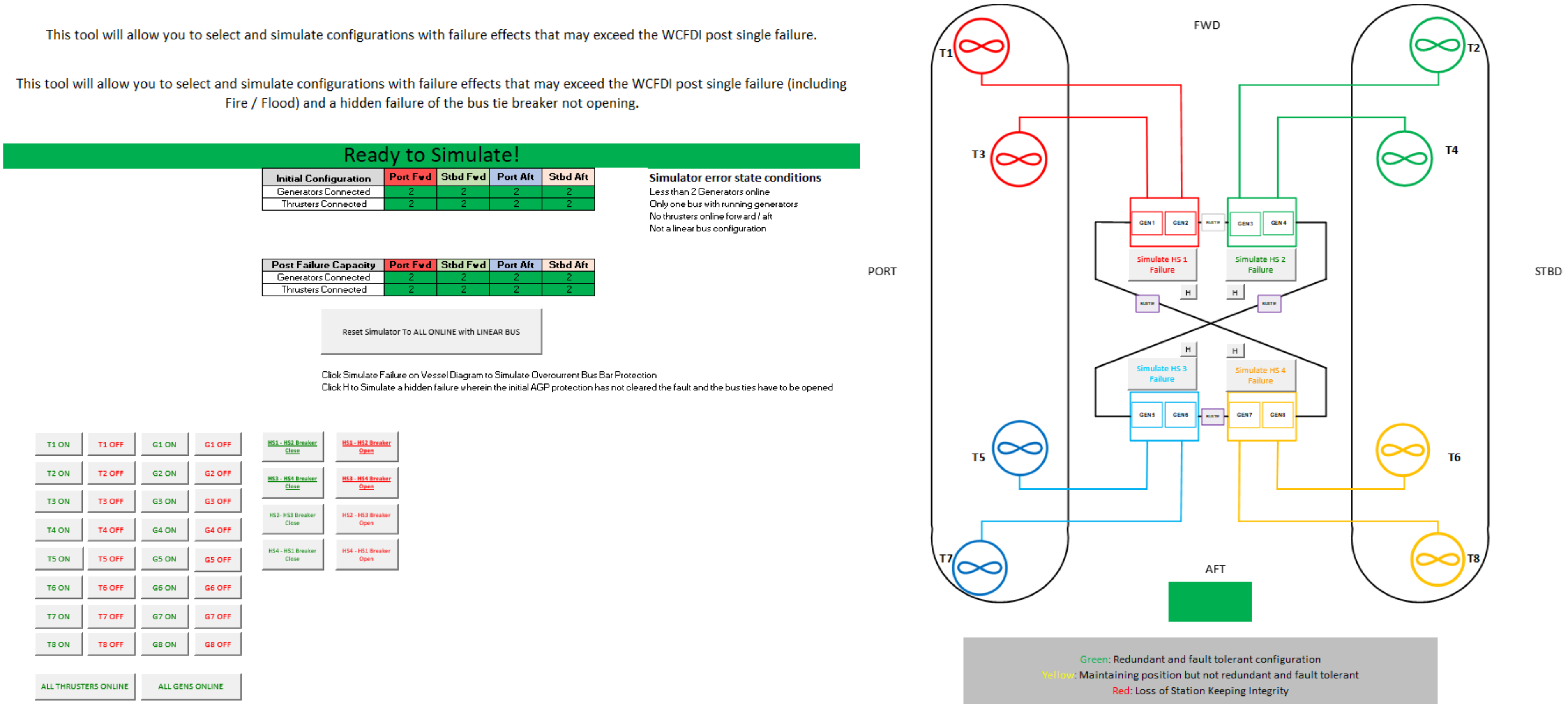
As power systems configured with closed busties have a greater reliance on protective functions, operations planning should reflect the need for confidence in the protections systems and attention to alarms and indication that can alert the crew to the possibility that there is deterioration in levels of performance, protection, and detection. The crew should have the means to recognise the onset of such conditions and be empowered to take pre-emptive measures, such as reverting to open busties configuration, when confidence levels are diminished. Examples of loss of confidence may include:

- Crew is uncertain
- do not understand:
    - alarms and / or indication
    - system actions / reactions/behaviour.

Other challenges that may be faced by the crew are associated with features such as redundancy in systems and fast acting protection systems where the loss of integrity may not be obvious. It may be hard to spot/understand consequence of such abnormal system indications, particularly when the indications may seem harmless.

Crew training on these issues combined with decision support tools, such as the example in Figure 9, can play an important role in assisting the crew in recognising the circumstances in which it is necessary to adopt additional risk mitigation measures. Decisions support tools can assist in the identification of unfavourable operating conditions and configurations but cannot account for every variation in system behaviour other than to reinforce the understanding that unease or uncertainty should be recognised as a trigger for adopting additional barriers to prevent abnormal power plant behaviour spreading from one redundant / independent DP equipment groups.

Heavily integrated DP systems are intended to assist the user and reduce burden on the operator. However, this complex ‘system of systems’ creates other, potentially higher demands, including higher cognitive burden on human operators related to performance optimization and dependency on sensors, software, and protection schemes, all of which are somewhat configurable and can exert influence over the fault tolerance of the DP system as a whole. Operators and maintenance personnel need to be aware of the role these features, and functions play in the DP design philosophy and its impact on the DP redundancy concept as described and analysed in the DP system FMEA for each vessel that they are assigned to. This need for awareness relates to the ability to assess confidence factor as well as responding to alarms or events.



This tool will allow you to select and simulate configurations with failure effects that may exceed the WCFDI post single failure.

This tool will allow you to select and simulate configurations with failure effects that may exceed the WCFDI post single failure (including Fire / Flood) and a hidden failure of the bus tie breaker not opening.

Ready to Simulate!

Initial Configuration	Port Fwd	Stbd Fwd	Port Aft	Stbd Aft
Generators Connected	2	2	2	2
Thrusters Connected	2	2	2	2

Simulator error state conditions
Less than 2 Generators online
Only one bus with running generators
No thrusters online forward / aft
Not a linear bus configuration

Post Failure Capacity	Port Fwd	Stbd Fwd	Port Aft	Stbd Aft
Generators Connected	2	2	2	2
Thrusters Connected	2	2	2	2

Click Simulate Failure on Vessel Diagram to Simulate Overcurrent Bus Bar Protection
Click H to Simulate a hidden failure wherein the initial AGP protection has not cleared the fault and the bus ties have to be opened

Green: Redundant and fault tolerant configuration
Yellow: Maintaining position but not redundant and fault tolerant
Red: Loss of Station Keeping Integrity

Figure 9 Decision Support Tool for DP Semi-Submersible

People

Engagement

The station keeping integrity of DP vessels is not only a facet of the technical design. A much higher level of technical engagement is needed from the engineering staff both shore-based and onboard the vessel to ensure that the significance of failure effects is understood, and that the health of the power system can be maintained.

Test anxiety

One factor that severely limits attempts to close the gap and establish confidence in the station keeping integrity of vessel's configured with closed busties is 'fear of testing'. More correctly, fear of the testing necessary to prove the correct operation of protection systems and essential power system attributes such as fault ride through capability under realistic conditions. This level of concern is not limited to fear of short circuit testing on the main bus but also, generator load acceptance and rejection testing, full power and thrust testing, control power short circuits and ground fault testing.

While this fear is understandable (and justifiable in some cases) it is a manifestation of the lack of confidence in the DP system and the consequences (perceived or otherwise) of damage to equipment that might render the vessel unavailable for a very extended period of time while expensive repairs to major systems are undertaken.

Those who have served as practical electrical engineers will be familiar with the expectation that an engineer responsible for proving a power system is earthed down and safe to work on will place their hands on the bus bars without hesitation, before allowing others to work on the system. This is done as evidence that they have full confidence in their actions and the isolations. Resistance to requests to prove that a nominally fully fault tolerant DP system is capable of resisting the effects of faults without loss of position is similar in so far as the risks of are now transferred to those that rely on that fault tolerance for their safety and to protect property, reputation, and the environment.

Fear of testing, and cost avoidance, is encountered more often once the DP vessel has entered service. Although there is often resistance to aggressive testing during the build phase, the vessel owner can at least rely upon the contract with the shipyard to produce a vessel that complies with requirements for fault tolerance and those verification and validation activities necessary to prove it. Classification society notations that specify short circuit and ground fault testing are an essential part of this process. During the build phase the OEMs are fully engaged and available to assist with the testing and carry out repairs.

A DP vessel may be advertised as fully complaint with a range of relevant closed bus notations but asking for this to be demonstrated by testing (particularly after an incident) can be met with fear and resistance.

Fear of testing manifests itself as:

- Pressure on classification societies to grant DP class 3 closed bus notations without realistic testing
- Pressure on classification societies to offer closed bus notations that do not require realistic testing
- Pressure on DP FMEA providers to develop test programs that only include non-aggressive testing
- Pressure to accept alternative forms of testing that may not properly test all essential attributes
- Resistance to carrying out testing as part of return-to-work protocols following a DP incident

Countering test anxiety

As with many challenging issues, fear of the unknown is mitigated by knowledge and experience. In 2012, heated debates raged within the DP community prior to the introduction of classification society requirements for live short circuit and ground fault testing, but 10 years on, this practice has become mainstream for major power system OEMs and resistance to its use at vessel delivery has all but subsided. While it is not uncommon for a DP vessel to fail live short circuit and ground fault testing at the first attempt it is unusual for there to be any significant damage. There is, so far, no evidence of any long-term consequences, and some vessels are approaching their third set of tests as part of periodic renewal. There are several ways to address fear of testing:

- Design and build power and control systems for the test conditions to which they must be periodically subjected – It is acknowledged that having the confidence to tests system that were not specifically designed to be tested may generate anxiety – Such system should operate with their busties open if there is no way to establish confidence
- Design closed bus power, control and protection system that do not require aggressive testing to prove their fault tolerance
- Make use of power system test-lab facilities to carry out aggressive tests where it is not absolutely necessary to use the vessel's power plant as the test set
- Develop alternative test methods that provide the same level of confidence as a realistic test.

While this last bullet point above would seem to solve several challenging 'technical' and 'people' issues it has proved difficult to develop tests that provide equivalent levels of assurance, in the correct modes of operation of protection systems and drive control systems as test programs which include live short circuit testing. This is related to:

- Limited use of mathematical modelling to predict, explore and improve understanding of fault tolerant power systems
- The complexity of protection schemes for power systems and their reactions to fault stimuli
- Lack of effective high speed data logging facilities (in the DP fleet) to allow lessons from power system failures to be studied so lessons can be learned and promulgated
- Limits to the DP communities' understanding of power systems and their failure modes
- Cost.

At present, the use of alternative test methods is considered most beneficial as part of preparations for more realistic testing – to improve confidence of a successful outcome at the first attempt. It can also be used for proving protection system performance and ride through capability at annual DP trials and class renewal (where appropriate notations exist) when there have been no significant changes or equipment replacement.

Process

Influential processes

The processes that most strongly influence the station keeping integrity of a closed bus power systems are the design philosophy and the verification and validation processes. Much has already been written and published in guidance on the subject of design philosophy but helpful objectives in the development of a closed bus DP power system include:

- Build to Test
- Test on Demand

- Healthy to Operate.

Satisfying the above objectives in a closed bus power system design address the challenges associated with:

- Proving the design under realistic failure conditions
- Reverifying the features and functions upon which its fault tolerance depends
- Continuously and/or periodically monitoring its performance for evidence of degradation that could defeat the redundancy concept.

Mathematical modelling of the power plant should be used at the design stage to explore the effects of various failure modes and variations in configuration. Reference should be made to literature on failure modes in power systems when defining a comprehensive set of protection functions and essential attributes. Modelling can also be used to extend the range of tests that can practically be carried out on the real vessel. This practice also helps to reduce reliance on experiential knowledge in the design of protections systems, essential attributes, and other mitigating measures. This process is the alternative to '*learning one blackout at a time'*.

Maintenance

The station keeping Integrity of DP vessels needs to be sustained during the whole life cycle. Control of Inspection Repair and Maintenance (IRM) activities during operations. Maintenance management is vital to achieve this, restoring the reliability of the safety and protective functions (redundant or not) through assessment (diagnosis, monitoring), correction (maintenance) and testing. IRM on critical infrastructure and components must only be allowed if it's clear that it will not compromise station keeping Integrity. Carrying out IRM on a DP vessel power plant operating with closed busties may carry additional risks associated with fault propagation through the tie lines. Although there will be protective functions (redundant functions in some cases) in place to addresses failure effects there may be no benefits in knowingly exposing the plant to a disturbance that can be avoided. Post failure DP capability may also be reduced by IRM even if fault tolerance is maintained.

Resource allocation for verification and reverification

Allocating sufficient time and resources is arguably more important than the verification and validation program itself. This is the case both for new buildings and in the sailing phase, where there can be a very large disparity between resources committed to building a DP vessel and that expended to test and verify that the owners have received what was ordered / agreed and that the design meets all its performance expectations. Nowhere is this disparity more visible than in the analysis, verification, and DP system FMEA activities.

Conclusion

The perception of a large gap in station keeping integrity between open and closed bus DP power plant owes much to the fact that for many years DP vessels were designed, analysed (FMEA), tested and approved with inadequate redundancy concepts and protection against faults that can propagate between redundant DP equipment groups by way of closed busties. Progressive insights from incidents have been leveraged by certain segments of the Supply Chain to address these issues. Much has been improved by leveraging the guidance published by industry bodies and forums and evolution of the tools that are currently available. These include a range of dedicated classification society notations and qualifiers for closed bus power systems specifying features, functions and test requirements intended to ensure fault tolerance.

Established Control and Power System Suppliers, a significant and influential community within the supply chain, have responded to industry needs by providing proven and effective protection systems with the ability to validate their efficacy by testing.

However, provision of these protection systems on their own is not sufficient to guarantee a fault tolerant closed bus power system. Nor are all protection systems of equal effectiveness. A range of other challenges have to be addressed and these have been discussed above under the themes of Design, Operations, People and Process. Adherence to good practice, established guidance on design and testing combined with a learner mindset offers the best path to gap closure leading to predictable, reliable, robust, and resilient closed bus power systems with equivalent (or better) station keeping integrity.

Certain segments of the DP industry are seeing a proliferation of DC power systems. DC power systems offer beneficial properties for control of fault development and propagation. Limitation imposed by power system rating are not the issues they once were. BESS are easily integrated into existing systems.

A conscious promulgation and adoption of the progressive insights, by the entire supply chain, on Industry’s ability to provide power systems designed to be operated in a closed bus configuration, meeting the assurance requirements of the most demanding stakeholders can help the DP Community deliver predictable, incident free DP operations and deliver on societal expectations on Green House Gas Emission Reductions. Adoption of the above approach by only a limited or select few sections of the DP community will erode the value that the DP community can deliver to society.

In simple terms, everything required to deliver on corporate and societal expectations (for GHG and SKI) already exists, (i.e., the technology, competence, tools etc) but not on the scale required. What may be lacking, is a full understanding of the scale of the commitment and resources required. Stakeholders in all aspects of DP vessel design and operation can expect to make significant changes to meet these challenges (because small incremental changes will not be sufficient in the timescale expected). It is unlikely that the DP community will be able to deliver on expectations if it continues to build and operate DP vessels in the same way it does today. Implementing all the changes needed in a single undertaking is likely to be impractical. More likely, is a series of significant ‘pushes’ towards what is required in each successive year.

References

1. Risk Management in the Oil and Gas Industry Testimony: Senate Committee on Energy and Natural Resources Prof. Nancy G. Leveson Aeronautics and Astronautics Dept. MIT May 17, 2011.
2. MODU Code 2009 ‘Code for the Construction and Equipment of Mobile Drilling Offshore Units’, 2009 Consolidated up to Resolution MSC.435 (98) (entry into force on the 1st January 2020).
3. ABS Guide for Dynamic Positioning Systems October 2021.
4. DNV Rules For Classification Ships Edition July 2022 Part 6 Additional Class Notations Chapter 3 Navigation, Manoeuvering and Position Keeping.
5. Techop (D-07 - Rev1 - Jan21), ‘A Method for Proving the Fault Ride-Through Capability of DP Vessels with HV Power Plant’, January 2021.
6. Transient Overvoltages on Ungrounded Systems from Intermittent Ground Faults, White Paper, Eaton, May 11th 2009.
7. STPA Handbook, Nancy G Leveson & John P Thomas, March 2018.