Return to Session Directory

DYNAMIC POSITIONING CONFERENCE
October 15-16, 2013

POWER SESSION

Challenges of Protection and Control System Verification on DP3 vessels with Focus on Ride Through Fault and Blackout

By Rune B. Andersen & Inge Haukaas

Siemens

Introduction

Worst case system disturbances manifest themselves in the form of short circuits between phases and/or ground. Short circuits produce high fault currents. The fault may be symmetrical three phase (to ground) faults. Other fault types produce non-symmetrical fault current. The magnitude of fault currents is usually largest for three phase faults. The severity and potential damage that can be caused by system disturbances influence the selection of protection systems.

There are also abnormal operating conditions that can lead to fault if not interrupted. These conditions are not associated with a fault current and involve:

- Over/under voltage
- Over/under frequency
- Thermal overload
- Unbalanced or asymmetric load

Purpose

The purpose of a protection system is to protect the electrical power system from equipment damages as well as to ensure safety and operational security. The protection cannot prevent system faults, but it can limit the damage. It shall protect people and plant from damage by clearing faults as fast as possible in a selective way.

Requirements

High demanding protection requirements are forced upon a system that is designed for class DP3 operations, which is applicable for all high risk operating modes such as drilling, where loss of position keeping capability may cause fatal accidents, severe pollution or damage with major economic consequences. The headlines in this context are technical redundancy, fault identification and isolation, fault ride through, high-speed fault clearance and selectivity. Furthermore, equally important as protection are prevention and mitigation of undesirable events, such as failsafe operability of the power plant and blackout recovery for generators.

Loss of position keeping ability is not to occur in the event of a single failure:

- In any component or system.
- Due to a single inadvertent act of operation.
- Due to failures or faults that can be hidden until a new fault occurs.

The stakes are even higher with more demanding challenges due to special requirements based on the power system operational ring configuration. A DP3 closed bus system takes system fault integrity to a higher level in comparison to the traditional power system solution with segregated power sub systems, i.e. open bus ties. It is thus desirable to improve such power systems of dynamically positioned vessel, and to reduce or even eliminate fault propagation in such power systems. It is desirable that most parts of the power system remain operable upon occurrence of faults.

This paper mainly considers the system protection against a single failure due to an electrical fault in the medium voltage generation and distribution system supplying the thrusters with power.

A fault protection system of a power system of dynamically positioned vessel must be provided. The power system has a power distribution bus having three or more bus subsections, electric connections including bus ties which connect the bus subsections in a ring configuration, and circuit breakers between the subsections. The fault protection system includes a generator circuit breaker for coupling a generator to a bus subsection, feeder circuit breaker(s) for coupling load(s) to the bus subsection, a first circuit breaker for connecting one end of the bus subsection to a bus tie that provides electric connection to another bus subsection, the first circuit breaker being a bus tie breaker, a second circuit breaker for coupling another end of the bus subsection to a further bus subsection, protection relays for operating the circuit breakers, and IEC 61850 communication links between protection relays that exchange high-speed information via said communication links.

The DP3 power system design including a fault protection system should be judged and rated by a failure mode and effects analysis (FMEA) in addition to trials by careful planning and execution of adequate test programs.

Redundancy

Redundancy in form of duplication of critical components, functions or systems increases the overall system's reliability with the intention to comply with the DP3 closed ring requirements. The duplication can either be fully independent as a parallel running backup system or partially independent as a fail-safe.

There are different forms of redundancy, such as hardware redundancy, information redundancy and software redundancy.

The protection system in principal is defined as shown in red outline in Figure 1. The circuit breaker mechanism is not defined as part of the protection system. The protection functional scope ends with the trip coils (open/close).

Hardware

In order to achieve a fault-tolerant design, the highest grade of hardware redundancy would be achieved by duplicating all of the sub components in the protection system. Two independent protection systems safeguard the power unit with a complete redundancy chain. An independent protection system is understood as a protection device with separate measurements, protection functions, control voltage supply and breaker trip coil. The prevailing philosophy is that the protection system is not stronger than the weakest link.

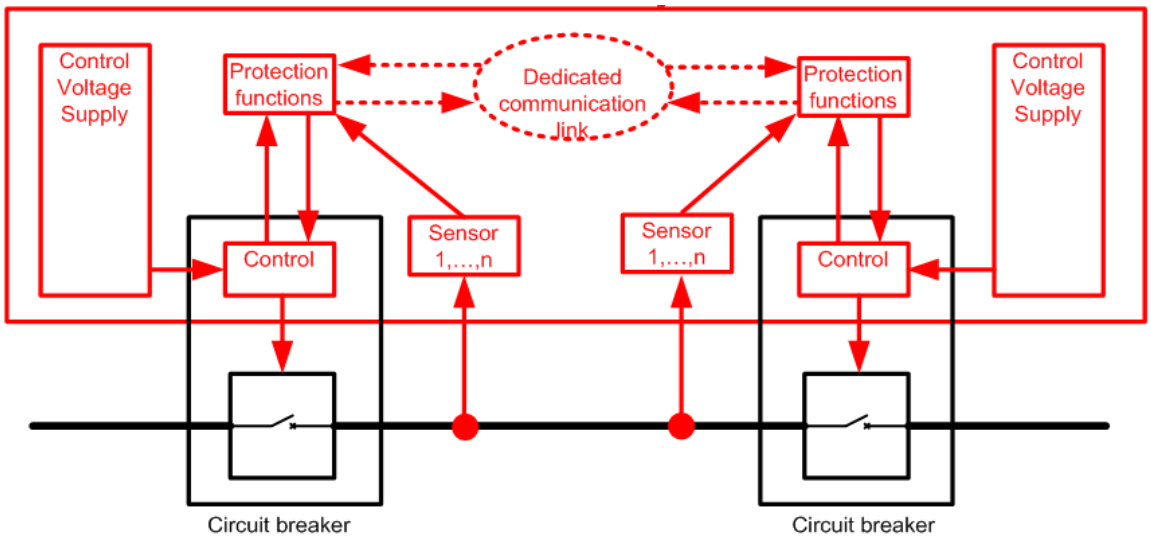

Figure 1 Protection system boundaries

Information

Information redundancy is achieved by designing an information system with high level of error detection and correction. If correction is not possible within the required time, safety is still maintained by turning the critical system functions into fail-safe mode. Fast communication directly between protection devices and bay control units is carried out according to IEC 61850-GOOSE. GOOSE is an especially fast and prioritized communication service that functions independently of communication between the server (bay unit) and client (centralized station controller). GOOSE is used for switchgear interlocking across bays as well as for special protection functions where the protection scheme is dependent on very fast signals between protection devices.
The DP3 closed ring automatic fault protection system is dependent on valid information. The communication link is achieved by a redundant fiber optical ring connection. GOOSE messages are monitored to avoid use of non-valid information. Signal interruption can occur during signal transmission. Transmission of messages from the sending end to the receiver is cyclic, even if no change of signal state occurs. The quiescent state is transferred to the receiver on a cyclic basis. The status of the IEC 61850-GOOSE annunciation obtained from the system communication interface is checked at the receiving device. For this purpose the logic module GET_STATUS is provided. The logic module decodes the status of a single point or double point indication, whereby the structure of the single point indication routed to the input is decoded to the VALUE of the signal and the status information ‘Not Valid’ (NV) when the annunciation is no longer updated within the expected time. The NV signal is used in the protection and control software for either blocking further actions such as protection functions or turning to safe-mode operations by the protection device.

Furthermore, extensive use of double point indications is preferred where high criticality or priority functions are dependent on the correct status information. Double point indications are designed reduce the risk of false status indications, such as breaker position. From two bit information, four combinations are possible where only two of the four states representing valid states such as OFF/ON or open/close.

The power system should be designed as a redundant high level information system feeding the operator in the control center with as much precise information as possible, enabling the operator to take the appropriate actions as soon as possible if manual operation in such a scenario is

required. Operator commands are carried out as a select before operate sequence, i.e. two stage command process with a software consistency check (quality tag) incorporated in the IEC 61850 command module. In this way, the risk of inadvertent operations is reduced to an acceptable level.

In an ever more modern power plant, large amounts of information are available for conditioned based monitoring, thus enhancing system reliability by failure prevention. Correct maintenance and service actions based on statistical values such as operating hours and trip counters could prevent failures to a larger extent.

Software

If possible, use of two different software protection algorithms or methodology will also enhance the system reliability by software redundancy. Modern numerical protection relays use complex protection algorithms and logic which place high demands on the protection engineer, e.g. relay secondary parameter settings such as pick up thresholds, time delays and directional determination must all unite in response to the primary fault in order to a detect and isolate the faulty power system.

A redundant protection system could be exemplified with a bus bar protection application realized through an independent bus bar differential protection system (System 1) running in parallel with an equally independent overcurrent protection system based on directional comparison end-to-end via GOOSE communication (System 2). System 1 could for instance use direct hardwired trip of all circuit breaker on associated faulty switchboard whilst System 2 makes use of GOOSE trip commands over the fiber ring.

Failsafe Operability

Failsafe operability of power plant and reduction of human error are mainly associated with switchgear interlocking.

Interlocking

The purpose of the system interlocking scheme is to prevent inadvertent energizing of generators, bus subsections and transformer feeders. Mechanical interlocks are provided as well as hardwired process level signals in combination with the introduction of IEC 61850 (GOOSE information exchange is accomplished by an integrated Ethernet switch) enables the system to achieve cross-bay interlock checks. Operation of devices such as circuit breakers, disconnectors and earth switches are subject to specific interlock conditions. Permissive for all switching operations in the system is governed by the system interlocking scheme which is executed by software logic configured in the combined protection and bay controlling device.

Trip Circuit Supervision

Redundant shunt trip circuits should be provided for each circuit breaker. Relays for supervision of the trip circuits of a circuit breaker enhance the fail-safe operability as part of the interlocking scheme. Trip circuit supervision relay monitors the trip circuit wiring from the positive supply to the negative supply whilst the circuit breaker is open or closed. In case of any failure in the circuit, an alarm is issued which are used as close permissive of the circuit breaker in the interlocking scheme. The operator should act on such an alarm by securing the plant operation, opening the circuit breaker and correct the fault.

Monitoring Functions

At process level, the medium voltage switchboard should be equipped with extensive monitoring capabilities – both for hardware, software and process monitoring. In addition, the measured values should also be constantly monitored for plausibility; therefore the current transformers and voltage transformer circuits are largely integrated in the monitoring. If any failures of these are detected, the criticality should be judged whether to alarm only, incorporate the alarm in the interlocking scheme, and block protection functions that depend on this information or finally trip the circuit breaker. A fault-tolerant design should aim to keep the component or system online as far as possible within reasonable limits.

Lockout

Particular protection function trips qualify for Lockout, i.e. following a protection trip the circuit breaker is interlocked against normal circuit breaker close operation. To yet again close a locked out breaker, it needs to be reset.

Sync check

When closing a generator or bus tie breaker, the synchronisation in the main switchboard must be given special attention to avoid un-synchronous power systems (U1 and U2) to be connected and thereby a possibility for total black-out. Due to the criticality of such a fault, at least three conditions must be achieved for safe closing; The bay controller ensures healthy measurements and interlocking, as well as two independent sync check relays in series in the circuit breaker close coil circuit.
The synchronization variables a) maximum voltage difference, b) maximum frequency difference and c) maximum angle difference are checked. When the variables on both sides are inside of permissible sync limits, the breaker shall automatically close.

Transformer Pre-magnetization

Connection of load(s) via transformer(s) must be given special attention. When transformers have been taken out for service and maintenance and shall be re-connected to the medium voltage bus, a pre-magnetization system should apply. The main objective for using pre-magnetization transformers is to reduce the inrush current and following voltage drop when a breaker feeding a large medium voltage transformer is being closed. Another important aspect is to verify that the transformer is healthy before closing the breaker.
Further important aspects are pre-magnetization conditions prior to closing the circuit breaker which is essential elements in the control sequence. A maximum voltage deviation over the circuit breaker both in voltage magnitude and phase angle should be used in the close permissive. After the circuit breaker is closed, the pre-magnetization source will be disconnected.

Connection of Dead Bus

Connection of a dead bus subsection to a live adjacent subsection (applicable if automatic blackout recovery failed) must be given special attention to avoid high inrush currents in cases where transformer feeders may still be connected to the dead system. If no measures are taken, high inrush current would flow through the bus tie towards the energized transformer(s) causing system voltage drop and relays to trip. Before closing a tie connection it is required to check bus voltage on side to be connected. If dead bus is acknowledged, trip of all associated breakers are required and tie breaker can close on affirmatively isolated bus. The energized subsection is ready for operation and transformer could be connected one by one, preferable pre-magnetized.

Fault Ride Through

Fault ride through for the relay protection plan is an important aspect to investigate in order to maintain the protection integrity of the system.

Short Circuit Fault

The severity of a short circuit fault is mainly dependent on fault location, i.e. the amount of impedance between the source and the fault location. In case of a short circuit fault on the medium voltage power bus (in proximity of generator), the bus voltage goes rapidly to zero and the short circuit current increases proportionally with numbers of generators online. After the fault is cleared the voltage recovers towards nominal voltage within 1...2 seconds, however the full transient may last several seconds depending on the performance of the automatic voltage regulator (AVR) as well as the generator parameters. The objective is to keep the voltage overshoot below 120% of nominal, regulate the transient back into normal operating voltage, and ensuring system stability.

In case of a short circuit fault at the transformer secondary, the bus voltage measured on the primary side is relatively low, could be less than 50% of nominal voltage. The short circuit current is dependent on the transformer rating and short circuit impedance. Measured at transformer secondary the voltage drops close to zero.

Generator overcurrent protection relay will detect the fault according to its short circuit decrement curve, whilst feeder relays of Thrusters, Drilling and Distribution transformers will depend on number of generators online. Bus tie relays will depend on number of generators online and the location of the fault, i.e. more complex fault detection is required.

All generators will absorb extra energy during the fault. Therefore, all generators will oscillate after the fault has cleared. As opposed to onshore power grids with an infinite bus system, gen-sets in offshore power grids share the energy between them before and after the fault. This reduces the out-of-step effect and provides damping of oscillations of the machines, thus regaining of the system stability. Fast fault clearing performance in terms of high-speed fault detection and isolation determines the system capability to regain stability after a fault on the medium voltage power bus. The time duration of a fault permits the generator rotor to accelerate. The shorter fault clearing time stops the acceleration sooner, reducing the risk of an out-of-step effect by having adequate synchronizing torque recovering to steady state.

Synchronization of Generators (or Systems)

Compared to the fault ride through, the synchronization of generators are more critical due to the fact that the gen-sets (or systems) are running on full voltage, unlike the a short circuit fault scenario when voltage drops to zero (approximately). This significantly reduces the fault consequences. The shaft torque may become dangerously high during synchronization, therefore sync check must be ensured to avoid connection of generators under non-synchronous conditions.

Sudden Disconnection of Loads

The voltage will abruptly increase if several loads are suddenly disconnected from the power grid due to e.g. false trip. The aim is to maintain the system voltage within 120% of nominal voltage during such a transient state. The relay plan must reflect this scenario in order to avoid spurious tripping due to over-voltage. Furthermore, the reverse power is relatively high on low loaded gen-sets, however only for a limited time, i.e. less than a second. The reverse power relay is usually set with a higher time delay than this, stabilizing the system against false tripping.

Fault Identification and Isolation

Fault identification and isolation by protection functions are discussed with focus on fault propagation in DP3 closed ring operation, i.e. closed bus ties.

When bus-ties are connected into one power ring, a fault in one section of the power system could propagate and lead to tripping of generators and thrusters in other sections of the power system, thus reducing the vessel's maneuverability and must be avoided. Running generators in parallel on a common bus have numerous advantages; however from a protection point of view it could also create higher risk for total black-out of the vessel's power system and resulting loss of position.

Healthy generators may act faulty due to the compensating response to a faulty generator's unhealthy behavior.

System Earthing

Each power cell (bus subsection) should have a high-resistance earthed neutral system. This is achieved by the main generators having a neutral earthing resistor (NER) rated for continuous e.g. 10A, connected to generator neutral. The NER is designed to limit the current flow to earth under fault conditions. The limited fault current is low enough to prevent damage to the generator, the distribution and other associated equipment, however high enough to for the protection relays to detect a faulty condition and take appropriate actions. Core-balanced current transformer with high accuracy (low current and angle error) for each circuit breaker should be provided. E.g., for a power system containing 6 generators the maximum ground fault current will be 60A. For such a system the core balance CTs must be according to IEC Class 1, 1FS10, 60/1A, in order to meet a trip level of 1...2A primary. The protection devices should have fault directional detection capability to selectively isolate the fault.

Selectivity

The protection system which interrupts and disconnects faults shall be implemented in such a way that the faultless part of the power system continues to operate as close to normal as possible. Protection functions shall never interfere with the normal load capacity of the unit protected, nor shall transient, dynamic or abnormal steady state phenomena owing to coupling operations be interrupted as long as these states does not lead to loss of station keeping capability. A normal fault clearing shall be done in a selective way so that the faulty part becomes isolated from the rest of the power system. The selectivity requirement can be departed in case of protection device or breaker failure. All short circuit and winding faults shall be disconnected by two independent protection systems if not other considerations are prioritized higher, such as risk of blackout.

The number of connected generator in each power cell (bus subsection) and distribution of these in the overall ring power system impacts on the protection trip philosophy with special attention to the bus ties, e.g. a bus bar short circuit fault cannot be tripped by a standalone protection device according to a traditional power system time-current selectivity on the bus tie since this action may isolate a healthy power cell where generator happens to be offline. Traditional time-current selectivity in case of short circuit and earth faults is not sufficient with respect to fault ride through in case of a fault near the generators. Strict selectivity requirements and low fault clearing times suggest that zone protection schemes should apply in order to isolate the faulty section of power system. Time-current selectivity on generator and bus-ties should only act as backup to the zone protection scheme.

Power Generation

The scope and choice of protection functions are influenced by the plant type, generator design and power system connection. The generator is usually directly and galvanically connected to the busbar, also known as a busbar connection. Several generators feed onto a common busbar. Table 1 comprises the protection functions suitable for an offshore power plant scale with medium sized generators +/- 5 MW.

Table 1 Fault identification and isolation

Fault type	Cause	Protection functions	Remarks
Overload	$S_{load} > S_{produced}$. Controller error. Maloperation.	Bearing an winding temperature monitoring (Pt100)	Evaluation of temperature sensor measurements.
Short-circuit (2 or 3 phase)	Deterioration of insulation. Winding displacement. Overvoltages. Manufacturing defects.	Overcurrent time protection (I>). Differential protection (ΔI).	Time delay must be coordinated with system protection.
Earth fault (stator)	Same as above.	Earth-fault direction in busbar connection (U0 and I0).	The protected zone is approximately 90% of stator windings.
Reverse power	Drive failure. Shutdown.	Reverse power protection (-P).	Necessary for diesel drive system.
Speed irregularities	Leaking stream valves. Sudden changes in active power. Controller error.	Frequency protection (f> and f<).	Multiple time-delayed stages recommended.
Overvoltage	Controller error. Manual maloperation.	Overvoltage protection (U>).	Evaluation of phase-to-phase voltage.
Impermissible under-excitation	Fault in exciter circuit. Operation in underexcited state (high reactive power demand in system). Maloperation. Controller error.	Underexcitation protection (-Q).	Only active if voltage is above a certain level. Field current 4-20 mA monitoring also incorporated.
Asymmetric load	Unequal loading of conductor. Loss of phase.	Negative sequence protection (I2>).	Time delay must be coordinated with system protection.

Highly advanced DP3 power system operating with closed bus-tie breakers requires additional protection functions to cover specific speed governor, engine, AVR and generator fault behavior. Monitoring of the generator performance based on available measurements and process information enables a generator performance controller to take appropriate actions to isolate the faulty generator and keep the healthy gen-sets online, thus regaining the system stability into steady state after the fault.

Power Distribution

A busbar is a point of convergence of many current branches, thus a concentration point of power. During a fault this will result in high destructive fault currents. A busbar fault endangers the stability of the plant as well as cause damage to the switchgear. Therefore a fast and selective

fault clearance is required (generally below 200 milliseconds including circuit breaker operation). The busbar system should be protected against short-circuit by use of differential protection devices as main protection. Redundant protection system could be employed by directional comparison overcurrent protection devices co-operating via automation and GOOSE communication as modern numerical protection devices also have fast PLC capability. High resistive earth-faults are detected and interrupted by directional comparison sensitive earth overcurrent protection system following the same concept. The power bus subsection is thus zone protected strictly selective, fully redundant with very fast fault clearing time in case of a short circuit or earth fault. Special design requirements prevails for the bus bar protection, the risk of overfunctioning must be eliminated so that it remains stable during through-flowing current in normal operation, likewise in the event of current transformer saturation.

The bus tie connects the bus subsections together via a power cable. Differential protection devices in each end are used in order to achieve a zone protection scheme as for busbars. The protection devices exchange protection data via fiber optical link. The link should also be used for remote tripping of the circuit breaker in remote end of the tie to ensure safety in case of a local breaker failure. Time coordinated and delayed towards up-and downstream breakers, multifunctional overcurrent relays are used for backup in case of failure of the primary protection system.

The transformer feeders are safeguarded by multifunctional overcurrent relays that detect and trip the fault as soon as possible. Thruster and Drilling transformer could trip instantaneous; however the Distribution transformer must be time-coordinated with low voltage distribution system. Two stages, one lower overcurrent stage and one higher stage, should prevail such that a fault on the transformer primary is disconnected instantaneous, and fault on transformer secondary is time delayed according to selectivity. Inrush detection should be used to block overcurrent trip in case of high content of 2^{nd} harmonics which are dominant when energizing a transformer.

Breaker failure protection should be employed on all circuit breaker in the system. A protection trip initiates a breaker failure start function that monitors the current flowing through the current transformer in conjunction with the auxiliary contacts of the circuit breaker. If there is no status change after a set time delay, the breaker failure protection issues a trip command to all circuit breakers feeding the fault, i.e. isolation of the fault.

Switch onto fault protection (SOTF) should be employed an all breakers where there is a risk of inadvertent energizing of an earthed feeder. The SOTF function initiates when a manual close command is given to the circuit breaker. By monitoring the current flowing through the current transformer and the said current is above a certain pickup threshold, the function will trip without time delay. The SOTF function must be stable with respect to inrush current, refer to inrush restraint.

Loss of conductor in the distribution system could cause fatal accidents and should be detected by negative sequence protection I2/I1 in conjunction with symmetrical current supervision. The pickup levels and time delays must be time coordinated with other breakers in the system.

Under/over- voltage and under/over-frequency in the closed ring power distribution system should be used with care. These system protection functions should always be coordinated with PMS, and only trip in the last resort due to risk of blackout.

Blackout Recovery

Loss of main power is a high criticality fault that is a threat to the vessel's maneuverability. A rapid and reliable recovery system should mitigate such a situation to the furthest possible extent. The recovery system is a joint effort from the switchboard detecting the dead bus condition at the same time initiating an automatic blackout recovery to the power management system which takes the appropriate further actions in order to live up the dead bus.

The first steps are controlled by internal switchboard logical controllers. Bus voltage blackout should be detected by a two-out-of-two criterion; analogue bus voltage measurements below e.g. 5% in conjunction with a dead bus signal from an external zero voltage blackout relay. The associated generator circuit breaker(s) and bus tie breakers should be tripped to isolate the bus subsection from the main power ring. (Trip command should be blocked if the dead bus is due to an isolated bus subsection fault or if manually isolated for service and maintenance purposes.) Transformer feeders should remain in the same position as prior to blackout. In order to enable rapid voltage recovery, the generator should keep on running, however de-excited by the dead bus trip. When the bus subsection are tripped due to black out, the system will be automatically reset so that it can be restarted and reconnected again according to a defined procedure avoiding any unexpected situations as to high load demand, high inrush currents or uncontrolled re-energizing of feeders.

The next steps are controlled by the PMS which will initiate the blackout restart after a plausibility check. The dead bus signal from the switchboard should be present, and the breaker positions should be open accordingly. Further important checks are that neither the generator nor the busbar are grounded, and no bay controller reporting that its own circuit breaker is in local position, indicating local or service operation of the switchboard. If plausibility checks are approved, the PMS starts the diesel engine (in case the engine was not running prior to blackout), closes the generator circuit breaker and generator excitation process is started. The AVR on the generator will ramp up the voltage to nominal value. The capability of the AVR to ramp up the voltage on dead bus allows the power system to soft-start with very low transformer inrush and thus avoiding spurious trips due to high inrush current and voltage drop. When reaching aprox 90% of the nominal value, the individual motors are started automatically based on the last running condition or by re-start from PMS. The pre-charge of the Thruster drive DC bus is initiated automatically by the drive itself when the supply voltage returns. When the Thruster drive DC voltage has reached aprox 85% of nominal voltage the incoming breakers will close and the drive is ready to start. The Drive is now ready for DP operation. The estimated time to achieve a successful automatic restart is below 20 seconds, depending on the diesel engine start up time.