TECHNICAL AND OPERATIONAL GUIDANCE (TECHOP)

TECHOP_ODP_10_(D) (EXTERNAL_INTERFACES)

AUGUST 2015

CONTENTS

FIGURES

1 INTRODUCTION - TECHOP (TECHNICAL AND OPERATIONAL GUIDANCE)

1.1 PREAMBLE

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

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

1.1.2 Feedback has also been received through the comments section provided in the MTS DP Technical Committee Web Site.

1.1.3 It became apparent that a mechanism needed to be developed and implemented to address the following in a pragmatic manner.

- Feedback provided by the various stakeholders.
- Additional information and guidance that the MTS DP Technical Committee wished to provide.
- Means to facilitate revisions to the documents and communication of the same to the various stakeholders.

1.1.4 The use of Technical and Operations Guidance Notes (TECHOP) was deemed to be a suitable vehicle to address the above. These TECHOP Notes will be in two categories.

- TECHOP_ODP.
- TECHOP_GEN.

1.2 TECHOP_ODP

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

1.2.2 The TECHOP will be identified by the following:

TECHOP_ODP_ SNO_ CATEGORY (DESIGN (D), OPERATIONS (O), PEOPLE (P))

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

1.3 TECHOP_GEN

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

TECHOP_GEN_SNO_DESCRIPTION.

- EG 1 TECHOP_GEN_01-WHITE PAPER ON DP INCIDENTS.

1.4 MTS DP GUIDANCE REVISION METHODOLOGY

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

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

1.4.3 Communications with stakeholders will be established as appropriate to ensure that they are notified of intended revisions. Stakeholders will be provided with the opportunity to participate in the review process and invited to be part of the review team as appropriate.

2 SCOPE AND IMPACT OF THIS TECHOP

2.1 SCOPE

2.1.1 TECHOP_ODP_10_(D)_(EXTERNAL_INTERFACES). The term ‘external interfaces’ as used in this Techop is not intended to refer to those interfaces that are routinely provided for station keeping purposes (example wind sensors, position reference sensors, gyros MRUs etc) but may be interfaced in certain industrial missions (example draught sensors, line tensions, pipelay tensions).

2.1.2 This Techop also addresses interfaces that may not be an input into the DP control system but could affect thrusters and generators and thereby position keeping integrity (example ESD systems, F&G systems, ventilation systems etc)

2.1.3 The increased emphasis on interfaces of ESD and F&G systems reflects the significant number of loss of position events experienced in industry.

2.2 IMPACT ON PUBLISHED GUIDANCE

2.2.1 This TECHOP impacts the DP Design Philosophy Guidelines and the DP Operations Guidance.

3 CASE FOR ACTION

3.1 FAULT TOLERANT SYSTEMS BASED ON REDUNDANCY

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

3.1.2 Loss of position may occur in several ways:

- **Drift off** – Insufficient thrust following a failure.
- **Drive off** – Exceeds thrust requirements or thrust in the wrong direction following a failure.
- **Large excursion** - Vessel returns to set point after a failure but with an unacceptably large deviation.
- **Force off** – The vessel has insufficient thrust in the intact condition to maintain position in the prevailing environmental conditions.

3.2 EXTERNAL INTERFACES

3.2.1 The term ‘DP system’ is defined as all equipment necessary for maintaining position and heading. However, there are other systems that interface to the DP system in various ways such as those listed in 2.1.1 and 2.1.2. Some of these interfaces may be provided to improve station keeping performance, but many play no direct role in station keeping. However, such interfaces have the potential to cause a loss of position if they fail or malfunction.

3.2.2 Such interfaces may not receive the scrutiny they deserve during design and verification phases, usually due to:

- Mis-categorisation as ‘not being part of the DP systems’.
- Often being retrofitted.
- The lack of a systems engineering approach in their implementation.
- A lack of understanding of the potential impacts due to failure or malfunction.
- A lack of testing of failure modes and their effects.
- Approval authority if applicable residing between different disciplines and potential for mis-alignment of understanding of impacts.

3.2.3 Existing rules and guidelines are adequate to guide the development and testing of these interfaces. Problems arise because of misinterpretation, misapplication or non-application of these rules and guidelines.

3.2.4 Reviewing the design of such systems and interfaces against the ‘seven pillars’ described in the MTS DP Vessel Design Philosophy Guidelines helps identify potential weaknesses or opportunities to increase robustness and predictability.

3.3 EXAMPLE EXTERNAL INTERFACES

3.3.1 Example external interfaces to the DP system include:

1. External force compensation.
2. Draught sensors.
3. Emergency Shutdown Systems (ESD).
4. Fire and Gas Systems (F&G).
5. Power control interfaces for industrial equipment.
6. Power and circuit breaker status for DP control system
7. Power distribution for industrial consumers.
8. Power distribution for life support consumers.
9. Fixed fire fighting systems – water mist – CO_2.
10. Communications equipment.
11. Navigation equipment.
12. Roll compensation.
13. Anti-heeling systems.
14. Group emergency stops

3.4 INCIDENTS CAUSED BY EXTERNAL INTERFACE FAILURES

3.4.1 Failure or malfunction of external interfaces have caused DP loss of position incidents. The examples below provide some insight into how and why these incidents occurred.

Example 1 Pipe layer - Failure of external force compensation input leading to buckling of pipe.

Example 2 Drillship - Failures of draught measurement system affects DP system model leading to drive off.

Example 3 Semi-submersible – Failure of industrial power control interface allows regenerated power from drawworks to trip all generators on reverse power leading to blackout.

Example 4 Drillship - Failure of ESD system- Communication errors in dual redundant remote I/O imitate activation of external ESD 0 causing the whole vessel to shutdown.

Example 5 Drillship - Failure of ESD system – Poor design of ventilation system combined with lack of robustness in declaring a confirmed fire. Automatic ESD 0 shutdown triggered by tank cleaning activities.

Example 6 Semi-submersible - Failure of ESD system – Excessive commonality introduced by using a single I/O card for all ESD pushbuttons – Software error trips all diesel generators when one card loses power and is reconnected.

Example 7 Pipe layer – Failure of water mist control system shuts down all three engine rooms when false pressure switch signal indicates water mist is being released.

Example 8 Pipe layer - Erroneous application of external force compensation led to loss of position and buckling of pipe.

3.5 GENERAL REQUIREMENTS FOR EXTERNAL INTERFACES

3.5.1 The general requirements for an external interface can be categorised as below:

- If complete loss of the external interface can adversely affect station keeping, then it must be redundant. – That is to say no single failure should cause loss of the service provided by the interface.
- If a failure of the interface does not affect station keeping, but malfunction of the interface could have an adverse effect, the interface must be designed to fail safe.
- Some types of interface will need to be redundant and fail safe
- Where redundancy is required it should be applied in a manner that supports the vessel's redundancy concept.
- Optionality for manual inputs to be provided if applicable (example external force compensation, pipe tension etc).
- Sensors, if any, to have optionality that provides use for monitoring without input as control.
- Any decision to use sensors / interface information for control should be supported by data obtained from implementation of a system's engineering approach which includes testing to prove failure modes and effects.
- Low level shutdowns of ESD and F&G systems should not automatically result in loss of thrust. They should trigger alarms and shutdown of equipment leading to loss of thrust should require manual intervention.

NOTE: Stakeholders may have additional requirements that may need to be addressed.

4 SUGGESTED IMPLEMENTATION STRATEGY

4.1 IDENTIFYING EXTERNAL INTERFACES

4.1.1 It should be possible to identify the external interfaces from the detailed design documents for the DP vessel or from a competently executed DP system FMEA. If the veracity of the FMEA is in doubt, consideration can be given to carrying out a DP FMEA Gap Analysis using MTS TECHOP_ODP_04_(D)_(FMEA GAP ANALYSIS).

4.2 ANALYSING EXTERNAL INTERFACES

4.2.1 Each application will present its own challenges:

- Identify failure modes that may propagate by way of these interfaces.
- Identify where redundant interfaces are required to provide continuity of essential information.
- Identify where a fail-safe design is required and the fail safe philosophy to be applied with consideration to the overall redundancy concept.
- Identify where unnecessary or unacceptable cross connections are introduced.
- Identify any lack of protective functions essential to ensure failsafe.
- Identify potential hidden failures.
- Identify any barriers that can be put in place such as adopting a manual control interface or isolating interfaces and cross connections.
- Identify and mitigate opportunities for configuration errors and acts of mal-operation.

NOTE: Due consideration to be given to adopting manual control interface or isolating interfaces and cross connections as the default unless adequate confidence can be demonstrated by implementation of a system's engineering approach including testing for failure modes and effects.

4.3 IMPROVING EXTERNAL INTERFACES

4.3.1 In addition to the points listed above it may be beneficial to carry out a review of the design against the desirable attributes listed in the MTS DP Vessel Design Philosophy Guidelines which are:

- Autonomy
- Independence
- Segregation
- Differentiation
- Fault resistance
- Fault tolerance
- Fault ride through

4.3.2 Not every system needs all of these attributes. A focused and systematic review of the design against these seven attributes may identify gaps, if any, as well as opportunities for improvement in the design.

4.3.3 In the context of this Techop, design for fault tolerance includes fail-safe philosophy.

4.3.4 Examples given in the sections which follow demonstrate how design issues have defeated DP redundancy concepts. Some of these design issues were identified during DP FMEA or proving trial but others only manifested themselves in service. The intent of inclusion of these examples in the Techop is to aid owners to conduct a review of their vessels for the presence of similar vulnerabilities.

5 FIRE & GAS AND EMERGENCY SHUTDOWN (ESD)

5.1 INTRODUCTION

5.1.1 Vessels conducting industrial missions with a 'gas hazard' are fitted with emergency shutdown systems (ESD) (example, MODUs- a requirement of the MODU code). Vessels which operate alongside vessels with the potential for hydrocarbon release may also be fitted with an ESD system.

5.1.2 The purpose of an ESD system is to prevent the escalation of the consequences of a hydrocarbon release and limit the severity and duration of such events. This is achieved by a combination of actions which includes cutting off the source of hydrocarbons and bringing equipment to a pre-defined safe condition. Isolation of sources of ignition is also performed on initiation of ESD.

5.1.3 Nothing in this guidance intends to contradict or replace classification society rules or flag state requirements for emergency shutdown systems. Neither does it intend to provide guidance on best practice in the design of ESD system in terms of their efficacy in controlling the escalation of events following a hydrocarbon release or other fire hazard. Reference should be made to other sources for this information.

5.1.4 Failing to consider the requirements of station keeping integrity in the design of such systems can lead to DP incidents which also represent a significant safety hazard. In general, the objective should be to develop a design that satisfies the requirements of ESD and station keeping. Information is presented on how the design of ESD systems has compromised station keeping integrity. The intent of this Techop is to provide guidance and awareness of these issues with a view to avoiding the same problems in future DP vessel designs and upgrades.

5.1.5 This guidance note is supplemental to Section 16 of the MTS, 'DP Vessel Design Philosophy Guidelines'.

5.2 REQUIREMENTS

5.2.1 Station keeping, ESD and F&G are all considered to be safety critical systems. The rules and guidelines acknowledge the necessity for the needs of one to be considered in the design of the other. IMO MSC 645, 'Guidelines for Vessel with Dynamic Positioning Systems', 1994, states in Section 3.6 'Requirements for essential non-DP systems':

5.2.2 3.6.1 For equipment classes 2 and 3, systems not directly part of the DP system but which, in the event of failure, could cause failure of the DP system, (e.g., common fire suppression systems, engine ventilation systems, shutdown systems, etc.), should also comply with relevant requirements of these guidelines.

5.2.3 The statement above is generally interpreted to mean that it is acceptable to shut down the DP system in response to a genuine safety condition that requires such action to be taken but it is not acceptable for a single failure in the safety system itself to adversely affect station keeping.

5.2.4 Similarly, the 2009 MODU Code allows for special consideration to be given to dynamically positioned vessels. Sections 6.5.2 and 6.5.4 of the code are particularly important from a DP FMEA perspective. In general the classification society rules for ESD now reflect the special status afforded to DP vessels and different rules are applied to vessels that require power for station keeping.

5.2.5 Section 6.5.2 states:

In the case of units using dynamic positioning systems as a sole means of position keeping, special consideration may be given to the selective disconnection or shutdown of machinery and equipment associated with maintaining the operability of the dynamic positioning system in order to preserve the integrity of the well.

5.2.6 Section 6.5.4 states:

Shutdown systems that are provided to comply with paragraph 6.5.1 should be so designed that the risk of unintentional stoppages caused by malfunction in a shutdown system and the risk of inadvertent operation of a shutdown are minimized.

5.2.7 It is of paramount importance that while it is required for equipment to be shutdown in a real event, spurious or unintended shutdowns should not affect station keeping. Efforts should be made to review and validate each vessel's ESD and F&G system design to identify and mitigate such potential. This review should be carried out as part of the DP system FMEA and include a review of the cause and effects matrix.

5.3 TYPICAL IMPLEMENTATION AND PROBLEMS

5.3.1 The IMO MODU Code 2009 requires the provision of ESD systems in drilling units and the classification societies have various rules in relation to the design of such systems. The main ESD control station is usually on the bridge with another in the Engine Control Room (ECR) or some other command and control location. Remote ESD buttons may also be located at the helideck, lifeboat stations and other locations. In some designs, there is a single ESD level pushbutton that initiates a total shutdown of the unit including propulsion, emergency and support facilities. This is sometimes referred to as All Vessel Shutdown (AVS) or 'dead ship'. Different ESD levels are used to denote an all vessel shutdown. These differences arise because there is more than one standard for ESD systems. Depending on the standard used, ESD 0 or ESD 3 may both mean total shut down level. In this guidance note, the example used is a DP vessel with a three-way split in its redundancy concept using the following convention:

1. ESD 0 Total shutdown.
2. ESD 1 Emergency power system.
3. ESD 2A Port power system.
4. ESD 2B Centre power system.
5. ESD 2C Starboard power system.
6. ESD 3, 4 etc Accommodation or industrial spaces.

5.3.2 In some designs there is a 'cascade down' function which automatically activates all levels below the level that has been manually activated. For example, if ESD 0 (total shutdown) is operated then all levels below that are automatically activated. If ESD 1 (typically emergency power shutdown) is activated then ESD 2A, 2B and 2C and so on will be activated which is the entire main power generation system. This is equivalent to a blackout on a DP vessel and will lead to a loss of position. Therefore even when there is some inhibit function (such as a bypass or lockout switch) on ESD 0, the cascade function may still cause a blackout if the ESD 1 function operates spuriously.

5.3.3 ESD and F&G system are generally required to have active redundancy. This is generally implemented to help ensure that the ESD system will operate on demand and not be in a failed state when required. Fail safe conditions are specified with reference to DP related equipment. Compliance with these requirements should ensure adequate integrity but incidents experienced in industry confirms that these arrangements have proven to be less robust than required in relation to ensuring the vessel is not shut down in response to a false or inadvertent shutdown activation.

5.3.4 Typical scenarios include:

- Inadvertent operation of the total shutdown ESD buttons at remote locations such as those in Figure 5-1. These events have occurred even when clear signage and inhibit functions formed part of the barriers to a 'single inadvertent act'. This sometimes occurs because crew members, unfamiliar with the arrangement, mistake the control for some other service they require to operate. As loss of position on a DP MODU carries significant safety and environmental risks it is not evident that these 'remote' ESD buttons actually contribute to overall safety in their present form.
- There have been several cases where internal software and hardware faults have caused unintended activation of the total shutdown ESD level. Such faults have occurred even when there has been no single total shutdown level and where there has been an ESD inhibit function that was in the correct 'inhibit position' when the shutdown occurred. Figure 5-2 shows just such an example where care had been taken to ensure that the digital outputs used to shut down the generators were segregated. Unfortunately, the generators stops were interfaced to one card. This commonality contributed to a condition where the processor believed all six pushbuttons had been operated and initiated a complete shutdown of the power plant.

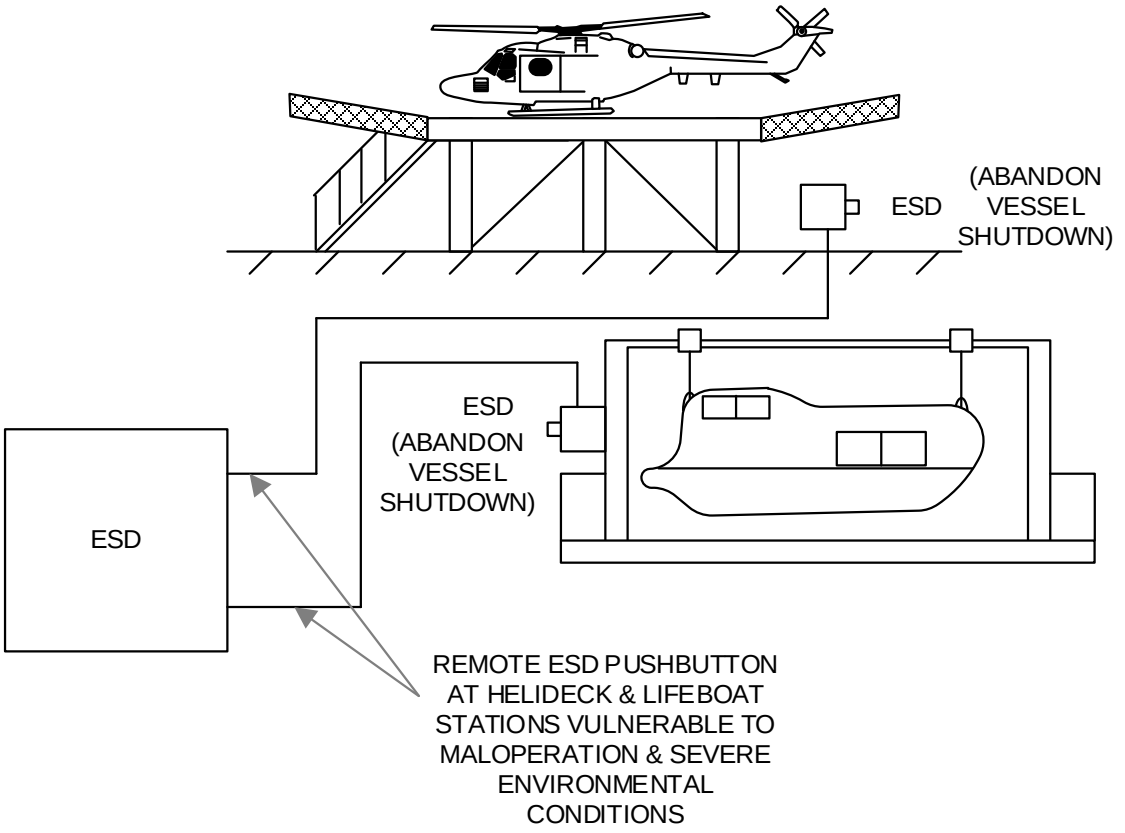

Figure 5-1 Abandon Vessel Shutdown at Remote Locations

5.3.5 Despite the fact that rules exist acknowledging the special circumstances of DP vessels, DP incidents associated with failure and maloperation of ESD and F&G systems continue to occur.

5.3.6 Some vessel operators, as a barrier to spurious and unintended shutdowns, have relied upon the security of operating the ESD and F&G system entirely in manual mode. This was expected to provide a very high level of security but even this barrier has been defeated by software related problems as the manual inhibit function is simply another status input to the ESD controller and not a physical barrier to unintended shutdown initiation.

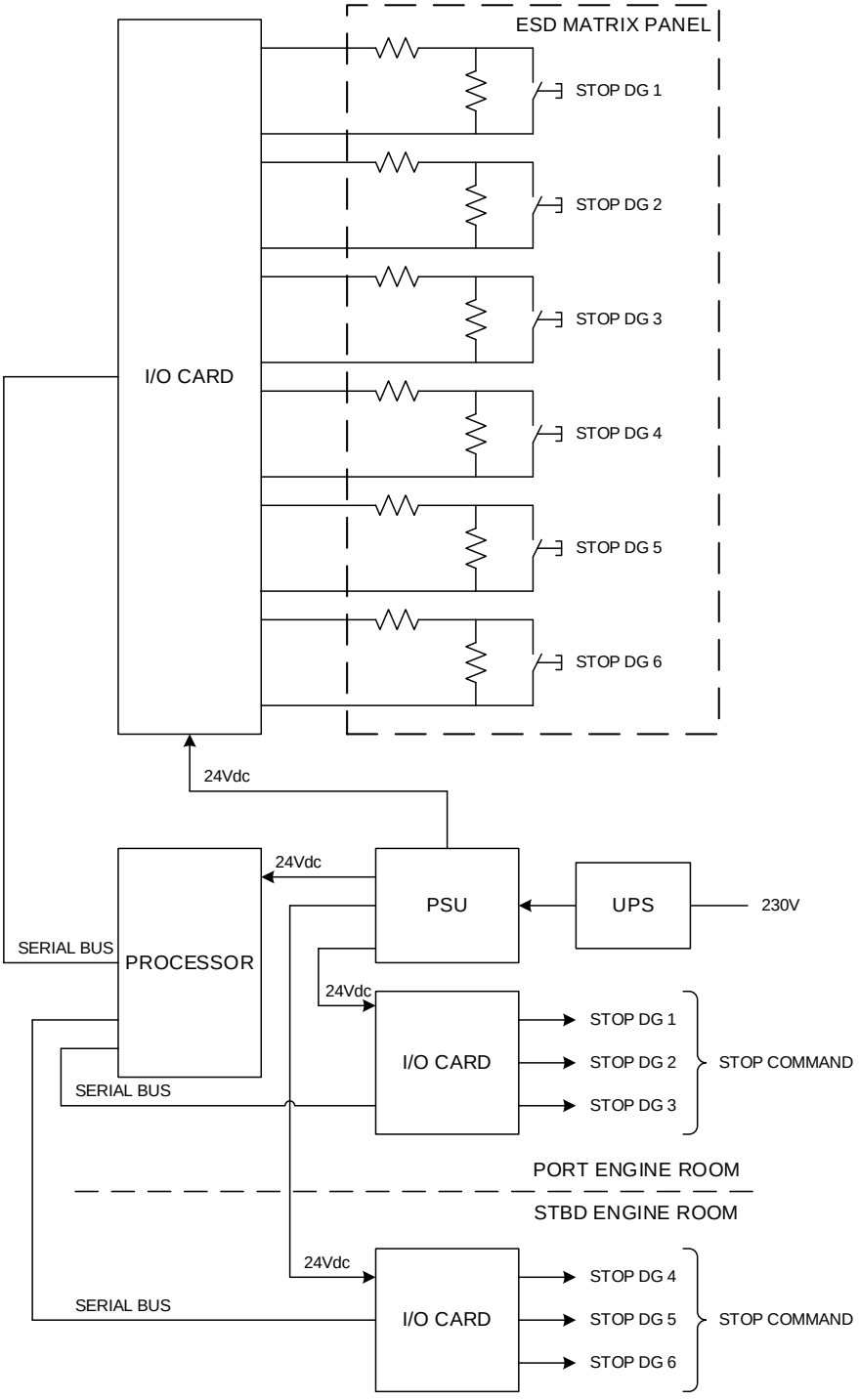

Figure 5-2 ESD Interface to Push Button Matrix

5.3.7 A much simplified schematic of an emergency shutdown system (propulsion part) is shown in Figure 5-3. Separate field stations for F&G and ESD communicate with a remote operator station over a dual redundant network. Each field station will usually have redundant processors and power supplies and be supplied from a UPS. Fire and gas detection is often provided by a specialist supplier and integrated by the automation system supplier. A hardwired interface from the ESD field station is provided for the ESD pushbutton matrix panel (several panels may exist in practice). In such designs, no attempt is made to provide any physical segregation of hardware along the lines of the DP redundancy concept. In practice there may be more than two field stations but this is more to do with the amount of I/O required rather than to achieve segregation of systems which provide redundancy. Even when some distribution of hardware is part of the design it may be used to create a fore/aft split for the convenience of cabling rather than a split that matches the DP redundancy concept. In some examples, I/O for redundant systems is separated onto different I/O cards without achieving full hardware segregation. This is an improvement over designs which are vulnerable due to commonality in the I/O distribution but less robust than full hardware segregation.

5.3.8 In the case of systems which are routinely operated in automatic mode, the severity of failure effects or acts of maloperation are often compounded by unacceptable levels of commonality in the design of the shutdown system. It is for this reason that the attribute of ‘separation’ along the lines of the divisions in the DP redundancy concept is promoted so strongly in MTS design philosophy. Separation helps to reduce the risk of unforeseen failure effects propagating from one redundant equipment group to another by way of that commonality. Figure 5-4 shows one such case where the F&G field station was redundant in terms of power supply and processors but had a common point connecting the internal dc supplies. When this common point was failed, all of the engine room fire dampers closed even though they were of ‘fail as set design’. A ‘fail-safe’ condition to the closed position had been inadvertently programmed on loss of communications between the F&G field station and the auxiliary field station.

In this example, the three-way split in the power system is not carried through into the ESD, F&G system.

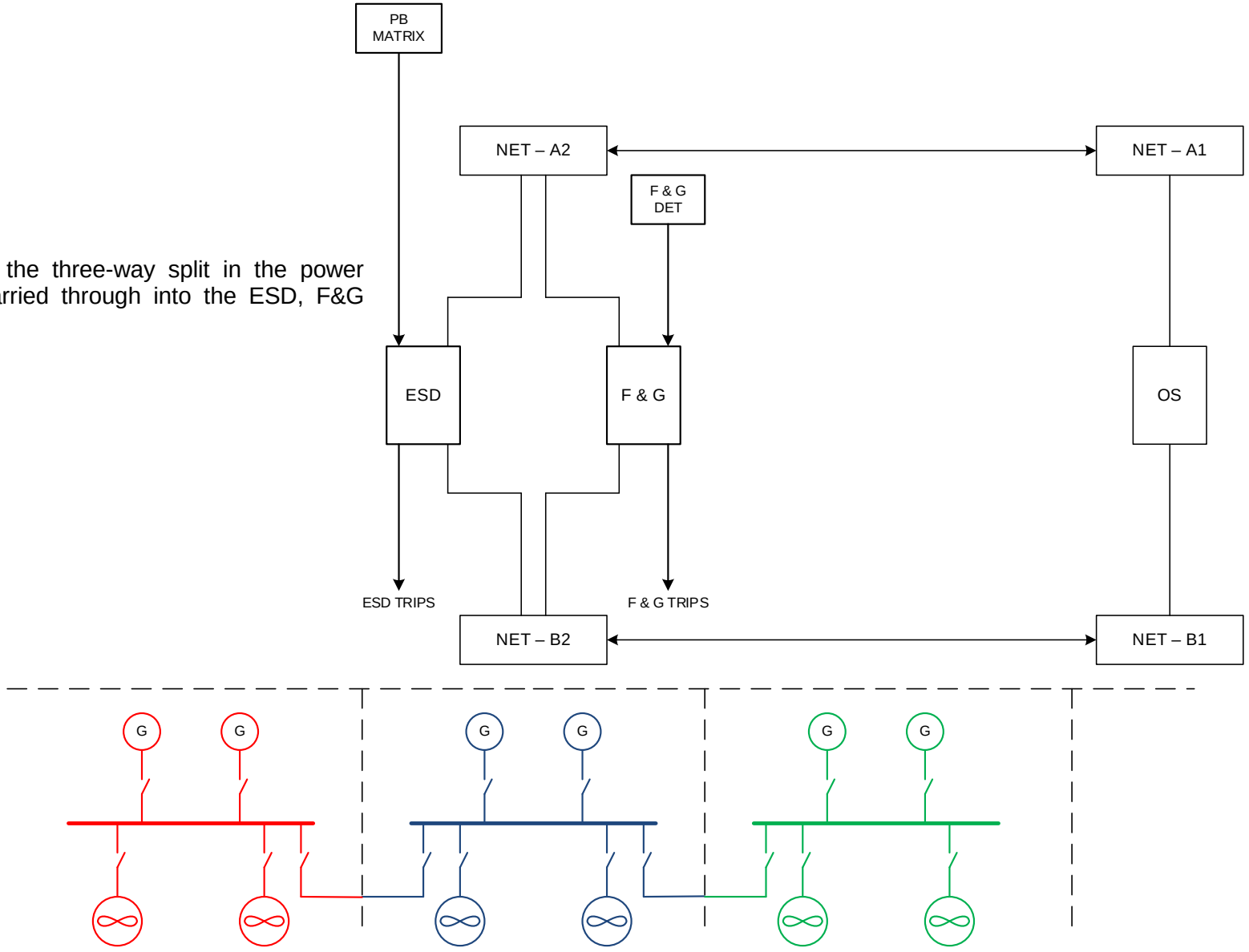

Figure 5-3 Simplified Schematic of a Monolithic Emergency Shutdown System (Propulsion Part)

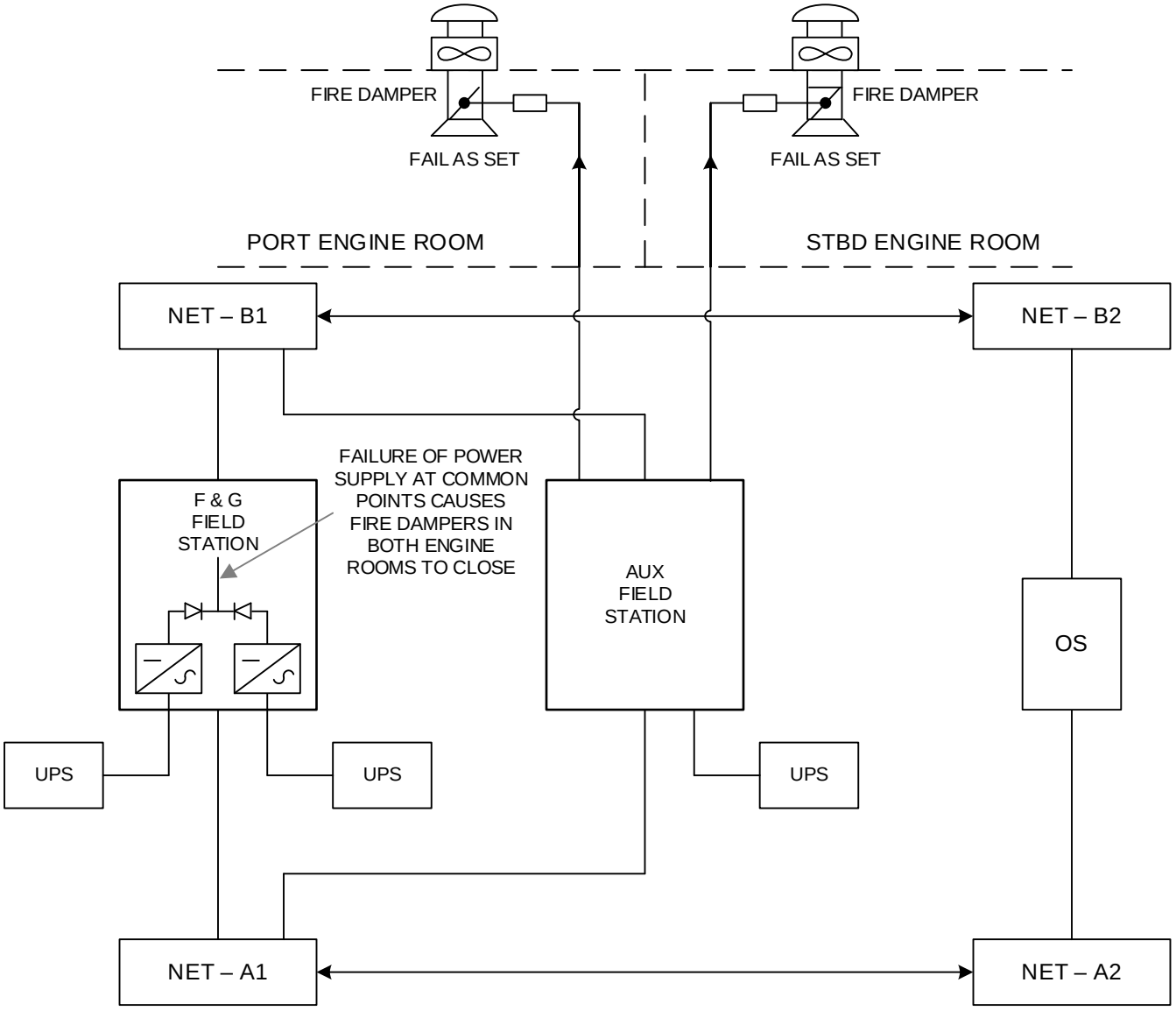

Figure 5-4 Fail as Set Fire Dampers Driven Closed by ESD System Failure

5.4 SUGGESTED IMPLEMENTATION FOR ESD F&G

5.4.1 The suggested design from a DP perspective is for the shutdown system to be split along the same lines as the overall DP redundancy concept with no single overall total shutdown function (e.g. ESD 0). Figure 5-5 show such how such a hypothetical design might be achieved. It is appreciated that such hardware segregation will need to be addressed in the software as well and there may be some challenges if not specified up front. The design philosophy's impacts on industrial mission systems should be assessed and addressed up front.

5.4.2 The following features can help to enhance robustness from a DP safety perspective:

1. Use of normally de-energised contacts for shutdown of essential DP equipment (class requirement in most cases anyway)
2. Line monitoring with alarm on cable faults or supply failure
3. Dual (or multiple) independent circuits to ESD push buttons (and dual buttons). Each push button circuit interfaces to a different FS or at least a different I/O card.
4. Shutdown actuation should originate from separate field stations in a manner that aligns with the overall division of the DP systems into redundant equipment groups.
5. Loop power for shutdowns should not originate from common points in a manner that makes cable route a potential single point failure for fire.
6. Suitable voting on multiple circuits. Signals that initiate an alarm but not a shutdown if they disagree.
7. Fail safe mode of ESD field stations should be to not shutdown on loss of power or communications.
8. ESD pushbuttons should be provided with.
    - Cover
    - Signage
    - Key switch inhibit – where appropriate
9. Manually operated 'inhibit function' of robust design on all ESD 0 or ESD 1(if there is a cascade to blackout)
10. The indication that the inhibit function is in the 'inhibit position' should be based on confirmation that the function is active from the controller and not just the switch position.
11. Fire dampers for generator combustion air need not be closed as part of ventilation shutdowns if they are designed such that they only provide air to the engine and compartment ventilation can be shut down separately. 'Rig savers' or equivalent are used to provide individual engine protection on MODUs.
12. Fire dampers for combustion air may be of the normally de-energised type which implies that its takes power to close them and therefore they remain open on loss of that power.

In this example, the three-way split in the power system is carried through into the ESD, F&G system.

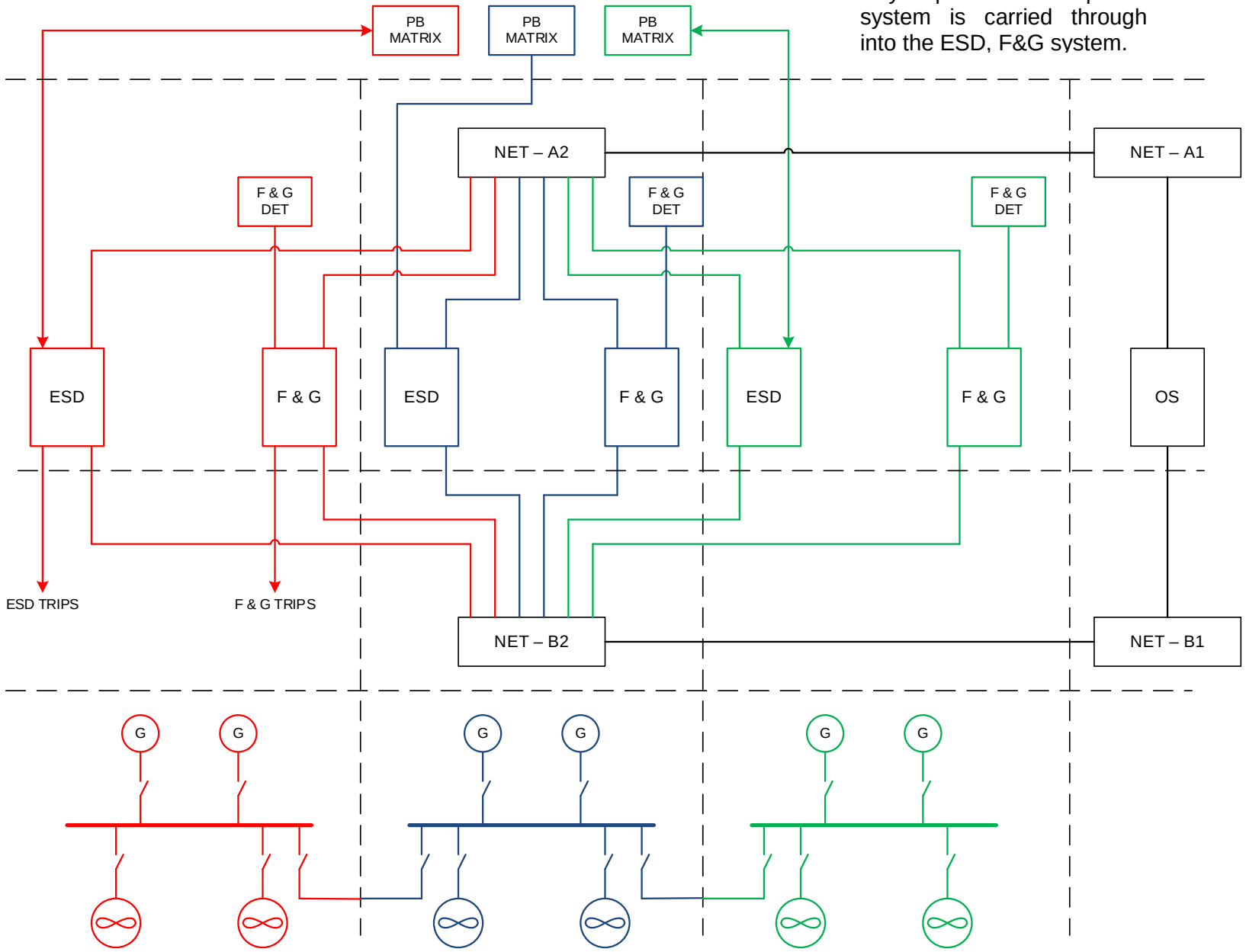

Figure 5-5 Simplified Schematic of a Distributed Emergency Shutdown System (Propulsion Part)

5.4.3 Sources of loop power:: One issue which is often the subject of discussion at design reviews of shutdown systems relates to the source of loop power and the effect the choice has on effects of failures in common cable routes. This is normally done correctly by the major suppliers but should be checked. The example in Figure 5-6 below shows a DP equipment class 3 design where shutdown signals originate in a common compartment and a common cable route eventually separates at the A60/WT divide to the port and starboard switchboard rooms.

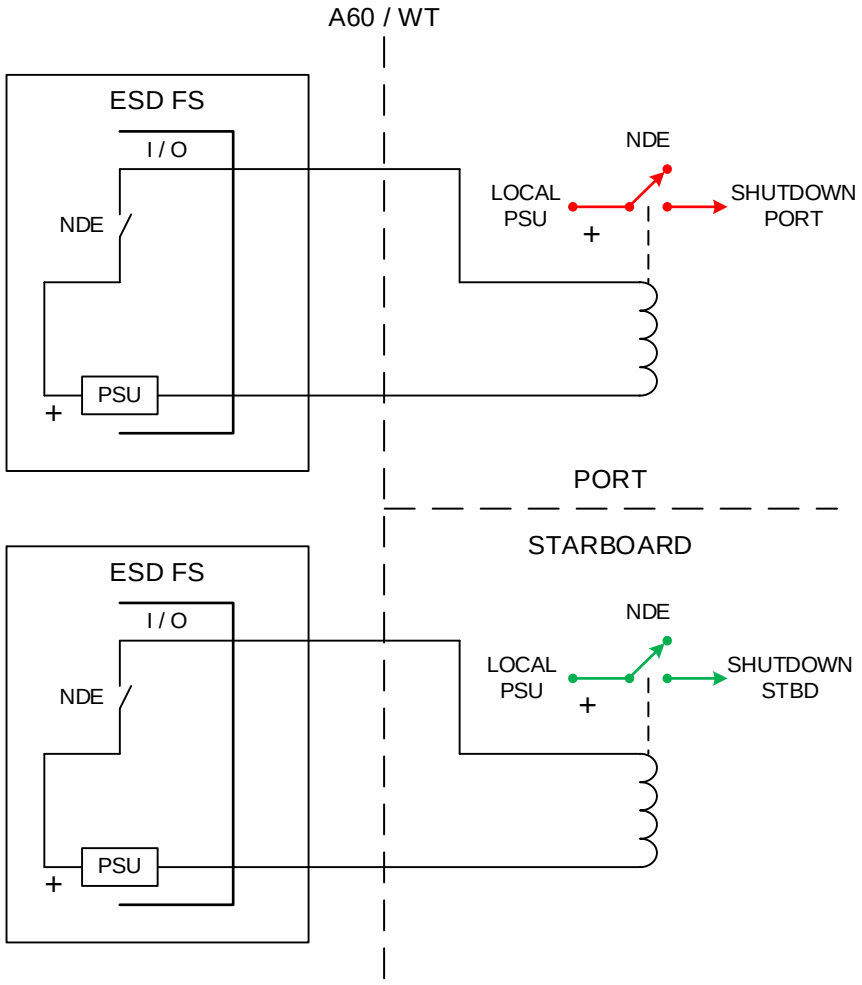

Figure 5-6 Preferred Method - Loop Power Originates at ESD Field Station

5.4.4 Although the shutdowns have been separated into two different field stations, the common cable route introduces some degree of commonality. However by sending loop power from the field station any short circuit in the damaged cables will operate the fuses on the power supplies and no propulsion shutdown should result. The fire can then be dealt with by the measures appropriate to its location. Providing fire and watertight segregation of the shutdown system and its cables along the lines of the redundancy concept would also have enhanced the robustness of the design but this practice is not yet universal.

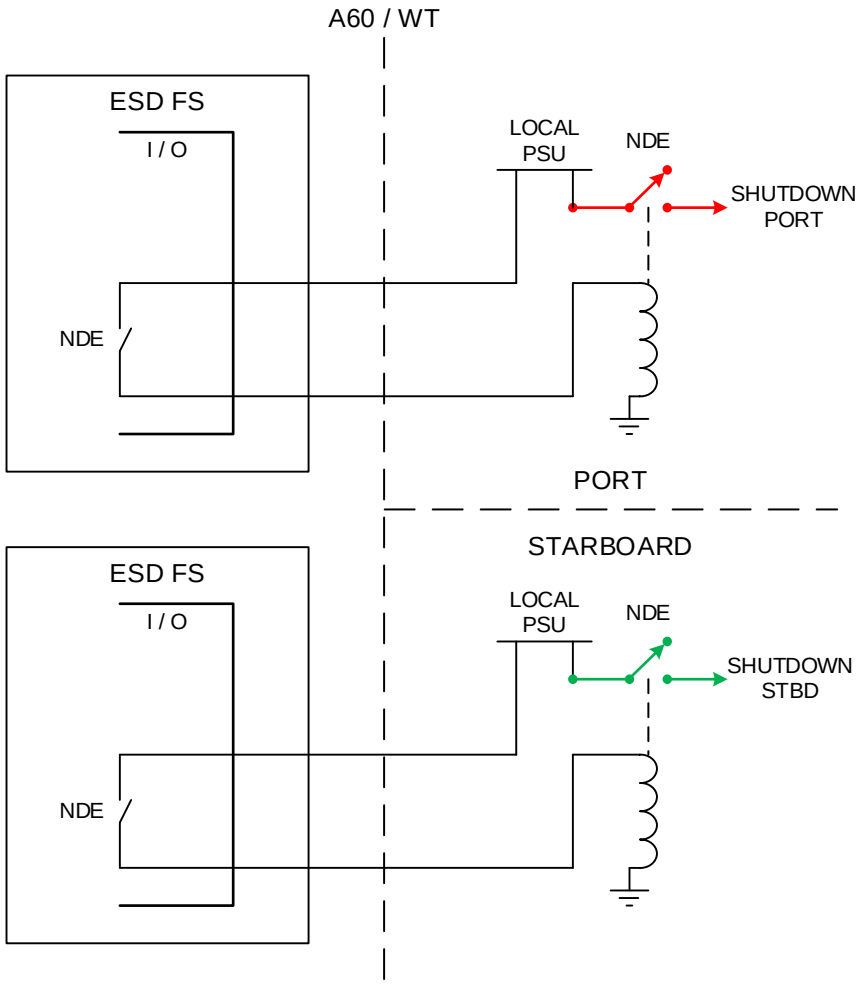

Figure 5-7 Sending Loop Power from Switchboard End

5.4.5 Figure 5-7 illustrates the other possibility which is to send the loop power from the switchboard power supply into the common space containing the shutdown systems. In this case, fire damage in the common cable routes effectively completes the circuits and shuts down the port and starboard power systems. Although the example discussed here is related to the shutdown system, similar issues are encountered in other systems such as power management system and remote valve control or thruster emergency stops where cables from redundant equipment are brought to a common point.

5.4.6 Line Monitoring: Line monitoring is a popular method of reducing the risk that cable faults cause by fire, mechanical damage, insulation failure or broken conductors will initiate an unwanted control system response. The principle of operation is that the control system will only respond to a defined step change in loop current between two defined values and not to any other current level as might be caused by a short circuit or open circuit or earth fault. These defined values are created by a series and parallel resistance installed across the switch contacts. The change in current is measured by an analogue I/O card or a dedicated switch amplifier. Figure 5-8 shows a typical installation. The example shows flow switches but could equally apply to shutdown push buttons.

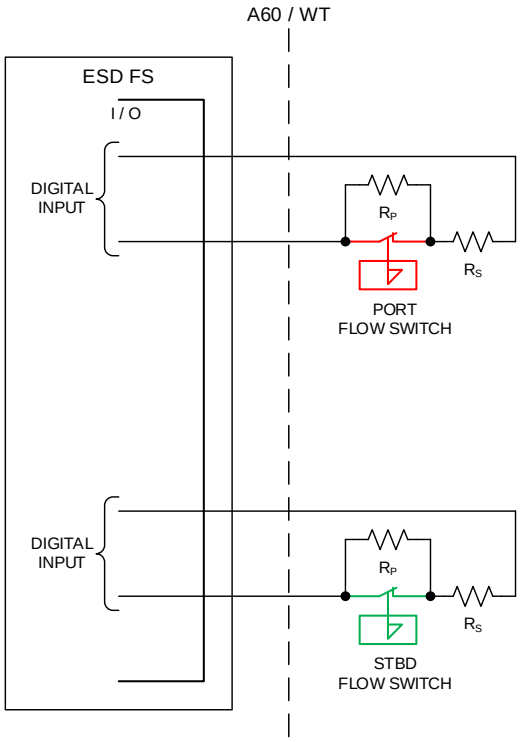

Figure 5-8 Preferred Method - Line Monitoring Resistors Installed at Switch

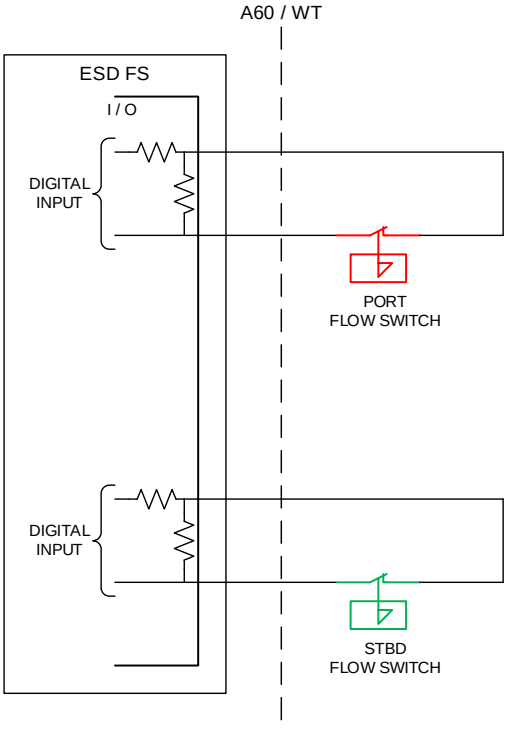

Figure 5-9 Line Monitoring Resistors Installed at I/O Card

5.4.7 Figure 5-9 shows an alternative location for the resistors which will work effectively as far as creating the desired current step is concerned but does not protect the cable run that crosses the A60/WT boundary. Why this alternative location would ever be chosen is unclear but when cables cross between one vendor's scope of supply and the other and one vendor has omitted to supply switches prepared with resistors, it may be a solution that allows the other vendor to commission the system with the required functionality. Unfortunately, the effect on the system's fault tolerance to fire damage is not addressed.

5.5 CONFIRMATION OF FIRE DETECTION AND GAS INGRESS

5.5.1 One of the most significant vulnerabilities in the application of ESD systems to DP vessels is the robustness of measures used to confirm the presence of gas or the occurrence of fire. Voting on multiple sensors is often used in the design of shutdown systems and this has the potential to enhance robustness. This potential may be overlooked and lack of implementation precludes realisation of robustness.

5.5.2 In DP equipment class 3 designs, the physical separation provided by the fire resistant and watertight bulkheads and deck heads is defined by the split in the DP redundancy concept and makes it possible to arrange ESD and F&G in a manner that supports the objective of providing a defined post worst case failure DP capability. Unfortunately, this objective can be defeated by:

- Commonality in ventilation systems that cross the A60/WT divisions
- Insufficient separation of air intakes and jalousies for compartments intended to provide redundancy.

5.5.3 Figure 5-10 shows the compartment and ventilation arrangement for the aft thrusters in a DP equipment class 3 drillship. Although the thruster compartments are separated by A60 rated watertight bulkheads, all three are served by a common ventilation system. Smoke or dust drawn in from activities on deck contaminated the air in all three thruster compartments activating the smoke detectors.The cause and effects matrix for F&G detectors was written to shut down the thrusters on detection of a confirmed fire. Setting aside any operational barriers that could have been used to mitigate this risk the design has two main vulnerabilities:

- A common ventilation system connecting redundant DP equipment groups
- Lack of robustness in detecting a confirmed fire.

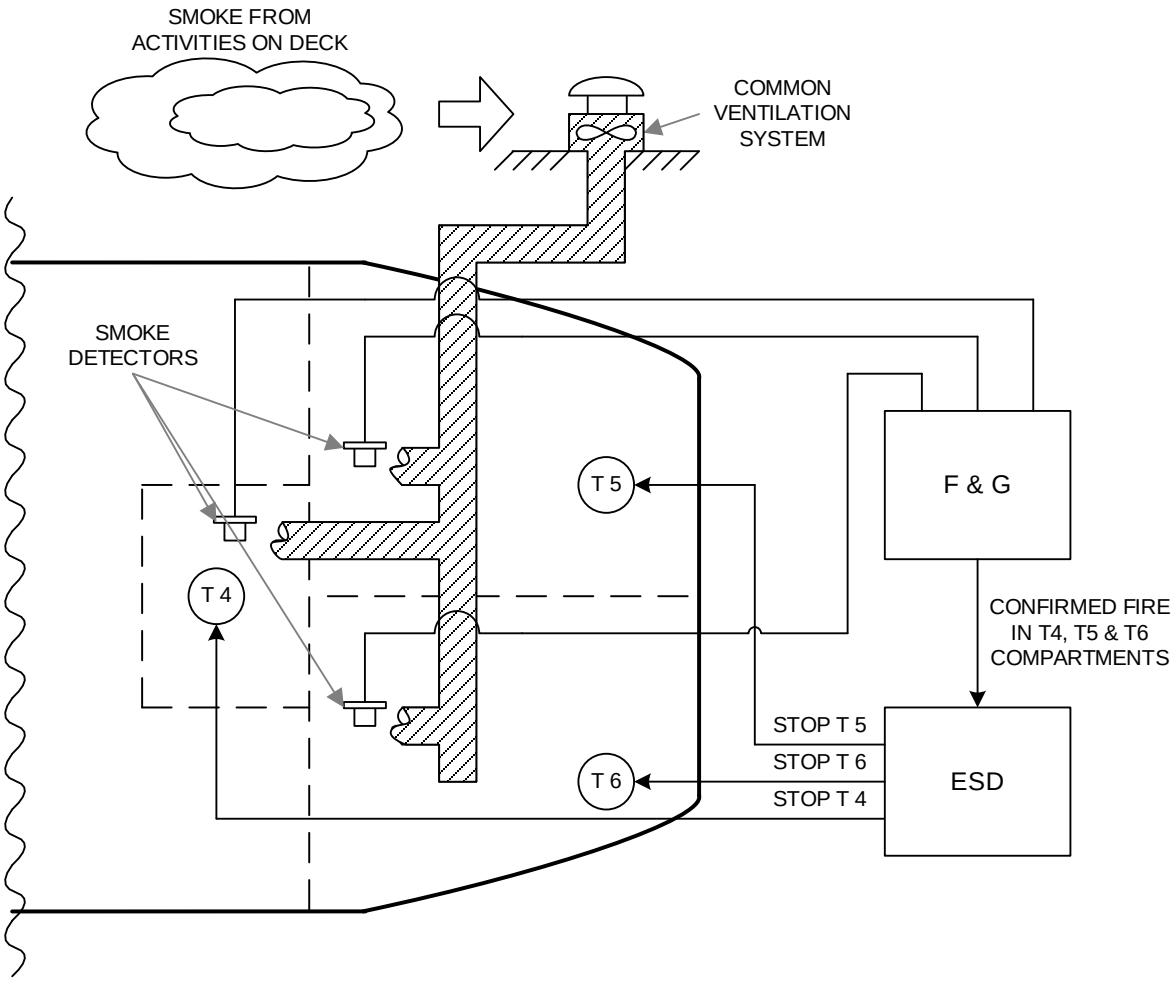

Figure 5-10 Common Ventilation Systems Defeats Redundancy

5.5.4 In DP equipment class 2 designs it is even more difficult where colocation of DP related equipment is permitted by the rules. In such circumstances it is even more important to have a robust fire and gas detection strategy that can confidently distinguish between a real fire or gas release and conditions with the potential to mimic the same conditions.

5.5.5 Gas detectors may be provided for flammable and toxic gas. In general, gas detectors have a better reputation for reliability in detection as they are designed to detect the presence of the hydrocarbon in the air. There is no direct equivalent for fire detectors and the existence of a fire is inferred from its effects including:

- Smoke
- Heat
- Light – IR/UV

5.5.6 Once it reaches a critical concentration, the risk of explosion from gas drawn into machinery or other spaces is such that it is reasonable to take immediate action to isolate sources of ignition. In DP class 2 designs this may mean accepting the consequences of a loss of position if gas is detected in a space containing more than one redundant group. Although gas detectors themselves have a good reputation for reliably reporting the presence of gas there are other vulnerabilities associated with the I/O cards and field stations which increase the risk of false indication. Thus, in any space containing elements of more than one redundant DP equipment group it would be prudent to have three gas detectors at the air intakes and confirm the presence of gas on two out of three detectors indicating the presence of hydrocarbons. Each detector would be interfaced to a separate I/O card in a redundant field station and different field stations if practical. Two out of three voting provides a reasonable compromise between a hidden failure preventing legitimate gas detection and a faulty detector or I/O channel causing a spurious shut down and loss of position.

5.5.7 For fire detectors it is even more important to have a robust detection system. If an ESD is to be initiated by a confirmed fire using multiple detectors there should be some diversity in the detection method. It is prudent to initiate an alarm on any detector activating to initiate investigation by the fire team but reserve initiation of executive action by ESD only when fire risk confirmed by multiple and diverse detection methods. The need for diversity in fire detection is highlighted by the number of DP incidents associated with false activation of ESD by smoke or dust from activities on deck being drawn into several compartments or a common ventilation system serving redundant DP equipment groups.

5.6 INTERNAL EQUIPMENT FIRE DETECTORS

5.6.1 The convertor cabinets for Variable Speed Drives (VSD) may be fitted with internal fire detectors designed to shut down the thruster drive if smoke is detected. This can introduce vulnerabilities similar to those that may be present in the ESD system. Typically shutdown is based on a single smoke detector. The ventilation fans on the VSD cabinets normally draw their air supply from the machinery space. DP equipment class 2 designs with redundant equipment groups in the same compartment are particularly vulnerable to this. Failure effects exceeding the severity of the worst case failure design intent have resulted from something as simple as the smoke produced from a slipping V-Belt on a service air compressor in the same space.

6 OTHER EXTERNAL INTERFACES

6.1 EXTERNAL FORCE COMPENSATION

6.1.1 External force compensation describes the process whereby the external force acting on the DP vessel is measured and therefore known separately from the environmental force. This value is then included in the DP calculation and treated as a force feed forward. This feature is used to account, for example, for the impact of pipe tensions in pipe layers and hawser tension in shuttle tankers etc. on station keeping. Generally, the signals originate at load cells or other measuring devices and are often 4-20mA current loop signals. In some designs, the interface may be dual redundant. Because the industrial mission equipment and load is often unavailable during DP FMEA proving trials and annual trials, the failure effects of these signals are seldom tested, nor the ability of the DP control system to reject erroneous readings. Because of the uncertainty and lack of predictability associated with these interfaces it is not unusual to require a manual force input mode during critical operations (CAM). Automatic correction may be acceptable in TAM. If the intent is to use this feature in automatic mode, the design of the interface should be subject to a system engineering approach validating redundancy and fail safe response to failure by analysis and testing.

6.2 DRAUGHT SENSORS

6.2.1 A manual input of draft is typically sufficient for DP control systems. With the advent of Vessel Management Systems (VMS), automatic draught measurement and input into the DP system is not uncommon as a feature of some DP control systems. The signal may be provided by hardware and sensors that form part of the ballast or tank gauging systems. This can be mis-categorised as ‘not part of the DP system’

6.2.2 Industry experience has recorded instances of such installations being problematic. Loss of position has resulted when the DP control system received erroneous information directly from sensors about the draught of the vessel. This corrupted the mathematical model leading to a drive off.

6.2.3 Typically there can be several draft sensors interfaced to the DP system at points around the vessel. The DP system will normally use the average of all sensors in its computation.

6.2.4 Model data such as mass and drag are tuned at pre-defined draughts during sea trials. Correct draught sensor signals are essential to the interpolation process of the mathematical model. The draught signal determines to some extent how much of the combined force acting on the vessel is assumed to be from tidal current and how much is from wind. If the wind and the current are from significantly different directions the thrust solution will be in error and the vessel will drive off.

6.2.5 On vessels with an integrated automation system, it is common practice for the draught sensors to be connected to a convenient field station. The DP control system then receives the draft information by way of the dual Ethernet connecting the automation system to the DP control system.

6.2.6 The following vulnerabilities have been identified and can be avoided in future designs

- All sensors connected to the same field station.
- No logical bounds on signal value, thus out of range signals can have a severe effect (e.g. negative draught).
- No analysis of draught sensor arrangement or failure modes in FMEAs or testing at proving trials.
- No real justification for requiring an automatic input of draught

6.3 POWER CONTROL FOR INDUSTRIALS CONSUMERS

6.3.1 The vast majority of DP vessels are designed around diesel electric propulsion systems based on the power station concept. This design provides all power for dynamic positioning and for hotel and industrial consumers from a combined source that may be operated as a single power system or as two or more independent and isolated power systems. DP vessel with large industrial loads such as drilling or pipe laying may have a dedicated power management system for the industrial consumers which is interfaced to the power management for the DP system so that functions such as load shedding may be prioritised.

6.3.2 Some industrial consumers such as active heave drawworks may need to regenerate significant amounts of power either to the main power system or to dynamic braking resistors or a combination of both.

6.3.3 Few if any of these vessels can operate with sufficient spinning reserve to prevent overload of the power plant following the worst case failure therefore the redundancy concept depends on shedding away the industrial consumers in a controlled manner but rapidly when required.

6.3.4 Information on the amount of power that can be safely drawn from and regenerated to the vessels power systems from the industrial consumer may be communicated over analogue or serial data links. As this link acts as part of a protective function it is important that it fails in a predicable manner and that there is no potential for effects exceeding the severity of the worst case failure design intent.

6.3.5 Typical issues to be considered include the failure modes of analogue 4-20mA loops used to indicate power available and power consumed for industrial consumers. These links typically fail out of range and provide an alarm but what condition should the PMS adopt? Whatever strategy is developed it should be robust, well explained, analysed in the DP system FMEA and proven at commissioning and trials.

6.3.6 All such links should provide an unambiguous alarm on failure. Consideration should be given to providing redundancy and voting in these links to allow continued operation.

6.3.7 Serial links may fail to the last valid data value. This may affect the DP system and industrial consumers.

6.3.8 Some designers rely upon the frequency of the power waveform in a common power system operating in speed droop for load sharing to also indicate power plant loading. This is a very robust way of communicating power plant load which can also be used to trigger load shedding at defined levels. No control links are required to achieve this.

6.3.9 In some drillship designs the drawworks is given priority for power over the thrusters when the active heave drawworks is operating in lock-to-bottom mode. There is variability in the the configuration of this lock-to-bottom mode across vessels. It is essential to fully understand and document vessel specific information and ensure familiarisation of the crew. In some designs, priority for power is only transferred from the drawworks to the thrusters if the vessel is not holding position within a defined watch circle. The issue here is not the relative merits of this particular function but that it introduces additional control links to the DP system which need careful consideration regarding their failure modes and fail safe condition. Additionally, power may not be available to thrusters without deliberate intervention.

6.4 POWER DISTRIBUTION FOR INDUSTRIAL AND HOTEL LOADS

6.4.1 Power consumers not directly related to DP can also be considered to be an external interface with the potential for failure effects to adversely impact the operation of the DP system. It is relatively straight forward to divide up power and propulsion systems for DP along well defined lines. The same is not always true of supplies from accommodation or industrial consumers and these often introduce unwanted asymmetries in the load or create common points between redundant equipment groups. Common points can be created by features such as dual supplies; auto-changeovers and colocation of non DP related consumers within the same A60/WT zone in the case of DP equipment class 3 designs. In earlier rules for DP class 3 designs it was accepted that the influence of their failure on the DP system should be demonstrated by analysis but in more recent revisions, the presence of such features triggers similar requirement's for analysis and testing that is more akin to that required to prove the fault tolerance and fault ride-through capability of a common power system even though the normal operating configuration is with the main busties open.

6.4.2 Methods that can be used to address these issues include:

- Where there is a need to provide a dual supply into a common compartment, determine whether it is necessary for both supplies to be live at the same time. – If not, it may be possible to isolate one supply or arrange for switching at the supply end (switchboard) rather than at the consumer. Issues related to transfer of fault should be addressed.
- Maintain the same split in industrial and hotel distributions as is provided for DP related consumers to as low a voltage distribution level as is practical. This will avoid issues of load asymmetry particularly when operating the power plants as independent power systems.
- Provide power to non DP related loads from their own service transformers so that there is some impedance between DP and non DP related consumers. This is particularly important for industrial power distributions on deck which may be subject to routine earth faults.
- A few DP applications may justify a separate industrial power plant. Some vessels have been built with this philosophy.

6.5 FIRE FIGHTING SYSTEMS

6.5.1 CO2 systems and similar gaseous extinguishing mediums have a reputation for reliability and there are very few, if any reports of unscheduled release of fire-fighting agent on DP vessels. The fire-fighting system should be arranged to allow fires in one DP equipment group to be addressed without significant impact on other DP equipment groups. This is easier to achieve on DP class 3 vessels. The opportunities for the design of CO2 systems to compromise DP redundancy concepts more often occurs in the conversion to commercial vessels for DP or repurposing of older vessels, particularly where some part of the original power plant is retained along with its fire-fighting installation. In such cases it is possible for unsuitable functionality to remain undetected. Examples include micro-switches intended to detect the opening of pilot cylinder cabinet doors. This feature has been used to stop fans, close fire dampers or even stop engines in preparation for the release of CO2 into the common engine room space on DP equipment class 2 vessels.

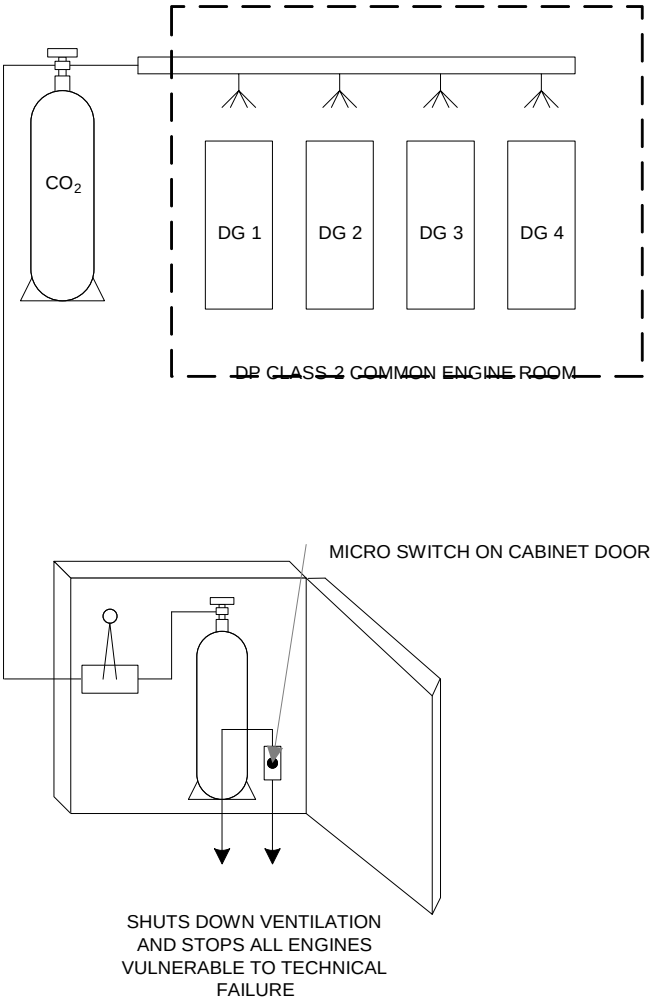

Figure 6-1 Fire - Fighting System with Ventilation and Engine Shutdown

6.5.2 Water mist is a relatively recent addition to fire-fighting systems on DP vessels and has brought with it a number of problems associated with unacceptable commonality in the interface. Figure 6-2 shows a very simplified schematic intended to illustrate one particular design issue. In the example below, the F&G system was designed to initiate release of water mist in the engine room. At the same time, the ESD system was ordered to open the generator circuit breakers in the associated switchboard room. The command to open the circuit breakers originated at flow switches which detect the flow of water to the nozzle. Unfortunately, the design of the system was such that failure of the internal 24Vdc supply had a similar effect in so far as it caused the relays controlled by the flow switches to de-energise and indicate to the ESD system that the flow switch was active even though it had not changed state. Because all the relays changed state on loss of 24Vdc power the ESD system tripped all the generator circuit breakers and the vessel blacked out.

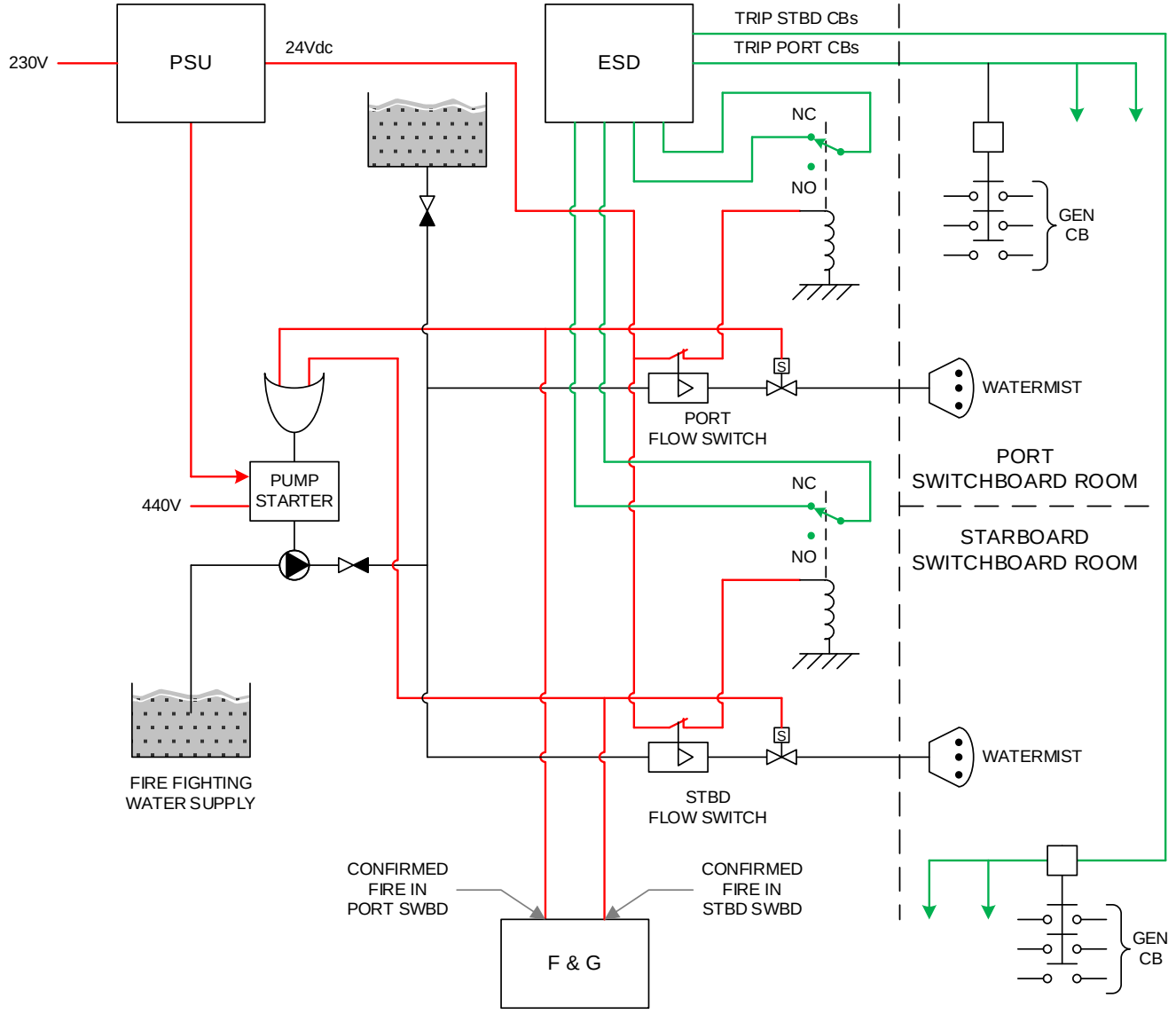

Figure 6-2 Simplified schematic of Water Mist System

6.5.3 Fire and watertight dampers: There are various designs of fire dampers including, variations on electrically operated and air operated designs. Watertight dampers are found in semi-submersible designs to limit the effects of down flooding. Motor operated versions tend to fail as set but some units are effectively spring operated and motor power or air power is simply used to charge the actuating spring. These units tend to be 'trip to close'. Air operated dampers may fail to any condition depending on designs. The use of non-return valves to hold 'failed closed' dampers open is vulnerable to hidden failures of such valves. Local air receivers for each damper or group of dampers may improve this

6.5.4 In the case of ventilation dampers, the effect of closure is not usually immediate and as long as there is an alarm and a means of opening the damper again, before equipment overheats, the failure modes of these dampers are less significant. A great deal of modern power and propulsion machinery is water cooled which limits heat rejection to the machinery space and thus it takes a long time for the compartment temperature to rise to unacceptable levels.

6.5.5 For combustion air dampers there are reasons to select a 'fail as set' damper. Experience from trials suggests that closing fire dampers may not always create sufficient seal to power limit engines but it can create a very substantial drop in engine room pressure which has disadvantages related to:

- Malfunction of crank case differential pressure detectors leading to multiple engine shutdowns exceeding WCFDI.
- Has been implicated in a number of fatalities related to doors slamming open or closed.

6.5.6 MTS DP Vessel Design Philosophy Guidelines recommend 'Fail as Set' for combustion air dampers.

6.6 COMMUNICATIONS AND NAVIGATION EQUIPMENT

6.6.1 North speed correction: An interface to a navigation GPS may be provided on gyros for correcting the deviation associated with the vessel's north speed. If one navigation GPS signal is interfaced to all three DP gyros this represents a common point by which a faulty GPS signal could affect all three heading signals to DP. Such incidents have happened and most DP vessels owner isolate this facility on DP if it is provided.

6.6.2 Shut down thrusters above defined hull speed: Retractable azimuth thrusters may have limits on speed through the water in the extended position. In at least one vessel design a signal from the navigation GPS was used to provide a vessel speed signal to the thruster drive which would shut down the thruster when the limiting speed was exceeded. Failure of the power supply to the navigation GPS was found to cause all the retractable thrusters to stop with effects exceeding the severity of the worst case failure design intent. Clearly this is an example of unacceptable commonality.

6.6.3 Gyro repeater switches: The DP gyros are often used to supply heading information to other systems such as radars, ECDIS, bridge wing repeaters, entertainment/ communications systems and so on. A gyro switching device may be provided to allow different gyros to provide the signal to these services. These non DP related heading consumers represent an external interface and the gyro switching unit represents a common point between redundant equipment groups that should be analysed in the DP FMEA.

6.7 ROLL STABILISATION

6.7.1 The characteristics of cycloidal thrusters allows them to be used for roll stabilisation in OSVs and other DP vessels because they can reverse thrust direction very quickly. The roll stabilisation function is active at the same time as DP and is usually a standalone control system which superimposes stabilisation commands upon those issued by the DP systems such that the resultant thrust vector satisfies both the requirements of DP and stabilisation. The roll stabilisation interface should be analysed in the DP FMEA from both a redundancy and fail-safe perspective.

6.8 GROUP EMERGENCY STOPS

6.8.1 Group emergency stops are fitted to many DP vessels and share some of the same problems as the more sophisticated or extensive ESD systems found on MODUs. Group emergency stop systems are provided to assist in fire-fighting and allow the operator to stop groups of consumers which may include DP related consumers such as:

- Ventilation fans,
- Electric fuel pumps.
- Hydraulic pumps for CPPs and azimuthing gear.
- Lubricating oil pumps.

6.8.2 The design of the group emergency stop system should be aligned with the overall split in the DP redundancy concept be analysed in the DP system FMEA. Stop groups should not, in general, include consumers from more than one redundant DP equipment group such that it is possible to stop one group at a time without loss of position.

6.8.3 Classification societies may have particular requirements in relation to the the nature of the control loops used. Typically, propulsion related equipment will usually be controlled by a normally open, Normally De-Energised (NDE) control loop with appropriate line monitoring for push buttons and power supply monitoring. A shunt trip coil is normally fitted to trip the consumer feeder circuit breaker on application of power. Normally Energised circuit should not normally be used to trip DP related consumers due to concerns about unreliability related to vibration of relay contacts and wire breaks.

6.8.4 External interfaces to the group energy stop system should also be considered. Smoke detectors may be interfaced to operate the group emergency stop system automatically in some designs. The nature of this interface should reflect and align with the overall split in the redundancy concept and fail to the safest conditions with appropriate alarms.

6.8.5 DP FMEA proving trials should confirm the effects of executive actions taken by group emergency stops and any fire detection systems that are interfaced to them.

7 MISCELLANEOUS

Stakeholders	Impacted	Remarks
MTS DP Committee	✓	To track and incorporate in next rev of MTS DP Design Philosophy Guidance Document. Communicate to DNV, USCG, Upload in MTS website part.
USCG	X	MTS to communicate- FR notice impacted when Rev is available.
DNV	✓	MTS to Communicate- DNV RP E306 impacted.
Equipment vendor community	✓	MTS to engage with suppliers.
Consultant community	✓	MTS members to cascade/ promulgate.
Training institutions	X	MTS members to cascade/ promulgate.
Vessel Owners/Operators	✓	Establish effective means to disseminate information to Vessel Management and Vessel Operational Teams.
Vessel Management/Operational teams	✓	Establish effective means to disseminate information to Vessel Operational Teams.