



DYNAMIC POSITIONING CONFERENCE
October 9-10, 2007

Risk

Failure is an Option

Doug Phillips
American Global Maritime

BACKGROUND

All DP vessels class 1 and above require some level of redundancy and therefore fault tolerance. So failure is always a consideration at the forefront of the DP vessel design and testing. The DP system design needs to be fault tolerant.

Frequently however designers and vessel crew are not comfortable with this concept of ‘thinking failure’ and seem to require the design to be fault resistant. They therefore choose to build in back up features that are brought into operation after a failure occurs (more in keeping with NASA’s motto – **‘failure is not an option’!!**). However all too often these create unnecessary complication, changeovers, operational traps, more failure modes etc.

INTRODUCTION

This paper will provide a number of examples from the author’s own experience and other examples canvassed from the DP community.

The intent is to raise awareness of this issue and encourage interested readers to review their own DP vessels and designs from the point of view of unnecessary complication.

Before the examples are given is a short review of what a **‘failure’** means in the context of a Dynamic Positioning system.

‘FAILURE’ – DEFINITION IN THE CONTEXT OF A DP SYSTEM

Generally in the context of Dynamically Positioning a vessel a loss of position is not to occur as a result of a **single failure** in any of the systems that support the positioning of the vessel (power generation, power distribution, power management, thruster, DP control system etc). The ability to withstand a **single failure** obviously requires redundancy in the way of dual or triple redundant systems and sensors. The types of failure that have to be withstood depend whether the vessel is class 2 or class 3. These are defined in the IMO DP Guidelines (MSC 645) guidelines -

***For equipment class 2**, a loss of position is not to occur in the event of a single fault in any active component or system. Normally static components will not be considered to fail where adequate protection from damage is demonstrated, and reliability is to the satisfaction of the Administration.*

•Single failure criteria include:

- Any active component or system
- Any normally static component (cables, pipes manual valves, etc.) which is not properly documented with respect to protection and reliability.

***For equipment class 3**, a single failure as class 2, and any normally static component is assumed to fail.*

- All components in any one watertight comp, from fire or flooding.
- All components in any one fire sub-division, from fire or flooding
- For equipment classes 2 and 3, a single inadvertent act should be considered as a single fault if such an act is reasonably probable.

The loss of position will only occur if the single failure leaves the vessel with insufficient equipment to withstand its ‘specified maximum environmental conditions’. This is the

environmental limits that can be withstood following the worse case failure (typically the failure of multiple thrusters).

ABS explains this concept as follows: -

DPS-2 For vessels which are fitted with a dynamic positioning system which is capable of automatically maintaining the position and heading of the vessel within a specified operating envelope under specified maximum environmental conditions during and following any single fault excluding a loss of compartment or compartments.

DPS-3 For vessels which are fitted with a dynamic positioning system which is capable of automatically maintaining the position and heading of the vessel within a specified operating envelope under specified maximum environmental conditions during and following any single fault including complete loss of a compartment due to fire or flood.

A failure modes and effect analysis (FMEA) is to be carried out for the entire DP system. Rom ABS –

The FMEA is to be sufficiently detailed to cover all the systems' major components and is to include but not be limited to the following information:

- A description of all the systems' major components and a functional block diagram showing their interaction with each other.
- All significant failure modes.
- The most predictable cause associated with each failure mode.
- The transient effect of each failure on the vessels position.
- The method of detecting that the failure has occurred.
- The effect of the failure upon the rest of the system's ability to maintain station.
- An analysis of possible common failure mode.

Where parts of the system are identified as non-redundant and where redundancy is not possible, these parts are to be further studied with consideration given to their reliability and mechanical protection. The results of this further study are to be submitted for review.

Upon completion and installation of the dynamic positioning system, complete performance tests are to be carried out to the Surveyor's satisfaction at the sea trials. The schedule of these tests is to be designed to demonstrate the level of redundancy established in the FMEA.

Further an annual test of all important systems and components should be carried out to document the ability of the DP-vessel to keep position after single failures associated with the assigned equipment class.

In reality designers and crew are often not comfortable with withstanding single failures (i.e. 'thinking failure') and try to include back ups, 'work around', changeovers, cross feeds, diode 'or' circuits, etc. They try to make the design fault tolerant. Invariably, as the examples in this paper will show, these do not leave the DP system as redundant system as required by class 2 or 3. Either the next failure would be worse than the as designed worse case failure; or they introduce potential for hidden failures and the possibility of cascade failures if the 'back up' can be failed by the same fault that failed the main system.

EXAMPLES

The following nine examples seek to illustrate where designs or modification have tried to improve fault tolerance rather than accepting that failure is an option.

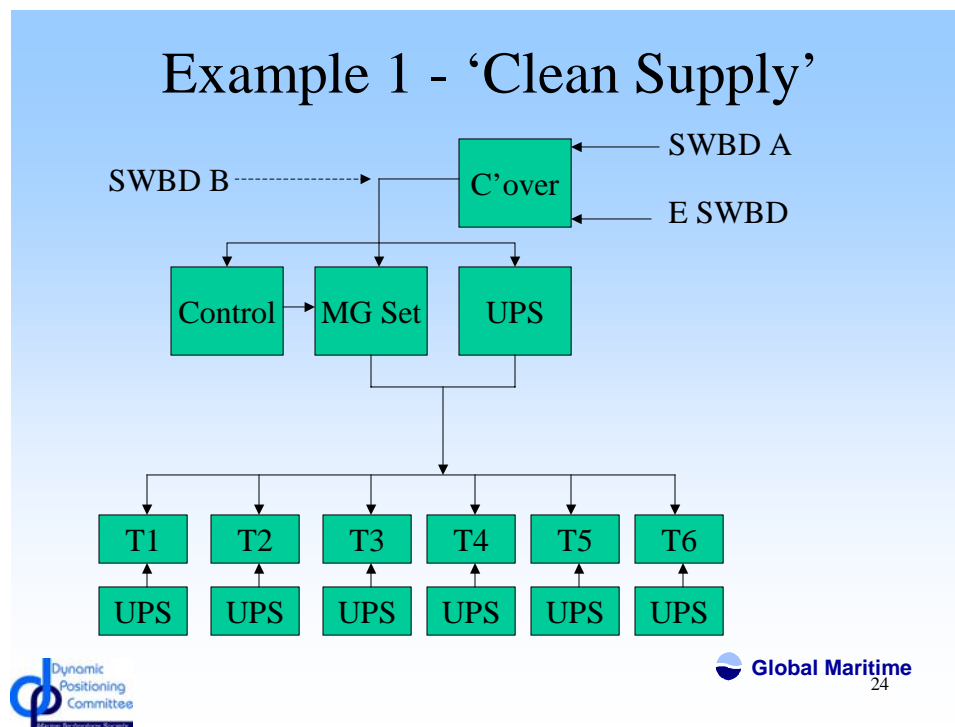
Notes are given with each diagram to explain the example. However as the author was not involved when many of these were implemented, the author has generally had to infer how a particular design has evolved.

Example 1 – ‘Clean Supply’

On this vessel the eight fixed pitch thrusters are variable frequency drives that require a ‘clean’ 220V supply for the control system and loss of that supply results in a thruster tripping. The original design provided this from a Motor Generator (MG) set and associated controller. This could be fed from the A side of the distribution that also powers half the thrusters main motors, or if that failed the emergency switchboard. This was obviously not totally redundant all thrusters could trip on failure of the MG set or its controller. A UPS was then introduced to back up the MG set. But when this failed to cut in on one occasion when required to do so all thrusters were lost. As a result a UPS was fitted per thruster but the MG set/ main UPS arrangement was left in. Now if SWBD A side fails three of the thrusters fail, as their main motor supply A is lost. The UPS should take over powering the remaining thrusters 220V requirements until (and if) the emergency generator starts. However if the UPS has a hidden failure and any of the three remaining healthy thrusters’ control system’s UPS has a hidden failure then more thrusters will fail – adding to the four that have already failed and exceeding the worst case failure for the DP system.

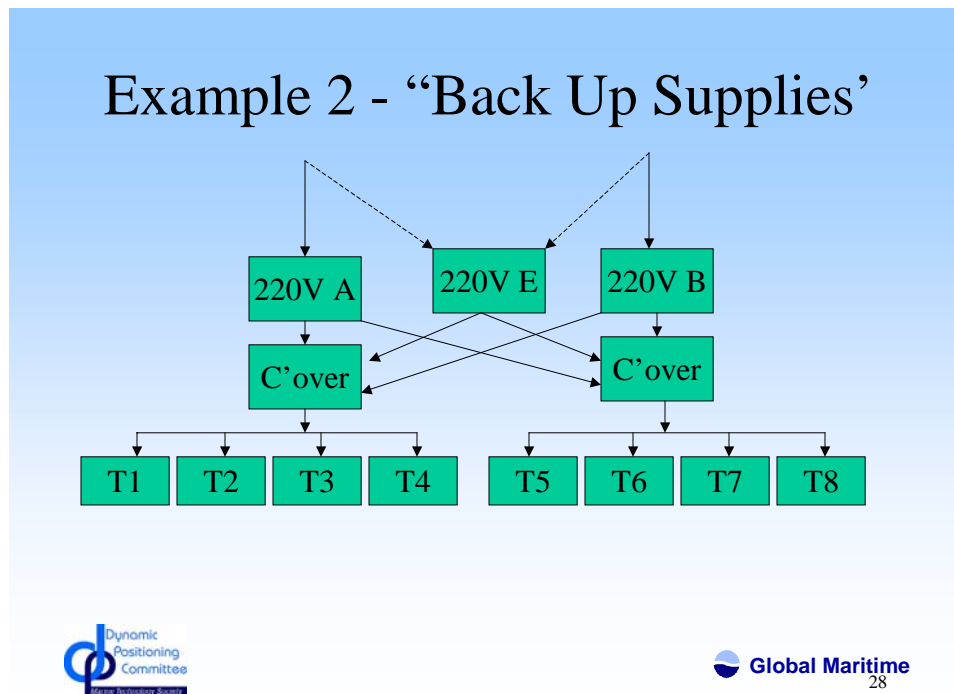
Adding to the complication the vessel personnel included a manual selected cross feed from the other switchboard B.

The overall resultant arrangement has a number of potential hidden failures and potential configuration errors that could result in the as designed worst case failure of three thrusters being exceeded.



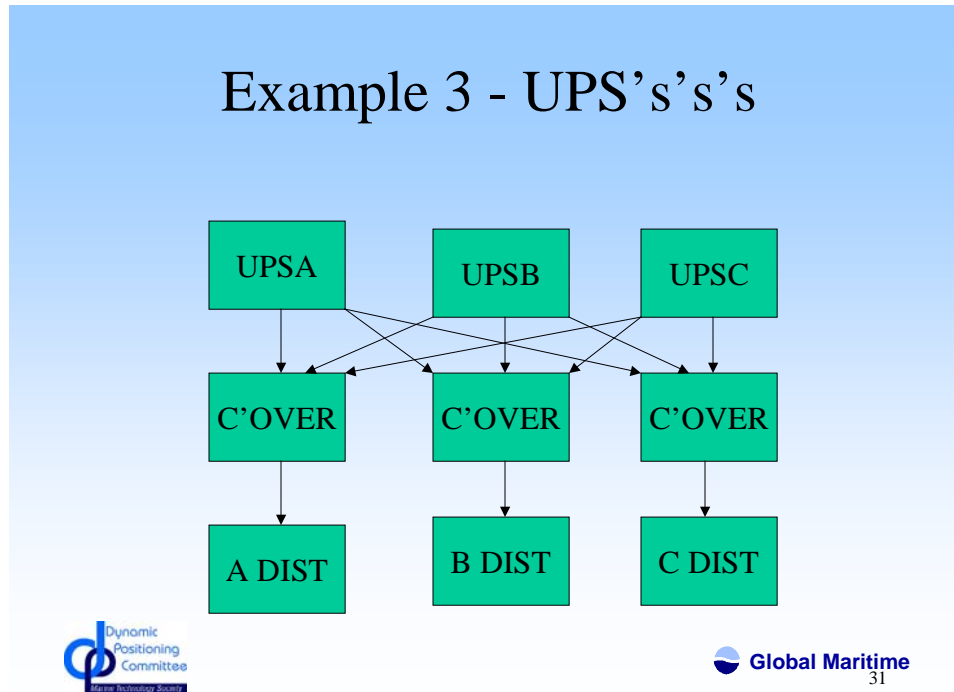
Example 2 – ‘Back Up Supplies

Here each thruster’s pitch control system requires a 220V supply and failure of that supply trips a thruster. This is sensibly four to each side of the distribution as per the high voltage supply to the thruster main motors. The designers however included a possibility to feed all thrusters from either side of the 220V or also from the emergency switchboard. While these features might be useful for ‘get you home’ propulsion they are cannot be used and remain in class 2 or class 3 DP. Additionally the changeover circuits have introduced other potential failure modes and the possibility of configuration errors that must be guarded against by procedure to avoid loss of all thrusters.



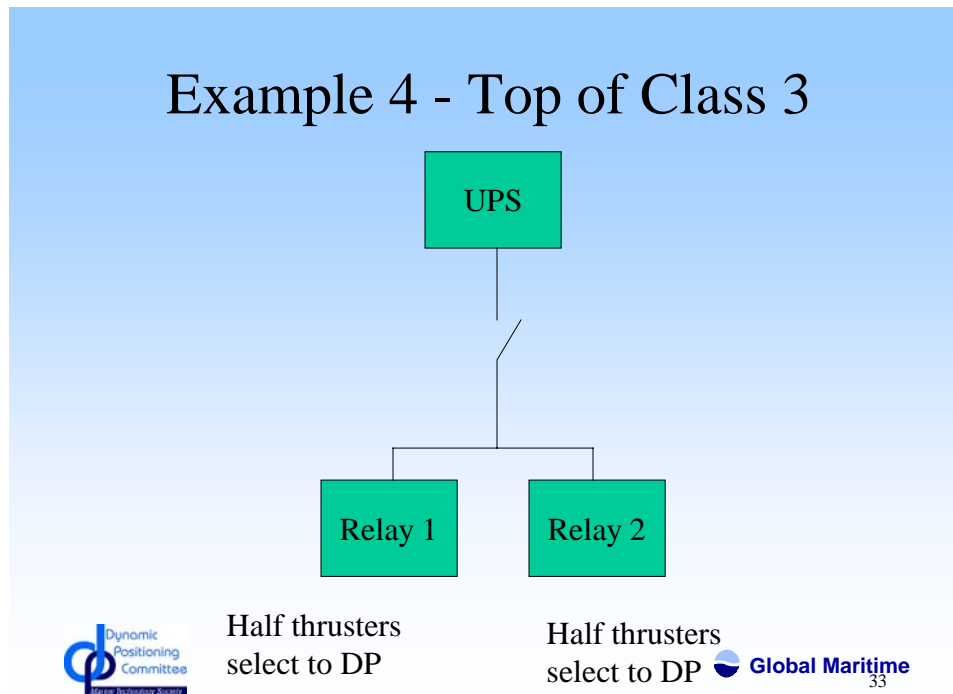
Example 3 – UPS's's's

The original design provided by the triple DP control system supplier had a dedicated UPS for each DP control system and one third of the sensors and position reference systems. On installation the vessel owner decided to 'improve' the design and include manual switches so any UPS could feed any other UPS's consumers. However when a UPS did fail and the DP operator attempted to feed the faulty units consumers from another UPS and that failed the healthy UPS as well. This arrangement has additional failure modes and potential configuration errors introduced by the supposed additional flexibility.



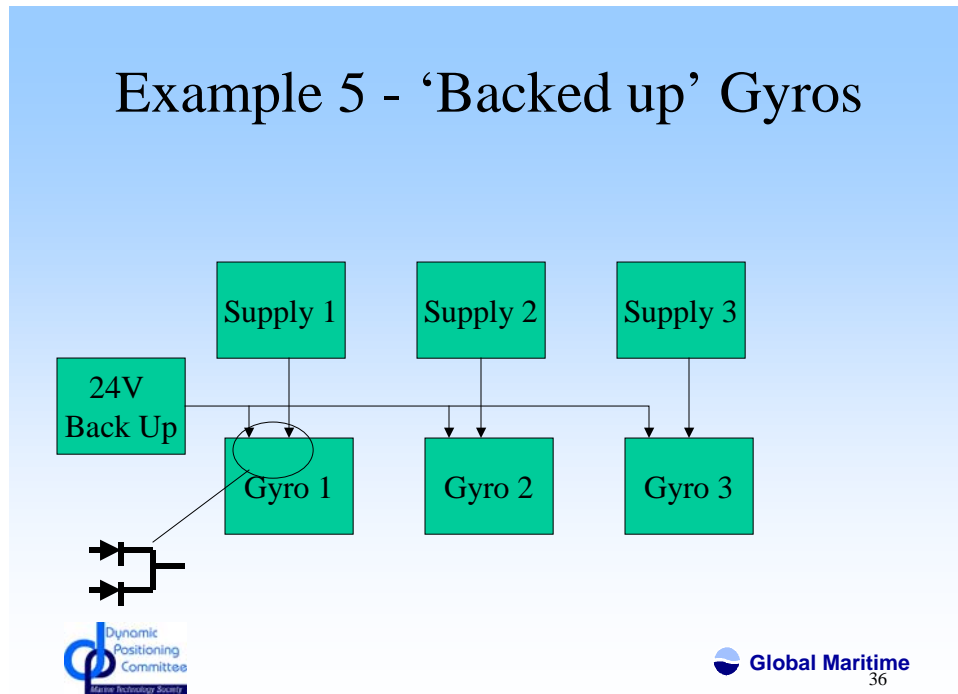
Example 4 Top of Class 3

This was a class 3 DP vessel with large amounts of redundancy. The design of the changeover between conventional manual control and DP control had not been the responsibility of either the thruster supplier or the DP control system supplier. This was left to the shipyard who fitted a single pole switch that energized two relays – one for half the thrusters. This put all the changeover of the thrusters on one contact, one supply and one wire (all against class 3). This was eventually realized but instead of segregating the circuit in two they fitted a UPS. Of course failure of the UPS still fails all the thrusters to a triple redundant DP control system and the ‘design’ does not meet class 2 let alone class 3.



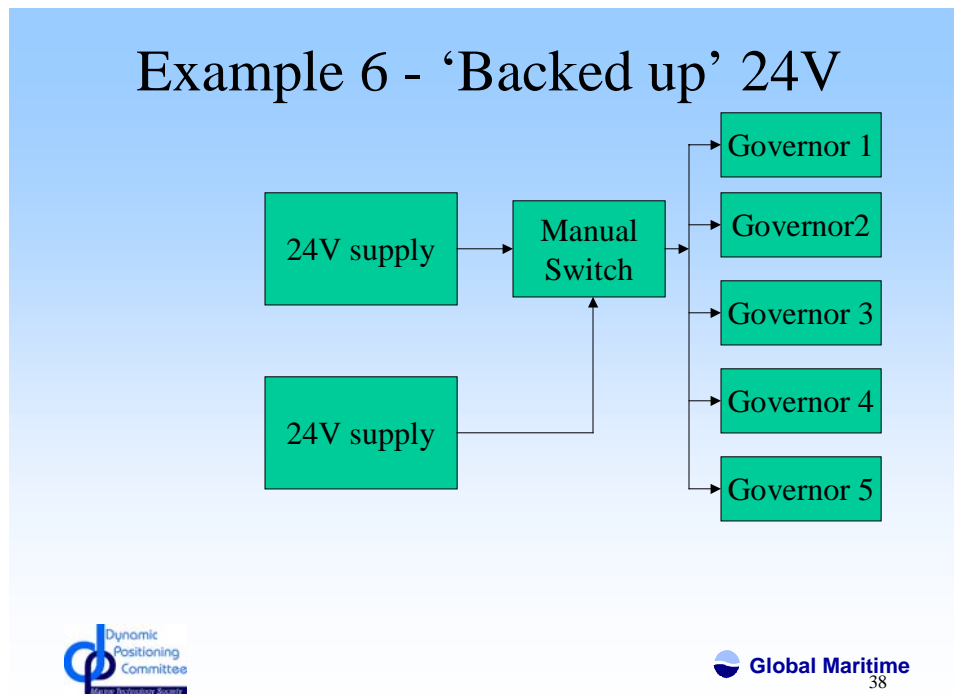
Example 5 – ‘Backed up’ gyros

Here a class 3 vessel had three gyros as required each powered from a separate UPS. Each gyro had the capability of back up 24V dc power feed. Presumably to save start up time for a gyro should its power be lost they were all connected to the same 24V supply. This provided for failure mode that did occur, a spike on the back up 24V took failed all three gyros to the DP and position was lost. Here three totally independent gyros where given a common failure mode by connecting them to the same 24V back up supply.



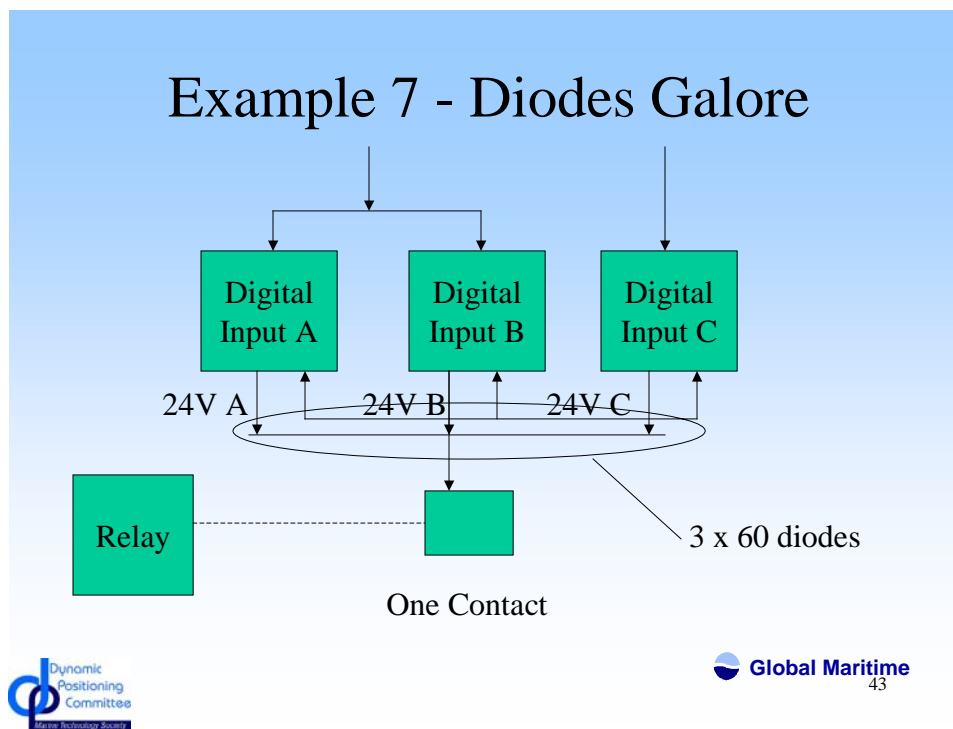
Example 6 – “Backed up’ 24V – redo diagram – error in numbers

The original design had all five of the vessel’s diesel’s governors powered from the same 24V. Loss of this supply resulted in a black out. The ‘solution’ on the vessel was to fit a back up 24V system with a manual switch with supplies being changed over every month to ensure that the back up should work if required. Then they had to have a procedure on what to do when a black out occurs and how to re supply the governors. The proper solution would normally be to supply half the governors from one supply and half from the other. However as this vessel has an odd number of diesels – with number three assignable to either side – a third supply would also be required.



Example 7 – Diodes Galore

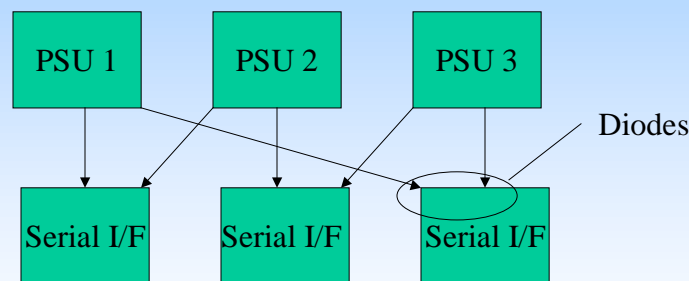
Here the system is a triple redundant control system where all three need read common volt free contacts as digital inputs (e.g. thruster readies). The solution was to provide power from each system through a diode to each contact. So three diodes per contact with about 60 contacts – 180 total. This provided for a large number of hidden failures where a power supply or two can be failed without alarm or warning edge and a number of diodes not found to be faulty until required to provide power. On one sea trials it was found that all were on one supply – the other two had failed some time in the past but had gone unnoticed. When class were asked why they accepted this design they stated that they considered diodes as static devices and not requiring to be considered as having hidden failure modes.



Example 8 – The Heart of a DPCS

This is triple redundant DP control system (DPCS). This had three serial interface cards shared by the three DPCS's providing an interface to the DGPS, acoustic systems, gyros, etc. However instead of powering the items on each serial interface in line with the way they are powered by the UPS – e.g. UPS powers say DGPS1, Gyro 1 etc as well as PSU 1 - which in turn powers the serial card that interface for DGPS 1, Gyro 1 etc. The serial cards interface a different set of items and are cross fed from two power supplies with a 'diode or' circuit. Any hidden failure in this circuit will not be realized until a PSU fails and its back up does not accept the load. In this case up two or possibly three (if there are two hidden failure) serial interface cards can fail and multiple system will therefore fail – beyond what might be expected for a single UPS failure.

Example 8 - the heart of a DPCS

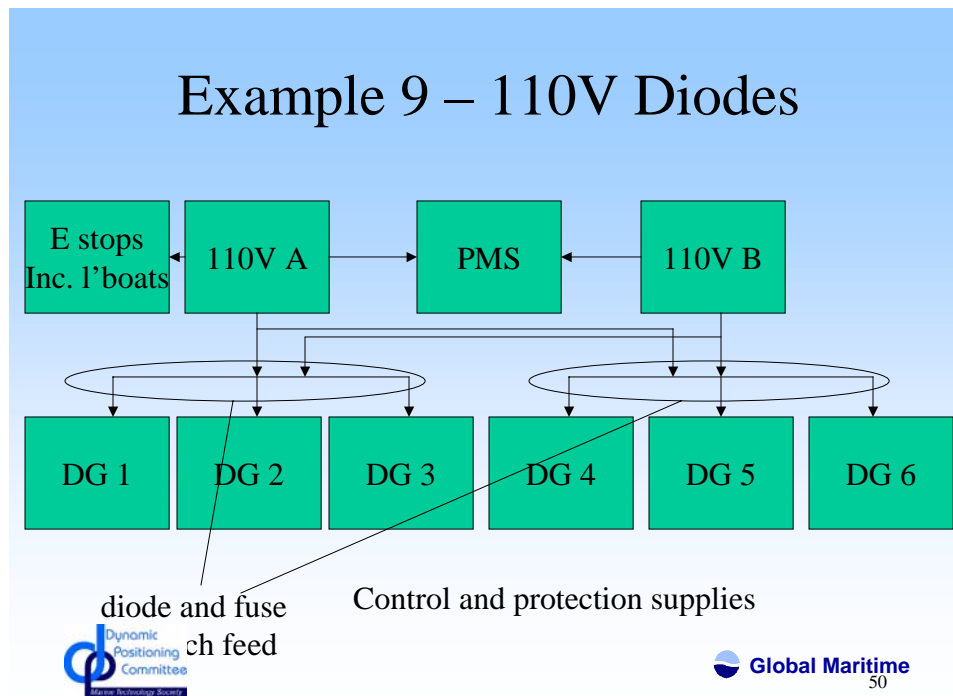


1/3 pos refs and sensors each per UPS

Example 9

Most high voltage switchboards on DP vessels use 110V DC, or thereabouts, for powering the protection circuits. Failure of this voltage either trips all generators on that switchboard or leaves them unprotected. The temptation then is to connect them through diodes so supplies can in theory always be maintained. This again though introduces hidden failure if one supply fails and the other fails to take the load and also fails both 110V DC are failed. A much worse case than failing just the one 110V.

(Aside - On one vessel the where only four large diodes were used, one must have been found faulty at some stage and lacking a spare the vessel electrician connected the 110V directly together without any diodes at all.)



CONCLUSIONS AND RECOMMENDATIONS

The nine examples are from different vessels and it is recommended that the owners of class 2 and class 3 DP vessels review their systems for similar ‘improvements’ and review them critically.

Of the nine examples given; five are site modifications that had no apparent input or peer review from the vessel owner’s engineering department at head office. None of the modifications were subjected to any modification control as would be expected of software modifications. Hardware modification control, with peer review and test procedures etc, needs to be in place for all DP class 2 and class 3 vessels.

All have introduced additional complication and made the system more prone to failure and therefore more unreliable.

Nearly all have introduced the potential for hidden failures and or cascade failure, they all require periodic testing/planned maintenance – hardly any off this was in place. Even if it were it would not totally guard against hidden failures, one can only be certain that there were none last time it was tested.

Many have also introduced the possibility of configuration errors.

The use diodes, to supposedly improve reliability, save contacts, save cabling, etc., – should be avoided. There are still DP control systems being produced that are reliant on a few diodes.

Introducing additional complication to make a design fault tolerant only introduces additional possible faults and generally does not leave the DP system in its required class. The design needs to be viewed from the point of view of failure is an option and kept as simple as possible.