Return to Session Directory

DYNAMIC POSITIONING CONFERENCE
October 15-16, 2013

Quality Assurance SESSION

The Meaning of Life

By Richard Purser

GL Noble Denton

Abstract

The Low Impact Failure Effect (LIFE) concept evolved from the development of the MTS DP Design Philosophy Guidelines. It is a simple design tool intended to help ensure a DP vessel design satisfies the owner's aspirations. It also provides the vessel with the operational flexibility and uptime to carry out its industrial mission efficiently and effectively taking into account the fact that equipment failures can occur and maintenance activities must be carried out. The origins of LIFE lie in recognition of the fact that classification society rules for DP provide a good minimum standard but do not address the vessel's industrial mission. The LIFE concept adds very little to the cost of building a DP vessel compared to class minimum standard (and could actually be less expensive in some applications) but the investment can be recovered many times over during the vessel's operational life. The basic principles are easily understood and can be applied by any design team. The important point is that they should be applied from design initiation and carried through the basic and detailed design phases. The concept can be applied to designs approved by any classification society and is fully compatible with all DP notations. The LIFE concept is applicable to vessels designed for all types of DP operations and is currently being applied to new build drillship and diving vessel designs. This paper describes the LIFE concept methodology using practical examples of how it is applied across a range of systems.

Abbreviations

ASOG	Activity Specific Operating Guidelines
CAM	Critical Activity Mode
DP	Dynamic Positioning
FMEA	Failure Mode Effect Analysis
IMCA	International Marine Contractors Association
IMO	International Maritime Organisation
LIFE	Low Impact Failure Effect
HEMP	Hazard & Effects Management Process
MTS	Marine Technology Society
TAM	Task Appropriate Mode
WCF	Worst Case Failure
WCFDI	Worst Case Failure Design Intent
WSOG	Well Specific Operating Guidelines

Introduction

Low Impact Failure Effect (LIFE) is not a new concept, it is simply the application of good practice and lessons learned. It is a design concept with which most practitioners in the DP community will be familiar. The LIFE concept simply gives a name to this practice and formalises its application in a simple methodology.

There is enormous variation in the effort applied to DP vessel design. At one extreme there are those vessel owners with extensive and experienced design teams who do much of the design development work themselves and at the other end of the spectrum those who rely almost entirely on the shipyard and vendor community to satisfy their requirements based on a fairly shallow specification. The current trend of building stock designs on turnkey projects appears highly attractive from a short term economic perspective but abdicating ones design responsibilities to others can have 'cost of ownership' consequences that may far exceed any initial savings.

The main driver in the development of many DP vessel designs is compliance with class rules. It is important to understand that the purpose of classification society rules is to satisfy insurers and investors that their expensive asset is not likely to be a poor risk or become a marine casualty. Classification society rules go a very long way to ensuring a DP vessel design is sound. However, they do not directly address the needs of the vessel's industrial mission. Compliance with class rules does not guarantee the vessel is fit for purpose or that it will meet the owner's expectations in terms of reliability and minimisation of non-productive time. As the typical working life of a DP vessel can be well in excess of 20 years there is ample time to regret any poor design decisions.

The LIFE concept does not purport to replace the class rules in any way, rather it augments them and fills the gap between a compliant design and a successful one, much in the same way that classification societies offer a combination of rules and recommended practice.

Applying the LIFE concept is not a matter of compliance rather it is intended to help vessel owners and designers understand where a class minimum design may be enhanced to commercial advantage by improving the overall reliability and reducing non-productive time.

This approach ensures the basic rules and regulations are met, whilst at the same time ensuring vessel performance meets expectations. Nothing in this concept is proprietary to the author or to GL Noble Denton and anyone is welcome to apply this concept. It is legitimate to question its efficacy and track record to which the response is that it is based on the established good practice and concepts espoused in the MTS DP Vessel Design Philosophy and Operations Guidelines which have been reviewed and published by DNV as RP-E306. They have also been adopted in large measure in the new DP guidelines by ABS. In the MTS documents, the concept was originally referred to as the LLRC (Low Loss Redundancy Concept) but changed to LIFE to avoid any confusion with similar terms already in use which are not related.

The Case for Applying the LIFE Concept

In addition to the benefits described above there are other reasons to be cognisant of the LIFE concept and its application to DP vessel design.

Regulatory Compliance: DNV, ABS and US Coast Guard are represented on the MTS DP Subcommittee for DP Guidance and Standards which develops the above guidelines. The MTS DP Committee is a technical advisor to the US Coast Guard and 'voluntary' compliance with MTS DP operations guidance is accepted as demonstrating compliance with US Coast Guard requirements for DP operations in the Gulf of Mexico. The International Marine Contactor's Association (IMCA) is currently revising IMCA M103, 'The Design and Operation of Dynamically Positioned Vessels'. It is anticipated that there will be significant alignment between IMCA and MTS on this subject. IMCA has already referenced or reproduced MTS guidance in IMCA M219 and M220. Similarly MTS operations guidance draws heavily on many IMCA guidelines. This convergence of rules, good practice and guidance should help to create a level playing field that benefits a wide range of stakeholders in the DP community and deserves their support.

High Availability for Work: The design philosophy applied in this concept is intended to maximize the vessel's availability for work and to provide a very high degree of reliability and fault tolerance while at the same time providing sufficient flexibility to allow the vessel to carry out repair or maintenance work on DP related equipment while retaining full fault tolerance with a reduced but well defined DP capability. These enhanced features are intended to ensure the vessel can remain operational and conduct DP class 2/3 operations (with a reduced environmental envelope) after major technical failures and even to a limited (but defined) extent after a compartment fire or flood.

Alignment with Operations Guidance: The DP community now recognizes that DP Equipment class is not, on its own, a very effective way of managing risk and non-productive time. DP Class 3 vessels are not more reliable than DP class 2 vessels because the influential failure modes that separate these two classes (passive component failure, fire and flooding) are swamped by factors that they have in common, such as reference systems, DP control systems, power management systems, networks and human error. What is capable of making a significant and measureable difference is the way in which the DP system is configured and operated and this led to the development of the concepts of Critical Activity Mode (CAM) and Task Appropriate Mode (TAM). The LIFE concept is intended to create designs that can take full advantage of these operating philosophies.

Critical Activity Mode (CAM): A DP system configuration and operational mode which recognizes that station keeping integrity must be the highest priority when the consequences of a loss of position include risk to life or damage to the environment.

Task Appropriate Mode (TAM): A DP system configuration which recognizes that other factors such as fuel consumption, emissions and maintenance requirements are also important and can be considered in the operational philosophy when the consequences of loss of position are purely commercial (e.g. equipment damage or non-productive time.

Not every industrial mission has activities that would be suitable for TAM. MODUs might expect to carry out 30% of a typical well program in CAM and the rest in TAM. Diving vessels on the other hand are likely to spend all of their time in CAM during diving operations. If the industrial mission of logistics vessels is defined as the time they spend on DP, loading and unloading cargo from platforms or floating assets, then there is little point in defining a TAM configuration, as their time on DP represents a relatively short part of their operational life cycle. If however, PSVs engage in other activities then it may be appropriate to develop a TAM based on appropriate HEMP (Hazard & Effects Management Process) assessment of the industrial mission. This is the approach taken for project and construction vessels.

The LIFE concept is applicable to all industrial missions, even those for which it is not possible to define a part of the mission that can be conducted in TAM. A pilot project for the concept includes DP class 3 MODUs with CAM and TAM and a DP 3 diving vessel with only a CAM.

Core concepts

The fundamental principles and processes that underpin the LIFE concept for DP vessel design are:

1. The key principles of fault tolerant design – performance, protection and detection.
2. The key processes – predict, prove and protect.
3. The ‘seven pillars of wisdom’ – desirable attributes in a fault tolerant system.

In practical terms:

1. Reduce the impact of the worst case ‘technical’ failure to as low a severity as reasonably achievable – typically one generator and/or one thruster in a diesel electric power plant.
2. Develop a Worst Case Failure Design Intent (WCFDI) and operating configuration for CAM and TAM using appropriate failure criteria and definitions.
3. Add non critical redundancy over and above that required for class to improve vessel reliability and availability where it makes economic sense to do so.
4. Reduce the number of cross-connections between redundant equipment groups.
5. Reduce the dependence on protective functions particularly for CAM.
6. Reduce the number of failure modes leading to effects equal to the Worst Case Failure Design Intent.

Failure criteria

IMO MSC645 Guidelines for Vessels With Dynamic Positioning Systems, 1994 introduced the concept of DP Equipment Class. The intention being to create a series of three classes that provide a level of reliability to match the consequences of a loss of position. The choice of equipment class was then a matter for the charterer to decide given the consequences of losing position during the planned operation. This variation in station keeping integrity was defined by the types of failures that were to be tolerated without loss of position. In broad terms:

- DP class 1 – No requirement for fault tolerance.
- DP class 2 – Tolerate technical failure of an active component.
- DP class 3 – Tolerate any technical failure including the effects of fire or flooding in one compartment.

Explicit within IMO MSC 645 is the idea that a vessel in any equipment class can carry out the work requiring a vessel of a lower class. In reality most work requiring a vessel with some degree of fault tolerance is carried out by DP class 2 or a DP class 3 vessel. Very few charters or coastal states make any stipulation beyond stating DP class 2 or better. Although there is no official recognition of the concept of 'operating class' this is in fact how it is understood by many. Unfortunately this led to cases where DP class 3 vessels that were approved by class on the basis that their power plants were operated as isolated power systems (busties open) simply closed their busties when they carried out operations requiring a DP class 2 vessel. This was done on the misguided assumption that this was in some way allowed by the DP rules and in spite of the fact that the power plants of such vessels were not fault tolerant in this configuration. The situation has improved significantly with the major classification societies requiring that all configurations which are considered to comply with their requirements are analyzed in the approved FMEA. This has led to the practice of DP class 3 vessels having two or more 'approved configurations'; one which complies with the rules for DP class 3 and another which complies with the rules for DP class 2. The advantage of this is that when DP class 2 failure criteria are applied it is possible to significantly extend the vessel's post worst case failure DP capability thus increasing its working environmental envelope before operations have to be suspended.

The philosophies of LIFE, CAM and TAM remain true to the fundamental principles of IMO MSC 645 that the equipment class for a particular operation is to be established by appropriate risk assessment or coastal state requirement as stated in IMO MSC 645 Section 2.1.

The equipment class of the vessel required for a particular operation should be agreed between the owner of the vessel and the customer based on a risk analysis of the consequence of a loss of position. Else, the Administration or coastal State may decide the equipment class for the particular operation.

The configuration used for CAM would always be a fully class approved configuration and typically that associated with the vessel's DP notation. TAM on the other hand may be a fully fault tolerant configuration associated with the failure criteria for the same equipment class or a lower class. Or, it may be accepted that the vessel is not fully fault tolerant in this configuration, but best use is made of the redundant systems it has, to reduce the risk of loss of position to a minimum whilst allowing the flexibility to reduce fuel consumption, emissions and running hours. This is often the case with older vessels where the redundancy concept would not pass modern standards of scrutiny and verification in this particular configuration, even though it may have been approved by class at the time the vessel was built. Some of these vessels are unable to carry out all aspects of their industrial mission in a fully fault tolerant configuration because of restrictions imposed by the power plant design.

Where the nature of the industrial mission permits it, the MTS DP Vessel Design Philosophy guidelines encourage vessel owners considering new buildings and major conversions to specify designs which can be operated as fully fault tolerant in a range of DP system configurations in respect of the failure criteria defined for the appropriate DP class notation. For CAM the emphasis is on fault tolerance based on passive protection such as isolated power systems. In the case of TAM however, there may be greater reliance on protective functions. For TAM, it is also accepted that the vessel owner may define their own failure criteria which may exempt certain low probability failures from consideration such as HV bus bar faults where the additional equipment, complexity and cost required to include it, is not justified by the improvement in station keeping integrity, particularly where it is already accepted that the power plant can be operated as a common power system. Provided the risks are well documented and understood by the vessel owner, charterer, regulators and other stakeholders then this approach satisfies the intentions of IMO MSC 645 and the MTS DP Operations Guidelines (also published as DNV RP E307).

One of the most readily understood and familiar ways of documenting the risks associated with a particular configuration is to analyse them in a DP system FMEA. Where a non-fault tolerant configuration or bespoke failure criteria are to be included in the FMEA for submission to class it is important to discuss with class what, if any, approval they can offer for this configuration. Where no approval can be given then the configuration could be considered as equivalent to an un-classed installation as DP notations are optional.

In the case of a specification for a new building, it is vitally important that the configurations, their failure criteria and associated worst case failure designs intents are included in the contract for the vessel to reduce the risk of disappointment.

Whatever the design criteria or operating configuration application of the LIFE concept can improve robustness, fault tolerance and vessel availability for work.

Understanding the Worst Case Failure Design Intent (WCFDI)

To understand the benefits and implementation of the LIFE concept it is important to be familiar with the terms that are used to define a DP vessel's redundancy concept. Principal amongst these is the Worst Case Failure Design Intent (WCFDI) which describes the minimum amount of propulsion and control equipment remaining operational following the worst case 'single' failure.

The worst case failure design intent:

- is used as the basis of design.
- establishes the vessel's post worst case failure DP capability (when the thruster ratings are known).
- establishes the vessel's operational environmental limit for redundancy in the intact condition.
- is achieved by the provision of redundant systems.

WCFDI is often confused with the Worst Case Failure (WCF), WCF is the actual worst failure the vessel will suffer from a single failure and not the stated WCFDI. If the DP system is fully fault tolerant in respect of the defined failure criteria then the WCF effect will be less or equal to the WCFDI. The WCF should be revealed by the FMEA process.

Definitions: In the context of this document, the term DP system is intended to mean all systems and equipment associated with automatically and manually maintaining the vessel's position and heading. The term 'DP related' means connected with the operations of the DP system whether failure has any effect on the vessel's ability to maintain position and heading or not.

A typical WCFDI can be stated as follows for a DP Class 2 design:

"No single failure of an active component (as defined for notation DPS-2) will have a greater effect on the vessel's ability to maintain position and heading than the loss of one of the two redundant equipment groups. This design intent applies when the power plant is configured as two isolated power systems or as a common power system. This design intent applies when each of the two power systems has generators and thrusters connected.' For this statement to be valid, all DP related equipment must be capable of its rated capacity and all protective functions must operate effectively on demand."

In practice, one of the two redundant equipment groups may be weaker in terms of DP capability and therefore loss of the stronger of the two redundant groups represents the worst case failure. It is also worth noting that in some designs the worst case failure can be heading dependent but this should become apparent from the DP capability plot.

Figure 1 shows the practical implementation of such a Worst Case Failure Design Intent in a DP class 2 semi-submersible design.

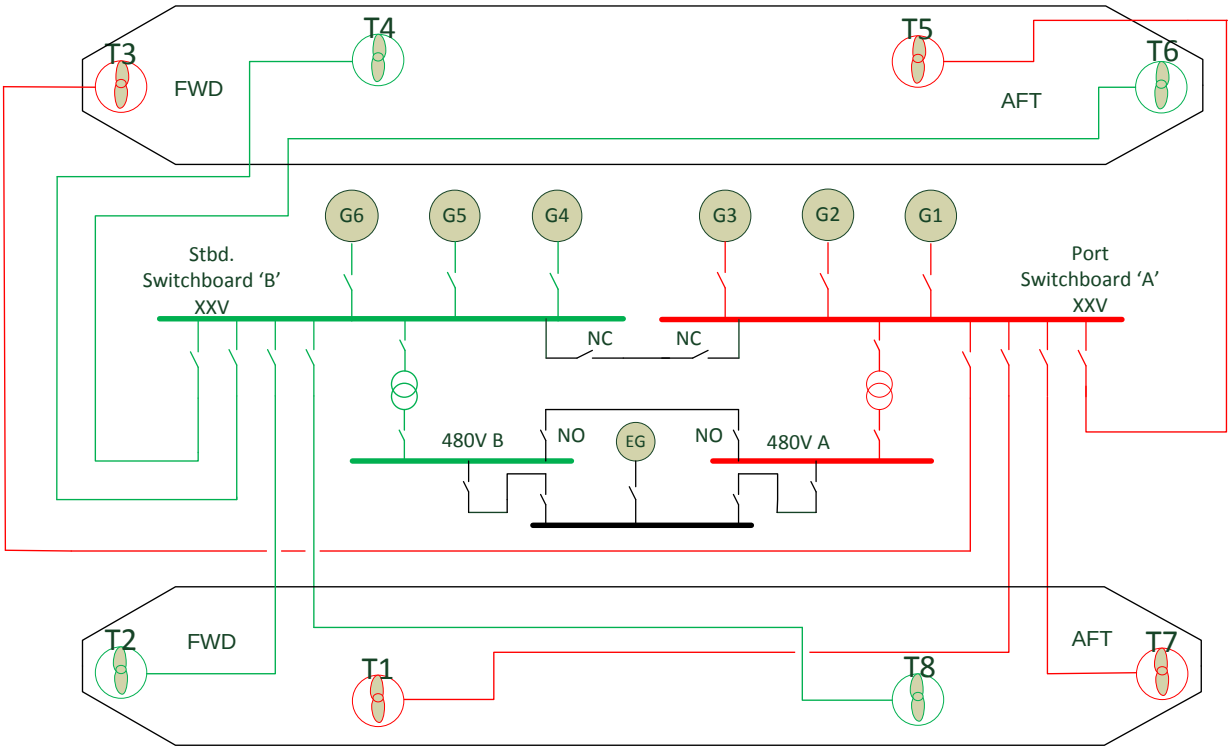

Figure 1 Two Way Split to Support the WCFDI

A typical WCFDI can be stated as follows for a three way spilt design:

"No single failure (as defined for Class notation XXX) will have a greater effect on the vessel's ability to maintain position than the loss of one main switchboard with two thrusters and up to three generators. No single failure will cause the loss of more than one thruster at each end of the vessel. This design intent applies when the power plant is configured as three independent power systems or as a common power system. This design intent applies when each of the three main power systems have generators connected, for this statement to be valid all DP related equipment must be capable of its rated capacity and all protective functions must operate effectively on demand."

Figure 2 shows the practical implementation of such a Worst Case Failure Design Intent in a DP class 2 or 3 monohull design

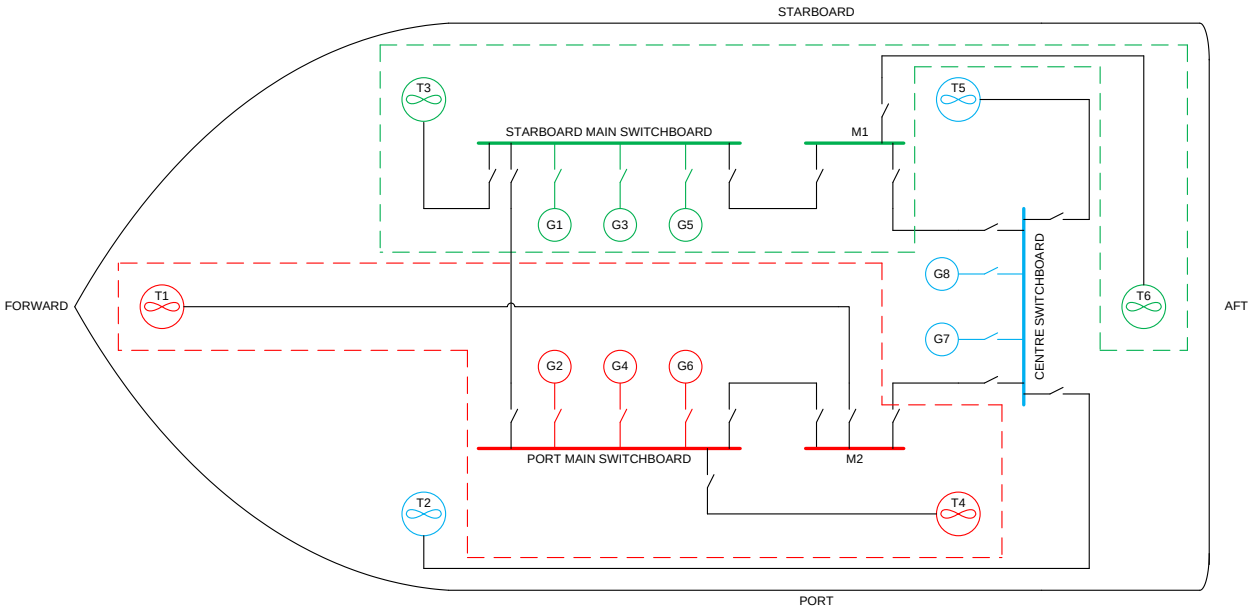

Figure 2 Three Way Split to support the WCFDI

Applying the Life Concept

Key elements of fault tolerant design

The process starts by recognising that the integrity of a fault tolerant DP system based on redundancy depends on three main elements:

- Performance
- Protection
- Detection

Performance: For a DP system to be fault tolerant each redundant equipment group and all the DP related machinery and systems within it must be capable of their defined performance – Performance means more than steady state capacity, it also includes dynamic performance, response time and accuracy for example.

Protection: Even the best separated DP systems inevitably have some common points between redundant equipment groups and these represent potential fault propagation paths. There must be effective protective functions or features to prevent faults in one system adversely affecting the operation of others.

Detection: It is important to know when full fault tolerance has been lost. Potential hidden failures can be detected by suitable alarms and periodic testing.

Desirable attributes

Seven desirable attributes for robust fault tolerant systems were identified in the MTS DP Vessel Design Philosophy Guidelines. Colloquially known as the 'Seven Pillars of Wisdom' they are considered to be desirable attributes in any DP related system or sub-system.

There are seven key attributes which are desirable elements for a robust DP system, these are:

1. Independence
2. Segregation
3. Autonomy
4. Differentiation
5. Fault tolerance
6. Fault resistance
7. Fault ride through capability

The significance of these attributes is as follows:

1. Independence: Main machinery should be made as independent as possible to limit most failures to loss of one generator or one thruster. Losing multiple generators and thrusters is an unnecessarily severe failure effect particularly if it is associated with relatively probable failures such as loss of a single 24Vdc power supply. Non critical redundancy to add another 24Vdc supply would improve this.

2. Segregation: Systems intended to provide redundancy should have as few common points connecting them as possible. Common points are responsible for the vast majority of failures that defeat redundancy concepts. In the example above, a second 24Vdc supply for each generator was recommended. This attribute would suggest that this is better than providing each generator with a common second supply as a backup which would link them all together. Using the generators PMG as a source of control power is one way of maintaining segregation.
3. Autonomy: Control and automation functions should be decentralised to the point that each item of main machinery (generators & thrusters) is capable of making itself ready for DP operations independently of any centralised or hierarchical control system. There have been several cases where standby machinery failed to connect or blackout recovery was delayed or incomplete because there were too many unnecessary permissives in the start sequence for main machinery. Similarly main machinery may not respond if the control systems has failed as part of the failure – Permissives and reliance on hierarchical control are all potential failures and vulnerable to timing errors etc.
4. Differentiation: The principles of differentiation, diversity and orthogonality in the design of redundant systems should be used to best advantage. Common mode failures associated with the use of common hardware and software are always a potential risk. Gyro compasses and DGPS systems have been notable examples. The aerospace industry recognises this and takes this principle to a much greater degree than the marine industry but even so there are reasonable steps that can be taken to reduce the risk. For example, specifying sensors and position references from a diversity of suppliers or changing the personality of a reference system by adding inertial navigation to at least one of the redundant references systems such as DGPS or HPR.
5. Fault tolerance: DP systems of equipment classes 2 & 3 are required to be fault tolerant with respect to the defined single failure criteria appropriate to each DP class notation. Applying the three key elements of fault tolerance when assessing this point helps to focus attention on the functions and features required to support it.
6. Fault resistance: DP related equipment should be selected on the basis of high reliability and resistance to internal and external influences which may reduce reliability. Temperature, humidity, vibration, harmonic distortion, voltage spikes, frequency excursions and saliferous atmospheres will all influence reliability.
7. Fault ride through capability: The ability of redundant systems to continue in operation without malfunction when subjected to the effects of failures in other systems to which surviving systems are connected. Voltage dip ride though is the most common manifestation of this issue but has analogies in pressure drops of hydraulic and pneumatic systems and the ability of data communication systems to handle spikes in data rate when a major equipment failure causes an avalanche of alarms.

Predictability

All the attributes and elements discussed above can be considered to contribute to the predictability of the DP system failures. Predictability is the most essential attribute of a fault tolerant DP system and is often represented graphically as being the foundation upon which the seven pillars stand. Discussion of predictability introduces the related subject of testing the redundancy concept. A combination of failure modes and effects is used along with analysis and proving trials to demonstrate the fault tolerance of the system and prove the DP system FMEA can predict the failure effects. The key elements in this process are known as the three ‘Ps’, which are:

- Predict
- Prove
- Protect

Predict: The FMEA must be able to predict the failure effects (in so far as there is information to allow it to do so).

Prove: The DP FMEA proving trials must demonstrate that the FMEA correctly describes the redundancy concept 'as built'.

Protect: Having predicted the failure effects for a comprehensive range of failure modes and proved that the analysis is correct (or not) the final step that closes the loop is to confirm that the redundant systems within the DP system have the performance, protective functions and detection features to defend the redundancy concept against failure modes that could defeat it. It is this part of the process that is carried over into the vessel's operational lifecycle as planned maintenance and annual trials. MTS DP Vessel Design Philosophy Guidelines and DNV RP-D102 FMEA of Redundant Systems, provide further guidance on this subject.

LIFE Example

The DP system of the example vessel in Figure 3 is an evolution of a stock DP class 3 design which is popular in drillships but is applied to a large diving vessel in this example. The DP system is designed around three independent/isolated power and propulsion systems, each capable of maintaining position and heading by developing the necessary surge, sway and yaw forces. Figure 4 shows the combination of azimuthing and tunnel thrusters which are arranged to provide propulsion for transit, berthing and dynamic positioning.

It is a common misconception to regard a three way split as exceeding class minimum requirements for redundancy. Multi-split arrangements simply make better use of installed machinery. In addition to the advantages of retaining fault tolerance with one power system unavailable, the vessel can have greater post failure DP capability for the same sized machinery or the same post failure capability with smaller (cheaper) machinery. Because of the requirement for fault tolerance, a DP class 3 (or 2) vessel's useable thrust envelope, in the intact state, is defined entirely by its post failure DP capability.

Those aspects of the LIFE concept that do exceed the class minimum standard are related to limiting the effects of single failures to the loss of one generator and/or one thruster for a limited range of failure criteria. These enhancements are intended to improve overall reliability and vessel availability for work. These enhancements are applied at the vessel owners' discretion and only where justified by increased vessel uptime, which is closely related to revenue.

Because this example is a diving support vessel, all DP operations are carried out in CAM with the main busties open. The owner sees no advantage in having a TAM configuration for DP given the nature of the work the vessel is intended to carry out.

The complete three way split offers the possibility of continuing to conduct DP operations with one redundant group down for maintenance or after a failure. Clearly after any failure it is prudent to suspend operations and confirm that the remaining redundant machinery groups are fully intact and not affected by the failure. However, once this has been established, the vessel is fully capable of continuing to work as though it were a more conventional two way split. The only parts of the DP system that are not easily split into three are the vessel management system networks and position reference systems. Failures in these systems can be addressed relatively quickly by carrying appropriate critical spares.

A diesel electric power plant becomes more robust the greater the number of generators connected. Power systems operating with all busties closed and all generators connected are the most robust of all in terms of their failure response to the most probable failure modes, but they can be vulnerable to a small number of well known 'killer' failure modes which can be addressed by the use of advanced protective functions. As this vessel intends to spend all off its time on DP operating in CAM and the safety and wellbeing of the divers is of paramount importance, the owner intends to base the primary protection around the passive protection afforded by three isolated power systems. However, each of these three power systems is relatively fragile by comparison and even more susceptible to the 'killer' failure modes. To prevent this from reducing overall DP system reliability, the owner intends to make use of advanced protection features to restore the level of robustness to something approaching that of a closed bus power system.

The vessel's Worst Case Failure Design Intent is effectively defined by the fire and watertight separation which is provided for the three isolated power trains. If the owners' were to rely solely on the class rules then nothing would prevent the development of a design where every failure, no matter how probable or improbable would lead to the complete loss of two thrusters and two generators in one of the isolated power systems. While these effects would not exceed the worst care failure design intent, the loss of reliability could result in non-productive time, particularly if a failure had already occurred in one of the other power systems.

To counter this, the owners' elected to apply the LIFE concept by defining two parts to the WCFDI in the vessel's specification:

- WCFDI $_{CLASS}$ to define the failure effects associated with failure criteria for DP class 3.
- WCFDI $_{LIFE}$ to define a set of failure criteria which would limit the loss of generators and thrusters to one, for all but the least probable of failure modes.

PART I - WCFDI $_{CLASS}$ - *'No single failure as defined for class notation DP3 will have a greater effect on the vessel's ability to maintain position and heading than the loss of one of the three independent power and propulsion systems consisting of two generators and two thrusters (one fwd & one aft). This statement is considered to be valid when the power plant is operated with all the bustie circuit breakers between the three power systems open and at least one generator connected to each of the three 6.6kV switchboards.'*

PART II - WCFDI $_{LIFE}$ - *'No single failure with the exception of the effects of fire, flooding, 6.6kV bus bar fault and passive components (as defined in IMO MSC 645) will have a greater effect on the vessel's ability to maintain position than the loss of one thruster and/or one generator in the same independent power and propulsion group. This statement is considered to be valid when the power plant is operated with all the bustie circuit breakers between the three power systems open and two generators connected to each of the three 6.6kV switchboards (it is accepted that the whole independent power system may be temporarily lost if only one generator is connected). Note: this requirement is not to be misunderstood as indicating any requirement for compliance with failure criteria other than that stipulated in this definition, for example class DP3 or IMCA guidance. This definition simply guides the development of non-critical redundancy intended to improve reliability and vessel availability.'*

Where any part of these statements conflict with the accompanying specification, the owner will be consulted for clarification.

In the case of the WCFDI $_{LIFE,}$ the owner was prepared to accept the risk of non-productive time associated with fire, flooding, HV bus bar faults and pipework failures, but not failure of active components such as power supplies, UPSs, pumps and compressors. In some systems the perceived risk associated with common pipework was not with failure of the pipework, but with the contamination of the common medium. To prevent any confusion, system sketches were provided to clarify the design intent in all systems. The entire DP system philosophy was then set out in a DP Redundancy Concept Document accompanying the invitation to tender.

Figure 4 shows the power system single line diagram that is developed from the WCFDI statements. The central bus coupler in the 6.6kV switchboards are shown as optional and were inserted for pricing purposes, and to allow the possibility that the power plant could be approved by class as a six way split under DP class 2 failure criteria. This could extend the vessels post failure DP capability but has to be offset by the additional cost and size of the switchboards and the additional complexity, against how often the vessel would be able to benefit from this extended capability. That in turn may also be influenced by other factors such as acceptable vessel motions etc. Table 1 gives an overview of the objectives in relation to failure effects within each major system.

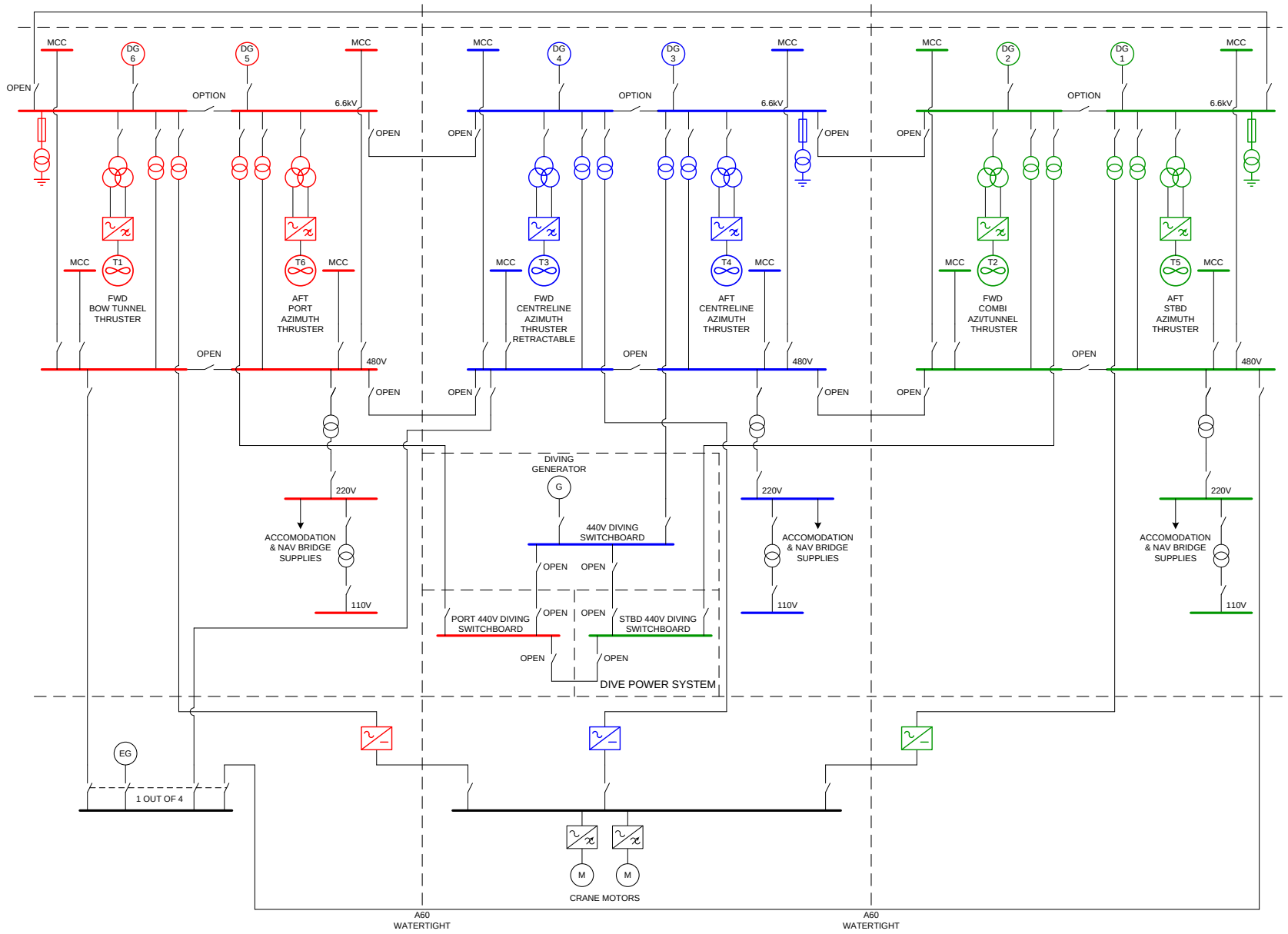

Figure 3 Single Line for Example Vessel

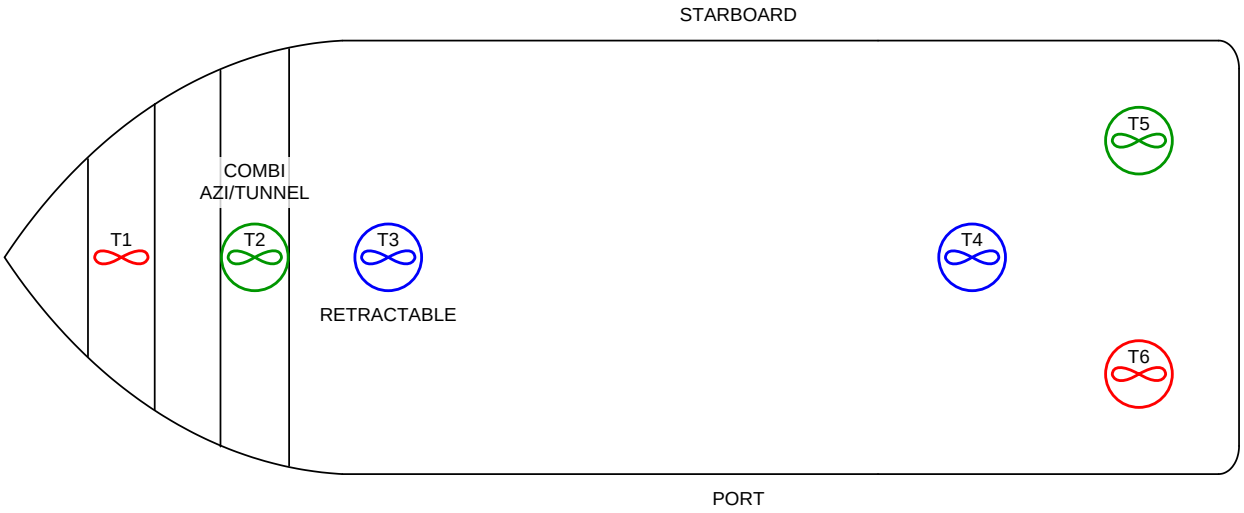

Figure 4 Thruster Layout of Example Vessel

Table 1 Summary of LIFE Redundancy Design Objectives on a System by System Basis

System	Fire & Flooding	Technical Faults (Excluding 6.6kV Bus Fault)
Generators	Two out of three groups survive any single failure	Independent (6 way split)
Thrusters	Two out of three groups survive any single failure	Independent (6 way split)
Marine Auxiliary	Two out of three groups survive any single failure	Single generator and/or single thruster affected
DP Control	Dual redundant (main & backup)	Triple redundant
Control Networks	Dual redundant	Dual redundant
VMS/PMS	Two out of three groups survive any single failure	Loss of associated machinery ≤ WCFDI Part II
Safety / ESD	Fail safe ≤ WCFDI Part I	Fail safe ≤ WCFDI Part I

LIFE Concept - Influence on System Design

The following passages are selected extracts from the redundancy concept documents showing how the key elements and seven pillars were applied in support of the LIFE concept.

General: The power plant is designed and configured as a three-way split arranged physically as port, centre and starboard power systems. This arrangement requires three A60 / watertight zones to be created which include cable and pipe routes to the forward and aft thrusters and also to those industrial consumers with a power supply from more than one of the independent power systems. Thruster control is by way of a dual fibre optic backbone. **- SEPARATION**

DP Redundancy relies on equipment being available in both number and capacity. Alarms combined with periodic testing are essential risk reduction measures and therefore the owner wishes to ensure the alarm and monitoring system is built to a good standard and the vessel operators are well informed about the condition of the plant and failures which might remain hidden otherwise. Unmanned machinery space notation will be sought even though the engine control room will be permanently manned. - **DETECTION**

With the exception of the fibre optic connections to the field stations for the vessel management system, no power or control lines will cross the A60 / watertight boundaries between the three redundant machinery groups. Exceptions for reference system connections to the back-up DP system will be made on a case by case basis where adequate isolation can be demonstrated. **– SEPARATION**

Maintaining complete electrical separation between redundant systems should eliminate the need for live short circuit and earth fault testing to prove voltage dip ride through, which requires specialist knowledge and rigorous preparation. **– SEPARATION**

Diesel Generators: The main generators are sized to provide the total thrust, hotel and industrial loads demonstrated in the load balance for the various operational scenarios defined in the specification. The calculation is to take into account that the maximum thrust requirement is determined by the WCFDI for DP Class 3 operations plus a practical working margin to be specified.

Each engine is independent in respect of auxiliary systems including combustion air supply, exhaust systems and crank-case breathers. Combustion air can be ducted direct to the turbo chargers. Air intakes for engines should be well separated to reduce the risk of more than one engine room drawing contaminated air. **- INDEPENDENCE**

The main generator engines will comply with IMO Tier 3 requirements for emission control. The design will consider the load acceptance and rejection characteristics of such engines in relation to typical loading conditions during DP operations. It is expected that fast acting and effective frequency based load shedding functions in the PMS, thruster and crane drives will act to prevent cascade failure of both engines if one trips or a large step load is applied. In the event that one power system is lost, it is anticipated that the DP control system, crane and industrial loads will transfer thrust load (phase back) to the surviving generators at a controlled rate which does not result in unacceptable position excursion or dip in system frequency and/or voltage. **- PROTECTION**

Alternators will be brushless self-excited machines fitted with Permanent Magnet Generators (PMGs) to ensure excitation support during short circuit fault clearance and provide independent control power supplies once the generators are running. - **INDEPENDENCE & AUTONOMY**

It will be possible to start the engines after blackout without recourse to energising the LV switchboards using the emergency generator. Pneumatically operated fuel and pre-lubrication pumps driven from the starting air systems may be used if required. - **INDEPENDENCE**

Each engine will have a self-contained control and safety system with a dedicated power supply with battery backup. Each engine control system will be separate from the engine safety system. The engine will receive either a ’start’, ‘connect’ or a ‘start and connect’ signal from the VMS and from that initiation signal, the dedicated engine control system will arrange for the starting of all auxiliary sites necessary for the generator to run. The generators will start, connect and load share without intervention from the VMS. **- AUTONOMY**

The engines will have suitable characteristics and starting systems to allow blackout recovery to be achieved in less than 20 seconds, including automatic thruster restart and resumption of automatic DP control. - **PERFORMANCE**

The gensets will be fitted with effective and accurate digital governors and AVRs operating in uncompensated droop mode for frequency and voltage control. There will be no load sharing lines of any type connecting generators. **- INDEPENDENCE**

Where possible, engine auxiliary services are to be served by engine driven pumps. Where the choice of engines precludes this, dedicated electric pumps supplied from the generator's own MCC are to be provided. Consideration can be given to providing a standby pump where justified on the basis of improved reliability and uptime. - **INDEPENDENCE & AUTONOMY**

HV and LV Switchboards: Refer to Figure 3. The HV switchboards are to be fully capable of remote manual operation of the vessel control and power management systems. This is required to ensure that a coordinated approach can be taken to controlling the vessel systems which allows the best oversight, clear communication and access to alarms and indications. Power management automation will be applied in a manner that enhances DP safety and reliability. The LV switchboards and MCCs are to be automated to an extent defined by the vessel owner but should in any case allow remote manual and automatic control of thrusters, generators and service transformers without local operator intervention. Sufficient automation of the LV switchboards should be provided to allow remote manual control of all marine and auxiliary systems, including full automatic blackout recovery. Where such automation is provided, I/O for control and monitoring will be divided up in a manner that supports Part I and Part II of the WCFDI. It will be possible to control the power plant using local controls in the event of remote control failure or vice versa. **- INDEPENDENCE & SEPARATION**

HV switchboards will be arc-proof and designed to withstand the maximum thermal stress and short circuit current that can flow with all switchboards, generators and loads connected. - **PROTECTION**

Although the vessel will always operate with open busties when conducting critical operations, there may be occasions when one power system will be connected to the other for maintenance purposes. The generator protection systems will be arranged to trip both busties at the ends of a bus section on detection of any generator fault. - **PROTECTION**

Optical arc protection (or equivalent) will be fitted to the HV switchboards to isolate arcing faults. **- PROTECTION**

Each of the HV bus sections is to be provided with two 110Vdc and two 24Vdc battery systems. Each group of battery systems (1 x 24Vdc & 1 x 110Vdc) will supply control power to one generator (including governor, AVR and circuit breaker), one thruster and their associated protection systems. Provision for manual cross connection to another generator and thruster in the same redundant machinery group will be provided for maintenance purposes but the normal position will be with the cross over open. An alarm will indicate if the cross over is in the wrong position. - **DETECTION**

All circuit breakers will fail 'as set' on loss and reinstatement of control power. Supplies for control and protection functions will be independent of each other. - **INDEPENDENCE**

LV switchboards will derive their control power from their own bus-bars except where a dedicated external source is required to provide voltage dip ride though capability. **- INDEPENDENCE & RIDE THROUGH**

Marine Auxiliary Systems

Fuel: Part II of the WCFDI would in theory have allowed a common fuel system for two engines provided there were two quick closing valves and other active components. However, the risk of contamination was considered sufficiently high to warrant further separation. Following the advice in the MTS DP Vessel Design Philosophy Guidelines, the systems were separated at the level of the service tanks. Figure 5 below shows the three redundant systems, each supplying two generating engines. Failures before the service tanks won't impact on the running engines provided effective fuel management procedures are in place.

Advantages are:

- Failure of one fuel supply from the service tank to the engine, be it pump, filter, contamination etc. will only affect the single engine connected.
- The affected engine can be brought back on line by cross connecting within its own redundancy group and not by crossing the redundancy barriers.
- With a single engine, the vessel can still carry out DP operations pertaining to its industrial mission.

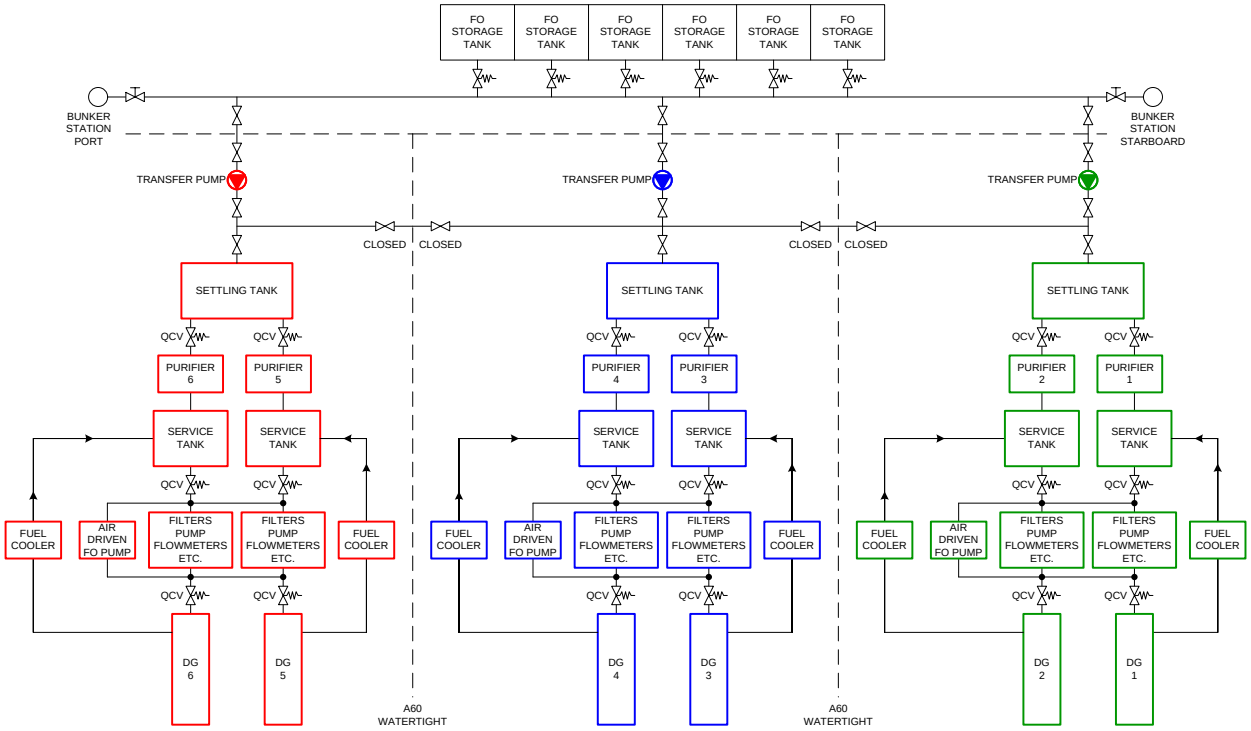

Figure 5 LIFE Fuel System

Sea Water Cooling: Figure 6 shows the design of the seawater cooling system which adheres to Part II of the WCFDI by providing redundancy in active components but accepting commonality in pipework. A single hydraulic valve is shown for each overboard to comply with part II of the WCFDI. This would need to be manually operated and protected from inadvertent operation, even if it fails as set. Following the advice in the MTS Design Guidelines, each redundant system has its own high and low sea suctions.

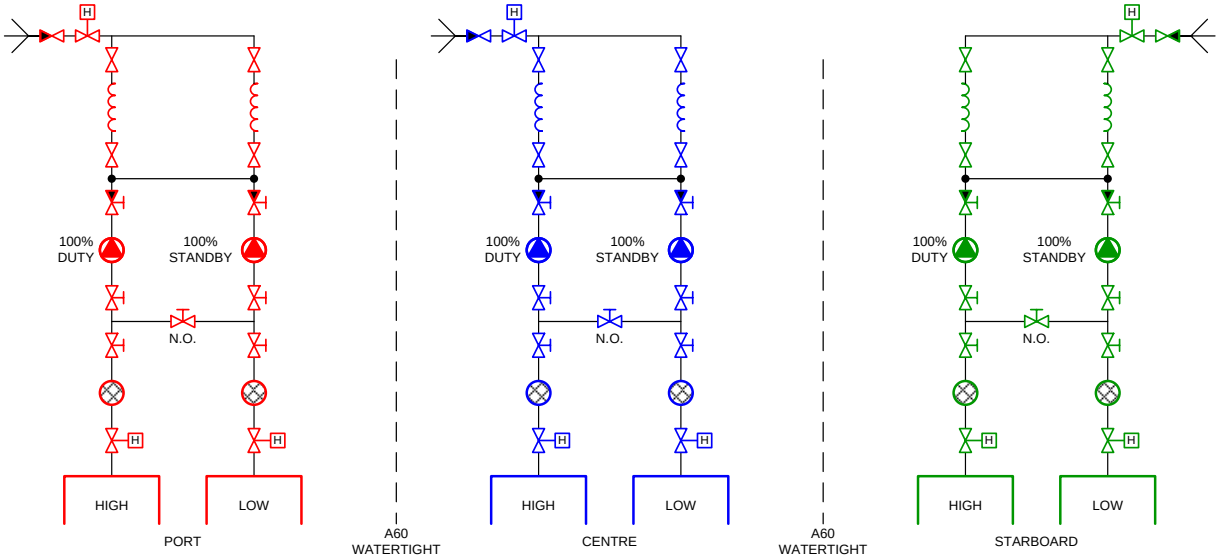

Figure 6 LIFE Sea Water Cooling for Engines and Aft Thruster System

Figure 7 below shows a separate sea water system that is designated for the use of the vessels industrial services, and has no impact on the three redundant DP equipment groups.

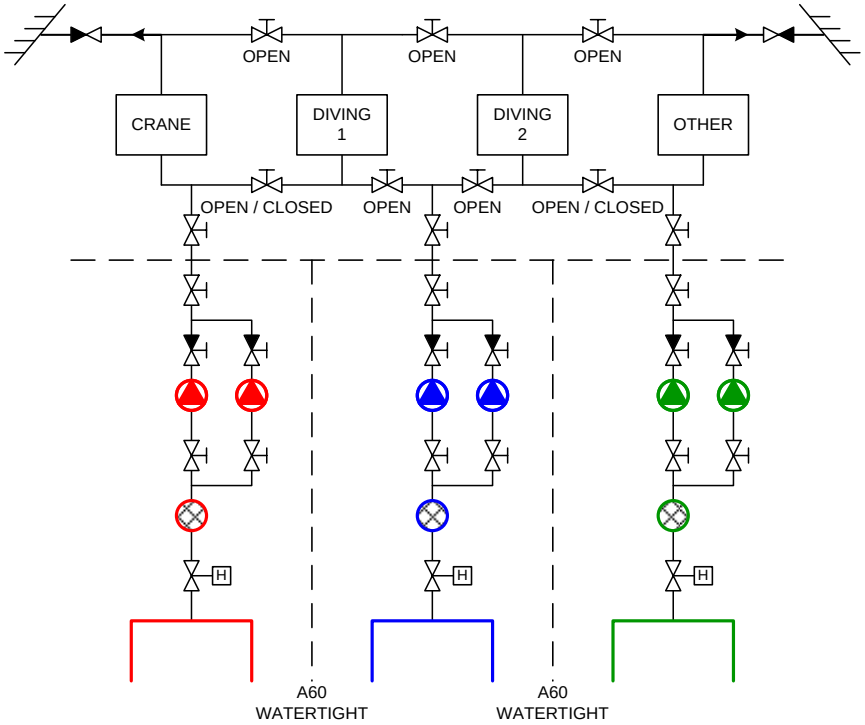

Figure 7 Industrial Equipment Independent Sea Water Cooling

Seawater cooling for industrial systems: This example demonstrates some of the difficulties that can be encountered trying to maintain good separation at the connection between a well segregated DP system, auxiliary systems and power supplies for industrial consumers which may have limited redundancy and no separation even in DP class 3 designs. In this case there was a desire to be able to supply the industrial / diving systems with SW cooling from any of the three redundant DP equipment groups. Connecting the industrial systems directly to all three redundant DP groups introduced potential common cause failures associated with damage to the pipework in the industrial systems and fire or flooding affecting the supplies to the pumps which could create voltage dips on all three isolated power systems either simultaneously or sequentially but the effect could potentially be the same – loss of all thrusters. One solution would be to have a single pump room for the industrial services out of which there would be three feeds, only one of which could be energised at any one time. However, due to the importance of the cooling water system to the industrial mission, the owner elected to provide greater redundancy. Each of the three DP pump rooms have a dedicated sea suction for the industrial consumers and a duty and a standby pump for added reliability. This maintains the A60 / watertight separation between the redundant power supplies and the independence of the seawater supply removes any threat to the DP system.

General: The sections outlined above give an example of how to apply the LIFE concept to a few of the vessel's marine auxiliary systems. This philosophy is followed through to the other systems, including but not limited to:

- Fresh water cooling
- Compressed air – start, control & service
- Engine room ventilation
- Combustion air
- Remote control valves
- Quick closing valves

Cabling and Pipework

Three independent A60 (and watertight where required by class) cable and pipe routes connect the thrusters, engine rooms and switchboard rooms in each independent power and propulsion system. Two independent routes for the automation system data highways are established.

Networks for Vessel Control

Vessel automation system networks are generally only available in a dual redundant configuration. Automation system components are small and relatively inexpensive. Repair times should be short by comparison to main machinery faults and therefore the expected level of vessel availability can be achieved by carrying sufficient on-board spare parts (and expertise to change them). The design should ensure there are adequate spare fibres within the main data backbones.

All automation system failures should leave the DP system operating in a stable pre failure condition and available for manual control.

Where possible, for environmental and reference sensors, it is advisable to employ differentiation, for example, where there are three wind sensors there should be a mixture of the ultrasonic type and the mechanical type.

LIFE and the FMEA Process

The purpose of the DP system FMEA is to confirm that the redundancy concept (or redundancy design intent) has been carried forward into the detailed design and construction phase and that no single failure effect has a severity exceeding that defined in the WCFDI.

- It is vitally important that the WCFDI and post failure DP capability are defined in the specification for the vessel. Failure to come to an agreement on these definitions may result in class minimum standard being applied in which case a two way split rather than a three way split may be approved.
- When several DP system configurations are planned, there may be different WCFDIs for each configuration and associated post failure DP capabilities.
- Where the failure criteria applied to each configuration aligns with a particular class DP notation, the vessel owner can expect that class will approve each of these configurations.
- Where the owner has elected to include alternative configurations with defined failure criteria that do not match a particular notation then class may not consider that configuration in their approval. This is not to say that such configurations cannot be used, only that they are a matter for the owner and charterer to agree.
- When it comes to the issue of non-compliances with the worst case failure design intent it can be very useful to have the support of class in confirming that the existing design does not meet their rules.
- In the case of configurations not supported by class, it is vitally important that all aspects of the alternative configurations are a matter of contractual agreement and that the shipyard arranges to include the configurations in the DP system FMEA and agrees to accept the findings therein with respect to such non-compliances, without recourse to class for arbitration.

Along with the FMEA document a ‘Concerns’ register is drawn up to alert the client of any issues arising from the analysis.

An example of the traditional concerns register definitions are as follows:

- Category A - The failure effect exceeds the worst case failure design intent or some aspect of the design is non-compliant with the Class rules for notation DP Class 3. Improvement is recommended.
- Category B - The failure effect equals the worst case failure design intent. The design complies with the class rules for notation DP Class 3 but should be reviewed to determine whether a cost effective improvement can be made.
- Category C - Observations, comments and suggestions associated with DP safety and reliability which the client may consider.

Concerns raised as part of verifying the worst case failure design intent for the LIFE concept configuration may need to be separated out from those that relate to the DP class notation. LIFE concept concerns can be identified using a colour code as follows:

RED	**A**	Contravenes the basic three-way split redundancy concept, WCFDI and/or Class DP 3 rules.
ORANGE	**A_{life}**	Contravenes single generator / single thruster failure criteria WCFDI $_{LIFE.}$
YELLOW	**B**	Complies with all WCFDI ($WCFDI_{CLASS}$ & $WCFDI_{LIFE}$) but the severity of the failure effect equals the WCFDI (CLASS & LIFE) and there may be an opportunity for cost effective improvement.
GREEN	**C**	Observations and suggestions related to DP safety and reliability.

Life = Redundancy Concept
WCFDI = Worst Case Failure Design Intent

WHY is LIFE not more widespread?

Elements of the LIFE concept will be familiar to many in the DP community and already exist, in part, in many designs, sometimes by intent, occasionally by accident.

So why isn't accepted good practice more prevalent than it is?

- It is generally accepted that cost is the main motivator when shipyards are tendering for vessels and owners are constantly seeking to minimise costs.
- Shipyards already have in house designs (templates) and are eager to quote low figures in order to secure several commissions.
- By enlightening vessel owners to think past the short term and consider the vessel's working life and the intended Industrial Mission, a more versatile & robust vessel can be achieved from the outset. But, it may be necessary to invest significant personal capital in convincing others of the validity of this case.
- If properly managed, the LIFE concept should not add significantly to a vessel's construction cost and early estimates suggest an impact of less than 10% on the cost of a MODU power plant (not the whole vessel). In general, the equipment is the same; it is only the way it is connected together that differs. Over the lifetime of the vessel, this would be negligible compared to the down time costs and penalties that could potentially be incurred due to constraints placed on the vessel from ASOGs, CAMs & TAMs and ever tightening rules and guidelines for industry best practice.

Upgrading an existing vessel to follow the LIFE concept would likely be very costly and time consuming and it would take an insightful owner to commit to this type of upgrade. However, implementing the LIFE concept at the design stage would have a cost implication, but a forward thinking owner would have a highly marketable vessel for a wide range of industrial missions once they have demonstrated the robustness of the redundancy and the reliability of each of the redundancy groups.

Conclusion

The LIFE concept is essentially the embodiment of the MTS DP Vessel Design Philosophy Guidelines tailored to take advantage of the trends in DP operations driven by the MTS DP Operations Guidance. It is not intended to be a matter of compliance but rather the application of good practice and common sense and should allow a vessel owner to identify where design improvements could be made that would bring commercial benefits in the vessel's operational life cycle.

In general, the major benefits are:

- Reduces the probability of experiencing the worst case failure.
- Reduces the risk of cascade failure when crane/drilling and thruster load is reallocated. This could be an issue with modern engines which have poor load acceptance characteristics.
- Provides a safety margin that reduces the risk that a hidden 'loss of capacity' in engines or thrusters (not capable of rated output power or thrust output) will lead to a loss of position.
- Provides additional resources for the industrial consumers such as crane etc. after a failure even if full thrust load is being consumed.
- The efficiency of power to thrust conversion increases with the number of thrusters online (particularly for FPP thrusters). Therefore LIFE concept designs make even more thrust available after a failure.
- Because the system has been designed to satisfy the single generator and / or single thruster failure criteria (LIFE concept) most of the more likely faults that occur will not completely disable the entire power train and therefore the surviving machinery should be able to contribute to the new post failure DP capability after the first fault. Thus, in the case of the example used above, the vessel's post failure DP capability becomes three generators and four thrusters instead of two generators and two thrusters. That extra thrust and generating capability might be the difference between being able to finish the work 'on hire' or not.

References

- MTS DP Vessel Design Philosophy Guidelines.
- MTS DP Operations Guidelines.
- DNV-RP-E307 Dynamic Positioning Vessel Design Philosophy Guidelines Sept. 2012.
- DNV-RP-D102 FMEA of Redundant Systems.
- GL Noble Denton internal DP FMEA guidance and documentation.