Marine Technology Society

DP Vessel Design Philosophy Guidelines

PART 1

TABLE OF CONTENTS

TABLES

REFERENCES

BIBLIOGRAPHY

ABBREVIATIONS

ABS	AMERICAN BUREAU OF SHIPPING
AC	ALTERNATING CURRENT
AFC	APPROVED FOR CONSTRUCTION
AGP	ADVANCED GENERATOR PROTECTION
AI	ASSET INTEGRITY
AODC	ASSOCIATION OF OFFSHORE DIVING CONTRACTORS
API	AMERICAN PETROLEUM INSTITUTE
ASOG	ACTIVITY SPECIFIC OPERATIONAL GUIDELINES
AVR	AUTOMATIC VOLTAGE REGULATOR
BOP	BLOW OUT PREVENTER
BV	BUREAU VERITAS
CFD	COMPUTATIONAL FLUID DYNAMICS
CMF	COMMON MODE FAILURE
CP	CONTROLLABLE PITCH
CPP	CONTROLLABLE PITCH PROPELLER
DGNSS	DIFFERENTIAL GLOBAL NAVIGATION SATELLITE SYSTEM
DGPS	DIFFERENTIAL GLOBAL POSITIONING SYSTEM
DNV	DET NORSKE VERITAS
DP	DYNAMIC POSITIONING
DPCS	DYNAMIC POSITIONING & CONTROL SYSTEMS
DPO	DYNAMIC POSITIONING OPERATOR
DPS	DYNAMIC POSITIONING SYSTEM
DPVOA	DYNAMICALLY POSITIONED VESSEL OWNERS ASSOCIATION
DSV	DIVING SUPPORT VESSEL
EARTH	GROUND
ECR	ENGINE CONTROL ROOM
ER	ENHANCED RELIABILITY
ESD	EMERGENCY SHUTDOWN SYSTEM
F & G	FIRE & GAS
FAT	FACTORY ACCEPTANCE TEST
FMEA	FAILURE MODES AND EFFECTS ANALYSIS
FMECA	FAILURE MODE EFFECT AND CRITICALITY ANALYSES
FOG	FIBRE OPTIC GYROS
FPP	FIXED PITCH PROPELLER
FPSO	FLOATING PRODUCTION STORAGE OFFTAKE
FSVAD	FLAG STATE VERIFICATION & ACCEPTANCE DOCUMENT
FW	FRESH WATER
GA	GENERAL ALARM
GNSS	GLOBAL NAVIGATION SATELLITE SYSTEM
GPS	GLOBAL POSITIONING SYSTEM
GROUND	EARTH
HAT	HARBOUR ACCEPTANCE TEST
HAZOP	HAZARD AND OPERABILITY
HDOP	HORIZONTAL DILUTION OF POSITION
HIL	HARDWARE IN LOOP
HMI	HUMAN MACHINE INTERFACE

HSE	HEALTH, SAFETY AND ENVIRONMENT
HSI	HUMAN SYSTEM INTEGRATION
HV	HIGH VOLTAGE, GENERALLY VOLTAGES OVER 1000 VOLTS
HVAC	HEATING VENTILATION AIR CONDITIONING
I/O	INPUT/OUTPUT
IAN	INERTIAL AIDED NAVIGATION
IEC	INTERNATIONAL ELECTROTECHNICAL COMMISSION
IJS	INDEPENDENT JOYSTICK
IMCA	INTERNATIONAL MARINE CONTRACTORS ASSOCIATION
IMO	INTERNATIONAL MARITIME ORGANISATION
IRM	INSPECTION REPAIR AND MAINTAINABILITY
LBL	LONG BASELINE
LCI	LOAD COMMUTATED INVERTER
LLRC	LOW LOSS REDUNDANCY CONCEPT
LRS	LLOYDS REGISTER OF SHIPPING
LUSBL	LONG ULTRASHORT BASELINE
LV	LOW VOLTAGE, GENERALLY VOLTAGES BELOW 1000 VOLTS
MOC	MANAGEMENT OF CHANGE
MODU	MOBILE OFFSHORE DRILLING UNIT
MOU	MOBILE OFFSHORE UNIT
MRU	MOTION REFERENCE UNIT
MSC	MARITIME SAFETY COMMITTEE
MTBF	MEAN TIME BETWEEN FAILURE
MTS	MARINE TECHNOLOGY SOCIETY
MTTR	MEAN TIME TO REPAIR
NMD	NORWEGIAN MARITIME DIRECTORATE
OIM	OFFSHORE INSTALLATION MANAGER
OSV	OFFSHORE SUPPORT VESSEL
PA	PUBLIC ADDRESS
PLC	PROGRAMMABLE LOGIC CONTROLLER
PMS	PLANNED MAINTENANCE SYSTEM
PRS	POSITION REFERENCE SYSTEM
PSU	POWER SUPPLY UNIT
PWM	PULSE WIDTH MODULATION
QCV	QUICK CLOSING VALVE
RAO	RESPONSE AMPLITUDE OPERATOR
RCA	REDUNDANCY AND CRITICALITY ANALYSES
RCU	REMOTE CONTROL UNIT
RESTRICTED EARTH FAULT PROTECTION	DIRECTIONAL EARTH FAULT PROTECTION
RIO	REMOTE INPUT OUTPUT
ROV	REMOTELY OPERATED VEHICLE
RPM	REVOLUTIONS PER MINUTE
SAT	SEA ACCEPTANCE TEST
SCE	SAFETY CRITICAL ELEMENTS
SIL	SAFETY INTEGRITY LEVELS
SIMOPS	SIMULTANEOUS OPERATIONS
SMO	SAFEST MODE OF OPERATION
SOLAS	SAFETY OF LIFE AT SEA

STCW	STANDARDS OF TRAINING CERTIFICATION AND WATCH KEEPING
SW	SEAWATER
TAGOS	THRUSTER AND GENERATOR OPERATING STRATEGY
TAM	TASK APPROPRIATE MODE
TCPC	TRAINING, CERTIFICATION & PERSONNEL COMPETENCE
THD	TOTAL HARMONIC DISTORTION
TTT	TIME TO TERMINATE
UKCS	UK CONTINENTAL SHELF
UPS	UNINTERRUPTED POWER SUPPLY
USBL	ULTRA SHORT BASE LINE
VAr	VOLT AMPERE REACTIVE
VCB	VACUUM CIRCUIT BREAKER
VFD	VARIABLE FREQUENCY DRIVES
VRU	VERTICAL REFERENCE UNIT
VRU	VERTICAL REFERENCE UNIT
WCF	WORST CASE FAILURE
WCFDI	WORST CASE FAILURE DESIGN INTENT
WSOG	WELL SPECIFIC OPERATIONAL GUIDELINES

1 INTRODUCTION

1.1 PURPOSE

1.1.1 This document has been generated by the MTS DP Technical Committee and has been provided to industry as a guidance document to aid in the design of DP Vessels.

1.1.2 This document is not meant to replace any rules, regulations or guidelines that are in existence. It is a compilation of experiences, practices and information gleaned from various sources in industry, some of which are not in the public domain. It is expected that compliance with applicable Class Rules will be ensured.

1.1.3 It is acknowledged that DP Class notation is governed by Class Rules which cover DP equipment and addresses redundancy requirements. However, these rules do not address the industrial mission of the vessel nor the overall performance and operational capability. Consequently vessels designed to obtain a DP Class Notation alone may not achieve the post worst case failure capability that could potentially be achieved by establishing and adopting philosophies that minimize loss of positioning capability after failure and enhance reliability.

Note:-LRS and DNV offer a means to compare DP vessel performance through the use of PCR and ERN numbers.

1.1.4 This is not intended to be an all encompassing document covering all aspects of DP vessel design. It attempts to provide guidance on a number of themes which have not been adequately defined by DP Class Rules or are subject to interpretation. Incorporating the guidance provided in this document during design should result in a vessel with enhanced capability to perform its industrial function and which meets Class Rules for the desired DP Class Notation.

1.1.5 Enhanced vessel capability as implied in this document means a more fault tolerant/fault resistant DP system which minimizes loss of positioning capability post worst case failure. This in turn translates into greater operational uptime and the ability to carry out its mission within a larger operating envelope.

1.1.6 The focus areas of this document have evolved from industry experience of technical failures. Addressing these vulnerabilities during design will result in a robust vessel capable of conducting its industrial mission. Exposure to environmental conditions is addressed by focusing on capability and sizing of thrusters and power plants. Technical failures are addressed by designing fault tolerant and fault resistant systems. Some technical faults require operator intervention to prevent escalation. Ergonomics and ‘decisions support tools’ aid effective operator intervention.

1.1.7 Implementation of the Guidance during design phase rather than later in the life cycle is expected to lower the cost of a ’fit for purpose‘ DP vessel.

1.1.8 The guidance provided in this document is not directed at any particular category of DP vessel. It is intended to apply to any Class 2 or Class 3 DP vessel operating in support of offshore oil and gas activities. The principles may be implemented as appropriate on Class 1 DP vessels. Examples include MODUs, MOUs, construction and logistics vessels where dynamic positioning is used for, or aiding, station keeping.

1.2 GENERAL GUIDANCE

1.2.1 The guidance provided in this document is intended to aid in the design of a fault tolerant, fault resistant DP vessel. It is intended to apply to any class of DP vessel operating in support of offshore oil and gas activities. The goals of the guidance are to:

1. Prevent loss of position
2. Prevent loss of redundancy

The objectives of the above are to meet class requirements and obtain operational uptime.

1.2.2 The industrial mission of DP vessels varies. Examples as follows:

1. DP MODUs
2. Project construction vessels
3. logistics vessels

1.2.3 Fault tolerant power systems can be achieved by the use of sophisticated protective functions or by configuring the power plant as two or more independent systems (open bus). Design should always facilitate effective open bus operations.

1.2.4 It is acknowledged that the level of sophistication and complexity required to achieve fault tolerance, fault resistance and uptime for DP MODUs and project construction vessels are likely to be higher than that applied to logistics vessels due to the nature of their industrial mission.

1.2.5 Diesel electric DP logistics vessels are also expected to be fault tolerant and fault resistant. Operational uptime on DP may not be the driver given the nature of their industrial mission. Acceptable levels of station keeping reliability and fault tolerance can be achieved using less sophisticated redundancy concepts.

1.2.6 It should be recognized that power plants need a larger level of integration than other components of DP systems. Care should be exercised in the concept and design phase of power systems to clearly establish the needs of the industrial mission, requirements of the Regulatory/Classification bodies and to define the system for all aspects of the project life cycle.

1.2.7 All vessels should be operated within their post failure DP capability as determined by their Worst Case Failure.

1.3 LAYOUT OF THE DOCUMENT

1.3.1 This document consists of two parts. Part 1 is a management guide explaining why each theme is important. Part 2 contains additional details on how to address these themes along with anecdotal examples.

1.3.2 The level of detail in the sections on power (generation, distribution and power management / vessel management) is deliberately and consciously greater than that provided in other sections. A well thought through power system design delivers a robust and capable vessel and enhances the ability of the vessel to perform its industrial mission. Note that the term ‘power system’ includes auxiliary systems and related pipework.

2 DEFINITIONS

2.1 GENERAL

1. **Reliability:** The probability that an item can perform a required function under given conditions for a given time interval.
2. **Redundancy:** The existence of more than one means of performing a required function.
3. **Full redundancy:** A system comprising two or more redundant elements each of which is capable of performing the function.
4. **Partial redundancy:** A system containing three of more redundant elements which are capable of performing the function in combination (e.g. any two-out-of-three).
5. **Availability**: The ratio of the total time a functional unit is capable of being used during a given interval to the length of the interval.
6. **Single fault tolerance:** The ability of a system to continue its function, following a single failure, without unacceptable interruption.
7. **Independence:** With reference to main machinery such as generators and thrusters. Auxiliary and control functions should be provided in a manner that makes the machinery as independent as practical to minimize the number of failures that can lead to the loss of more than one main item of machinery.
8. **Separation:** With reference to systems or equipment intended to provide redundancy. Reduce the number of connections between systems to reduce the risk that failure effects may propagate from one redundant system to the other.
9. **Physical separation:** With reference to DP Class 3 vessels, fire and watertight subdivisions required to support the worst case failure design intent in respect of DP 3 failure criteria.
10. **Monitoring:** Alarms and indications required to reveal hidden failures. Monitoring should be of a design and implementation that positively identifies a fault or degradation of functionality in the system e.g. lack of flow not just loss of pressure.
11. **Critical redundancy:** Equipment provided to support the worst case failure design intent.
12. **Non critical redundancy:** Equipment provided over and above that required to support the worst case failure design intent. Its purpose it to improve the reliability and availability of systems.
13. **Industrial Mission:** The industrial mission is the primary operational role of the vessel, typically applicable to MODUs and Project and Construction vessels (e.g. Pipe-lay/Heavy-lift). (Note Industrial mission by definition for Logistic Vessels is to support logistics)
14. **Diversity:** The property of introducing differences into redundant elements to avoid common mode, common cause failures. Different levels of diversity are possible such as specifying different manufacturers for redundant GNSS systems. Even greater diversity can be achieved through orthogonality which requires redundant elements to operate on different principles.

15. **Orthogonality:** With reference to redundant systems the secondary means of providing a function should be based on completely different principles to reduce the risk of common mode failures (e.g. Gyros-spinning mass versus Fiber Optic Gyros (FOG), anemometers (ultrasonic versus mechanical).

16. **Differentiation:** A method to avoid common mode failures by introducing a change in personality of redundant systems based on the same principle (e.g. use of Inertial Aided Navigation (IAN) on one of the two redundant GNSS systems)

17. **Suitability:** In this document 'suitability' pertains to the vessel having the appropriate position reference sensors to undertake its industrial mission.

18. **Position/heading keeping:** The ability of the DP system to maintain a desired position or heading within the normal excursions of the control system and environmental conditions.

19. **Loss of Position:** The vessel's position is outside the limits set for carrying out the industrial activity in progress as defined in the WSOG/ASOG.

20. **Thruster Phaseback:** A method utilized to temporarily reduce power consumption following an event, to stabilize the power plant and avoid a black-out.

21. **The Critical Activity Mode of Operation (CAMO):** This is generally a tabulated presentation of how to configure the vessel's DP system, including power generation and distribution, propulsion and position reference systems, so that the DP system, as a whole is fault tolerant and fault resistant. The CAMO table also sets out the operator actions should the required configuration fail to be met. The term Safest Mode of operation (SMO) has been previously used to describe CAMO.

22. **Systematic failure:** Failures due to flaws in the system. Systems subjected to the same conditions fail consistently.

23. **Wear out:** Specific class of failure when an item of limited life has worn out.

24. **Random failure:** Failure due to physical causes such as corrosion, thermal stressing. Statistical information can be derived from historical data.

25. **'Task Appropriate Mode' (TAM) is a risk based mode:** Task Appropriate Mode is the configuration that the vessel's DP system may be set up and operated in, accepting that a failure could result in effects exceeding the worst case failure such as blackout or loss of position. This is a choice that is consciously made. This mode may be appropriate in situations where it is determined that the risks associated with a loss of position are low and where the time to terminate is low. (Not to be confused with Thruster Assisted Mooring)

26. **'Active redundancy':** Redundancy wherein all means for performing a required function are intended to operate simultaneously.

27. **WCFDI:** The worst case failure design intent (WCFDI) describes the minimum amount of propulsion and control equipment remaining operational following the worst case failure. The worst case failure design intent is used as the basis of design. Single fault tolerance is to be achieved by the provision of redundant systems.

28. **Time to Terminate:** This time is calculated as the amount of time required in an emergency to physically free the DP vessel from its operational activity following a DP abort status and allowing it to be maneuvered clear and to proceed to safety.

3 DP VESSEL DESIGN PHILOSOPHY

3.1 RESPONSIBILITIES

3.1.1 This document is intended to be a design philosophy guide. However, it is important to note that carrying the process of the design concept to completion of a vessel involves many stakeholders. Consequently, it should be recognized that the contracting philosophy employed at each level of design and the various disciplines involved directly affect both the design and execution of the design.

3.1.2 Whether the contract is turnkey "design and build" or the owner presents a fully developed and reviewed design complete with owner furnished equipment to the shipyard, the fact remains that oversight of the process as a whole is a key factor in the success of the design.

3.1.3 Regardless of the contracting philosophy the key disciplines and stakeholders in the process remain the same. The responsibilities of each stakeholder for a given project should be clearly defined by contract, communicated to, and understood by all parties involved in the design and execution of the design. The following list attempts to provide a high level description of the scope of design responsibilities for the various stakeholders; it does not address financial responsibilities:

1. **Senior Management:** The owner's senior management is responsible for the project charter, which should clearly define the mission parameters for the design. The charter should include the basis of design. Strict guidelines should be incorporated for management of change to mitigate scope creep.
2. **Project Team:** The owners project team will vary depending on the type of contract, however there are common skill sets required on the team including project management, engineering and administration. While each contract will differ, it is important to state that it is the responsibility of the owner to adequately staff the project in order to diligently oversee the entire design process as well as the implementation of the design.
3. **Naval Architects / Designers:** Naval architects and designer are responsible for the conceptual design. The naval architect does not provide detailed engineering or systems designs. In general the naval architect provides hull form drawings, scantlings, conceptual general arrangement drawings, and reports such as weight estimates, hull friction, stability, etc. The Naval architect's drawing must be translated by others into detailed production design drawings.
4. **Flag State:** The flag state administers the rules adopted by legislation for the flag state. In general these rules are mainly Health, Safety and Environment and manning related. Flag state rules will normally enforce international conventions such as IMO, SOLAS and Marpol. While some flag states have extensive design codes in place, it is not uncommon for flag state rules to defer to one of the class society's codes for design criteria.

5. **Class Society:** Class societies establish design codes, review and certify adherence to the codes during design, review the vessel while it is being built and tested, and ultimately certify that the completed vessel complies with their rules. Class societies do not have any governmental authority other than that which may be granted by a flag state. They developed first as a method of providing insurers with technical reviews of vessels to determine whether a vessel was safe and fit for the purpose it was designed for.

6. **Shipyard:** While there are many forms of shipyard contracts and many levels of ability within shipyards throughout the world, it must be noted that the shipyard generally either does or subcontracts the detailed design. With the exception of a complete design and build contract, the shipyard works from a conceptual design by others. The shipyard must interpret the design from the naval architects, various systems designers and vendors, produce detailed designs across disciplines, then fabricate and assemble the hull and systems per the design. Ultimately, the design must be tested as a completed system per the basis of design.

7. **Integrator:** Regardless of the contracting philosophy, the equipment specified by the design must be integrated into a system. It should be noted that when the term "Dynamic Positioning System" is used it refers to the fully integrated vessel systems. There are numerous disciplines, vendors, flag state requirements, class society requirements and design basis requirements that must be integrated into a fully functional, 'fit for purpose' system. The integration process must be closely monitored from the basis of design through to the delivery of the vessel. Design/system reviews at identified points with participation by relevant stake holders could facilitate the integration process.

3.2 RELIABILITY OF STATION KEEPING

3.2.1 Reliability and redundancy should not be considered as synonymous. DP class rules have redundancy requirements stipulated to achieve fault tolerant systems and meet the objective of not having a single failure leading to a loss of position. They often do not address the ability of the vessel to continue its industrial mission.

3.2.2 For the purposes of this document the properties of redundancy and single fault tolerance are considered to be synonymous. It is acknowledged that this interpretation is not universal.

1. Often, redundancy is interpreted as having two items of equipment required to perform a function with no consideration given to ensuring that the redundant unit can take over from the failed unit without unacceptable interruption of the function.

2. Similarly, there may be no consideration of how to prevent a fault in one redundant element affecting the operation of others.

3. The above factors should be taken into consideration during design and avoided by incorporation into specifications.

4. The terms 'redundancy' and 'single fault tolerance' are used interchangeably throughout this document.

3.2.3 DP vessels should have a sufficient level of station keeping reliability. Reliability is a product of the quality of the equipment and suppliers selected, the competence of the engineers who design and build the DP vessel and the competence of the crew and management who maintain and operate it.

3.2.4 Redundancy does not in itself guarantee a sufficient level of reliability leading to overall availability. It can contribute to availability if the redundant elements themselves are sufficiently reliable. DP rules and guidelines do not specify a level of reliability. When mentioned it is in the context of the consequences of loss of position.

3.2.5 The vessel's availability to work can be related to the probability of losing fault tolerance. The vessel's industrial mission should determine what overall level of reliability should be attained to achieve the required vessel availability. Higher vessel availability can be achieved by the application of non critical redundancy and attention to reliability. A robust design can provide high reliability and availability and this should be the primary objective of any design process. . Vessel build specifications that make reference to Class rules alone without explicitly addressing Industrial mission requirements and robust design may not achieve the above goal.

3.2.6 This goal may not be achieved if the only objective is compliance with class rules.

3.2.7 Requirements for single fault tolerance must be satisfied in any design to comply with the rules.

3.2.8 This guidance document only deals with design.

The guidance provided in this document is intended to assist with delivering a robust design capable of:

1. Preventing loss of position
2. Preventing loss of redundancy

This is expected to result in a vessel that meets class requirements and delivers the desired availability to carry out its industrial mission.

3.3 DP EQUIPMENT CLASS

3.3.1 IMO Marine Safety Committee Circular 645 (MSC 645),'Guidelines for Vessel's with Dynamic Positioning Systems', 1994 is intended to provide an international standard for dynamic positioning systems. This document defines three DP equipment classes which are intended to provide different levels of station keeping reliability which can be matched to the consequences of loss of position. The three equipment classes are defined by the effect of failure and the nature of the failures which must be considered.

3.3.2 IMO MSC 645 does not address the industrial mission of the vessel.

3.3.3 The equipment class of the vessel required for a particular operation should be agreed between the owner(s) of the vessel and their respective customer based on a risk analysis of a loss of position. Some Coastal States imposes minimum DP Equipment Class requirements for activities carried out within their domain.

3.4 DP EQUIPMENT CLASS 1

3.4.1 Loss of position may occur in the event of a single failure.

3.5 DP EQUIPMENT CLASS 2

3.5.1 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:

1. Any active component or system (generators, thrusters, switchboards remote controlled valves, etc).
2. Any normally static component (cables, pipes, manual valves, etc) which is not properly documented with respect to protection.

3.6 DP EQUIPMENT CLASS 3

3.6.1 A single failure includes:

1. Items listed for class 2, and any normally static component are assumed to fail.
2. All components in any watertight compartment, from fire or flooding.
3. All components in any one fire subdivision from fire or flooding.

3.7 CLASSIFICATION SOCIETY DP NOTATION

3.7.1 Each of the main classification societies produces its own DP rules which align to different degrees with the requirements of IMO MSC 645.

3.7.2 Classification society rules are generally updated twice a year and are not applied retrospectively.

Table 3-1 Class Equivalent Notation

IMO	Class 1	Class 2	Class 3
DNV	DYNPOS-AUT DPS 1	DYNPOS-AUTR DPS 2	DYNPOS-AUTRO DPS 3
ABS	DPS-1	DPS-2	DPS-3
LRS	A	AA	AAA
GL	DP1	DP2	DP3

3.7.3 This document only considers requirements for Equipment Class 2 and Equipment Class 3. Several classification societies offer other notations. Examples of these additional notations are DNV's DYNPOS ER (Enhanced Reliability) and Germanischer Lloyd's DP3 (DP2)

3.7.4 DYNPOS ER allows greater freedom in the use of features and functions intended to improve post failure station keeping capability. For DYNPOS AUTR and DPS 3, it is accepted that a vessel with DYNPOS-AUTRO or DPS 3 notation can have alternative configurations complying with the requirements of DYNPOS AUTR or DPS 2. No additional notation is given but compliance is visible through the approved FMEA.

3.7.5 Germanischer Lloyd's DP3 (DP2) allows a DP vessel to have a dual DP notation with different worst case failure design intents and post failure DP capabilities created by applying the failure criteria for both DP2 and DP3.

3.8 FUNCTIONAL REQUIREMENTS

3.8.1 In order to meet the single failure criteria it will normally be necessary to provide:

1. For equipment class 2 - redundancy of all active components.
2. For equipment class 3 - redundancy of all components and physical separation of the components.

3.9 TIME TO TERMINATE

3.9.1 DP rules and guidelines require only that DP vessels be able to maintain station following a single failure for long enough to safely terminate the work in progress.

3.9.2 Different industrial activities have different termination times and this may influence the design of the DP system and choice of operating configuration. For example, in certain drilling activities the drilling rig can disconnect fairly rapidly and move off station in a controlled manner. In other activities a much longer time to terminate is required. Diving support, Pipelay, umbilical-lay and heavy lift activities may have longer time restrictions in some cases.

3.9.3 Industrial missions that inherently require longer duration time to terminate should consider designs that limit loss of thrust, post failure. Fuel service tank capacity thermal capacity of cooling systems or provision of HVAC are factors that could influence achieving the desired duration necessary for time to terminate.

3.10 MITIGATION OF FAILURES

3.10.1 DP rules and guidelines generally require that equipment intended to provide redundancy is available immediately and with a minimum of operator intervention. Classification societies interpret this differently and some DP notations require that the vessel must be able to hold position with the main machinery that remains operational following the worst case failure. Others accept that standby machinery may be brought online automatically. The requirement for all redundant machinery to be 'active redundancy' was sometimes relaxed in the case of seawater cooling systems. This was reasonable if the time taken for temperatures to reach critical levels was long. As interpretation of rule requirements changes over time it is important to clarify such issues at the redundancy concept development stage to avoid delay and rework at a later date.

3.10.2 Operator intervention can be considered as part of the failure mitigation process. In a limited number of cases, operator intervention may be accepted provided there is sufficient time for the operator to act before the failure effects escalate to unacceptable levels and there are clear alarms and indication to identify the fault. 'Drive off' is an example of a failure effect where operator intervention is likely to be required. Unambiguous instruction and procedures should be developed for all cases where operator intervention is part of the failure mitigation. Training and drills should also form part of the confidence building measures designed to ensure the failure can be safely mitigated by operator intervention.

3.11 REDUNDANCY CONCEPT AND WORST CASE FAILURE DESIGN INTENT

3.11.1 The worst case failure design intent describes the minimum amount of propulsion and control equipment remaining operational following the worst case failure. The worst case failure design intent is used as the basis of design. Single fault tolerance is to be achieved by the provision of redundant systems. Adequate holding capability is to be achieved by provision of adequate remaining power and thrust.

3.11.2 The redundancy concept is the means by which the worst case failure design intent is achieved and should be documented as part of the preliminary design process. This is highlighted and emphasized as it determines the ability of the vessel to undertake critical activities associated with its Industrial Mission in the desired range of environmental parameters.

3.11.3 The redundancy concept and post failure DP capability should take into account the long term loss of a major item of machinery such as a generator or thruster. This is not a requirement but will aid in system availability and operational uptime for a wider range of environmental conditions. It adds flexibility in maintenance and improved efficiency. It should also be possible to account for long term unavailability in the consequence analysis.

3.11.4 Design should precede ordering of capital equipment. Long lead times for equipments such as engines or thrusters may preclude this. Features and design attributes of such pre-purchased items may influence design development and needs to be accounted for in the development of the redundancy concept.

3.12 AVAILABILITY AND POST FAILURE DP CAPABILITY

3.12.1 System availability and post failure capability strongly influences the ability of the vessel to undertake its industrial mission in a range of environmental conditions. This influences operational uptime.

3.12.2 The Worst Case Failure Design Intent (WCFDI) is the basis of DP vessel design. The Worst Case Failure is the failure that has the greatest effect on station keeping capability. A successful DP vessel design is one where the WCF achieved is less than or equal to the WCFDI. The WCF is used in the DP control system online consequence analyzer.

3.12.3 The philosophy espoused within this document strives to limit loss of thrust capacity post worst case failure. In the discussion that follows, redundancy depends on systems being available in both number and capacity to produce the required post worst case failure DP capability.

3.12.4 The redundancy concept can have a very significant impact on DP vessel design and there are several variations on how to provide a fault tolerant system. In general terms the redundancy concept is based on power and propulsion systems that are independent in respect of single point failures. That is to say no defined single point failure in one independent system will disrupt the operation of the other. Independent systems can be designed to provide full or partial redundancy.

3.12.5 An independent system is said to provide full redundancy if it can develop the necessary surge, sway and yaw forces required to maintain position and heading in the defined post worst case failure environmental conditions.

3.12.6 An independent system is said to provide partial redundancy if it can only provide the necessary surge, sway and yaw forces in combination with another independent system. For example, all independent systems may be able to provide equal surge, sway and yaw forces but more than one independent system is required to produce the level of thrust required by the defined post worst case failure DP capability. The redundancy concept must ensure that suitable combinations of systems are available following any defined failure. Alternatively one independent system may develop alongships thrust and the other athwartships thrust, thus redundancy is required in each axis.

3.12.7 The simplest diesel electric redundancy concepts have two fully redundant power and propulsion systems each capable of maintaining position and heading if the other fails. More complex designs make use of multiple systems each providing partial redundancy such that the vessel can maintain position with all combinations of independent systems that survive any defined failure. For example, a vessel with three systems can hold position with any two of the three systems available.

3.12.8 An advantage of redundancy concepts based on multiple independent systems, each providing partial redundancy, is that provided each system can develop surge, sway and yaw forces and has all necessary services required to support DP it is possible to consider these systems as providing full redundancy in reduced environmental conditions. Thus a DP system with three independent power and propulsion systems can still be considered fault tolerant if only two of the three systems are available and may be able to continue DP operations in this degraded condition if environmental conditions allow. However, it is important to establish this as a design objective as it is possible to create redundancy concepts based on partially redundant system which do not remain fully redundant with reduced capacity when one system has failed.

3.12.9 The use of multiple independent systems offers other advantages. A vessel with four independent systems can in theory remain fault tolerant up to 75% power compared to one with only two systems which can only operate up to 50% power. Thus the design based on multiple independent systems can have smaller machinery for the same post failure DP capability or use the same machinery and have a greater DP capability.

3.12.10 The redundancy concept has a strong influence on machinery sizing. Design should ensure adequate margins to accommodate increased demand for power and thrust associated with development of the detailed design.

3.12.11 A basic redundancy concept and WCFDI should be developed as a precursor to design and before orders are placed for long lead items (e.g. engines and thrusters to ensure the correct ratings are ordered). Designers and naval architects will have established the amount of thrust required. The equipment required to provide the stipulated uptime in the expected range of operating conditions will determine the required post worst case failure DP capability. The redundancy concept will determine how that post failure DP capability is provided by establishing the number of generators and thrusters available after worst case failure. This is likely to be an iterative process influenced to some extent by the equipment that can be purchased in the expected development and construction timescale. See also Section 3.11.4.

3.13 EXTERNAL FACTORS

3.13.1 When considering the type of failures that can occur it is normal to consider the vessel and its DP related equipment. Influences external to the vessel can also initiate failures in the vessel's power plant and control systems. Typical external influences that must be considered include:

1. Uncommon environmental effects:
    a. Sudden squalls.
    b. Winter storms.
    c. Hurricanes
    d. Typhoons.
    e. Micro-bursts.
    f. Waterspouts.
    g. Solitons.
2. Seawater - fouling - aeration – contamination.
3. Combustion air – contamination.
4. Ventilation – contamination.
5. Fuel - contamination - microbial – water.
6. Position reference signal path (Sea and Sky).
7. Lightning.

3.14 KEY ELEMENTS OF DP SYSTEM PERFORMANCE

3.14.1 There are two key elements in DP performance:

1. Holding capability.
2. Reliability.

3.14.2 **Station keeping capability:** Is the ability of the vessel to maintain position and heading in defined environmental conditions.

3.14.3 **Component reliability:** As used in this document is the choice of individual elements of equipment or software for prolonging Mean Time Between Failure (MTBF).

3.14.4 Redundancy is provided to give the required level of reliability and comply with classification society requirements for fault tolerance. Holding capability gives the expected uptime in the intended area of operation. Redundancy applied to ensure there is no loss of position following a single fault is defined as critical redundancy. Additional equipment intended to ensure the vessel remains fault tolerant following a single failure is defined as non critical redundancy.

3.15 KEY ELEMENTS OF REDUNDANT SYSTEMS

3.15.1 There are three key elements in any redundancy concept:

1. Performance.

2. Protection.
3. Detection.

3.15.2 **Performance:** Holding capacity is fundamental to the design process. Appropriate engineering studies establish the amount of installed thrust and power generation for the environmental ranges the vessel is designed to operate in.

3.15.3 When establishing thrust requirements for ship shaped hulls, designs should not be overly reliant on keeping the bow into the weather as the design basis. This has proven inadequate in many cases, as heading often cannot be changed fast enough to follow changes in wind direction. The design should account for operations that might require a non-optimal heading including a beam environment. Experience has shown that DP MODUs, designed to cope with 70 knots of wind on the beam (zero waves or current) in an intact condition, have proved to have adequate capability to undertake operations in most environments. This is a good rough check.

3.15.4 At system and component level all equipment must be capable of its rated performance to ensure fault tolerance.

3.15.5 **Protection:** Fault tolerant systems based on redundancy require protective functions to prevent faults in one redundant system being coupled to others by way of common connections or equipment. The design should ensure all necessary protective functions are provided. Operator intervention should not be considered a protective function.

3.15.6 Protective functions exist in many different systems including DP control, automation and power generation. The drivers for applying protection may be compliance with Class Rules, safety, equipment protection or in support of the redundancy concept. Addition of a protective function should not conflict with DP redundancy. Where conflicts exist, a solution should be developed to satisfy all requirements.

3.15.7 **Detection:** Equipment intended to provide redundancy must be available in both number and capacity. The design must include means to detect reduction in capability or unavailability. Redundant components should be immediately available and with such capacity that DP operations can be continued for long enough to safely terminate the work in progress.

3.16 COMMUNICATING AND SUPPORTING THE REDUNDANCY CONCEPT

3.16.1 Once the preliminary redundancy concept has been developed it is important that it be communicated to all stakeholders and understood. As a minimum the stakeholders should include:

1. Shipyard.
2. Classification societies.
3. DP control system provider.
4. Automation system provider.
5. Power system provider.
6. Propulsion system provider.
7. Integrators if applicable.

8. FMEA contractor.
9. Vessel owner's site team.
10. Crew.
11. Charterer if applicable.

3.16.2 Interface issues between various vendors should be carefully managed. Responsibility for this may lie with the shipyard or owner's team depending on the nature of the contract. Responsibility should be clearly defined, identified and made visible.

3.16.3 It is important to concurrently develop vessel specific Inspection, Repair and Maintenance (IRM) procedures, operating procedures, guidelines and reference materials such as DP Operations Manuals to develop and support the redundancy concept. Supporting documentation may include Activity / Well Specific Operating Guidelines (A/WSOG) and Thruster and Generator Operating Strategy (TAGOS).

3.17 CONNECTIONS BETWEEN REDUNDANT SYSTEMS

3.17.1 Experience suggests that common connections between systems intended to provide redundancy create the paths by which a fault in one redundant system may affect another independent system. Some connection points are unavoidable such as remote control systems, and may be beneficial to the design. Where common points exist between redundant systems, risk assessments on impacts of failure propagation should be carried out, documented in the FMEA and adequately mitigated.

3.18 MULTIPLE POWER PLANT CONFIGURATIONS

3.18.1 Diesel electric plant design should incorporate configuration flexibility to cope with equipment unavailability (e.g. failures or equipment taken down for maintenance). However, it is important that the effect of such reconfigurations are understood as some may not be redundant. Major configurations should be identified and analyzed in the vessel's DP system FMEA to prove the DP system remains redundant. Fault tolerance of configurations should be made visible and understood by the crew. Where there is configuration flexibility in the design, the Critical Activity Mode of Operation (CAMO) should be clearly defined in addition to other Task Appropriate Modes (TAM) for use on DP with any additional risks made visible. For example, some task appropriate modes may rely more heavily on protective functions than others.

3.18.2 It may not be practical to consider every possible variation particularly in vessels that have complex power distributions systems and some classification societies state that the vessel is only considered to comply with their requirements for the DP notation when operated in one of the configurations analyzed in the approved FMEA. Vessels with complex power distribution systems should consider the most likely configurations that the vessel will be operated in and have them analyzed in the FMEA. If there is a need to operate in a configuration that is not addressed in the FMEA, it may be necessary to supplement the FMEA with additional analysis and tests to confirm the level of redundancy provided by the intended configuration. This will be required if verification of class compliance is required.

3.19 CRITICAL AND NON CRITICAL REDUNDANCY

3.19.1 Class rules require DP systems to be redundant with the primary objective of achieving no loss of position. However, redundancy in itself does not guarantee a particular level of reliability. Loss of fault tolerance could cause operational issues impacting the industrial mission of the vessel. Where aspects of the design are identified as being of lower reliability or there is a need to ensure higher availability it may be beneficial to provide redundancy over and above that required to meet class requirements.

1. Critical redundancy is defined as equipment required to ensure the vessel is single fault tolerant. To remove such equipment would either remove the DP system's fault tolerance entirely or reduce its post failure DP capability.
2. Non critical redundancy is equipment intended to provide greater availability.

3.19.2 If redundant elements are highly reliable, there is no need for non critical redundancy but it can be usefully applied to allow maintenance or in cases where it is uneconomical or impractical to increase the reliability further.

3.20 AUTONOMY AND DECENTRALIZATION

3.20.1 Modern DP vessels are complex machines with several layers of automation. Experience suggests that there are benefits to be derived from making generators and thrusters independent in the provision of auxiliary support services and control functions. Designs should be resistant to internal and external common cause and common mode failures. Designs in which the control function has been decentralized are considered to be more fault tolerant. In such designs, each major item of machinery is responsible for making itself ready for operation and ensuring that all necessary services are online. In general, control system failure effects are less likely to exceed loss of the associated engine or thruster. It can be more difficult to prove that the effects of failures in centralized systems do not exceed the worst case failure design intent. This is an important consideration when choosing a control system topology for fault tolerant systems. There is still a requirement for a remote control system in decentralized designs but the functions of this control layer are limited to scheduling and remote manual control.

3.21 ORTHOGONALITY, DIVERSITY AND DIFFERENTIATION

3.21.1 Diversity is a desirable property in the design of fault tolerant systems based on redundancy. Different degrees of diversity are possible such as choosing equipment from different suppliers or using different principles of operation (orthogonal design).

3.21.2 In the field of reliability engineering the term orthogonal design indicates that a completely different method has been used to provide redundancy from that used as the primary method. Orthogonality by design reduces the risk of common mode failures in redundant systems compared to systems using identical redundant elements.

3.21.3 DP class rules require orthogonality in measurement methods used for position references. A minimum of three position references are required for DP class 2 and DP class 3. Two of these three should be based on different measurement principles.

3.21.4 It is good practice to have orthogonality in sensors such as gyros, anemometers and MRUs. Different measurement principles (orthogonality) offers the greatest advantages but where this is not practical a diversity of manufacturers is desirable.

3.21.5 Differentiation can reduce the risk of common mode failures. Differentiation can be achieved on redundant position reference systems operating on the same principle by combining one of the position references with position information from an inertial navigation systems to create Inertial Aided Navigation (IAN) (e.g. dual DGNSS or dual acoustics). IAN changes the characteristics of how the reference behaves and minimizes the probability of both (IAN and non IAN) systems being rejected.

3.22 COST EFFECTIVE RISK REDUCTION

3.22.1 When the redundancy concept is developed there will be a number of failures that have a severity equal to the worst case failure design intent (WCFDI). Design should focus on minimizing the number of failures equal to the WCFDI. These failures should be reviewed to determine whether a cost effective improvement can be made. When considering cost benefit analysis it is the lifecycle cost that should be considered including the penalties for non availability. For example, the worst case failure design intent for a particular vessel accepts that three out of six generators may be lost as the result of a single failure. The design is such that this failure effect may occur because of a main switchboard bus bar failure or because a 24Vdc power supply fails. Given the relative probabilities of failure it may be cost effective to provide a second 24Vdc power supply or possibly one for each generator. This would reduce the severity of the failure effect associated with the 24Vdc supply system.

3.23 ENHANCING CLASS MINIMUM STANDARD

3.23.1 Classification society rules are generally intended to provide a minimum technical standard. The Industrial mission and desire to achieve greater availability may influence vessel owners to exceed the minimum requirements and improve reliability, operability and maintainability. Vessel owners should be aware that any such improvements to the DP system need to be expressly agreed in the shipyard contract for the vessel. The default position for shipyards is to meet class requirements. Where the owner wishes to apply a different worst case failure design intent to some aspect of the redundancy concept over and above that required by class this needs to be agreed to and reflected in the contract. If the shipyard contract only requires the design to meet class requirements the additional features may not be provided. For example, the redundancy concept for a DP class 3 vessel may accept that that three of six generators are be lost because of an engine room fire but the owner wishes to limit the effects of technical failures to loss of a single engine or thruster. Class 2 DP rules allow all generators to be located in a single space. Many vessel owners prefer to have two or more engine rooms. Such arrangements limit the risk from crank case explosions and engine room fires and other risks such as flying debris.

3.23.2 A fully automatic blackout recovery system is not a class requirement. Main class rules and SOLAS have requirements for some degree of automatic restart of electric power systems but for a DP vessel it may be unwise to rely on this to ensure a full blackout recovery system is provided. A fully automatic black out recovery system can be supplied by all the major marine automation providers and should be specified by vessel owners. Modern blackout recovery systems can typically restore thrust in less than one minute from blackout. DYNPOS ER has higher requirements for automatic blackout recovery compared to traditional DP notations.

3.23.3 The classification society may limit its plan approval process to proving compliance with the worst case failure arising from application of the failure criteria defined in the rules appropriate to the DP notation being sought (e.g. fire or flooding). The FMEA and proving trials should cover the redundancy concept and worst case failure design intent at all levels in addition to addressing class requirements. The contract with the shipyard should expressly stipulate this. Consideration could also be given to stipulating the choice of FMEA vendor if the owner or charterer has a preference. Class will accept an FMEA commissioned or carried out by the shipyard.

3.24 INFLUENCE OF THE VESSEL'S INDUSTRIAL MISSION

3.24.1 Dynamic positioning is provided to allow the vessel to carry out its industrial function such as drilling, pipe laying, or heavy lifting. In diesel electric designs based on the power station concept, the electric power systems supply all power for propulsion, hotel, auxiliary systems and the consumers associated with the vessel's industrial mission. There may be competing requirements for power between station keeping and the industrial function. This needs to be defined and carefully managed to ensure the propulsion system has access to the power it needs to prevent loss of position in the range of environmental conditions the vessel is operating in. The requirements of the industrial consumers may dictate or favor a particular power plant configuration. Such configurations should not conflict with the redundancy concept or compromise the industrial mission.

3.24.2 Rules for DP notations are intended to ensure a satisfactory level of station keeping integrity. They do not specifically address the vessel's industrial mission so it is important when specifying the DP system to ensure that it has all the appropriate features and functions required to carry out its mission effectively. For example, number and type of position reference systems should be appropriate to the type of work to be carried out. In the case of multi purpose DP vessels, design should consider systems appropriate to all types of work that may be required of a vessel.

3.25 REGULATORY REQUIREMENTS

3.25.1 Although IMO MSC 645 is intended to provide an international standard, compliance with this standard or rules for DP notations do not guarantee compliance with other regulatory requirements imposed by flag and coastal states. For example, requirements related to environmental legislation such as emission control may be difficult to reconcile with requirements for active redundancy contained in DP rules (DYNPOS ER differs from traditional DP notations in this respect). Operating large diesel engines at low load levels is inefficient and may not achieve the gas temperature required for exhaust gas scrubbers to work efficiently. Asymmetric thruster loading of independent power systems may assist to some extent. Thruster bias can similarly be used to increase load levels which consumes more fuel. It is a challenge to reconcile a scheme that requires burning more fuel with an environmentally conscious policy.

3.25.2 A low loss worst case failure design intent allows the power plant to be much more heavily loaded than the class minimum of a two way split. This is of benefit in the efficient operation of pollution control equipment. A larger number of smaller generators can assist in addressing this issue. If the power consumers related to the vessel's industrial mission are large these can be used in such a way that the power plant is operated efficiently provided there are effective means to shed load when power is required for station keeping either as a result of deteriorating weather or partial power plant failure.

4 CAPABILITY

4.1 INITIAL DESIGN PROCESS

4.1.1 It should be recognized that Classification Rules or Regulations do not specify the station keeping capability of DP vessels.

4.1.2 The first step in the design process is to establish the desired capability and is typically stipulated by the owner. Achieving the required capability is an iterative process during design and should be carried out to establish amount of thrust and power to be installed. The following should be taken into consideration:

1. Industrial Mission of the vessel.
2. Objectives to be achieved (Operational uptime, limiting loss of post failure thrust capability).
3. Environmental parameters under which the Industrial mission is to be undertaken.
4. Transit capability desired.
5. Limitations imposed by:
    - Hull form (impacts on wind and current drag coefficients, thruster to thruster and thruster to hull interaction).
    - Environment (current inflow and impact on thrust).

4.1.3 A robust iterative process as described above should result in well designed vessel with matched power plant (station keeping and industrial mission requirements being met) capable of accomplishing its industrial mission.

4.1.4 The Holding Capability of a vessel is depicted in capability plots. IMCA M 140 addresses specification for capability plots.

4.1.5 Online capability plots are capable of being provided by DP equipment manufacturers. This is a desirable feature and should be specified.

5 MODELING

5.1 SCOPE OF MODELING

5.1.1 Modeling as referenced in this section addresses pertinent topics related to design in the following areas:

1. Naval Architecture.
2. Power and Safety Systems.
3. Operability Parameters.

5.2 NAVAL ARCHITECTURE

5.2.1 Modeling in Naval Architecture can be accomplished in the following three ways:

1. Modeling by example (prior example - build like before).
2. Analytical modeling.
3. Hull form modeling.

5.3 MODELING BY EXAMPLE

5.3.1 Prior example is the simplest modeling technique. In this method an existing design with validated performance characteristics is used. Prior example could be effective when replication allows cost and schedule benefits without compromising the performance of the industrial mission.

5.3.2 Designing by prior example may preclude opportunities for improvement. When opportunities for improvement are pursued as an objective, it should be accompanied by a robust MOC process. It is important to consider the impact in differences between applications and avoid replicating any inherent weaknesses in the design.

5.4 ANALYTICAL MODELING

5.4.1 Use of analytical modeling, early in design, facilitates delivery of a robust vessel. Advances in computing technology have resulted in effective tools capable of aiding design decisions (e.g. Computational Fluid Dynamics (CFD), optimization of tilt of azimuthing thrusters).

5.4.2 Analytical modeling could be used as a technique to aid in establishing preliminary thrust requirements for further iterations in the design cycle (Station keeping capability).

5.5 HULL FORM MODELING

5.5.1 Hull form modeling for DP vessel design is suggested when:

1. Validation of Analytical Modeling data is warranted.
2. Novel hull forms or prototypes are being considered.

5.5.2 Hull form modeling is accomplished at:

1. Test Basins.
2. Wind tunnels (to establish wind and current drag coefficients).

5.5.3 Hull form modeling for non prototype/ non novel vessels, as the primary means of establishing station keeping performance, delivers limited value due to cost, scaling factors, and availability of alternate means of establishing equivalent data.

5.5.4 Information availability on station keeping performance is usually the driver to initiate hull form modeling. This information can be established by analytical modeling.

5.6 POWER AND SAFETY SYSTEMS

5.6.1 **Power systems:** Advances in computing technology have facilitated the ability to accurately model power plants:

1. Stability.
2. Harmonics.
3. Resonance.
4. Protection coordination.
5. Short circuit withstand capability.
6. Load analysis.

5.6.2 Adopting these techniques in the design phase enables delivery of a fault tolerant/fault resistant system capable of meeting station keeping requirements and the industrial mission of the vessel.

5.6.3 **Safety systems:** Advances in computing technology have facilitated the ability to use modeling as an effective technique to:

1. Analyze Major Events (e.g. gas dispersion studies).
2. Safety Integrity Levels (SIL) (Establishing and analyzing Cause and Effects Matrix for ESD systems, ability to carry out “what if analysis”).

Modeling techniques mentioned above provide design support and can be carried into operations by facilitating decision support.

5.7 OPERABILITY PARAMETERS

5.7.1 The ability of the vessel to carry out its industrial mission is dependent on the respective vessel motions in addition to its station keeping capability. The optimum heading for reducing thrust for station keeping may not be the optimum heading to be within the limits for motions to carry out the Industrial mission. Modeling to establish RAOs (Response Amplitude Operators), during the iterative design process for determining thrust requirements, aids in decisions such as evaluating the benefits of additional thrust versus potential mission uptime

6 MANAGEMENT OF CHANGE IN DESIGN (MOC)

6.1 REQUIREMENTS FOR MOC

6.1.1 A robust Management of Change Process should be established at the concept phase, implemented systematically and followed diligently throughout the Project life cycle. The MOC process should be in place prior to finalizing the redundancy concept for the vessel. Any changes to the redundancy concept should be subjected to the MOC process.

7 THRUSTERS

7.1 PRINCIPLES

7.1.1 Thrusters as referenced in this section means propulsion to achieve:

1. Transit.
2. Station keeping using dynamic positioning.

7.1.2 Designers of DP vessel propulsion systems should incorporate the following principles in design:

1. Robustness.
2. Reliability.
3. Simplicity.
4. Redundancy.
5. Efficiency.
6. Maintainability (routine and intrusive IRM).
7. World Wide Operations (temperature ranges, ice).

7.2 PROPULSION CHOICES

7.2.1 Propulsion system choices are mainly threefold:

1. Azimuthing propulsors & cycloidal.
2. Fixed direction propulsors.
3. Vessels using a combination of fixed and azimuthing propulsors.

7.2.2 When choosing propulsors during the design phase, the following should be taken into account:

1. Reliability.
2. Service intervals.
3. The industrial mission (station keeping versus transit requirements).
4. Desired hydrodynamic aspects.
5. Number of thrusters with respect to post failure thrust capability and ability to exercise control in surge, sway and yaw axis.
6. Location and geometric arrangement.
7. Installation and maintainability methodology over life cycle of vessel - Service access (keel haul, dry dock, retractable).
8. Influence of the hull form.
9. Drive system.
10. Control of thrust.
11. Regulatory requirements for dry docking of vessels with tail shafts.

12. Draught restrictions.

7.2.3 The impact on the Industrial mission and the stated objectives due to a loss/reduction of thrust following a failure event should be recognized and carried through all phases of the design cycle. Particular attention is to be bestowed on:

1. Seals.
2. Auxiliary systems (principles of independence to be followed).
3. Ease of maintenance.
4. Specification and testing of key components (e.g. gears).
5. Impacts of vibration.
6. Introduction of vulnerabilities to thrusters not in use during transit.
7. Life extension of components and thruster.

7.2.4 Incorporating non critical redundancy into identified elements of the propulsion systems could aid in mission uptime. Robust FMEA/FMECA techniques can aid in identifying such key elements.

7.2.5 There has been a noticeable reduction in failure rates of thrusters since the introduction of variable frequency drives (VFDs) with fixed pitch propellers. VFDs facilitate fast phase back capability, a key feature to prevent power plant instability.

8 MARINE SYSTEMS

8.1 DESIGN OF MARINE SYSTEMS

8.1.1 The design of Marine systems supporting DP should follow the redundancy concept and WCFDI. Design of such systems should reflect the Industrial Mission and the objectives to be achieved. The benefits of incorporating design features of independence, segregation, critical redundancy, non critical redundancy and monitoring beyond Class Requirements should be assessed. These enhanced features should result in vessel that meets the objectives of its industrial mission and achieve the desired Class Notation.

8.1.2 Marine Systems as addressed in this section include:

1. Fuel oil system.
2. Seawater cooling systems.
3. Fresh water cooling systems.
4. Compressed air.
5. Lubricating oil systems.
6. HVAC and ventilation.
7. Remote controlled valves.
8. Water tight integrity /Subdivision Integrity.
9. Pipe work.

9 POWER GENERATION

9.1 ATTRIBUTES OF A ROBUST REDUNDANCY CONCEPT

9.1.1 DP class notation dictates the redundancy requirements. A robust redundancy concept has the following attributes:

1. Fully fault tolerant in relation to the defined failure criteria.
2. Main machinery is independent to the maximum extent feasible.
3. Redundant systems are clearly defined and well separated.
4. The division of systems into redundant groups is maintained throughout the design.
5. Low loss worst case failure effect.
6. Minimum number of failures leading to the worst case failure effect.

9.1.2 A robust redundancy concept should be rigorously applied to the design of the power generation system.

9.1.3 The design of the power generation system should take into account:

1. The Industrial mission of the vessel.
2. Power required to maintain station and perform the industrial mission in the desired range of environment.
3. The need to work efficiently in all required power plant configurations.
4. Power required to maintain station in the defined environmental limits in
   a. Intact condition.
   b. And post worst case failure.
5. The need for a robust blackout recovery system as a risk reduction measure
6. Any restrictions imposed by particular choice of main machinery

9.1.4 The key power system attributes that need to be considered during the design phase are:

1. Power, voltage, current, frequency and operating power factor.
2. Short circuit withstand capability.
3. Protection philosophy.
4. Power management.
5. Phase back of large consumers.
6. Regeneration from large consumers.
7. Starting of large consumers.
8. Load acceptance and rejection.
9. Load balance.
10. Voltage transient ride through.
11. Stability.

12. Efficiency.
13. Harmonic distortion.
14. Electromagnetic compatibility.
15. Maintenance requirements.
16. Environmental and pollution requirements.

9.1.5 The design effort should incorporate the necessary analysis and studies required to deliver a robust power plant, delivering effective capacity to undertake its industrial mission in the stipulated environmental conditions.

9.1.6 It should be recognized that Class Rules addressing the above attributes are minimum requirements for vessels and do not consider the industrial mission the vessel will be undertaking. The design philosophy should integrate the requirements of the Class Rules and the Industrial mission. This will translate into a more comprehensive and sophisticated design effort resulting in a more effective vessel.

9.1.7 Power generation design should deliver:

1. Flexibility (Optimize the number of generators in favor of flexibility for example six smaller generators rather than four larger ones).
2. Maximum independence and separation.
3. High availability.
4. Fault tolerance and fault resistance.
5. Continuity of supply of power.
6. Maximize post failure capacity.
7. Optimized Black Start requirements (minimize recovery time).

10 POWER DISTRIBUTION

10.1 DISTRIBUTION PHILOSOPHY

10.1.1 The design philosophy for the power distribution should:

1. Support the worst case failure design intent.
2. Be fully fault tolerant in respect of the defined failure criteria.
3. Follow the divisions in the redundancy concept which define redundant systems.
4. Maintain independence and separation.
5. Closely associate the power source of auxiliary systems for engines and thrusters with their respective main feeders.
6. Ensure the electrical protection scheme supports the redundancy concept.
7. Provide sufficient flexibility without compromising redundancy.

10.1.2 Failure modes in the power distribution should be minimized. Some of the common areas for vulnerabilities to be avoided are:

1. Single busties circuit breakers in DP Class 2 systems. Most classification societies accept a single switchboard being divided in two using a single bustie breaker. Consideration should be given to installing two bustie breakers.

   Note GL may require two circuit breakers between any two bus sections intended to provide redundancy.
2. Dependence on emergency switchboard / generator.
3. Voltage dips associated with short circuit faults.
4. Vulnerability to earth faults in deck equipment on DP distributions.
5. Poor regulation in service transformers.
6. Poor separation of DP and non DP related power consumers.
7. Control lines for interlocks, intertrips and protective functions which cross the divisions in the redundancy concept without adequate protection or selectivity.
8. Poor design of auto changeovers, backup supplies and common connections which can transfer faults.
9. Common backup supplies which span the divisions in the redundancy concept.
10. Co-location of services (DP and/or non DP related) fed from power systems intended to be redundant creates a common point under DP Class 3 failure criteria.
11. In DP Class 3 a common point is created by cable routes supplying non DP essential services where the route includes cables from power systems intended to be redundant.
12. Providing duty standby supplies for auxiliary systems confined to one redundant machinery group from power systems intended to provide redundancy.

11 POWER & VESSEL MANAGEMENT

11.1 KEY PRINCIPLES OF POWER AND VESSEL MANAGEMENT

11.1.1 The key principles to be taken into account when designing management systems for power and vessel systems are:

1. Topology.
2. Autonomy.
3. Detection.
4. Simplification.

11.2 FAILURE EFFECTS OF POWER MANAGEMENT SYSTEMS

11.2.1 It is accepted that power management systems can fail and that single failures can lead to loss of functionality and remote control.

11.2.2 Design should ensure that the effects of failures are benign. Benign effects have been achieved by adopting a ‘fail safe’ philosophy. The ‘fail safe’ condition may be context sensitive but is typically ‘fail as set’ for PMS functions. Machinery should continue to operate without interruption.

11.2.3 Total failure of the power management system should not produce failure effects exceeding the worst case failure design intent.

11.2.4 Failure of the PMS should not inhibit local manual control.

11.2.5 Protective functions provided by the PMS should be tested periodically to prevent those becoming hidden failures which could compound another failure.

11.2.6 Some class Societies require two independent power management systems in order to ensure that the remaining system can maintain sufficient power to hold position after failure of the other power management system.

11.3 TOPOLOGY

11.3.1 The choice of topology between distributed and centralized systems should take into consideration.

1. Industrial mission of the vessel.
2. Size of the vessel (Number of I/Os).
3. Separation of control, monitoring and protection functions.
4. Separation of redundant machinery groups.
5. Independence of main machinery.
6. Failure effects.
7. Class notation being sought.

11.3.2 Failure effects of distributed control systems tend to be less severe than centralized control systems.

11.3.3 Control systems can fail in either a benign way (absence of performance) or an active way (potential cascading effect). The assumption that control systems fail in a benign way can be misleading and should be avoided. The fail safe condition for each application may be context sensitive (operation in progress) and should be clearly defined with the reasons thereof. Vulnerabilities in control systems can be minimized by addressing this in a design that facilitates simplification, detection and autonomy.

11.3.4 The temptation to use the vessel / power management system to solve unforeseen problems in the redundancy concept late in the commissioning phase should be avoided. If unavoidable, such resolutions should be treated with caution and accompanied with the appropriate MOC, and additional verification to ensure that further vulnerabilities are not added.

11.3.5 Field I/O should be assigned to field stations in line with the overall division of the DP system into redundant machinery groups. Field stations should be provided in such a way as to make main machinery such as generators and thrusters as independent as possible. Links between field station in different redundant groups should be kept to a minimum and any such links should have well defined error handling arrangements and fail to the safest state possible. The ‘safe state’ must be considered with respect to the industrial mission of the vessel.

11.3.6 In modern power management systems there is a tendency to utilize the same hardware and software for control, monitoring and for protection functions for reasons of convenience. This is contrary to established engineering practice and should be avoided. When unavoidable, there should be separate power supplies, processors, software and I/O interfaces for protective functions.

11.3.7 The key factors that need to be considered in Power Management systems:

1. Redundancy.
2. Remote / local control.
3. Auto / manual.
4. Load sharing (if applicable).
5. Blackout prevention - heavy consumer control, load limitation and reduction.
6. Blackout recovery.
7. Industrial mission and industrial power consumers.
8. Power available calculation.
9. Power priority.
10. Starting standby gen sets - maintenance of spinning reserve, load dependent and alarm start functions.

11.3.8 While designing Power and Vessel Management Systems particular care is to be exercised in:

1. Automation.
2. Analysis Capability.
3. Data loggers.

4. Redundancy and criticality analyzers.

11.3.9 OWNER must approve, and specifies, that all control systems be supplied with Instrument Loop Diagrams as per Instrument Society of America Standard ISA-5.4-1991, or equivalent international standard (i.e. IEC, DIN, etc.)

11.4 AUTOMATION

11.4.1 Automation of key equipment systems can allow a predictable response to disturbances and provide rapid restoration of operation of those systems.

11.4.2 Automation associated with the power and vessel management systems must follow the redundancy concept and the WCFDI for the vessel. A distributed system minimizes the risk of failures exceeding the WCFDI.

11.4.3 Load Sharing: It should be recognized that any method of load sharing has the potential to cause power plant instability. Design should consider a method that minimizes risk of a blackout and ensure that independent protection is provided to address all possible failure modes of the load sharing system.

11.5 BLACKOUT PREVENTION

11.5.1 A distinction is to be made between a blackout and brownout and the consequences thereof.

11.5.2 An efficient design should result in minimizing the potential for a black out accepting that a brown out may be a consequence.

11.5.3 Brownouts have the potential to impact the industrial mission and may impact station keeping depending on the environment. A blackout not only compromises the industrial mission but also the station keeping ability.

11.5.4 Effective blackout prevention depends upon:

1. Recognition of immediate potential for a blackout.
2. Immediate Increase of online generating capacity.
3. Stabilize consumption while increasing capacity.
4. Security of blackout detection.

11.6 INDUSTRIAL MISSION

11.6.1 The Industrial mission may dictate assigning the same power priority to some industrial consumers as those required for station keeping. The identification of such industrial mission consumers should be analyzed, rationalized and appropriately addressed in the Power Management System.

11.7 BLACKOUT RECOVERY

11.7.1 Fully automatic blackout recovery of the power plant to pre blackout conditions is not a requirement for the traditional DP class notation but should be considered in the design as an essential risk reduction measure (it is a requirement of DYNPOS ER).

11.7.2 Key factors to be taken into consideration while designing blackout recovery systems are:

1. Speed of recovery.
2. Minimize potential for false initiation of blackout recovery.
3. Reduce risk of recurrence of blackout on or during recovery.
4. Automatic return (e.g. enabling) of thrusters to DP.
5. Independence from the Emergency Switchboard.

11.8 POWER AVAILABLE CALCULATION

11.8.1 Station keeping is vulnerable to errors in the power available calculation. The philosophy and integrity of this crucial function is to be recognized and appropriately addressed in the design. There has been a history of incidents in this area and therefore attention is drawn. Effective error handling is essential.

11.9 ANALYSIS

11.9.1 Power and Vessel Management systems should have capabilities to facilitate analysis. (predictive as well as post event). Post event analysis is typically facilitated by the use of data loggers. Predictive analysis may be accomplished by Redundancy Criticality Analysis (RCA).

11.9.2 Data loggers:

1. A data logger can be invaluable for post incident investigations, because of its ability to demonstrate the sequence of events, identify the initiating event and root cause. However, to be able to accomplish this, the data logger must have certain characteristics, relating to the number of data channels, selection of data that is to be recorded, time resolution and time stamping of data, and data resolution.
2. A data logger should facilitate trend monitoring.
3. Data logger files should be in a format that supports efficient plotting of data.
4. Guidance on desirable features for data loggers is given in Section **Error! Reference source not found.**.

11.9.3 Redundancy and Criticality Analyzers (RCA):

1. A properly configured RCA can help with configuration of complex systems by drawing attention to non redundant configurations where WCF can be exceeded.
2. RCA should align with the WCFDI, redundancy concept, and results of FMEA and proving trials.

12 NETWORKS AND SERIAL LINES

12.1 DESIGN

12.1.1 Network design has evolved to Ethernet based solutions and use of communication switches rather than hubs. Configuration of network equipment is a key element of providing the necessary level of fault tolerance.

12.1.2 Networks, as discussed in this section are comprised of:

1. Human machine Interface.
2. Two independent full duplex data highways.
3. Remote Control Unit (RCU) / processor / Programmable Logic Controller (PLC).
4. Network switches.
5. Source of power.

12.1.3 A network topology with a proven track record and demonstrable history of reliability is recommended. The physical star, logical bus network is one such example.

12.1.4 Design of networks for DP should provide

1. Required speed and capacity.
2. Adequate bandwidth to accommodate and support the system design data load.
3. Predictable response across the full range of traffic conditions.
4. Reliability in a harsh environment.
5. Minimum downtime.
6. Ease of maintenance and repair.

12.1.5 Design should facilitate monitoring of the status of the network by the DPO. The alarm terminology used for network alarms should be designed to be readily interpreted and avoid misinterpretation.

12.1.6 Network design has evolved to Ethernet based designs and use of switches and is typically within the scope of supply of the DP control system vendor. In some projects, the VMS network may be provided by an automation system vendor who is not the DP control system provider.

12.1.7 Design should facilitate monitoring of the status of the network by the DPO. The alarm terminology used for network alarms should be designed to be readily interpreted and avoid misinterpretation.

13 UNINTERRUPTIBLE POWER SUPPLIES

13.1 PURPOSE

13.1.1 The purpose of a UPS in a DP system is to provide:

1. Stable, clean power.
2. Continuity of power during main power system outage.
3. Power system transient ride through capabilities.

13.1.2 Design of UPS systems follow either a centralized topology or distributed topology. Centralized topology lends itself to a robust system but introduces commonality while a distributed system potentially could be less robust but minimizes commonality. Commonality potentially increases the amount of equipment lost as a consequence of failure.

13.1.3 The design of UPS systems, their power sources and distribution should:

1. Accomplish robustness.
2. Follow the WCFDI.
3. Not introduce additional vulnerabilities.

14 DP CONTROL SYSTEMS

14.1 DESIGN FACTORS TO BE CONSIDERED

14.1.1 DP Control systems, due to their maturity, tend to receive less attention and scrutiny during the design phase. It should be recognized that lack of attention in the design phase can introduce vulnerabilities that can impact the Industrial mission of the vessel. Certification of DP Control Systems by Classification Society is a requirement of obtaining a Class Notation.

14.1.2 Enhanced redundancy over the minimum requirements for Class Notation in Control Systems may be desired to increase operational uptime while executing the vessel's industrial mission.

14.1.3 Ergonomics in the DP control system and HMI play a key role and should be focused upon in the design phase.

14.1.4 Factors that need to be considered in selection of DP control systems are:

1. Reliability and potential service life of components, subsystems and systems.
2. Availability.
3. Stability.
4. Topology.
5. HMI.
6. Mathematical modeling (Optimal control theory).
7. Sensor handling.
8. Appropriate modes for its industrial mission.
9. Power limiting.
10. Independent simulation capability for use as a trainer.
11. Consequence analysis aligned with WCFDI.
12. Independent joystick system.
13. Alarms and alarm management.
14. Alarms and display printers.
15. Data logging.
16. Source of power.
17. Remote diagnostic capability.
18. Potential service life and obsolescense

15 SENSORS

15.1 DESIGN PRINCIPLES

15.1.1 Sensors as referenced in this section include:

1. Position reference sensors.
2. Sensors used for environmental monitoring including weather radar and Doppler current profilers.
3. Vessel Motion Sensors.
4. Draught sensors.

15.1.2 During Design the following should be taken into account:

1. Suitability.
2. Differentiation.
3. Diversity.
4. Independence.
5. Location / installation.
6. Maintainability

15.1.3 The industrial mission of the vessel will dictate the setting of the objectives to be achieved and the degree of focus on each of the above elements as it pertains to position reference sensors.

16 EXTERNAL INTERFACES

16.1 SYSTEMS ENGINEERING APPROACH

16.1.1 The vessels industrial mission may require the DPCS to be interfaced with non station keeping related equipment (for example, pipe tensioners, riser tensioner stroke, draught sensors or fire monitors). Design of such interfaces should follow a system engineering approach and may result in a degree of complexity that was not initially envisaged. Examples of systems engineering approaches are FMEA and consequence analysis.

16.1.2 Interfaces into the DPCS providing input (automatic and manual) data should be 'bound' or 'limited' (e.g. range of permissible data) to minimize the consequences of erroneous data or input.

16.1.3 The vessels sensors may require to be interfaced with non station keeping related equipment (for example, RADAR, GMDSS, Survey systems). Design of such interfaces should follow a system engineering approach and may result in a degree of complexity that was not initially envisaged.

17 SAFETY SYSTEMS

17.1 SAFETY SYSTEM DESIGN WHICH MAY AFFECT DP

17.1.1 Vessels safety systems as referenced in this document comprise of:

1. F & G systems.
2. Fixed firefighting systems.
3. ESD systems.
4. QCVs (Quick Closing Valves).

17.1.2 The redundancy concept for station keeping is to be followed through to these systems to ensure that actions or failures initiated by these systems do not cause consequences that exceed the WCFDI. The actions initiated by these systems should be scaled to the detected threat level.

17.2 ARRANGEMENT OF MACHINERY SPACES

17.2.1 DP equipment class 2 allows for redundant machinery to be located in a common space. This can make it difficult to fight fires or deal with other emergency situations without compromising station keeping. Whilst not a class requirement for DP 2 notation, fire protection over and above that required by main class rules may be considered in high risk areas such as engine rooms when warranted by the industrial mission (e.g. engine rooms divided). Owners may, at their discretion, opt for a DP Class 3 redundancy concept with full separation and protection against the effects of fire and flooding. Any additional fire and flood protection applied to DP Class 2 designs should be along the lines of the overall split in the DP redundancy concept

18 ERGONOMICS

18.1 OPERATOR INTERVENTION

18.1.1 It is acknowledged that technical faults are triggers that sometimes require operator intervention to prevent escalation. Addressing ergonomics and decision support in the design enables effective operator intervention.

19 ALARM MANAGEMENT

19.1 THE NEED FOR ALARM MANAGEMENT

19.1.1 An effective Alarm Management System should be incorporated into the design. Alarm management enables two fundamental functions:

1. Intervention.
2. Post incident analysis.

19.1.2 Poorly designed alarm management systems do not facilitate effective operator intervention. An effective design should facilitate:

1. Instant awareness of criticality and consequence.
2. Interpretation leading to effective response.
3. Focus and avoidance of alarm ‘fatigue’.

20 COMMUNICATIONS

20.1 DESIGN CONSIDERATIONS

20.1.1 Communications as referenced in this document incorporates visual and audible means of communication.

20.1.2 Communication is a key management tool during execution. This should be incorporated in the design phase. The following should be taken into account:

1. Identification of locations where DP related communication is essential.
2. Means of communication (audible and visual).
3. Layered topology for audible and verbal communications.
4. Methods of transmission.
5. Independence of power supply.
6. Visual Communication to follow systematic processes that tie in with the DP Procedures and responses.

21 INSPECTION REPAIR AND MAINTAINABILITY

21.1 INFLUENCE OF MAINTENANCE ISSUES ON REDUNDANCY CONCEPTS

21.1.1 Design philosophy and redundancy concept should take into account Inspection Repair and Maintenance over the life cycle of the vessel. Equipment related to station keeping should be identified as Safety Critical Elements (SCE) and addressed in the Planned Maintenance System accordingly.

21.1.2 The following IRM factors need to be considered during the design phase:

1. Impact on post failure capability due to non availability of equipment as a result of planned or unplanned maintenance.
2. Optimum sizing of equipment to enhance post failure capability.
3. Copackaging / colocation of redundant equipment limiting accessibility to IRM.
4. Non intrusive means to facilitate testing.

22 COMMISSIONING AND TESTING

22.1 THE INFLUENCE OF COMMISSIONING AND TESTING

22.1.1 The design of the DP system has a significant impact on the commissioning and pre commissioning. A philosophy that incorporates facilities to carry out efficient testing by design is likely to deliver a vessel with fewer hidden failures (e.g. testing of protective functions). Addressing testing and commissioning at the preliminary stages of design, (i.e. development of the redundancy concept), enables optimization of the time required for commissioning and proving trials.

22.1.2 Equipment that is largely self contained lends itself to fewer integration interfaces and is less likely to introduce issues at the pre commissioning and commissioning phases.

22.1.3 A uniform labeling/numbering system should be incorporated in the design phase and systematically followed through in all aspects of the project. This should be clearly communicated to all stakeholders (e.g. design house, yard, vendors, FMEA providers and operational manual generators).

22.1.4 There are five distinct phases in the project cycle as it pertains to this section:

1. Factory Acceptance Test (FAT).
2. Mechanical “completion” (when equipment is installed, cabled and cables rung out).
3. Pre commissioning (Pre-commissioning should be done with the equipment set up in the defined operational configurations and must include loop testing).
4. Commissioning (Commissioning of equipment should be validated following tuning, and tested under load and stability established. It should be recognized that accurate tuning is a precursor to effective commissioning. Time required to accomplish tuning is not to be underestimated).
5. Testing (The activity encompassing testing of the fully integrated system with the objective of proving that the performance meets specifications and that tuning is consistently effective across a representative range of conditions). Testing also includes proving the FMEA to demonstrate the following:
    a. The redundancy concept.
    b. Effectiveness of protective functions.
    c. Stability of the system under the full range of load/operational conditions.
    d. Monitoring functions.
    e. Degraded and failure conditions.

The above should be sequential activities.

22.1.5 FAT is an important phase of testing and should be carried out with the necessary diligence and participation of required stakeholders (i.e. FMEA providers, Project and Operational personnel deemed necessary). This is of particular significance for equipment that has the potential to be damaged if tested during proving trials and that would have schedule impact (e.g. internal control loops for thruster variable speed drives), and on equipment whose design does not lend itself to field testing (e.g. MRUs - no means to check calibration). It is acknowledged that the quality of the FAT tests from an FMEA perspective will depend on the degree of progress and access to detailed information to perform an FMEA analysis of the equipment being Factory Acceptance tested.

22.1.6 When feasible the FAT should include all Inputs and Outputs, particularly interfaces with other systems, simulated and measured to meet the full range of expected operating criteria.

22.1.7 Vessels with complex designs requiring extensive integration should consider the need for a full scale integration test.

22.1.8 A robust pre commissioning and commissioning process is fundamental to the execution philosophy and should be integral to the project from concept. Three legs that contribute to a robust pre-commissioning and commissioning process are:

1. Documentation.
2. Verification.
3. Clearly defined Performance Acceptance Criteria.

22.1.9 The responsible party for designing the commissioning and testing process should be clearly identified, and made visible to all stakeholders. The party responsible for integration should be specifically included in the list of stakeholders.

22.1.10 It is highlighted that Class participation in the testing and commissioning process may be limited to those elements required by Class rules. Testing geared towards the station keeping elements supporting the Industrial mission and not covered by Class rules needs to be addressed specifically in the shipyard contract and in the FMEA. Performance and acceptance criteria should be clearly established.

REFERENCES

BIBLIOGRAPHY