DYNAMIC POSITIONING CONFERENCE
September 28-30, 2004

Risk

Can Less Than DP2 Class Vessels be Accepted for More Work Close to Platforms?

Required reliability efficiently demonstrated by FMEA and sea trials tests

---

Odd Fagerjord

Det Norske Veritas Consulting[i]

[i] http://www.dnv.us/

Return to session directory

Abstract

Vessel operations close to live offshore platforms are usually restricted. The restrictions will depend on the documented reliability of the manoeuvring and station keeping capability of the vessel, and the risks involved for the particular operation. Typically IMO equipment class DP2 or higher may be requested.

Many supply vessels have some built-in positioning redundancy, but the positioning is carried out manually for example by use of a joystick. This will not give the same positioning accuracy as with DP, but may give about the same position keeping reliability. A standard for documentation of technical redundancy has been issued in Norway. Vessels complying with this standard should technically not lose position due to any single failure comparable to what is required by DP2 vessels, but do not need a dynamic system for the positioning. For operations where position accuracy is not very important such vessels may easier be accepted by e.g. platform operator for upwind operations of platform or other special operations within the safety zone.

Vessels with some built in propulsion redundancy as well as redundancy in the manoeuvring systems may comply with the technical redundancy standard directly or may do by introducing only moderate modifications.

The purpose of this paper is to demonstrate what is required to obtain a "letter of compliance" and how this shall be documented. The main focus is put on the documentation, which is principally a "Failure Mode and Effect Analysis" (FMEA). The structure and technical depth of the FMEA is discussed and illustrated by practical examples. The aim is to show how an efficient and sufficient FMEA can be structured. This includes requirements for thrusters, piping arrangement for machinery, electrical distribution and control systems.

In order to obtain the letter of compliance a test program has to be approved and verified at a sea trial. An outline of a typical test program is presented.

This paper should give owners of supply vessels e.g. of IMO DP1 class or less, a better basis to evaluate if it is feasible to upgrade a vessel and what will be required to obtain "letter of compliance".

Introduction

Vessel operations close to live offshore platforms are usually restricted. The restrictions will depend on the documented reliability of the manoeuvring and station keeping capability of the vessel. Typically IMO[†] equipment class DP2 or higher may be requested. For less than DP2 class vessels individual acceptance for each type of operation has to be obtained

Many supply vessels have some built-in positioning redundancy, but the positioning is carried out manually for example by use of joystick. This may give approximately same position keeping reliability as for automated systems if the system is designed so that no single equipment failure can cause loss of the positioning function. This has been called *technical redundancy* in position keeping (PK) ability.

The offshore industry in Norway has requested a standard to document sufficient redundancy in technical design of the positioning system[‡]. This has been requested in order to simplify the work permit process without compromising safety during vessel activities inside the safety zone. Vessels built and tested in compliance with the requirements in this standard shall not lose position keeping ability in the event of any defined single failure. This implies that after any single failure the vessel shall be able to produce sufficient transverse thrust, longitudinal thrust and a yawing moment to keep its position and to safely terminate the operation. This "single failure" concept is mostly identical to the IMO DP2 requirement. However, the standard accepts that the positioning may be provided without "dynamic" control and position reference equipments, given that the vessel operator is provided with efficient means to control the propulsion system and to observe movement response of the vessel. I.e. the PK system may not necessarily require a "dynamic" system which is mandatory for the DP classes. The standard, however, requires that the vessel shall as minimum be equipped with selectable automatic heading control combined with joystick operation. Further it shall be possible to override the joystick control by operating each thruster individually by separate control levers.

Documentation of technical redundancy

In order to document that the vessel has the required technical redundancy a Failure Mode and Effect Analysis (FMEA) has to be provided. This analysis shall verify that the vessel after a single failure without disruption shall be able to keep the position to safely terminate the ongoing operation.[§] The FMEA conclusion shall highlight all failures that may influence the redundancy. The specific conclusions of the FMEA for the different systems are to be verified by tests. The test procedure for redundancy is to be based on the simulation of identified failures and shall be performed under as realistic conditions as practicable.

Loss of position keeping ability is not to occur in the event of a single failure in any active component or system as specified. Normally static components will not be considered to fail if adequate protection is provided.

The single failure criterion comprises:

- Any active component or system
- Static components which are not properly documented with respect to protection
- A single inadvertent act of operation. If such an act is reasonably probable
- Systematic failures or faults that can be hidden until a new fault appears

[†] IMO; International Maritime Organisation
[‡] DNV Standards for Certifications 2.16; *Specification for Redundancy in Position Keeping Ability*
[§] No time limit is specified, but backup battery capacity at maximum load output power shall be minimum 30 minutes after loss of charger input power

Minimum thruster/propulsion configurations for position keeping

There are several possibilities to configure thruster systems that enable position keeping (PK). Presented below are four of the most common minimum solutions that provide control of longitudinal forces, transverse forces and turning moments.

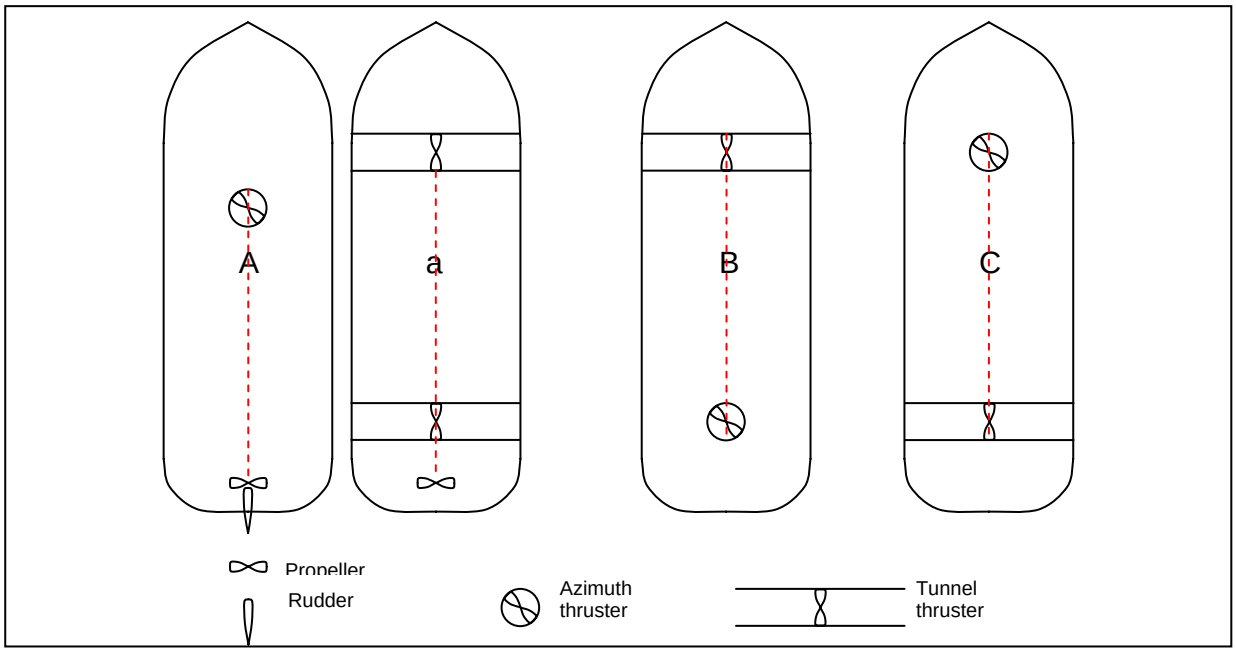

Figure 1 - Minimum thruster/propulsion configurations for position keeping

The “A” alternative uses the rudder to obtain side force in the aft which is created by the water flow from the propeller. Thus another source must compensate the propeller axial thrust force if less or opposite longitudinal force is required. This is supplied by the azimuth thruster in the fore-ship. The azimuth can give thrust in any direction thus providing both axial and side thrust. Combined with the rudder side force the “azimuth” creates turning moment. Without utilising the rudder for side force (alternative “a”), minimum a side thruster aft is required. With this solution no compensation for propeller axial force is required and it is sufficient with a side thruster in the front to provide turning moment, i.e. the azimuth function is not required. Alternative “B” and “C” are symmetrical solutions to each other and do not require a main aft propeller.

Any significant failure (e.g. stop) of one or more of the thrusters in each configuration will jeopardise the positioning ability and exceed the maximum acceptable failure.

Technical redundancy

Any selection of two of the alternatives above will give adequate positioning redundancy provided that the thruster system is designed to produce the required forces for the operation condition. The selections can be: AA, Aa, AB, AC, aa, aB, aC, BB, BC or CC. Actually the standard accepts use of rudder/propeller for side force only as backup in case of aft thruster side force failure. Thus the AA configuration should be avoided. There will of course not be any restrictions to improve the flexibility by replacing a propeller or side thruster with an azimuth thruster or include more than the required thrusters. Some of the combinations that give adequate redundancy are shown below.

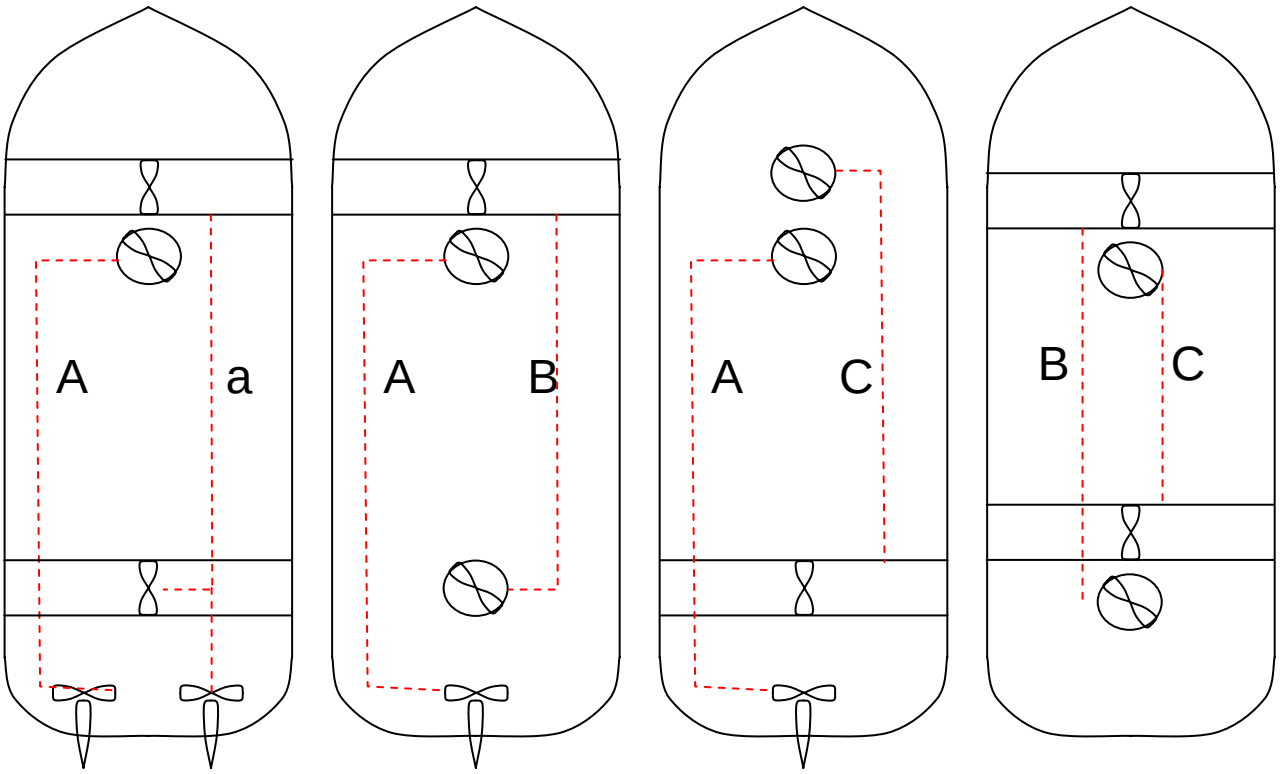

Figure 2 Example on thruster configurations for technical redundancy

Technical redundancy

In order to maintain full redundancy the individual configurations (see Figure 2) should be independent from each other with respect to the defined single failures. Otherwise a failure could be a common cause for both redundant configurations to fail. Full separation may however be hard to achieve. System redundancy for systems that serves both configuration sides is accepted if sufficient reliability is obtained. Further, the standard requires redundancy mainly for active components, as for the DP2 class.

Essential systems that shall have redundancy are:

- Power supply to main propeller and thrusters including power generation (selectivity accepted)
- Fuel supply to propeller engine or generator engines (redundant systems)
- Lubrication and hydraulic systems (redundancy in active components)
- Cooling systems (SW redundancy in active components, FW redundant systems)
- Reference system (redundant gyro)
- Power supply to auxiliaries (Redundant systems: fuel, lubrication, cooling and control)

Incomplete split typically for auxiliary systems may be common-cause for loss of both PK systems.

For example redundant power supply to the thruster motors are not enough if the fuel supply to the generator engines is through a common line, or if separated fuel supplies have supply pumps that use the same electrical source. The FMEA shall demonstrate that the electrical power supplies to the auxiliaries have redundancy between the two PK systems according to the defined failure modes. This feature shall further on be verified by testing that outage of one net will not cause loss of PK ability.

Often pumping for fuel, hydraulics, lubrication and cooling are provided with dual pumps with one in standby and automatic start-up. This is provided for both redundant systems. The standby pumps may be electrically connected to the “other side” net. In that case one should be aware that if a main pump is

maintained one has not any longer full redundancy. This can be retained if the standby pump is reconnected to the primary net during the maintenance, e.g. with manual changeover, or both pumps are supplied from the same net as standard.

In order to obtain separated nets, it is a requirement that the power generation is carried out with minimum two generators that supply a main switchboard that can be separated between the two generators by bus bar breakers. In case running with closed separation breakers short circuit or earthing could cause full blackout if all generators will be disconnected. In order to avoid potential for black-out, the switchboard breakers must be selective for all failures (short circuit, earthing, frequency etc.), so that the bus bars are separated faster than the breakers to the generators.

Control system independence

All the IMO DP classes require a reference system and a control system that automatically positions the vessel. For the PK vessel a reference system is not mandatory except for the heading reference, i.e. gyro compass. The control system shall facilitate automatic heading control and joystick operation. Failure to the control system might disable the positioning. Therefore the PK standard requires that it shall be possible to operate each thruster individually and separated from the Joystick control system.

I.e. the position keeping system is to include:

- Independent joystick with heading control
- Manual leavers for each thruster

The thruster control mode, i.e. manual and joystick, is to be selectable by a simple device located in the position keeping control centre. The control mode selector is to be arranged so that it is always possible to select manual controls after any single failure in the automatic/semi-automatic position keeping control mode, or in the switching system itself.

When the joystick and/or a dynamic positioning control system uses a data communication link, this link is to be separate from the communication link(s) for manual control. When two or more thruster systems and their manual controls are using the same data communication link, this link is to be arranged with redundancy in technical design.

Any failure in the joystick control system shall not cause potential for drive-off. A solution in case of failure can be to set the thrust commands to zero and initiate an alarm.

In order to avoid a potential drive off, it shall further be possible to stop the thrusters individually from the position keeping control station by means independent of the positioning and thruster control systems. This emergency stop is to be arranged with separate cables for each thruster. Further the loops shall be monitored with failure alarm in order to safeguard that the emergency stop function always is available.

The joystick system and the gyro compasses are to be powered from continuously charged battery/UPS. The battery/UPS is to have alarm for charging failure. The battery is to be able to provide maximum load output power for 30 minutes after loss of charger input power.

Power management

An automatic power management system is to be arranged, operating with both open and closed bus-bar breakers. This system is to perform the following functions:

- load dependent starting of additional generators
- prevent starting of large consumers when there is not adequate running generator capacity, and to start up generators as required, and hence to permit requested consumer start to proceed
- if load dependent stop of running generators is provided, facilities for disconnection of this function is to be arranged
- if breaker control is provided, facilities for disconnection of this function is to be arranged.

A failure in the power management system is not to cause alteration to the power generation, and is to initiate an alarm in the position keeping control centre.

It shall be possible to operate the switchboards in manual, with the power management system disconnected.

Exemption to have PMS system may be accepted if a PMS will give small, if any, contribution to improved regularity and the safeguarding of the functions listed above is catered for by other means.

Failure Mode and Effect Analysis (FMEA)

Most classification societies require failure mode and effect analysis (FMEA) as part of the documentation of vessel classed similar to IMO DP2 or higher. This is also recommended by the PK standard.

Quote:

> *Documentation of the reliability of the position keeping system is required in the form of a failure mode and effect analysis (FMEA). The purpose of the FMEA is to give a description of the different failure modes of the equipment when referred to its functional task. Special attention shall be paid to the analysis of systems that may enter a number of failure modes and thus induce a number of different effects on the position keeping system. The FMEA shall include the information specified below:*
>
> - *A breakdown of the position keeping system into functional blocks shall be made. The functions of each block shall be described. The breakdown shall be performed to such a level of detail that the functional interfaces between the functional blocks are shown.*
> - *A description of each physically and functionally independent item and the associated failure modes with their failure causes related to normal operational modes of the item is to be furnished.*
> - *A description of the effects of each failure mode alone on other items within the system and on the overall position keeping system is to be made.*

The requirement for “functional blocks” is quoted in almost any reference discussing FMEA. Nevertheless it is not clear into what extent this should be, i.e. into which detail. This has sometimes resulted in comprehensive FMEAs shooting far ahead of what is necessary, and also unusable block diagrams. For the PK the intention should be to make it clearer which items that must function in order to obtain the desired result, and to make it easy to verify that systematic common causes for redundant system to fail are prevented.

Overview of functional blocks that normally are contained in a PK system are illustrated in Figure 3 below.

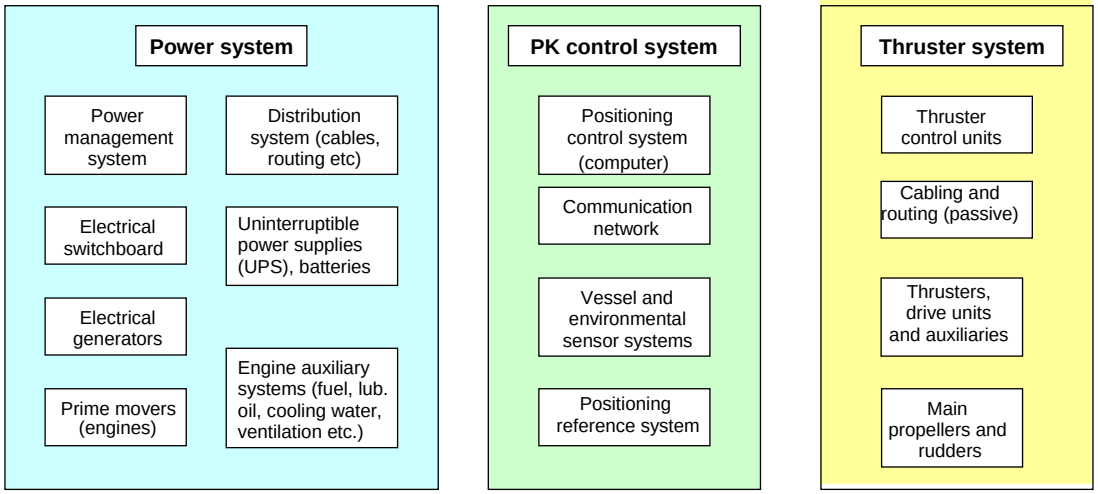

Figure 3, Position Keeping System, block diagram

The intention with the "functional blocks" and the descriptive part is to give easy understanding on how the PK system is organised, which sub-systems are essential and how the redundancy is safeguarded. It is not necessary to go into details on for example all possibilities for a fuel pump to fail, except for causes that could be in common with pumps or sub-systems supporting the redundant part of the PK system, e.g. el. power or control signals.

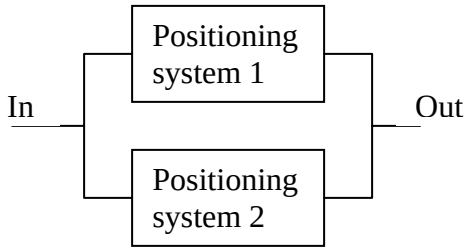

Figure 4, Simple reliability block diagram for PK technical redundancy

Simple reliability block diagrams may be useful to visualise how systems are separated and/or connected.

Principally any redundant PK system will have the two functional blocks as shown in Figure 4. To lose the desired output both blocks must be out of function. The causes for the blocks to fail may be several and will depend on the subsystems that each block comprises. For example the subsystems block diagram for the Aa configuration in Figure 2 above will be as in Figure 5 below. Failure to any of the single elements in each parallel (redundant) line will cause loss of redundancy, or in other words will be a "maximum (allowable) failure".

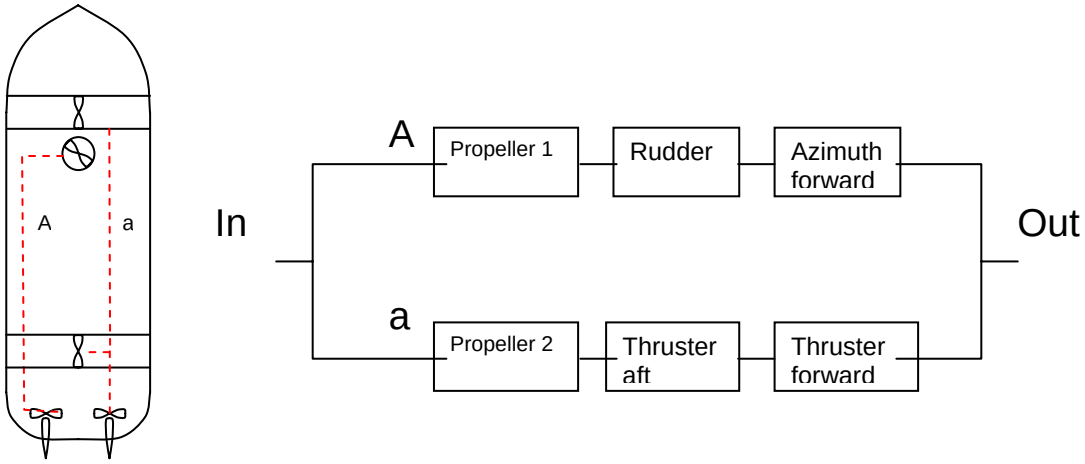

Figure 5, Functional diagram and reliability block diagram with main systems for redundant PK

Still these block diagrams hardly give any more contribution to the understanding of the total system than the diagrams shown in Figure 2. Therefore the reliability block diagram can be omitted if the analyst is not familiar with this presentation form. The “functional blocks” are sufficiently illustrated in the principle drawing to the left in Figure 5.

A one line power diagram as shown in Figure 6below is also a sufficient illustration of the electrical system and does not be backed up by a “block diagram”.

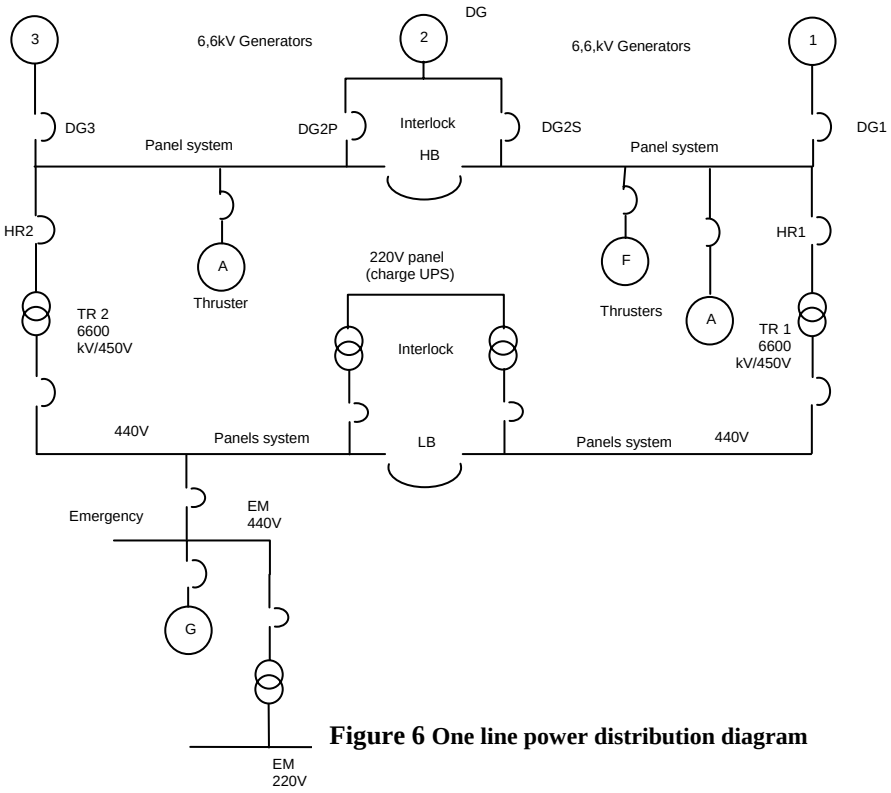

Figure 6 One line power distribution diagram

For some systems it will be necessary to analyse subsystems on a lower level. For example failures to the engine or failure to the propeller pitch control may be a maximum failure. On the other hand it does not matter why the e.g. engine stops or the pitch control is lost as long as it can be demonstrated that the fault causing the failure will not also cause a failure on the other redundant line (or can not be compensated). For example the fuel systems are separated for the two engines, but the fuel pumps require electrical power. Thus it has to be demonstrated that loss of electrical power will not stop fuel supply to both engines. Collapse of pump or valve failure etc. will not have potential to be common and can be omitted from further discussion.
Therefore it is sufficient to describe the functional blocks that are required for both redundant configurations. It shall be demonstrated that functions/supplies required of both sides are properly independent or made redundant. The systems that usually have to be analysed are shown in the Table 1 below:

Table 1 Systems that should be contained in FMEA

- Control system (computer, signal transmission/network, reference system, displays and consoles)
- El. power one line power distribution diagram
- Low voltage power supply to control system and pilot systems (valves, breakers etc.)
- Fuel supply system (from- and including the service tanks)
- Lubrication and hydraulic systems Propeller shaft, gear, pitch control lubrication Thruster lubrication Engine lubrication
- Cooling systems Lubrication/hydraulic cooling Thruster cooling Engine cooling
- Ventilation systems (if essential for some of the PK units)
- Control air (if used e.g. for governor control, closure of dampers, operation of valves), "fail to safe"

Formally, if the overview and discussions are properly carried out for the relevant sub-systems, the PK standard FMEA requirement is fulfilled. The standard, however also as guidance, refers to standards for FMEA systematic[**]

These descriptions also include "FMEA worksheets" that shall give systematic presentation of all single point maximum acceptable failures. Development of worksheets is recommended. They will give a good overview of the system and can support failure finding should that be necessary. Further, design changes concerning the PK reliability may easily be implemented into worksheets.

Recommended contents of the FMEA worksheets are:

Item	The name or identification of the item being analysed for failure
Failure mode	Mode of failures that is relevant for the PK
Cause	Various causes (if more) for each failure mode
Consequence	Failure effect on the function of the item and totally on PK.
Detection	List detection means. Can the failure remain undetected
Safeguards	List existing provisions that shall prevent this failure to occur or that mitigate the effect
Consequence classification	1. Critical, may lose position 2. Maximum, PK redundancy lost 3. Degraded, reduced operational capacity on one of the redundant PK systems 4. Not relevant or Insignificant for PK operation
Comments	Recommendations assumptions or other relevant remarks
Test method	Information on how the failure can be simulated

The presentation of FMEA work sheets may be given in a condensed table format. An example is shown below:

[**] Description of FMEA systematic may be found in IEC Publication 60812 or IMO HSC Code, Annex 4.

Vessel Name, Project Title								Date: xx xx
System								Recorder: nn.NN
Item	**Failure mode**	**Cause**	**Consequence**	**Detection**	**Safeguards**	**Consequence classification**	**Comments**	**Test method**

Typical example of filled in FMEA work sheet is shown below:

Vessel Name, Project Title							Date: xx xx
Control system							Recorder: nn.NN
SYSTEM EQUIPMENT FAILURE	**CAUSE**	**CONSEQUENCE A: LOCAL/IMMEDIATE B: OVERALL**	**DETECTION**	**MITIGATION/ COMPENSATION/ SYSTEM RESPONSE**	***CRITICALITY* COMMENTS**	**TEST Y/N**
Main controller	Processor failure, power failure	A: Main controller dead B: All thrusters, propellers rudders and engines to be operated manually	Alarm	Positioning and manoeuvring can be done by manual control.	*Maximum*	Y Disconnect power
Signals and supply to controller	Line, card or power failure	A: Main Controller dead B: All thrusters, propellers rudders and engines to be operated manually	Alarm	Positioning and manoeuvring can be done by manual control	*Maximum*	(Y) (See above, disconnect power)
Data to remote controller	Line or card failure	A: Remote stations not usable B: Main controller working as well as manual controls	Alarm	Main console should be useable, "manual" operation is backup	*Maximum (Degraded)* Test will show criticality **FMEA to be updated after test**	Y Disconnect line
Main controller mode selector	Line or card failure	A: Out of order B: No change or incorrect selection.	Visual or alarm	Faulty switch will most probably give zero signal that means "manual". If stuck at other selection, operator may cut power and transfer control to "manual" Positioning and manoeuvring can be done by manual control	*Maximum* Test not necessary. Line cut will give 0 V and "manual"	N Verify that manual control can be obtained also if selection is Auto or joystick
Etc.						

Trial test program

The PK standard requires that the findings from the FMEA shall be verified by tests. Typically all maximum failures shall be simulated and it shall be proved that no failure has more serious consequence than anticipated. In order to obtain a "letter of compliance" for PK a "test program" have to be issued and

approved by Class or other approval 3.rd. party, and the tests have later on to be supervised by the approval institution.

The test program shall include:

- operation condition (technically) before initiating the failure
- how to simulate the failure (cross check with the FMEA)
- description of anticipated effects (shall be described in the FMEA)

The condition before simulating the tests should normally be for PK condition in “Joystick mode” with heading control. Same tests in “Joystick mode” without heading control or just in “Manual mode” may be considered if potential failures only can be discovered in that mode.

Tests should be carried out when the power supply system is divided into a minimum of two redundant systems by opening the necessary switchboard bus-tie breakers. Special tests shall then be made when bus-tie breakers are closed.

Outline of which tests that should be carried out is given below:

Main AC switchboards

- No generator (including emergency generator shall be in automatic starting mode)
- Provoke blackout at one side at a time, preferentially at all voltage levels starting with the lowest level
- This can be achieved by stopping generators or tripping breakers.

Electrical DC systems

- Simulate failure on battery systems by switching off fuse-breakers from battery and charger
- Make sure that closed crossovers do not destroy the test
- Record which equipment are influenced

UPS (Uninterruptible Power Systems)

- Switch off all outputs from one UPS at a time
- Run for a while and observe side effects

Systems operating with normally closed bus-tie breakers

Load sharing Systems

- Disconnect power supply
- Disconnect load sharing lines

Governors

- Simulate over speed
- Simulate shut down
- Disconnect power supply

Generator voltage regulators

Discuss with manufacture how tests can be simulated without damaging e.g. generators.

Thrusters

Test failure of signals in each thruster system and include check that the thruster can be manually deselected:

- Disconnection of order thrust signal from joystick controller / feedback thrust signal to joystick controller
- Disconnection of order RPM signal to frequency converter/feedback RPM signal from frequency converter
- Disconnection of feedback pitch signal propeller
- Disconnection of blackout prevention signal to frequency converter
- Disconnection of “available power” signal from frequency converter to PMS
- Disconnection of blackout prevention signal from main switchboard to frequency converter

The requirement is that such failures shall not lead to significant increase of thrust output nor make the thruster rotate so that the vessel can be driven off position, i.e.

- the thrust shall not increase significantly
- the thrust direction shall not change significantly

Freeze/ reduction in output or stop of thruster is accepted
It is accepted that the thruster rotates if at the time thrust is zero

Control system

Test of the control system shall verify that no failure will disable both the joystick operation mode and the possibility to operate the thrusters manually. Further, failures shall not prevent the possibility to change to manual operation or disable the function to stop single thrusters. How to carry out the tests will depend on how the signal transmission is provided and how "manual" and "joystick" modes are separated.

- Simulate joystick controller blackout by turning off power (if redundant supply and not already done by the power failure tests)
- Disconnect redundant communication links, one at a time. I.e. links that carry signals to more than one thruster system.
- Sensors and position references. Disrupt signal and observe that position (if position reference is installed) and heading can be maintained.
  (Only heading reference is obligatory for PK, but all systems that are installed shall be included in the FMEA and also tested).-

Potential failures to mode change (Joystick/Manual), emergency stop, and blackout prevention systems should also be simulated.

Test program format

The test program shall contain the start-up condition for the test, the method used to simulate a failure, the results expected and also leave space for writing down the results from the tests. This is also the outline that IMCA[††] recommends. An example of a test description is given on next page.

Some findings from the tests may tell that the FMEA were wrong on some points. Such observations shall be highlighted in the test report and the FMEA should be corrected. Also future alterations to the PK system should be followed up by evaluating if the FMEA needs corrections. Thus the FMEA will be a useable living document for reference during operation and fault finding.

Table 2 Example description for testing positioning main controller

Method:	1. Keep vessel in position using the joystick, all thrusters running 2. Cut power to the main controller (disconnect line xxx) 3. Use manual control for positioning 4. Reconnect line xxx and establish joystick positioning at remote station 5. Disconnect data signal line to remote (yyy) 6. Use main station joystick for positioning 7. Reconnect yyy, continue joystick positioning 8. Disconnect serial data signal line (zzz) 9. Check reactions on joystick, change to manual control for positioning and check functionality
Results expected:	2. Joystick inoperable 3. Automatic change to "manual" mode 5. Remote operation not possible, but control from main station still possible 8. Possibly the joystick operation is jeopardised. Manual control shall be possible.

[††] IMCA; " The International Marine Contractors Association

Results found:	
Comments:	
Witness:	**Date:**