DYNAMIC POSITIONING CONFERENCE
October 13 – 14, 1998

DESIGN

FMEA as an Integral Part of Vessel Design and Construction: Producing a Fault Tolerant DP Vessel

Roger Cornes
Wavespec, Ltd. (U.K.)

and

Thomas R Stockton
Systems Engineering International (San Diego)

FMEA as an Integral Part of Vessel Design and Construction: Producing a Fault Tolerant DP Vessel

Abstract: Failure Modes and Effects Analysis (FMEA) techniques have been used for a number of years to identify single point failures on DP vessels. It is a requirement of the Classification Societies that an FMEA be completed for DP Class 2 and 3 notations. When FMEA is used in this manner, a study is usually carried out near the end of the vessel construction phase with the purpose of identifying any single point failures.

There is an enormous advantage to be gained by employing FMEA techniques throughout vessel development. This paper discusses applying FMEA as an integral part of vessel design and construction, and describes the FMEA methodology developed by the authors specifically for this purpose.

When FMEA is applied from this perspective, FMEA is a process, not a study, and the function of the process is to produce a fault tolerant DP vessel. Over the course of the vessel design and construction, FMEA is used to identify and assess the impact of the failure modes of all items of equipment that have an effect on the ability of the vessel to remain on station. When critical failure possibilities are identified, they are either eliminated or mitigated through design changes and/or operational procedures.

1.0 Introduction

Failure Modes and Effects Analysis (FMEA) is a tool which has been used for a number of years as a means of identifying single point failures on DP vessels. When used in this manner, the FMEA is carried out in the form of a study. On new builds and conversions, the vessel owner or yard typically contracts for the study near the end of the vessel construction phase with the objective of identifying any single point failures. Although well intended, this is akin to using FMEA as the means to assure oneself that the horses haven't escaped after the barn door has been closed. The time to identify and eliminate/mitigate the effects of equipment failure is during the design process, not in the latter stages of vessel construction.

Producing a fault tolerant DP vessel is by its very nature a multi-disciplinary exercise. The ability of a DP vessel to remain on station is dependent on the proper functioning and interaction of a number of vessel systems. In the presence of equipment failures, these interactions can become quite complex, and it requires a systematic and thorough systems approach to make sure that there are no inherent vessel deficiencies that could, in the presence of particular equipment failures, compromise the ability to remain on station.

During vessel design and construction the primary focus of engineering personnel is on capacity and functionality. Consideration is certainly given to redundancy and fault tolerance but it is not the central focus of any one group, and by default, it is not carried out from an overall vessel perspective.

When properly applied over the course of vessel design and construction, FMEA methodology provides the means of producing a fault tolerant DP vessel. When FMEA is used in this manner, the analysis starts with the owner's conceptual design and continues through the various stages of the owner's detailed design, yard design and construction, and vessel commissioning and sea-trials.

Over the course of vessel development, the FMEA is used to identify and access the impact of the failure modes of all items of equipment that have an effect on the ability of the DP vessel to remain on station. When critical failure possibilities are identified, they can be eliminated or mitigated through design changes and/or operational procedures. Specific FMEA testing is carried out, as an integral part of vessel commissioning and sea-trials, to verify system fault tolerance and document response to equipment failure.

Using Failure Modes and Effects Analysis in this manner goes well beyond the current FMEA thinking, that is, that a FMEA is a study carried out near the end of vessel construction to identify any single point failures.

2.0 Overview

The FMEA is carried out in a top down approach, starting with a system redundancy philosophy statement and a top level redundancy design specification specifying how the redundancy philosophy is to be achieved. It should be noted that whilst consideration is made to Class notation, the FMEA is carried out with respect to the redundancy philosophy/redundancy specification considering failure modes and their effects, including fire and flooding, notwithstanding the fact that the vessel may be Classed less than DP Class 3.

As a precursor to the main analysis, a review is made of the concept drawings that are usually prepared by the owner's design team. These are the drawings that are interpreted by the shipyard into single line system drawings and drawings for construction. In this way, it is ensured that the redundancy philosophy statement is reflected in the owner's concept drawings with any potential problems obvious to the FMEA analysts being identified/corrected at an early stage.

Next, block diagrams of all major equipment groups (i.e., Dynamic Positioning Control System, Vessel Management System, Fire and Gas, Emergency Shutdown, Electrical Generation and Distribution, Uninterruptible Power Supplies, Propulsion, Fuel System, Air Conditioning and Ventilation, etc.) are generated. From the block diagrams, the groups of equipment are identified for which the failure modes and effects are to be assessed.

The most intensive analysis takes place during yard design and construction. Yard construction drawings and equipment suppliers documentation are reviewed to assess both the overall design and the failure modes and effects of the various pieces of equipment. An FMEA Worksheet is compiled for each equipment failure assessment, even if it is determined that the failure does not impact station keeping. The worksheets form the body of the FMEA. They are contained in the FMEA database. An FMEA Report Form is generated whenever a problem area is identified. The Report Forms are also contained in the FMEA database. In response to the problem identification, design changes are made to eliminate or reduce the criticality of the fault (i.e., produce a more fault tolerant system). FMEA documentation and Worksheets are updated to reflect the design change.

As the vessel is being built, the build is audited to ensure that the build follows design. During this period the FMEA test program is developed. The FMEA tests become an integral part of

commissioning and sea trials. FMEA testing is done, amongst other reasons, to verify system fault tolerance and to document system response to specific equipment failures.

3.0 The FMEA Process

The FMEA is carried out over the course of the vessel design and build in three distinct Phases,

- Initial Concept Design Phase
- Yard Design and Construction Phase
- Test and Commissioning Phase

There are several different standards for FMEA's, including the guidelines contained in BS 5760: Part 5: 1991 and the guidelines found in the US Department of Defense MIL-STD 1629-A. The FMEA's carried out by Wavespec/SEI are broadly based on the latter guidelines.

Each of the three FMEA Phases are discussed in more detail in the sections below.

3.1 FMEA During Conceptual Design Phase

The objectives of the FMEA carried out during the conceptual design phase are threefold,

- To establish and document the level of redundancy and fault tolerance to be built into the vessel
- To assure that the owner's conceptual design fulfills the established system redundancy and fault tolerance levels
- To identify the equipment groups to be analyzed in the FMEA.

These areas are expanded upon below.

3.1.1 Redundancy and Fault Tolerance Statement

The redundancy and fault tolerance statement is generated to be a guide during vessel design and build. The redundancy and fault tolerance statement is made up of three documents.

- Redundancy Philosophy
- Operational Philosophy
- Redundancy Specification

The Redundancy Philosophy states the owner's philosophy as to the level of redundancy to be built into the vessel. The Redundancy Philosophy would include such items as the philosophy for the architecture of the power generation and distribution, the thruster/propulsion architecture, the data network architecture, and the levels of redundancy and fault tolerance to be achieved in each area.

The Operational Philosophy establishes such items as how the electrical generation and thrusters/propulsion are to be operated, (e.g., spinning reserve, bus tie-breaker positions, thrusters/propulsion online, etc.), equipment manning levels, system fault levels that would cause operations to be suspended.

The Redundancy Specification specifies the level of redundancy and fault tolerance to be built into the various vessel systems. It is generated considering the Redundancy and Operational Philosophies as requirements documents.

During the course of the yard design and construction, if the philosophies change, the redundancy and fault tolerance statement documents are updated to reflect the revised thinking.

3.1.2 Compliance with Redundancy and Fault Tolerance Requirements

The FMEA group, as part of the design team, provides an independent review of the owner's conceptual design. The review is directed specifically toward redundancy and fault tolerance with the objective of assuring that,

- The design reflects the Redundancy Philosophy
- The design supports the Operational Philosophy
- The design meets the Redundancy Specification.

Any problems identified in the conceptual design are easily corrected, as at this stage the design is only on paper.

3.1.3 Identification of Equipment to be Analyzed

Block diagrams of all major equipment groups are generated from the owner's top level design (i.e., from the concept drawings). The block diagrams are used to categorize and identify the equipment which will be analyzed during the yard design and construction phase. Major equipment grouping usually is organized as follows,

- **Electrical Power:** HV, MV, LV, and Emergency systems configuration and distribution, UPS systems configuration and distribution, power management.
- **Instrumentation and Control:** DP Control System, Vessel Management System, Fire & Gas, Emergency Shutdown, Data network.
- **Machinery:** Prime movers, thrusters, fuel system, cooling systems, lubrication systems, compressed air systems, heating, ventilation, and air conditioning.

3.2 FMEA During Yard Design and Construction Phase

The emphasis during the yard design and construction phase is the detailed review and analysis of the vessel design to assess:

- The compliance of the yard's design with respect to the redundancy specification
- The fault tolerance of the DP system.

The analysis is carried out by a thorough review of both yard construction drawings and equipment suppliers' drawings and documentation. It is of utmost importance during this phase that all relevant design changes are made known to the FMEA team in a timely manner. At the onset, the FMEA team will review the yard and suppliers' drawing lists and identify drawings which are needed for the analysis. Thereafter, whenever design changes are made and drawings revised, the changes need to be called out and copies of the revised drawings forwarded to the FMEA team.

As the build commences, the vessel is periodically audited to assure that the vessel build is being carried out as per the approved design.

It should be stressed that the team of designers and the FMEA team should operate as one team and not operate in an isolated manner. Constructive criticism of a design by the FMEA analysts should not be accepted with bad grace by the designers. It is not uncommon that the designers can get involved with a particular problem and not adequately consider whether the change violates the original design philosophy and/or how it might impact DP system fault tolerance.

3.2.1 FMEA Worksheets

An FMEA Worksheet is compiled for each equipment failure assessment. A description of the information contained in the Worksheet (the worksheet components) is provided in Appendix 1.

Some pertinent aspects of the Worksheets are,

- Equipment failures are given a severity classification (based on the consequences of the failure) consisting of three components …

    1. Consequences of equipment failure with respect to ability of the faulted DP system to be able to maintain station.
    2. Consequences with respect to the impact of the equipment failure on the operator (i.e., operator action required to keep the vessel on station).
    3. Consequences of the failure with respect to reduction or loss of system redundancy.

- Having the Worksheets in electronic form in a database allows the Worksheets to be sorted based on equipment categories and severity levels. This provides an effective means of identifying and ranking the problems, thereby focusing on the issues that require attention.

- Having the Worksheets in a database provides an effective means of information distribution via e-mail amongst the various parties that will be involved with the FMEA.

The Worksheets form part of the FMEA Final Report. They verify that each sub-system or component part of the system has been analyzed and document the results of the analysis.

3.2.2 FMEA Report Forms

Whenever a potential problem is identified, an FMEA Report Form is completed and forwarded to the design department. Report Forms are sequentially numbered and list the date issued, the person responsible for identifying the problem, the title and number of the drawing in question, and the reference number of the associated worksheet. Where appropriate, the FMEA analysts will provide a recommended solution to the problem. To complete the loop, the designers return the updated drawing and, subject to a satisfactory resolution, the corrective actions taken are indicated on the Report Form.

The Report Forms are also held in the FMEA database for ease of retrieval, sorting, and transmission by e-mail.

3.2.3 Vessel Audits

From time to time over the course of the vessel build, audits are carried out to ensure that the vessel is being built as designed. Much of the audit is taken up with physically checking compartments containing DP related equipment. The equipment layout is observed to verify that the DP equipment is not vulnerable to failure due to failures in other equipment in the same compartment. For example, failure in a flange in a water pipe could cause failure of DP electronics if the equipment was arranged such that water spray could hit the electronics. Another aspect of the physical inspection is to assess the operator action required to deal with equipment failure. That is, is it reasonable to expect that, in the event of a particular failure, the operator can carry out the proper corrective action in a timely manner so that the vessel does not go off location.

Part of the analysis for Class 2 and Class 3 vessels includes review and verification of equipment powering. As an aid to the review, a list of all equipment necessary for station keeping and the location from which it is powered is setup in the FMEA database. The powering is then verified during audits.

Verification of cable routing is also part of the analysis. It is usually not possible to perform a complete check on cable routing as the cost/time resources required are too great. Some shipyards have a cable routing data base which makes the analysis easier (depending somewhat on data content), though generally only drawings are available. The paper analysis can verify the routing concept but it ultimately comes down to the installation team.

The designers, installation foremen, and the owner's inspectors should have a sound appreciation of the redundancy philosophy. The designers need to be aware of what cables require segregation and how to run the cables to ensure segregation. The foremen should also have this awareness as it has been known for corners to be cut in the installation stage to make installation easier and/or to save on cable. The owner's inspectors need to make spot checks to ensure that proper cable routing practice is being followed.

3.3 Test and Commissioning

The DP system of a vessel is a dynamic system, made up of subsystems which dynamically interact with each other. Commissioning and testing normally carried out by shipyards and equipment vendors tends to test at the subsystem level without fully testing the total "DP system". Also, vendor commissioning and Customer Acceptance Tests (CAT's) are primarily focused on demonstrating the correct functioning of their systems in the fully operational (i.e., no fault) condition. FMEA tests are designed to test the full "DP system" and demonstrate system redundancy and the fault-tolerance of the overall DP system to failures of individual pieces of equipment in the various subsystems. To accomplish this goal, FMEA tests are carried out both dockside and as an integral part of sea trials.

FMEA testing has multiple objectives,

1) The findings of the paper FMEA are confirmed (or otherwise).
2) The failure modes and effects of "gray areas" (areas which could not be adequately analyzed by study of system drawings and vendor documentation) are established.

3) Correct system wiring is confirmed (or otherwise).
4) As the FMEA concentrates on analyzing hardware failures, the tests demonstrate and verify the response of control software that contributes to the correction of a hardware failure.
5) Operational personnel are able to witness first hand the effects of failures.
6) Information is gathered to allow updating of the FMEA database to reflect the "as built" configuration of the vessel.

In general Classification Societies will require some FMEA proving trials, in addition to the DP vendor CAT, to verify system redundancy for Class 2 or 3 vessels. The Classification Societies are not, however, obligated or desirous to carry out any FMEA testing beyond what is required for Class notation. Thus, if the owner's redundancy philosophy/specification is such that it does not exactly coincide with Class rules (as is normally the case), then the required Classification Society failure mode testing will not adequately test the system. For example, it may be that a vessel is specified to have a Class 2 notation, but is designed to have redundancy over and above Class 2 requirements (i.e., an enhanced Class 2). It is therefore up to the owner to ensure that adequate FMEA tests to demonstrate and validate the enhanced features of the system are included in the yard tests and trials.

If a vessel is to be thoroughly tested, the coordination of interface checkout and devising of tests should be undertaken by a very small team of specialists who have a sound knowledge of the concept of redundancy and a "helicopter view" of the whole DP system (DP Coordination Team). This approach can be extended to other vessel systems such as the vessel management system and safety systems.

During the Test and Commissioning phase the scope of the FMEA testing is established by the FMEA team and coordinated with the owner and yard test teams well before trials commence. The FMEA team generates the FMEA test list and corresponding test procedures. Tests which can be carried out dockside are identified and the remainder are integrated into the sea trials testing.

The FMEA test procedures describe the purpose of the test, the vessel and equipment setup for the test, how the equipment failure is to be induced or simulated, and the expected results of the test (i.e., the effects of the failure). A section in the test procedure is provided for documenting the actual test results. The test list/procedures are included in the FMEA database.

Practical FMEA testing must be a structured and well coordinated exercise. Alarm and event logging must be 100% operational and a suitable number of personnel for witnessing the tests must be arranged. The test procedures should be reviewed by all participants so that the procedures and expected failure effects are well understood.

It should be stressed that, should any problem be found during trials, it is better found at this time than later when the vessel is working.

4.0 FMEA Documentation and Ongoing QA

FMEA documentation consists of the Redundancy and Fault Tolerance Statement (Redundancy Philosophy, Operational Philosophy, Redundancy Specification), The FMEA Worksheets, FMEA Report Forms, and FMEA Test Procedures contained in the FMEA database, and FMEA Reports which are issued at the completion of each FMEA Phase. The FMEA Final Report is issued after completion of sea trials.

It is intended that the FMEA Final Report be held on board the vessel in hard copy and electronic (with accompanying FMEA database) format as part of the Quality Management System of the vessel. The FMEA should be made available to all of the vessel's staff who operate or maintain the DP system. As modifications which have a bearing on the DP system are made to the vessel, the FMEA should be reviewed and updated to reflect the changes. Any recommendations arising from the review should be acted upon accordingly.

Assuming it is possible, workscope and worksite permitting, the vessel should be put through a series of DP tests on an annual basis. This will confirm that the system is functioning correctly and that responses to equipment failures are as expected. It also provides new operators that extra knowledge of how the system responds to failures, knowledge which may be crucial in an emergency.

The yearly test results are incorporated into the FMEA database. Any auditor visiting the vessel during the intervening year would confine testing to alarm demonstrations and function tests.

5.0 Conclusions

FMEA is a tool which has been around for years and has been recognized in many industries as forming an essential part of the design process, from concept to putting to work. This being the case, it is puzzling that FMEA has not been utilized in this manner more than it has been before in the Offshore Industry. Typically for DP vessels the FMEA is commenced late in the project whereby it confirms or otherwise the design intent but it is often too late to do anything about identified problems without major surgery. This leaves operational procedures as the only safeguard. For maximum benefit, the FMEA must be initiated at as early a stage as possible so as to influence decisions in the design stage.

During the FMEA process a considerable amount of data gathering and information exchange takes place. The setting up of a FMEA database, as described in this paper, greatly facilitates data organization, distribution, and analysis.

Even though the paper FMEA will be thorough, FMEA testing of the "total DP system" during commissioning and sea trials is essential. It is not sufficient to rely on shipyards and/or Classification Societies to develop FMEA test programs. Owners must take steps to ensure that adequate measures are taken to thoroughly test and validate the DP system.

The FMEA information should become a part of the Vessel Quality Management System and be kept up-to-date reflecting modifications to the vessel. Yearly testing should be carried out to insure that the DP system is functioning correctly and that system response to failures is as expected.

Appendix 1

FMEA Worksheet Components

1. Worksheet ID

2. Equipment Component Identification

3. Function: Concise statement of the function performed by the hardware item.

4. Operation Mode: Operational mode in which the failure occurs.

5. Failure Modes and Causes

6. Failure Effects

7. Failure Detection: A description of the means by which the operator determines that a failure has occurred.

8. Compensating Provisions: The compensating provisions, either equipment redundancy, control system response, or operator action, which circumvent or mitigate the effect of the failure.

9. Impact on DP Capability

10. Severity Classification: Severity classification based on the impact of the failure on DP capability. The severity classification is composed of three elements.

Severity Level	Operator Fault Management	Redundancy Limitation
1. Catastrophic	1. Immediate	R
2. Critical	2. Moderate	
3. Serious	3. Observational	
4. Marginal		
5. Minor		

11. Remarks

12. Testing: Description of any special testing required with respect to the failure mode and/or its consequences.

Appendix 1

FMEA Worksheet

1. Worksheet ID

2. Equipment Component Identification

3. Function: Concise statement of the function performed by the hardware item.

4. Operation Mode: Operational mode in which the failure occurs.

5. Failure Modes and Causes

6. Failure Effects

7. Failure Detection: A description of the means by which the operator determines that a failure has occurred.

8. Compensating Provisions: The compensating provisions, either equipment redundancy, control system response, or operator action, which circumvent or mitigate the effect of the failure.

9. Impact on DP Capability

10. Severity Classification: Severity classification based on the impact of the failure on DP capability. The severity classification is composed of three elements.

Severity Level	Operator Fault Management	Redundancy Limitation
1. Catastrophic	1. Immediate	R
2. Critical	2. Moderate	
3. Serious	3. Observational	
4. Marginal		
5. Minor		

11. Remarks

12. Testing: Description of any special testing required with respect to the failure mode and/or its consequences.