The International Marine Contractors Association

Guidance on Failure Modes & Effects Analyses (FMEAs)

www.imca-int.com

IMCA M 166
April 2002

The International Marine Contractors Association (IMCA) is the international trade association representing offshore, marine and underwater engineering companies.

IMCA promotes improvements in quality, health, safety, environmental and technical standards through the publication of information notes, codes of practice and by other appropriate means.

Members are self-regulating through the adoption of IMCA guidelines as appropriate. They commit to act as responsible members by following relevant guidelines and being willing to be audited against compliance with them by their clients.

There are two core committees that relate to all members:

- Safety, Environment & Legislation
- Training, Certification & Personnel Competence

The Association is organised through four distinct divisions, each covering a specific area of members' interests: Diving, Marine, Offshore Survey, Remote Systems & ROV.

There are also four regional sections which facilitate work on issues affecting members in their local geographic area – Americas Deepwater, Asia-Pacific, Europe & Africa and Middle East & India.

IMCA M 166

This report was prepared for IMCA, under the direction of its Marine Division Management Committee, by Wavespec.

www.imca-int.com/marine

CONTENTS

EXECUTIVE SUMMARY **2**

INTRODUCTION: **8**

CHAPTER 1: FAQS **9**

What is an FMEA? 9
What are the objectives of an FMEA? 9
What does an FMEA contain? 9
Who wants an FMEA and why? 10
When is an FMEA carried out? 10
What is needed to perform an FMEA? 11
Who carries out an FMEA? 11
What standards are used for an FMEA? 11
What practical FMEA tests are required? 12
What types of unacceptable failure modes have been uncovered by FMEAs? 12
What is done when an unacceptable failure mode is identified? 12
Who decides what is an acceptable solution to the unacceptable effects of a failure mode? 13
Is it necessary to carry out a physical inspection of the equipment being analysed? 13
How often should the FMEA be updated? 13
What is a Criticality Analysis? 13
What does a formal FMEA cost? 14

CHAPTER 2: MURPHY'S LAW AND FMEAS **15**

2.1 Murphy's Law 15
2.2 The FMEA in the Design Process 15
2.3 The FMEA Objectives 16
2.4 How Did FMEAs Start? 16

CHAPTER 3: FMEA STANDARDS & THE CLASSIFICATION SOCIETIES **17**

3.1 Standards 17
3.2 Classification Societies 18

CHAPTER 4: DP FMEA – HOW FAR DO WE GO? **20**

4.1 How Far Do We Go? 20
4.2 Bottom Up or Top Down? 20

CHAPTER 5: THE FMEA PROCESS 22
5.1 The Process 22
5.2 Selecting the Team 22
5.3 Defining the Standard 23
5.4 Defining the Reporting Procedures 23
5.5 Defining the Boundaries of the System to be Analysed 23
5.6 Organising System Design Information 26
5.7 Evaluating the Effects of each Failure Mode on the System 29
5.8 Identifying Failure Detection Methods/Corrective Actions 30
5.9 Recommendations 30
5.10 The FMEA Report 31
5.11 FMEA Documentation and Ongoing QA 32

CHAPTER 6: VESSEL AUDITS AND PRACTICAL FMEA TESTING 33
6.1 Vessel Audits 33
6.2 Arranging Practical FMEA Tests, Dockside/At Sea/On Full DP 33

CHAPTER 7: OPERATIONS AND MAINTENANCE 36

CHAPTER 8: ADDITIONS TO THE FMEA PROCESS 37
8.1 Criticality Analysis 37
8.2 Qualitative and Quantitative Risk Assessment (QRA) 38
8.3 Criticality and Probability 38
8.4 Fault Tree Analysis and Event Tree Analysis 39
8.5 RAM (Reliability, Availability and Maintainability) 40
8.6 Software for FMEA 41
8.7 FMEA on Control Software 41

APPENDIX 1: DEFINITIONS OF TERMS USED IN THE FMEA PROCESS 42

APPENDIX 2: EXAMPLE OF AN FMEA WORKSHEET AND DESCRIPTION OF THE FMEA WORKSHEET FIELDS 44

APPENDIX 3: BACKGROUND AND EXPLANATIONS OF DP CLASS 2 AND CLASS 3 48

APPENDIX 4: TYPES OF DP FAILURE MODE UNCOVERED BY FMEAS 57

APPENDIX 5: REFERENCES 64

This document and the advice contained in it may change with developments in the industry. It is intended to review the guidance and make any necessary improvements on a regular basis.

Any person with suggested improvements is invited to forward these to IMCA.

EXECUTIVE SUMMARY

This Executive Summary is designed in a *what, why, when, how* format to allow the reader a relatively quick overview of the main issues surrounding an FMEA which are contained in the main part of the Guidance Document itself. It does not attempt to give comprehensive answers to the frequently answered questions (FAQs), which are addressed in the main document. The summary includes an FMEA Process Flow Sheet, which provides an overview of the processes involved in carrying out an FMEA. An FMEA can be applied to any item, system or process that could fail.

WHAT

What is an FMEA?

A systematic analysis of the systems to whatever level of detail is required to demonstrate that no single failure will cause an undesired event.

What are its objectives?

To identify potential design and process failures before they occur and to minimise the risk of failure by either proposing design changes or, if these cannot be formulated, proposing operational procedures. Essentially the FMEA is to:

- Identify the equipment or subsystem, mode of operation and the equipment;
- Identify potential failure modes and their causes;
- Evaluate the effects on the system of each failure mode;
- Identify measures for eliminating or reducing the risks associated with each failure mode;
- Identify trials and testing necessary to prove the conclusions; and
- Provide information to the operators and maintainers so that they understand the capabilities and limitations of the system to achieve best performance.

What does it contain?

The report will be structured to outline the findings that have been developed from worksheets. The findings will concentrate on the failure modes found which would have significant effects on the system and grade them into categories, e.g. catastrophic, critical, etc, down to minimal or nuisance value. An FMEA covering the complete system (which may include FMEAs of various subsystem manufacturers) should encompass those FMEAs by a review and an analysis of the interfaces between the subsystems. An FMEA should contain a practical test programme and the results from those tests.

What practical tests are required?

During the course of the analysis, there will be failure modes that are difficult to assess, so during the analysis a series of tests are devised to assess those failure modes in practice.

What types of failure mode have been uncovered by FMEAs?

Many types of failure mode have been revealed during an FMEA. Numerous examples are given later in this document.

What is criticality analysis?

FMECA or Failure Modes, Effects and Criticality Analysis is an extension to the FMEA process with the addition of a risk (criticality) assessment. Risk is a measurement of the combination of the consequence of a failure mode and its probability of occurrence. The results of the risk assessment can be prioritised to indicate high risk failure modes that should receive risk reduction considerations.

WHY

Who wants one and why do they want one?

It is both common sense and responsible design practice to carry out an FMEA on an item of equipment or a system whenever it is required to work in an environment where any failure mode has the potential for a catastrophic effect on the process. The organisations and persons who want an FMEA may include:

- *Classification Societies* - who require an FMEA as part of the acceptance criteria for IMO Class 2 and Class 3 type DP vessels.
- *Charterers* - who will require an FMEA so that they can have confidence that the vessel is fit for purpose. An appropriate FMEA will give an enhanced comfort factor that the operation will be performed without problem or risk.
- *Owners* – who require an FMEA to satisfy a charterer's needs and to give themselves confidence in the safety and robustness of their operations.
- *Operators* – who require an FMEA so that procedures can be developed to mitigate the effects of any failure modes.
- *Maintenance staff* – who require an FMEA so that any critical areas which could give rise to a serious problem in the event of a failure can be targeted by planned maintenance techniques during periods of downtime.

WHEN

When is an FMEA carried out? (new vessel/existing vessel)

The FMEA should be commenced at the earliest stage that the design and development programme will allow – even to assist at a higher level in identifying potential weaknesses during the conceptual design.

If the vessel is in the process of design or construction, then the detailed FMEA should run in parallel with the design process, with any FMEA testing deemed necessary being integrated into the shipyard sea trials programme. If the vessel is an existing vessel then the FMEA can be carried out at any time though the FMEA tests will require to be programmed during a convenient period of downtime.

HOW

How is the FMEA Process Progressed?

- Selecting the team
  - Nominating the required specialists
- Defining the standard
- Defining the reporting procedures
  - e.g. FMEA Team → Client Focal Point → Designers → Client Focal Point → FMEA Team.
- Defining the boundaries of the system to be analysed
  - The benefit of block diagrams. These break the DP system down from a high system level to lower system levels to give a graphic representation of how each system level interacts with another.
- Organising system design information
  - Drawing log
  - Question and Answer ("Q&A") Punchlists
  - Worksheets
  - FMEA Report Forms
  - Traceability of information
  - Evaluating the effects on the system of each failure mode
- Identifying failure detection methods/corrective actions
- Formulating practical FMEA tests, dockside/at sea/on full DP
  - A comprehensive trials programme will establish conclusively the failure effects of certain modes of failure that the desk top study has failed to establish. The intention is, essentially, to confirm failure modes and not test the whole system for correct installation.
- Recommendations
  - Grade each into, for example, A) For Immediate Action, B) Important and C) Nice To Have. List of recommendations.
- Conclusions
- FMEA report structure
  - Formulation of report template.

How is the FMEA presented?

This document gives guidance on what form the FMEA deliverables should take.

How often should the FMEA be updated?

The FMEA should grow and mature with the life of the vessel. Any changes to the design of systems relevant to the DP should be analysed in line with the original FMEA and recorded as annexes to the FMEA. At suitable intervals,

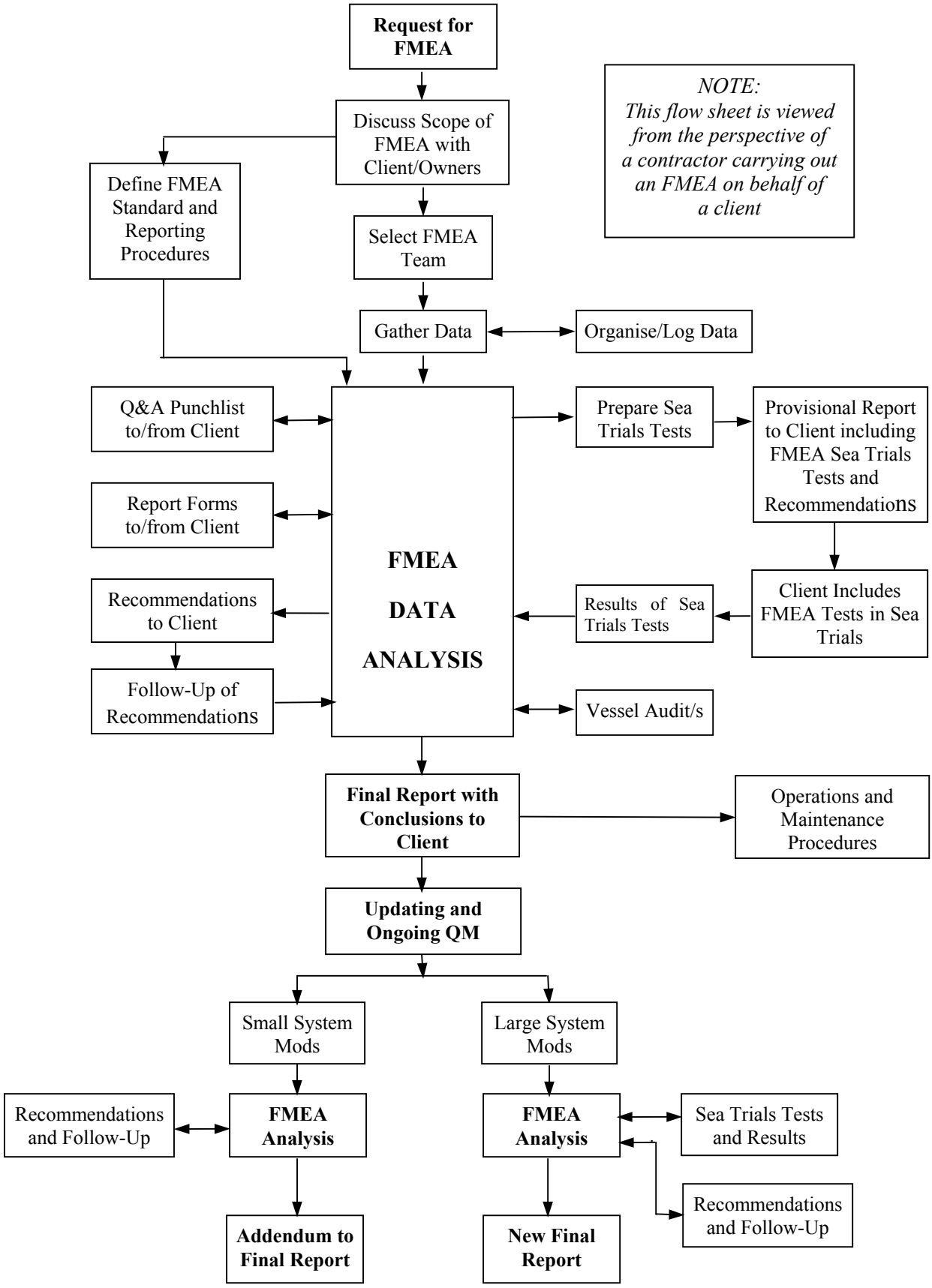
depending on the number of relevant design changes made, the FMEA should be formally updated.

Extensions to The FMEA Process

The following are also briefly discussed in this document:

- Criticality Analysis
- Failure Probability Determination – Qualitative and Quantative
- Fault Tree Analysis
- Event Tree Analysis
- RAM (Reliability and Maintainability)
- Software for FMEA
- FMEA on control software

FMEA Process Flowsheet



INTRODUCTION

This guidance document was commissioned by IMCA to highlight best practice in the use of Failure Modes and Effects Analysis (FMEA) techniques when applied to the technical systems associated with offshore vessels. An FMEA is an easy to use yet powerful pro-active engineering quality tool that assists in the identification and countering of weak points in the early design phase of products and processes. Whilst the emphasis of this document is on dynamic positioning (DP) systems, FMEA techniques can be applied to any system, whether applied to land, sea or air based equipment or systems, in which it is required that "no single failure shall cause a total failure of the system or process".

The document firstly answers frequently asked questions (FAQs) relating to FMEAs and explains the background to FMEA work and the role of FMEAs in Classification work. The depth of FMEA reporting, the procedures and the format of the final FMEA report are discussed. Finally, the additions to the FMEA process, which can compliment the analysis, are briefly explored.

When progressing through this document, it should be remembered that the FMEA process itself is not sufficient to ensure a meaningful analysis. It is a tool to assist in carrying out a job. A tool in the hands of an inexperienced craftsman will not produce a good product and so it is with an FMEA. An analyst expert in the use of FMEAs and fully conversant in the architecture and operation of the system or process to be analysed, is essential to ensure a good final product.

1 FAQS

This opening chapter is based on FAQs, or "Frequently Asked Questions", relating to FMEAs. Each question and answer is intended to be a brief idea of the type of question raised relating to FMEAs and, in most cases, the answer will lead the reader on to more in-depth discussion in a later Chapter. Each FAQ will be cross-referenced to sections later in the report where relevant.

What is an FMEA?

An FMEA is a design tool that has been around for many years and is recognised as an essential function in design from concept through to the development of every conceivable type of equipment. It is commonly defined as "a systematic process for identifying potential design and process failures before they occur, with the intent to eliminate them or minimise the risk associated with them". FMEA procedures are based on standards in the reliability engineering industry, both military and commercial.

(Refer to Chapter 2)

What are the objectives of an FMEA?

The fundamental purpose of an FMEA is to prove that the worst case failure in practice does not exceed that stated by the designers in the functional design specification. Where DP is concerned, the objective is to develop a fault tolerant system that can not only hold station in the face of adverse circumstances, but allows faults to be corrected as they occur, without jeopardy to the operation at hand.

(Refer to Chapter 2 Section 2.3)

What does an FMEA contain?

The scope of the FMEA should be established at the outset. In the case of a DP vessel, it should encompass all those parts of the system involved in stationkeeping, e.g. DP control system, power generation and distribution, power management, thrusters and propulsion, DP environment and position sensors.

The FMEA report itself is structured to outline the findings which have been developed from FMEA Worksheets, which are tabular forms recording the findings. The findings will concentrate on the failure modes found, which would have significant effects on the station keeping ability of the vessel and are graded into categories, e.g. catastrophic, critical, etc, down to minor or nuisance value. It should contain a practical test programme, which, in the case of a DP vessel, is carried out mainly at sea when in full DP mode, together with the test results. The FMEA will usually contain recommendations that improve the design, which need to be adequately addressed in the FMEA process. The structure of an FMEA can be found in Chapter 5, Section 5.10.

An FMEA covering the complete DP system, which may include the FMEAs of various subsystem manufacturers, should encompass those FMEAs by a review and an analysis of the interfaces between those subsystems.

Who wants an FMEA and why?

Whenever the function of an item of equipment or system is for it to work in an environment in which any failure mode has the potential for a catastrophic effect on the process, it is common sense and responsible design practice to carry out an FMEA. Consequently, a number of people, organisations, bodies, etc., should be very interested in the findings of an FMEA. These include:

- Classification Societies, who require an FMEA as part of the acceptance criteria for IMO Class 2 and Class 3 type DP vessels. Whilst not actually specifying FMEA, the US Code of Federal Regulations requires a qualitative failure analysis technique to be applied to vital marine automation systems and an FMEA is usually the technique applied.

- National regulatory authorities, who often require an FMEA as part of the safety case for an offshore installation or DP vessel.

- Charterers, who will require an FMEA as part of the vessel acceptance criteria so that they can have confidence that the vessel is fit for purpose. A thorough FMEA will give an enhanced comfort factor that the operation will be performed with the minimum of disruption.

- Owners, who require an FMEA to satisfy a charterer. It is also common sense for an Owner to have a thorough FMEA carried out on his vessels as it provides him the assurance that any risk has been minimised, if not eliminated. The FMEA should be one of the inputs to the overall "Safest Operating Mode" analysis for a DP vessel.

- Operators, who require an FMEA so that procedures can be developed to mitigate the effects of any failure modes. The FMEA will assist in development of the operations manuals and training programmes.

- Maintenance staff, who require an FMEA so that any critical areas which could give rise to a serious problem in the event of a failure can be targetted by planned maintenance techniques during periods of downtime.

(Refer to Chapter 3 Section 3.1, etc)

When is an FMEA carried out?

Ideally, the FMEA should be initiated at as early a stage in the design process as possible, and then run in parallel with the design phase. Where DP is concerned, on new builds and conversions, the vessel owner or yard typically contracts for the study near the end of the vessel construction or conversion phase with the objective of identifying any single point failures. Although well intended, this is akin to using the FMEA as the means to confirm that the horses haven't escaped after the stable door has been bolted. It is, therefore, often too

late to do anything about identified problems without major surgery. For maximum benefit, the time to identify and eliminate or mitigate the effect of equipment failure is during the design process, not in the latter stages of vessel construction or conversion.

(Refer to Chapter 2 Section 2.2)

What is needed to perform an FMEA?

Once the FMEA team has been selected and the scope, standard and format of the FMEA have been agreed and the administration of the documentation has been put into place, full co-operation is required from shipyard, owners, operators, vessel's staff and any others involved in the design process. Access will be required, to all documentation relating to the DP system, i.e. DP control system, electrical systems, machinery systems, machinery control systems, and all the equipment necessary to maintain the vessel on station. All relevant information should be made available from the shipyard (if a new vessel in the process of build), from the vessel's Owners/Operators or from the vessel itself. A physical inspection may also be necessary and access to the vessel will have to be arranged.

(Refer to Chapter 5)

Who carries out an FMEA?

An FMEA team should be gathered together, which includes specialists each having a discipline in each of the systems required in the design process, e.g. machinery systems, electrical systems, DP control systems and other control systems. It is also likely that access to specialist advice from naval architects and operations personnel will be required.

(Refer to Chapter 5 Section 5.2)

What standards are used for an FMEA?

There are a number of standards to which an FMEA can be carried out. The use of standards is important so that the FMEA will be accepted by all parties interested in it.

Using a common standard for an FMEA has other benefits; such as the customer gets a report to a consistent standard and the companies bidding to carry out FMEA will also benefit because they will have a level playing field

Standards include:

- US Department of Defense MIL-STD-1629A,
- CEI/IEC812 – Analysis techniques for system reliability - Procedure for failure modes and effects analysis (FMEA)
- BSI (BS 5760-5:1991 (Reliability of systems, equipment and components. Guide to failure modes, effects and criticality analysis).

- IMO MSC Resolution 36(63) Annex 4 – Procedures for Failure Mode and Effects Analysis (Whilst this is primarily for high speed craft, it gives good guidance on FMEA procedures).

(Refer to Chapter 3 Section 3.1)

What practical FMEA tests are required?

During the course of the analysis, there will be failure modes that are difficult to assess. In the case of a DP system, it is by definition a dynamic system with many parts interacting with each other. When the effect of a failure mode cannot be firmly established as a result of the desktop study, an FMEA test trials programme is devised to assess the failure mode in practice.

On completion of the FMEA trials programme, any recommendations that arise from the results of the trials should be assessed to ensure that the correct action is taken and that the required verification is completed to allow close out in each case. These tests together with the results will form part of the final FMEA report.

The FMEA trials test programme should be developed into an Annual DP Trials Document that will be used as the ongoing acceptance criteria for DP vessels.

(Refer to Chapter 6 Section 6.2)

What types of unacceptable failure modes have been uncovered by FMEAs?

Many types of failure mode have been revealed by an FMEA, each having different failure effects on the overall system; from ones of solely nuisance value to others that could have resulted in events of catastrophic proportion if left undetected. This is due to the searching nature of the FMEA process. Significant types of failure mode that have been revealed during FMEAs, including some failure modes revealed that could have had a major effect on a DP system, are discussed in Appendix 4.

What is done when an unacceptable failure mode is identified?

The FMEA administration process should contain a reporting procedure so that, as soon as a failure mode is uncovered that has the potential to result in an undesirable effect on the system, it can be notified to the client and the system designers. It should be documented on a dedicated form called an FMEA Corrective Action Report Form and forwarded to the designers with a suggestion for design correction or, if this is not possible, a suggestion to adopt operational measures to reduce the risk.

(Refer to Chapter 5 Section 5.6)

Who decides what is an acceptable solution to the unacceptable effects of a failure mode?

The solution should be discussed with the Owner and the design team. Sometimes the charterer is included if they are party to the FMEA procedure. A charterer may put pressure on an Owner to make design changes, but, naturally, it depends on when the unacceptable failure mode is uncovered; as the later it is uncovered the more difficult it is to rectify, and hence there is more time and cost penalty.

Any major change to the system would also have to be discussed with Class to determine whether or not it contravened their requirements.

Is it necessary to carry out a physical inspection of the equipment being analysed?

If the design of the equipment being analysed is still on paper then clearly this is not possible. However, if the equipment is being built or is already built then a physical inspection is recommended. In the case of a DP vessel, say, which is in the process of construction, there is scope for a number of visits to the vessel to audit the build progress and check the installation of equipment. In this way, it can be seen how it is being installed and how other items of equipment are located in relation to equipment under analysis, to see if a failure of one will have an impact on the other.

(Refer to Chapter 6 Section 6.1)

How often should the FMEA be updated?

The FMEA should grow and mature with the life of the vessel. Any changes to the design of the equipment or systems, covered by the FMEA, should be analysed in line with the original FMEA and recorded as annexes to the FMEA. At suitable intervals, depending on the number of relevant design changes made, the FMEA should be formally updated.

(Refer to Chapter 5 Section 5.11)

What is a Criticality Analysis?

An FMECA, or Failure Modes, Effects and Criticality Analysis, is an extension to the FMEA process by the addition of a criticality assessment. It is effectively a means of estimating how often each item in the system will fail, usually by using actual failure data gathered in the field, and then calculating how often the whole system will fail. Whilst in knowing a system will fail, say, every 10 years, it is not known when it will fail. However, the added benefit is in knowing which areas in the system are likely to be less reliable, and either the system is redesigned to increase reliability or maintenance routines can be modified to concentrate on these areas. Obviously, this extra work will drive up the cost of the overall analysis, as would other extensions to the FMEA process, such as fault tree analysis, and it is generally the sponsor of the analysis who decides whether or not it is appropriate.

Risk is a measurement of the consequence of a failure mode related to its probability of occurrence (criticality). The results of the risk assessment can be prioritised to indicate high risk failure modes/ items/ systems that should receive risk reduction considerations.

(Refer to Chapter 8 Section 8.1)

What does a formal FMEA cost?

It is difficult to put a figure on the cost of an FMEA as it would clearly depend on the complexity of the equipment or system under analysis. In the case of a new build vessel, the FMEA process can run for a considerable number of months, though not necessarily on a continuous basis, and as a result incur a significant cost. In cases where the design process is short, the FMEA may only take days or weeks. So the cost will depend on the effort necessary to produce a meaningful analysis.

In the course of carrying out an FMEA, if the design is proven to be sound and no significant single point failures are found, then it would be quite natural for the ship owner or client commissioning the FMEA to ridicule it and call it a waste of money. But this should not be so. A thorough FMEA will mean that the design has undergone a rigorous analysis. The designers will get a pat on the back for catering for all eventualities, and the operator and charterer will be able to sleep peacefully in the assurance that all exposure to risk of DP failure has been minimised as far as is reasonably practicable. However, if a significant failure mode is found, then the additional cost of carrying out the FMEA is small when compared to the potential effect that that failure mode could have. It is not just the cost to the owner of a lost day's hire or more. The cost of the FMEA could pale into insignificance when compared to the cost due to the potential for loss of life or limb and damage to installations and the environment that could result from a hidden fault. The results of a thorough FMEA can also be used to refine maintenance routines that can produce operational savings.

(Refer to Chapter 4)

2 MURPHY'S LAW AND FMEAS

2.1 Murphy's Law

"Everything that can fail, shall fail". This is known as Murphy's Law and is one of the main reasons behind the FMEA technique. Experience shows that we can add to this "….and it will usually fail at the worst possible moment!"

Consequently, during the design of a system or product, the designer must always think in terms of:

- What could go wrong with the system or process?
- How badly might it go wrong?
- What needs to be done to prevent failures?

2.2 The FMEA in the Design Process

The FMEA technique is an iterative process that promotes systematic thinking during the design phase of a system or product. It is a design tool that has been around for a number of years and is used as a means of identifying single point failures or common mode failures in the design of any type of equipment, whether it is a simple widget or a complex system such as a DP system. When used in this manner, the FMEA is carried out in the form of a desktop study.

Ideally, the FMEA should be initiated as early as possible and then run in parallel with the design phase. One of the major limitations imposed on design, production and testing is time, and, in the case of a DP vessel, the build or conversion process for a vessel can involve continuous design changes and delays in producing final drawings. When everyone is up against a tight delivery deadline (in terms of both schedule and cost), there can often be major resistance from both project team members and contractors to the challenges and questions resulting from an FMEA study.

Thus, the earlier in the project schedule that the FMEA requirements are known, the easier it is to ensure that they are met. If the high level design issues can be known and analysed during the early stages, then the more detailed and in-depth analysis can be programmed and achieved before time constraints intervene. Commissioning and delivery pressures are not the right environment under which to argue the scope of work of the FMEA. The FMEA must, therefore, be initiated at as early a stage in the design process as possible, and at a time when there is something to analyse. It should then continue to run in parallel but slightly lagging the design effort.

For a new vessel, this approach should be taken, with any FMEA testing deemed necessary being integrated into the shipyard sea trials programme. If the vessel is an existing vessel, then the FMEA can be carried out at any time, though the FMEA tests will need to be programmed during a convenient period of downtime.

Also, with regard to DP, the FMEA is usually applied to vessels with redundant, or duplex, systems to confirm that the design intent with regard to redundancy is achieved. However, FMEA techniques can be applied to non-redundant, or simplex, systems. Obviously, a single failure will mean loss of the system function, but the FMEA will be able to pin point areas where inexpensive changes could be made that will increase the availability of the system, for example, adding duplicated power supplies.

2.3 The FMEA Objectives

The FMEA should give a description of the different failure modes for all the items of equipment in respect of their functional objectives. In this way, all catastrophic or critical single point failure possibilities can be identified, and either eliminated or minimised at an early stage in the project through design correction or the introduction of clear operational procedures. The FMEA considers a single failure only at any one time (single point failure). A failure that is not revealed to an operator by way of monitoring and alarm is classed as a hidden failure. These failures, such as a backup unit without a failure alarm, must also be considered.

Essentially the FMEA is to:

- Identify the equipment or subsystem, mode of operation and the equipment;
- Identify potential failure modes and their causes;
- Evaluate the effects on the system of each failure mode;
- Identify measures for eliminating or reducing the risks associated with each failure mode;
- Identify trials and testing necessary to prove the conclusions; and
- Provide information to operators and maintainers of the system in order that they understand the capabilities and limitations of the system to achieve best performance.

2.4 How Did FMEAs Start?

The FMEA discipline was developed in the United States military. Military Procedure MIL-P-1629, titled “Procedures for Performing a Failure Modes, Effects and Criticality Analysis”, is dated November 9, 1949. It was used as a reliability evaluation technique to determine the effect of system and equipment failures. Failures were classified according to their impact on mission success and personnel/equipment safety.

The technique has therefore been in use for quite a long time in military circles, particularly the aerospace field. It has evolved over the years, and more and more industries have seen the benefits to be gained by using FMEAs to compliment their design processes, notably the automotive industry.

3 FMEA STANDARDS AND THE CLASSIFICATION SOCIETIES

3.1 Standards

It is important to specify the standard to which the FMEA is to be carried out. The use of a clearly defined methodology for carrying out the FMEA will allow the required in-depth study to be attained without the uncertainty and indiscipline that a less structured approach would bring. Consequently, whoever requires the analysis to be undertaken will know that it has been performed in a structured manner. They will have increased confidence that all parties interested in it will accept the FMEA.

Standards that are usually referred to when carrying out an FMEA include:

- US Department of Defense MIL-STD-1629A,
- IEC Standard, IEC 60812: 'Analysis Techniques for System Reliability -
- Procedure for Failure Mode and Effects Analysis (FMEA)',
- BSI (BS 5760-5:1991 (Reliability of systems, equipment and components. Guide to failure modes, effects and criticality analysis (FMEA and FMECA), and
- IMO MSC Resolution 36(63) Annex 4 – Procedures for Failure Mode and Effects Analysis (Whilst this is primarily for high speed craft under the HSC Code, it gives good guidance on FMEA procedures).

There are other standards, such as that included in the Japanese Industrial Standard, which use similar techniques but the ones above are sufficient for reference purposes.

Where DP vessels are concerned, the FMEA should also make use of all current DP related guidelines that can assist in improving the redundancy and operability of a DP vessel. These include the IMO “Guidelines for Vessels with Dynamic Positioning Systems” (issued as MSC Circular 645 - 1994) and IMCA “Guidelines for the Design and Operation of Dynamically Positioned Vessels” (IMCA M 103 – February, 1999). They give a good guide as to which shipboard systems relating to DP need to be covered.

Specifying a standard will not guarantee an acceptable FMEA but it will guarantee an acceptable procedure and format for carrying out an FMEA. It will not dictate what areas should be analysed in a particular system or to what level of detail they should be analysed. This can only be achieved by an expert analyst fully conversant in the standard selected, the system architecture and the characteristics and performances of the different components of the system.

Also, specifying an FMEA standard will not limit design innovation, as has been stated in some circles. The FMEA does not carry out the design itself but analyses a particular design, be it innovative or traditional design, for weaknesses with respect to failure modes. The IMO FMEA standard quoted in Lloyd’s Rules, IMO MSC Resolution 36(63) Annex 4 – Procedures for Failure

Mode and Effects Analysis, is primarily for high speed craft, the design of which has been quite innovative in recent years.

3.2 Classification Societies

Those Classification Societies allocating notations for DP vessels require an FMEA for DP vessels of Class 2 and Class 3 in order to confirm the levels of redundancy. They will also generally specify to what standard the FMEA should be carried out.

Lloyd's Register (LR) measures FMEAs presented to it against the following standards:

- IEC Standard, IEC 60812: 'Analysis Techniques for System Reliability - Procedure for Failure Mode and Effects Analysis (FMEA)',
- BSI Standard, BS 5760: 'Reliability of Systems, Equipment and Components', Part 5: 'Guide to Failure Modes, Effects and Criticality Analysis (FMEA and FMECA), and
- IMO MSC Resolution 36(63) Annex 4 – Procedures for Failure Mode and Effects Analysis (HSC Code).

LR also gives consideration to the potential hazards (fire and mechanical damage) to cables, pipes and other components relevant to the effective functioning of the DP system. It also uses FMEA techniques to ensure redundancy in the vessel systems classed under the Propulsion and Steering Machinery Redundancy provisional rule notations PMR, SMR or PSMR. These notations are applied to vessels having machinery systems in compliance with the requirements for navigation in sensitive waterways where total loss of propulsion or steering could have a major impact on the environment.

The American Bureau of Shipping (ABS) Rules are intended to be read as a stand alone document and lay down general rules for DP FMEA. These can be found in Part 4, Chapter 3, Section 5, Sub section 15.1.4. Although the Rules only consist of the minimum requirements, it is the responsibility of the designer to ensure all the safety criteria are met. The FMEA document is considered to be acceptable as long as all the relevant information contained therein meets the intent of the Rules. It is very much up to the interpretation of the Rules by the surveyor reviewing the FMEA.

In the July 2001 Rules, Part 6 Chapter 7 Section1 D, Det Norske Veritas (DnV) specify IEC Publication 60812 and IMO MSC Code, Annex 4, to be used as guidance against which all FMEA formats should be gauged. A brief outline of the FMEA requirements is given and, later in the document, states the requirement for a test procedure to demonstrate redundancy in the system. The tests are to be based on the simulation of failures and are to be performed under as realistic conditions as practicable.

It is not intended here to review the requirements of all of the other Classification Societies to carry out FMEAs, but to use the outlines of the requirements of the three societies above to give a general picture of what is generally required.

Both IMO and the classification societies make it incumbent upon the owner to ensure the correct documentation and procedures are in place to obtain the required DP notation, though the level of documentation and the extent of the trials procedure is very much left to the discretion of the responsible surveyor. It seems logical, therefore, that the classification societies should work to common guidelines, though this is not always the case.

The background behind the IMO DP Class 2 and Class 3 requirements, together with the requirements of the DP notations of ABS, Lloyd's Register and DnV compared to the IMO requirements can be found in Appendix 3.

4 DP FMEA – HOW FAR DO WE GO?

4.1 How Far Do We Go?

The answer to this question is, basically, "as far as it takes", meaning that the FMEA should pursue its investigations as far as is necessary to identify all possible failure modes and to confirm the system's responses to those failures. Putting artificial limits on the depth of the analysis, either in the availability of detailed drawings or in preventing specific FMEA trials, say, will not meet the required objectives. After all, at the end of each day, the vessel's owner, operator and charterer will all want to be able to sleep peacefully in the assurance that all exposure to risk of DP failure has been minimised as far as is reasonably practicable. To this end, it must be left to the experience of the FMEA team to assess to what levels the analysis should be taken. Of course, this should not and cannot justify a blank cheque for the FMEA auditor and it would be in nobody's long-term interest if it did.

4.2 Bottom Up or Top Down?

There are two methods in which the data can be analysed. These are the "Bottom Up" method and the "Top Down" method.

In certain circles, an FMEA is described as a bottom up analysis of component-level failures and their effects on higher-level systems. An FMEA that is bottom up can be built upwards from component data by considering first the effects of failure of individual components. The analysis would then progress further to the effects of failure of items made up from those individual components and so on up through the system levels until the system as a whole has been analysed. This is effective but tedious and expensive and has now been all but abandoned, even by the US Military.

To analyse every individual component within a complete DP system would take an inordinate amount of time, money and resources. In an ideal world, where time, money and resources are unlimited, this approach would leave no stone unturned. But, unfortunately, in the real world this is just not the case, so the top down method is used.

A top down FMEA starts from the overall system level and progresses to the next level down, or subsystem level, and on down to the equipment item and component level. However, if it can be justifiably shown that at a certain level between overall system level and component level that there is no further effect on the overall system if a failure occurs, then it is not necessary to continue to the next level down. In this case, it would certainly not be necessary to continue to analyse all of the system levels down to component level. For example, at subsystem level, it is generally acceptable to consider failure of equipment items and their functions, e.g. failure of a pump to produce flow or pressure head. It is not necessary to analyse the failure of components within the pump itself providing the pump has a redundant twin. Component failure within the pump need only be considered as a cause of failure of the pump. This method is not so

thorough as the bottom up method, but is obviously less wasteful of time and effort and hence money, all of which may be in short supply.

Furthermore, for redundant items of equipment carrying out the same duty, if one item has been analysed to component level, it is reasonable to assume that the other item will behave the same as the first item, rendering further component analysis unnecessary. If deeper analysis is deemed necessary, it is not uncommon for local bottom up analyses to form part of an overall top down analysis.

5 THE FMEA PROCESS

5.1 The Process

At the beginning of an FMEA, it is important that a certain number of issues be agreed or set up. These are:

- Selecting the team
- Defining the standard
- Defining the reporting procedures
- Defining the boundaries of the system to be analysed
- Organising system design information

During the FMEA, the process includes:

- Evaluating the effects of each failure mode on the system.
- Identifying failure detection methods/corrective actions.
- Arranging vessel audits.
- Arranging practical FMEA tests, dockside/at sea/on full DP.
- Advising of any recommendations.

Completion of the FMEA entails:

- Producing the FMEA Report

After the FMEA, the following should be addressed:

- FMEA Documentation and Ongoing QA

5.2 Selecting the Team

The team approach is essential in identifying FMEA elements. Although actual document preparation and data input to the FMEA is often the responsibility of an individual, FMEA input should come from a multi-disciplinary team. Each should have previous experience to some degree in carrying out FMEAs. Where DP is concerned, the team should consist of knowledgeable individuals with expertise in systems relating to machinery, control, electrical and naval architecture. They should also have knowledge of design, manufacturing, assembly, service, quality and reliability. The company carrying out the FMEA should make qualifications of the team members available for scrutiny by the client.

A responsible engineer, who is fully conversant with the type of system to be analysed and its intended operation and who has good communication and administration skills, typically leads the FMEA team. Members and leadership may vary as the system design matures. Initially, it is important that some time is taken for the team to get to know the system under analysis.

5.3 Defining the Standard

The standard to which the FMEA will be carried out should be defined. (Please refer to Chapter 3). Any modifications to the standard that may be needed and are specific to the FMEA project in hand should also be defined.

5.4 Defining the Reporting Procedures

Another one of the essential requirements of the FMEA process is effective communication. Frequently, the effectiveness of an FMEA is limited by the lack of awareness of the necessary interface between designers and the FMEA team. Without an efficient interface, the FMEA will not have current design information and could develop without adequate input from the designers. This can have the effect of preventing the improvement in design of a piece of equipment as it evolves, or reaching the wrong conclusions when analysing system design.

Therefore, at the beginning of an FMEA, the reporting procedures should be defined.

For example:

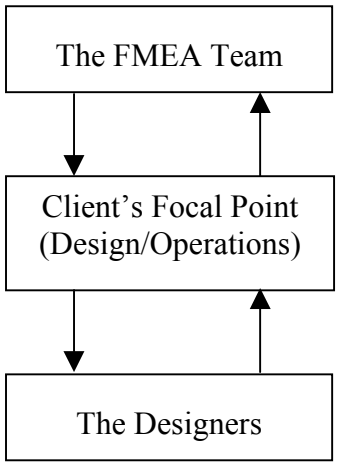


Fig. 5.1: Reporting Procedures

It should be stressed that the team of designers and the FMEA team should operate as parts of an overall 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. Provided the designers carry out the design with failure in mind, then the FMEA is a double check on the process. It is not uncommon that the designers can get involved with a particular problem and not adequately consider whether or not the change violates the original design philosophy and, if so, how it might impact DP system fault tolerance.

5.5 Defining the Boundaries of the System to be Analysed

It is necessary to define the boundaries of the system being analysed, so that all parties involved in the FMEA are aware of the extent of the system to be analysed and in what operating conditions the system is expected to perform.

The functional design specification for the system should provide a definition of the acceptable performance levels from the system when operating in the maximum specified working conditions, both before and following a single failure.

The boundaries of the system consist of the following:

- The physical boundaries, and
- The operational boundaries.

5.5.1 The physical boundaries:

Before proceeding with a detailed FMEA on a particular system, the physical boundaries of the overall system undergoing the analysis should be defined. Systems that appear to be on the periphery of the main control system should undergo a functional failure analysis to ensure that they have no impact on the main control system if they fail and can be excluded from the main analysis. When a DP system is being considered, for example, it is a waste of time and effort to analyse systems such as domestic hot water, if they do not have any bearing at all on the DP system.

It is helpful to use block diagrams when defining the boundaries of the system. These break the main system down from a high system level to lower system levels and give a graphic representation of how each system level interacts with another. The IMO standard quotes: "The functional interdependence of these systems should be described in either block diagrams or fault trees diagrams or in a narrative format to enable the failure effects to be understood". It is believed that a narrative format could possibly leave parts of a system overlooked, unless the analyst carrying out the work is very thorough. Block diagrams or fault trees are graphic methods of presenting the interdependence between elements and are more likely to ensure that no critical element is overlooked.

The block diagrams referred to here are, more specifically, called Reliability Block Diagrams (RBD) and are different to Functional Block Diagrams (FBD). An FBD models the interconnection and relationships among physical system parameters. An RBD connects all parts of the system in order to show the operational relationships between each subsystem or component which are required for successful operation of the overall system.

For example, for an electronic card, the FBD will give the input signal and the output signal. For the same electronic card, the RBD will include a combination of series and parallel blocks, i.e. the amplifiers, the filter networks, the power supplies, and whatever else is necessary for successful circuit board operation. The flow of the signal in the electronics is not important in the RBD, only the chain of required elements needed for successful operation is important. However, individual RBDs will be strung together to form the overall system, so

the functional interdependence between the various RBDs making up the system is still required.

The block diagrams of all major equipment groups are generated from the top level design (i.e., from the single line drawings). They are used to categorise and identify the equipment that will be analysed during the design and construction phase. Where DP is concerned, major equipment grouping is usually organised as follows:

- **Electrical Power:** Generators, high voltage, medium voltage and low voltage AC distribution systems, emergency systems configuration and distribution, power management (including load sharing, load shedding, load reduction, and black out recovery), UPS systems configuration and distribution, low voltage DC distribution systems and control power supplies.

- **Instrumentation and Control:** Thruster control systems, DP control system and interfaces (including position reference systems, gyros, vertical reference sensors and wind sensors), vessel management system, fire and gas systems, emergency shutdown system and data networks.

- **Machinery:** Prime movers, thruster drives, fuel system, freshwater and seawater cooling systems, lubrication systems, compressed air systems, heating, ventilation, and air conditioning.

The examples of block diagrams below serve to illustrate how the system under analysis is broken down into the different levels.

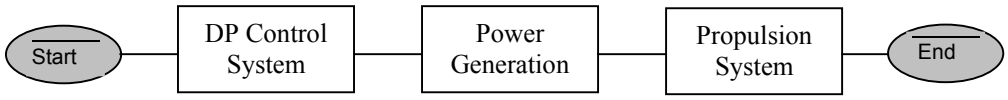


Fig. 5.2: Basic Block Diagram of DP System

Fig. 5.2 shows a block diagram of a basic DP system. As all of the blocks are in series, if any one of the blocks fails completely then the system will fail as there are no redundant or parallel paths.

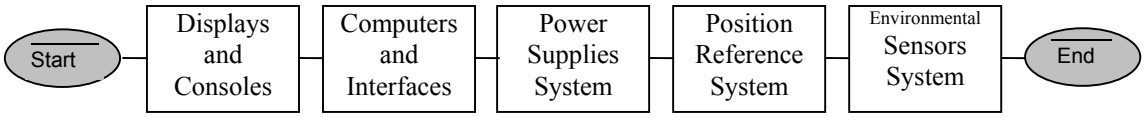


Fig. 5.3: Block Diagram of DP Control System

Fig. 5.3 shows the DP control system block from Fig. 5.2 broken down into its component parts. Again, if any one of the blocks fails completely then the system will fail as there are no redundant paths. In practice, this should not happen as redundancy is built into each of the blocks and the analysis should determine whether or not this is the case.

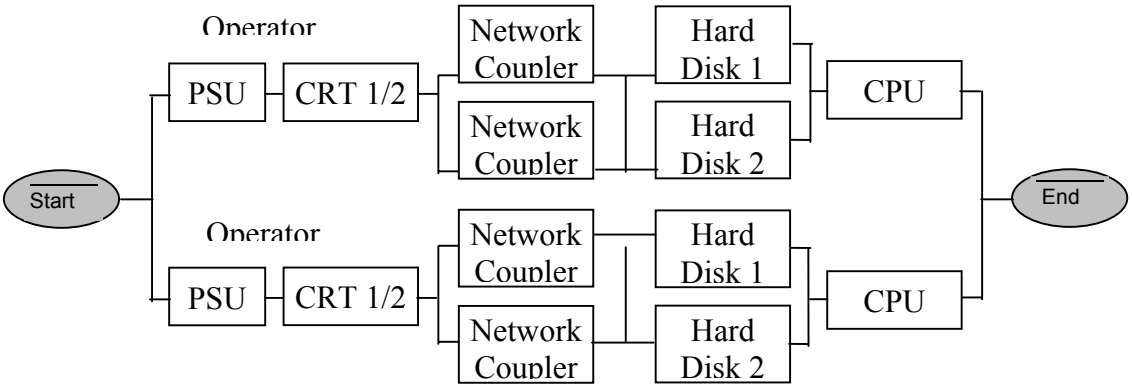


Fig. 5.4: Block Diagram of Display and Consoles

Fig. 5.4 shows an example of how the the Displays and Consoles block from Fig.5.3 can be broken down into its component parts. In this case, there are two operator stations each carrying out the same task (operator interface) and hence two parallel paths. Should one of the parallel paths fail, then the system will not fail as the other path is still available.

Note that for a Failure Modes and Criticality Analysis (FMECA), each block can be assigned a failure rate figure from failure data and the overall system reliability calculated (see Section 8.1).

5.5.2 The operational boundaries:

The environments in which the system is to operate should be defined and the performance level expected in each should be specified. This information is usually to be found in the Functional Design Specification. The performance level should include that for an intact system with no failures and also that for a system suffering a single failure (usually the worst case failure scenario). The functional design specification should define the worst case failure that is acceptable and the FMEA should be undertaken to confirm that the stated worst case failure condition will not be exceeded. Where DP is concerned, these boundaries would include the capability plots.

In conducting the FMEA, consideration should be given to environmental factors such as temperature, humidity and vibration, which could have the same effect on both items in a redundant pair, and to the systems which control these environmental factors. Other consideration should be given to ergonomics and factors which affect human performance.

5.6 Organising System Design Information

There is likely to be a considerable amount of correspondence and design information generated during an FMEA. A tight control is therefore required from the outset when keeping track of the inevitable avalanche of data, and when reporting the failure modes that require attention from the designers.

Also, a considerable number of worksheets are generated, so to assist in this part of the process, the following areas require addressing:

- Document Log Database
- Question and Answer ("Q&A") Punchlists
- FMEA Worksheets
- FMEA Corrective Action Report Forms

All of the documentation should be in a widely accessible format for the design and FMEA teams during and after the FMEA. At some stage in the future, the FMEA may be updated and the documentation will need to be accessed.

5.6.1 Document Log Database

It is of utmost importance, during the FMEA, that all relevant design changes are made known to the FMEA team in a timely manner. At the onset, the FMEA team will receive and review the yard and suppliers' drawing lists and identify drawings that are needed for the analysis. Thereafter, whenever design changes are made and drawings revised, the changes need to be recorded and copies of the revised drawings forwarded to the FMEA team. It is easiest to track all drawings received, reviewed and revised using a database.

The database can be extended to log all in and out correspondence and design information received. Separate databases can be used, if necessary, to record the Question and Answer ("Q&A") Punchlists, FMEA Worksheets and FMEA Corrective Action Report Forms (see below).

5.6.2 Question and Answer ("Q&A") Punchlists

A formal FMEA will inevitably raise questions and in turn generate answers. In order to ensure that all questions and the responses are fully documented, a Question and Answer ("Q&A") Punchlist should be instigated. Questions are added to the list as appropriate and the responses to the questions recorded when received. Each question, together with its answer, should have a discrete number such that, when it is being referred to, it can be traced quickly. There should be fields in the punchlist for the question or item number, the question, the response or answer, and whether the item has been closed out or not. The Question and Answer ("Q&A") Punchlist should form part of the FMEA documentation.

5.6.3 FMEA Worksheets

An FMEA Worksheet is compiled for each equipment failure assessment. An example of a worksheet is shown in Fig. 1 in Appendix 2 and a description of the contents of each field contained in the Worksheet (the worksheet components) is shown in Table 1, also in

Appendix 2. Each worksheet should have a discrete number for traceability purposes.

Some pertinent aspects of the Worksheets are:

- Equipment failures are given a severity classification (based on the consequences of the failure). These consist of the three components given below, but they can be tailored to suit the requirements of the analysis. Normally, in the past, only Component a) has been utilised, but, recently, there have been moves to include one or both of the other two components.

  a) consequences of the failure with respect to the ability of the degraded system to be able to maintain its function. These fall into four categories after the failure, i.e. **1.Catastrophic**, **2.Critical**, **3.Serious** and **4.Minor**.

  b) Consequences of the failure with respect to the impact of the equipment failure on the operator (i.e., operator action required to keep the vessel on station). These fall into three categories after the failure, i.e. **1.Immediate**, **2.Moderate**, and **3.Observational**.

  c) Consequences of the failure with respect to the reduction or loss of system redundancy. These fall into three categories after the failure, i.e. **1.Redundant**, **2.Reduced Redundancy,** and **3.Lost Redundancy**.

  Each category requires a definition. Where DP is concerned, the following are examples of the definitions of the categories in Component a):

  1. **Severity Class 1 – Catastrophic**. A failure due to major system failure which will cause total loss of DP capability regardless of any limitations put on the vessel. This would mean a loss of station keeping ability leading to an excursion, drive off, or drift off from position and which will lead to an immediate termination of the operation.

  2. **Severity Class 2 – Critical**. A failure due to major system failure which will cause loss of DP capability if operational limitations are not adhered to. This will include loss of redundancy where a further failure may cause loss of position.

  3. **Severity Class 3 – Serious**. A failure which will have an effect on operational capability but does not result in termination of the operation.

  4. **Severity Class 4 – Minor**. A failure which has negligible effect on system or subsystem level generally at component level and results in minor unscheduled repair.

- 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.

5.6.4 FMEA Corrective Action Report Forms

Whenever a potential problem is identified, an FMEA Corrective Action Report Form should be completed and forwarded to the designers via the client's focal point. Corrective Action 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. This assists in traceability of information. 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 Corrective Action Report Form.

Essentially, the items on the Corrective Action Report Forms are recommendations which are to be listed in the Report. As with the Q&A Punchlist, it should be recorded which recommendations have been closed out during the analysis and which items are still outstanding.

The Corrective Action Report Forms can be held in a database for ease of retrieval, sorting, and transmission by e-mail.

5.7 Evaluating the Effects of each Failure Mode on the System

The potential failures should be identified in a gradual way. The technique of brain storming by members of the FMEA team has been proven to be useful during this stage. The effectiveness of this part of the process is related to the technical strength of the team members in their respective disciplines.

Where DP is concerned, the general scope for carrying out a DP FMEA is outlined in Section 5.5. This is only a brief guide. Most FMEA analysts will be experts in their own field and have experience in evaluating the associated failure modes and their effects, so it is not the intention of this document to teach how this is done. However, owing to technological developments, the knowledge base must be kept updated.

Recently, there has been concern that expertise is not widespread in one particular area. This area is redundancy in data networks. Very often the DP

control system manufacturer's FMEA is relied upon in this area due to a lack of expertise. It is insufficient to note that there are two networks and failure of one will leave the other operational. Specialists familiar with network design should critically review the appropriateness of a type of network for the purpose, robustness of the network against damage, the amount of data traffic carried on the network to prevent communication overload, protocol, and so on. Tests should be devised to confirm the effects of failure of one net. Depending on these, it may be that a continuous monitoring of the level of data traffic on the network is required as a recommendation to the designers, or, perhaps, transfer of control data on one dual network and alarm data on another dual network.

5.8 Identifying Failure Detection Methods/Corrective Actions

The FMEA study in general only analyses failure effects based on a single failure in the system. Should a failure in the system remain hidden, with the system not alerting the operator to the failure, and a further failure occurs which has a significant effect on system availability, then this is considered to be only a single failure. In this case, the effects of the second failure should be determined to ensure that, in combination with the first undetectable failure, it does not result in a more severe failure effect, e.g. a hazardous or catastrophic effect. If so, the first failure should be alarmed. It is therefore important that the system alerts the operator to failures and means of failure detection, such as audible and visual warning devices, automatic sensing devices, sensing instrumentation and such like, should be identified.

Once the failure is detected, then the system should warn the operator that the failure has taken place. Depending on the severity of the failure mode the operator will take corrective action by manual means, or the system will automatically take corrective action by, say, starting a backup unit, and advising the operator that it has carried out the action. These are the compensating provisions.

Adding verification or validation controls (e.g alarms on failure) can reduce the probability of a failure being undetected and having a greater effect on the system if a further failure occurs. Design revisions can result either in a failure having less impact on a system if it occurs or in making a failure less frequent.

5.9 Recommendations

When a failure mode is analysed and it is revealed that a potentially serious effect on the system could result if it occurs, then this should be notified immediately to the client and the designers on the FMEA Corrective Action Report Form. A recommendation for corrective action is usually offered. The recommendations should each be graded, for example, A) "For Immediate Action", B) "Important", and C) "Nice To Have". If the decision is that no action is to be taken, then this decision should also be recorded.

It is useful to highlight by listing in the Final Report those recommendations that have been actioned or not actioned during the course of the FMEA. Effective follow-up programmes are essential as the purpose of the FMEA is defeated if any recommended actions are left unaddressed.

5.10 The FMEA Report

The FMEA report should be a self-contained document containing a full description of the system under analysis, broken down into its component parts with their functions. The failure modes and their causes and effects should be able to be understood without any need to refer to other plans and documents not in the report. The analysis assumptions and system block diagrams should be included where appropriate. The report should contain a summary of conclusions and recommendations for the system analysed. It should also include the FMEA test programme results plus any outstanding or unresolved action items. Naturally, the extent of the report will vary depending upon the extent of the system being analysed as this generally determines how much documentation is generated. There is no set maximum and minimum content, but sufficient documentation must be included in the report to substantiate what has been done during the analysis and how the findings were achieved.

5.10.1 Report Structure

The FMEA report would be expected to contain the following:

- Executive Summary
- Introduction
  - FMEA Introduction
  - Scope of Work
  - FMEA Procedure or Methodology
  - Vessel Application and Particulars
  - Any Assumptions Made in the Analysis, e.g. the operational mode the vessel is in when the analysis is carried out
  - Documentation
- Method of analysis
  - Block diagrams
  - FMEA Worksheet: Format, description of fields, definitions of severity levels
  - FMEA Corrective Action Report Form: Format
- Description of Systems , for example:
  - DP Control System.
  - Electrical Systems.
  - Machinery Systems.
  - Safety Systems.

  Each section should include details of any significant failure modes identified together with the FMEA recommendations put forward.
- Recommendations
  - Summary of FMEA recommendations and actions
- Conclusions
- Appendices:

- Worksheets
- Trials Test Sheets
- Question and Answer ("Q&A") Punchlist
- FMEA Report Sheets
- List of Vessel/Shipyard and Vendor Drawings Received and Reviewed

5.11 FMEA Documentation and Ongoing QA

The FMEA documentation consists of the FMEA Report and the database/s. For a DP vessel, it is intended that this documentation be held on board the vessel in hard copy and electronic 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. It should also be made available to charterers' representatives as part of the acceptance criteria during pre-charter audits. As modifications are made to the vessel that have a bearing on the DP system, the FMEA should be reviewed and updated to reflect the changes. Any recommendations arising from the review should be acted upon accordingly.

During the life of a system, inevitably modifications will be made to either improve the system operation or alter it to provide additional or different functions. Minor system modifications can be analysed and, together with any recommendations and follow-up, included as an addendum to the Final Report. Larger system modifications may require further FMEA tests and results to complete the analysis and, together with any recommendations and follow-up, presented in a new revised Final Report.

Following the FMEA and assuming it is possible, workscope and worksite permitting, the vessel should be put through a series of DP tests on an annual basis using a test plan derived from the FMEA trials test sheets. These will confirm that the system is functioning correctly and that responses to equipment failures are as expected. It also provides new operators with that extra knowledge of how the system responds to failures, knowledge that may be crucial in an emergency. It also helps prove any alterations to the system that have been made in the intervening period. The yearly test results should be incorporated into the FMEA database.

6 VESSEL AUDITS AND PRACTICAL FMEA TESTING

6.1 Vessel Audits

From time to time over the course of the vessel build, audits are necessary to ensure that the vessel is being built as designed and that construction faults that could cause single point failures are avoided where possible. 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 through failures in other equipment in the same compartment. For example, failure of a flange in a water pipe could cause failure of DP related 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 DP 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.

For DP Class 3 vessels, verification of cable routing is necessary as 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 database 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.

In a similar manner, vessel audits are necessary when an FMEA is being carried out on an existing vessel. Minor inexpensive modifications, such as shrouding of piping flanges to protect electronic equipment in the example above, which make the system more secure can have potentially huge reward against cost benefits.

6.2 Arranging Practical FMEA Tests, Dockside/At Sea/On Full DP

The DP system of a vessel is a dynamic system, made up of subsystems that 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 overall 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 overall system's response to failure. They are intended to confirm system redundancy and fault-tolerance 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:

- The findings of the paper FMEA are confirmed (or otherwise).
- The failure modes and effects of "grey areas" (areas which could not be adequately analyzed by study of system drawings and vendor documentation) are established, e.g. the behaviour of any interlocks that may inhibit operation of essential systems.
- Correct system wiring is confirmed (or otherwise).
- 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.
- Operational personnel are able to witness first hand the effects of failures and an evaluation can be made of their response to these failures.
- Information is gathered to allow updating of the FMEA database to reflect the "as built" configuration of the vessel.
- The FMEA test plan can be used as the basis of an Annual DP Trials Programme that requires function tests and failure mode tests once per year to confirm correct system operation as part of the vessel's ongoing QA.

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 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). These specialists will have been part of the FMEA 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 the trials commence. The FMEA team generates the FMEA test list and corresponding test procedures. Those tests that can be carried out dockside are identified and the remainder are integrated into the sea trials testing. If the vessel is an existing operational vessel, FMEA testing is carried out in much the same way during down times between contracts. In each case it is beneficial to have the operators or intended operators at the control stations as it is often the case that it is only during the controlled failure testing do they get a chance to witness the effects of various failures.

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 co-ordinated exercise. The system must be 100% operational, particularly alarm and event logging, and a suitable number of personnel for witnessing the tests must be arranged. All participants should review the test procedures so that the procedures and expected failure effects are well understood.

It should be remembered that these tests are part of the FMEA process and should not be treated in isolation. The FMEA will use the results of the tests in the final analysis and usually include the test sheets in the report.

It is important that practical testing is thorough. It is better that any unacceptable failure mode is uncovered during trials rather than later when the vessel is working.

7 OPERATIONS AND MAINTENANCE

When addressing the recommendations arising from the FMEA of a new build vessel, modifications can usually be carried out to either eliminate or reduce the seriousness of a failure. Where this is not possible, operational procedures can be put into play to warn the operators of the potential for a certain failure to occur and if it does what action should be taken, the maxim being "forewarned is forearmed". This naturally tends to affect existing vessels more where there is less scope for design changes.

The FMEA is of great benefit to maintenance staff as it can identify critical areas which could give rise to a serious problem in the event of a failure. These can be targeted by the introduction of planned maintenance routines, which sometimes can only be carried out safely during periods of downtime of a vessel. The results of a thorough FMEA can also be used to refine maintenance routines that can produce operational savings. FMECA techniques, discussed in Chapter 8, can also assist with maintenance by estimating the criticality or failure rate of each part of the system, as well as the failure rate of the overall system, so that the maintenance routines can concentrate on the areas that are less reliable. Chapter 8 also discusses RAM (Reliability, Availability and Maintainability), Reliability Centered Maintenance (RCM) and Risk Based Inspection (RBI), all of which can assist the maintenance engineer.

The FMEA can be used to address the aspect of carrying out maintenance of various items of equipment during normal operations and what effect this maintenance would have on operations should a failure occur.

It is possible to consider a single failure with one item only unavailable at a time due to maintenance. It is appreciated that under certain conditions more than one item will be undergoing planned maintenance, and unplanned maintenance on further equipment may be necessary. If this is the case, then the Maintenance Supervisor will have to carefully consider what maintenance can be allowed. The Maintenance Supervisor should have in mind the following questions:

- What is being worked on at the time?
- What is to be worked on?
- What the worst case single failure is that could occur whilst the maintenance is being carried out?
- What would be the effect on the station keeping should all of this occur simultaneously?

To assist the Supervisor in the decision making process, the FMEA database could be modified to include each item intended for maintenance and consulted prior to the maintenance being carried out. This would detail the equipment item down for maintenance, give the items critical to position keeping most likely to have a significant effect should they fail, and, for each case, give the effect of failure and a suggested alert status whilst the maintenance is being carried out.

8 ADDITIONS TO THE FMEA PROCESS

8.1 Criticality Analysis

If required, and cost, time and resources permit, the FMEA can be extended to include a criticality analysis. In a criticality analysis, the reliability block diagrams are analysed and each block assigned a failure rate, λ, in failures per million hours. From this, a reliability figure for the overall system can be determined, which will indicate how often the system will fail completely. Adding to each block an inverse repair rate, T_R, in hours-to-repair, which will indicate how long it will take to recover the intact system after repair, can further extend the analysis.

However, this requires that more time will be needed accessing the reliability data, sometimes involving a review of actual plant records to determine the failure rates for items of plant which are not covered elsewhere, e.g. in the oil companies' OREDA Handbook or Database (OREDA - Offshore Reliability Data). Sometimes, if the failure rates are not available, they are estimated, which will dilute the credibility of the final figure.

This additional work will obviously drive up the cost of a project. The question is: Is it necessary? What is initially required, when analysing a system, is to know whether the system can or cannot fail, and not necessarily how often it will fail. If it is shown that a single failure will cause the overall system to fail, modifications to the design can be made to eliminate or reduce the risk of failure. If after the criticality analysis, it is shown to fail every ten years, what the analysis does not do is to indicate when it will fail, i.e. it could fail next week or in ten years time.

If, when analysing a system, a single point failure is identified in a subsystem and the design cannot be modified to eliminate it, then a criticality analysis can be carried out on the subsystem to indicate how often it will fail. If it will fail every two years, then the maintenance routines can be modified such that, during downtimes when the system can be shut down, the subsystem can be either overhauled or replaced. During normal operations, procedures would have to be drawn up to ensure the effects of failure are mitigated.

Should cost, time and resources permit, and the FMEA be extended to include criticality analysis, if some failure rates of redundant equipment are deemed rather high and they cannot be modified, then these can be attended to during system downtimes as part of the maintenance programme.

FMECA is therefore dependent on the time, money and resources available. It is more than a "nice to have" and extremely useful to the maintenance department; however, it is not essential to establishing the weaknesses in the system under analysis.

8.2 Qualitative and Quantitative Risk Assessment (QRA)

QRA is intended to give an idea of how often (i.e. the frequency) something bad might happen at a facility (Quantitative), and what kind of injuries, damage, etc., might result, i.e. the consequences (Qualitative). Estimates of the frequencies and consequences associated with potential accident scenarios define the risk the facility presents.

QRA is a tool to help plant operators understand how accidents can occur and what equipment and/or human errors are most likely to contribute to an accident. It provides data about the different kinds of accidents so safeguards can be evaluated. What QRA cannot do is make the decisions about safeguarding against accidents. This is dependent upon advice from safety experts in the QRA field. There are software packages available that can assist in performing QRA but the software cannot perform the analysis itself. Again, a trained analyst is essential to assess the structure of the system under analysis and to enter the right data into the software.

Defining the goals of the QRA is important. If the QRA is commenced without knowing what is required, then this may result in overworking of the problem, leading to a waste of time, money and resources, or having to expand the scope later, causing costly additions to the project schedule.

QRA sometimes needs fault tree analysis and event tree analysis (see below) if the results of the QRA are required to be more rigorous and precise. However, this requires more time to be expended developing the fault trees, which will obviously drive up the cost of a project.

8.3 Criticality and Probability

The criticality, or severity, of a failure mode can be combined with the probability of that event occurring, in order to assess whether the risk of a failure occurring is acceptable, tolerable or unacceptable.

Risk = probability of failure x severity category

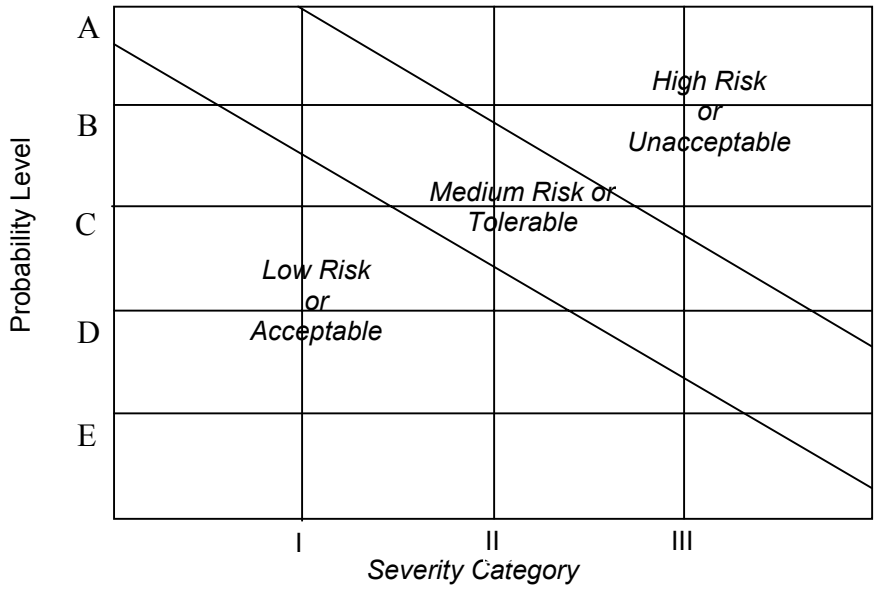
The severity of a failure mode can be categorised as follows:

Category	Degree	Description
I	Minor	Functional failure of part of a machine or process with no potential for injury, damage or pollution
II	Critical	Failure will probably occur without major damage to system, pollution or serious injury
III	Major	Major damage to system with a potential for serious injury to personnel and minor pollution
IV	Catastrophic	Failure causes complete system loss with a high potential for fatal injury and major pollution.

The probability of an event occurring can be categorised as follows:

Level	Probability	Description
A	10^{-1}	Likely to occur frequently
B	10^{-2}	Probable – may occur several times in the life of an item
C	10^{-3}	Occasional – may occur sometime in the life of an item
D	10^{-4}	Remote – unlikely to occur but possible
E	10^{-5}	Improbable – unlikely to occur at all

These are entered into a table to form a risk assessment matrix:



8.4 Fault Tree Analysis and Event Tree Analysis

A fault tree analysis (FTA) is a deductive, top down method of analysing system design and performance and is sometimes used in QRA. It involves specifying a top event to analyse, such as a fire, followed by identifying all of the associated elements in the system that could cause that top event to occur.

Fault trees provide a convenient symbolic representation of the combination of events resulting in the occurrence of the top event. Events and gates in fault tree analysis are represented by symbols.

FTAs are generally performed graphically using a logical structure of AND and OR gates. Sometimes certain elements or basic events may need to occur together in order for the top event to occur. In this case these events would be arranged under an AND gate, meaning that all of the basic events would need to occur to trigger the top event. If the basic events alone would trigger the top event then they would be grouped under an OR gate. The entire system as well as human interactions would be analysed when performing a fault tree analysis. The primary events of a high-order tree may be the top events of lower order trees.

Fault trees are used in the IMCA Publication "Reliability of Position Reference Systems for Deepwater Drilling" (IMCA Document M 160 January 2001). Also, when the overall "Safest Operating Mode" analysis for a DP vessel is being determined, fault tree analysis, together with an FMEA, should be included in the inputs into this study (IMCA Document M 164 October 2001).

Besides fault trees, event trees can be used in QRA. An event tree is a simple model that shows an "initiating event" for a potential accident, i.e. it shows how an accident scenario might start, for instance, with a pipe break. Safeguards that are designed to prevent or mitigate the accident are also shown (for example a relief valve or backup cooling system). Again, event trees would require to be developed with extra cost.

Event trees are used in the IMCA Database of DP Incidents (IMCA Document M 156 May 2000). This is a collection of real DP incidents reported to IMCA, which are represented as event trees.

8.5 RAM (Reliability, Availability and Maintainability)

RAM analyses are undertaken using a series of techniques. The specific techniques that are used and the level of detail with which they are applied are dependent on the scope of the study. Some of the techniques used for RAM analysis include:

- FMEA
- Reliability predictions
- Reliability block diagrams (RBDs)
- Availability assessments using reliability simulation techniques
- Fault tree analysis (FTA)
- Human factor assessments (ergonomics and man-machine interfaces)
- Human error analysis and task analysis

These techniques are used to identify critical RAM Parameters. A RAM Parameter is a measure of an event, e.g. the duration of a maintenance activity or the frequency of a failure. By measuring these events it is possible to determine whether or not the availability targets of the system will be met. These targets are developed by the client and contractor early in the project by setting the reliability goals and defining the RAM activities. RAM activities can also continue into the operational phase of the systems life.

If RAM parameters show that the failure occurrences are more frequent than desired or maintenance takes longer, then the availability target of the system will not be met and corrective action will be required.

RAM activities also address interfaces between each of the defined activities in the RAM analysis and the design and operation of the system. They include issues regarding spares, maintenance information and requirements for procedures.

During the design process, Reliability Centered Maintenance (RCM) and Risk Based Inspection (RBI) processes can also be used to review the design, to determine means for minimising maintenance and inspection and to define optimum maintenance and inspection routines that will be required during the operational phase. Recent experience with thrusters has shown that one of the major reasons for thruster problems is poor maintenance.

8.6 Software for FMEA

There are many different software programs available to assist in carrying out FMEAs. Most will specify one of the standards listed in Chapter 3. Some are specific to the type of system being analysed, e.g. electronic, automobile and aerospace industries. Many contain, not just the FMEA, but also the additions to the process mentioned in this Chapter, such as FMECA, QRA and RAM, and utilise links such that a change in one document will update all the other documents affected by the change. Many are capable of generating worksheets, reporting forms and the report itself to the required standard, however, it is still necessary to have experienced analysts entering and assessing the data.

As there are so many of these programs, it is not possible to list them, but many can be found advertised on the Internet with brief descriptions of their functions.

8.7 FMEA on Control Software

Where software functions for control are being considered in the FMEA, it is generally sufficient for the failure of the software function to be considered rather than a specific analysis of the software code itself. Only extensive testing of the system, either during factory tests using the actual hardware, or during shipboard commissioning and sea trials, will reveal any problems with software bugs. Software failure modes should result in a watchdog trip or system failure.

APPENDIX 1: DEFINITIONS OF TERMS USED IN THE FMEA PROCESS

The following definitions of terms used in the FMEA process and the extensions to the FMEA process.

Active Redundancy	The term used when all redundant units are functioning simultaneously (see Standby Redundancy).
Availability	is the proportion of time for which the item is working or fit for work. It combines the ideas of reliability and maintainability.
Cause	A Cause is the means by which a particular element of the design or process results in a Failure Mode.
Criticality	The measure of effect of a malfunction of an item on the performance of a system.
Criticality Rating	The Criticality Rating is the mathematical product of the Severity and Occurrence ratings. Criticality = (S) x (O). This number is used to place priority on items that require additional quality planning.
Detection	Detection is an assessment of the likelihood that the mechanisms provided to prevent the Cause of the Failure Mode from occurring will detect the Cause of the Failure Mode or the Failure Mode itself.
Effect:	An Effect is an adverse consequence that the item, subsystem or overall system might suffer.
Ergonomics	The study of man-machine interfaces in order to minimise human errors due to mental or physical fatigue.
Failure	Failure is the cessation of satisfactory operation, either temporarily or permanently. "Satisfactory" should be defined and may depend on the mode of operation.
Failure Mode	Failure Modes are sometimes described as categories of failure. A potential Failure Mode describes the way in which a system or process could fail to perform its desired function (design intent or performance requirements) as described by the specification.
Failure Rate	The number of failures of an item per unit of time.
Fault Mechanism	The physical or chemical process that causes the failure.
FMEA Element	FMEA elements are identified or analysed in the FMEA process. Common examples are Functions, Failure Modes, Causes, Effects, Controls and Actions. FMEA elements appear as column headings in the FMEA worksheet.
Function	A Function could be any intended purpose of a system or process.

Human Factors	The human psychological characteristics relative to complex systems and the development and application of principles and procedures for accomplishing optimum man-machine integration and utilisation.
Maintainability	The ease with which a failed item may be repaired. The usual measures are the mean times or distribution of times to repair.
Maintenance	All actions necessary for retaining an item in, or restoring it to, a serviceable condition. Includes servicing, repair, modification, upgrading, overhaul, inspection and condition determination.
Mean	The arithmetic mean which is the sum of a number of values divided by the number itself.
Median	That value such that 50% of the values in question are greater and 50% less than it.
Mean Time To Repair	MTTR – The statistical mean of the distribution of times-to-repair. The cumulation of active repair times during a given period divided by the number of malfunctions during the same interval of time.
Mean Time Between Failure	MTBF – The total cumulative functioning time of a component or system divided by the number of failures. Also Mean Time To Failure (MTTF)
Occurrence	Occurrence is an assessment of the likelihood that a particular Cause will happen and result in the Failure Mode during the intended life of the system or process.
Quality	Quality is a concept which embodies variously, and as appropriate, the ideas of performance (or fitness for purpose), durability, freedom from repairable failure, maintainability, and even aesthetics. It does not include any consideration of price or cost.
Reliability	Reliability is the ability of an item to perform a required function for a stated period of time.
Risk Priority Number	The Risk Priority Number is a mathematical product of the numerical Severity, Occurrence and Detection ratings. RPN = (S) x (O) x (D). This number is used to place priority on items that require additional quality planning.
Severity	Severity is an assessment of how serious the Effect of the potential Failure Mode is on the overall system or process.
Standby Redundancy	The term used when one unit is functioning and one or more units are on standby, i.e. not active but available to take over if the one functioning fails (see Active Redundancy).

APPENDIX 2: EXAMPLE OF AN FMEA WORKSHEET AND DESCRIPTION OF THE FMEA WORKSHEET FIELDS

FMEA Worksheet

Worksheet No.		Date		Compiled By
Main System		System		Subsystem
Reference Drawing:				
1 Code/Ref.				
2 Item				
3 Function				
4 Operational Mode				
5 Failure Modes				
6 Failure Causes				
7 Failure Effects: Component/Subsystem/ System				
8 Failure Detection				
9 Compensating Provisions				
10 Testing				
11 Remarks				
12 Severity Class				

Fig. 1: Example of an FMEA Worksheet

Appendix 2, Table 1: ***Description of the FMEA Worksheet Fields***

Worksheet ID	Discrete number assigned to the worksheet.
Main System/System/ Sub-System:	A brief description of the parts of the system under study broken down into levels.
Reference Drawing:	Number of the drawing under analysis.
1 Code/Ref.	A serial number or reference designation identification number for each item is assigned for traceability purposes and entered on the worksheet.
2 Item	The name or nomenclature of the item or system function being analysed for failure mode and effects is listed.
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	The predictable failure modes for each systems level analysed will be identified. Potential failure modes will be determined by examination of item outputs and functional outputs identified in applicable block diagrams and schematics.
6 Failure Causes	The most probable causes associated with the assumed failure mode will be identified and described. Since a failure mode may have more than one cause, all probable independent causes for each failure mode will be identified.
7 Failure Effects	The consequences of each assumed failure mode on item operation, function, or status will be identified, evaluated, and recorded. The failure under consideration may affect several systems levels in addition to the systems level under analysis; therefore, "component", "subsystem", and "system" effects will be evaluated. ♦ Component. Component effects concentrate specifically on the impact an assumed failure mode has on the operation and function of the item in the systems level under consideration. The consequences of each assumed failure affecting the item is described along with any second-order effects which may result. ♦ Subsystem. Subsystem effects concentrate on the effect an assumed failure has on the operation and function of the items in the next and higher systems levels above the systems level under consideration. The consequences of each assumed failure affecting the next higher systems level will be described. ♦ System. System effects evaluate and define the total effect an assumed failure has on the operation, function, or status of the main system.
8 Failure Detection	A description of the methods by which occurrence of the failure mode is detected by the operator will be recorded. The failure detection means, such as visual, alarm devices, or none, will be identified.
9 Compensating Provisions:	The compensating provisions, either equipment redundancy, control system response, or operator action, which circumvent or mitigate the effect of the failure.
10 Testing	Description of any special testing required with respect to the failure mode and/or its consequences.
11 Remarks	Additional field in which any remarks can be made regarding recommendations or other considerations.
12 Severity Classification	Severity classification based on the impact of the failure on DP capability. The severity classification can be composed of three elements: 1.Severity Level; 2.Operator Fault Management; 3.Redundancy Limitation. (See text)

APPENDIX 3: BACKGROUND AND EXPLANATIONS OF DP CLASS 2 AND CLASS 3

1. Background

How much redundancy is required in a DP system? The location in which a DP vessel is allowed to work and the scope of the work it is going to carry out should be governed by the amount of redundancy the vessel has in its DP system. This was originally addressed by the NMD (Norwegian Maritime Directorate) and IMO and led to the introduction of "Consequence Classes" and "Equipment Classes".

The NMD grouped the "consequence" of failure into four classes:

- Consequence Class 0 operations, which are operations where loss of position keeping capability is not considered to endanger human life or cause damage;
- Consequence Class 1 operations, which are operations where damage or pollution of small consequence may occur in case of failure of the positioning capability;
- Consequence Class 2 operations, which are operations where failure of the positioning capability may cause pollution or damage with large economic consequence, or personnel injury; and
- Consequence Class 3 operations, which are operations where loss of position keeping capability will probably cause loss of life, severe pollution and damage with major economic consequences.

IMO defines the vessel "equipment" classes by their worst case failure modes. For example, for Equipment Class 2, a loss of position is not to occur in the event of a single fault in any active component or system. Normally, static components such as manual valves and piping systems are not considered to fail provided they can be shown to be adequately protected from damage and reliability is proven. Single failure criteria include any active component or system, eg. generators, thrusters, switchboards, remote controlled valves, etc., together with any normally static component (cables, pipelines, manual valves, etc.) that cannot be shown to have adequate protection from damage or have proven reliability.

For Equipment Class 3, the single failure modes include those in Equipment Class 2 plus those in which any normally static component is assumed to fail. Additionally, all components in any one watertight compartment are assumed to fail due to the effects of fire or flooding and all components in any one fire subdivision are assumed to fail due to the effects of fire or possibly flooding. For Equipment Class 3, a single inadvertent act is classed as a single failure.

The design of a vessel's DP system complying with Equipment Class 3 would have a power system divided into two or more systems so that failure of one will have no effect on the other(s). The power generation system will have a minimum of two enginerooms separated by an A60 bulkhead. In the case of a two engineroom system, half of the generating capacity would be located in one engineroom and the other half in the other engineroom. The switchboard room would similarly be split into two rooms with half of the switchboard located in one room and half in the other room. The sections of bus bars would be coupled by two bus tiebreakers one located in each section of switchboard. The supplies to the thrusters would be configured such that only half of

the thrust capability in both alongships and athwartships direction is lost should a section of switchboard fail. Thrusters would be located in compartments such that those located in a single compartment would not be supplied from both sections of switchboard. With the effect of fire being considered, a backup DP control station would be located in a separate compartment to that in which the main control station is located. Cabling to items of redundant equipment would not be run through the same compartment, but be run segregated such that a cable blow out or a fire would not affect both units.

The design of a vessel's DP system complying with Equipment Class 2 would have similar redundancy in terms of system architecture, but would not need to comply with the compartmentalisation requirements with respect to fire and flooding, e.g. two switchboards, but they do not need to be located in two switchboard rooms.

These Consequence Classes and Equipment Classes therefore dictate that a Consequence Class 0 operation can be carried out by the equivalent of an Equipment Class 1 vessel with little or no redundancy or, indeed, a vessel with much more redundancy, whereas a Consequence Class 3 operation can only be carried out by the equivalent of an Equipment Class 3 vessel with considerable redundancy.

IMO Equipment Class 2 is generally consistent with ABS DPS-2, DnV AUTR and LR (AA) and IMO Equipment Class 3 is generally consistent with ABS DPS-3, DnV AUTRO and LR (AAA). The basic requirements in these categories are given below for ABS, DnV and Lloyd's Register. Table 1 in this Appendix shows a summary of IMO Class 2 and Class 3 requirements in comparison with the corresponding requirements for ABS, DnV and Lloyd's Register.

Some DP vessel owners require their vessels to have DP systems that lie somewhere between the IMO Class 2 and Class 3 requirements (DP Class 2½ say). These have added redundancy over and above the Class 2 requirements, but do not quite comply with Class 3 requirements. Classification Societies will only assess the system to either Class 2 or Class 3 and nothing in between. It is left to the owner of the vessel to ensure that the added redundancy (i.e. the added ½) is as the Owner intended. This is best included in an FMEA of the overall system.

2. DPS-2 and DPS-3 Class Notations From ABS Rules

(As given in ABS Rules 2001, Part 4, Chapter 3, Section 5, 15 - Dynamic Positioning Systems).

DPS-2 Class Notation

As per ABS Class notation (ABS DPS-2), the vessel has to comply with the following basic rules:

- Vessels are to be fitted with a DP system providing automatic and manual position and heading control under specified maximum environmental conditions, during and following any single fault excluding a loss of compartment or compartments.
- Two independent self monitoring control systems must be installed.
- The cabling for the control systems is to be arranged such that under single fault conditions, it will remain possible to control sufficient thrusters to stay within the specified operating envelope.
- The generators and the distribution systems must be arranged such that in the event of the largest section of bus bar being lost, there is sufficient power to supply essential ship's load and remain within the specified operating envelope. Essential services for the generators such as fuel oil and cooling systems are to be arranged such that in the event of a single fault the same operational criteria are met.
- At least three independent position reference systems, of which two may operate on the same measurement principle, and two sets of gyro compasses must be fitted. Two wind sensors are required in the Rules, however, the requirements for motion reference units are not stated.

DPS-3 Class Notation:

As per ABS Class notation (ABS DPS-3), the vessel has to comply with the following basic rules (in bold where it differs from DPS-2):

- Vessels are to be fitted with a DP system providing automatic and manual position and heading control under specified maximum environmental conditions, during and following any single fault **including loss of a compartment due to fire or flood.**
- Two independent self monitoring control systems **with a separate backup system** must be installed. **The backup system must be installed in a backup control station and separated from the other two control systems by a A60 Class fire division.**
- The cabling for the control systems is to be arranged such that under single fault conditions, **including loss of a compartment due to fire or flood,** it will remain possible to control sufficient thrusters to stay within the specified operating envelope.

- The generators and the distribution systems must be arranged **in at least two different compartments,** so that in **the event of loss of any compartment due to fire or flooding** there is sufficient power to remain within the specified operating envelope and be able to start any non running load. **Essential services for the generators such as fuel oil and cooling systems are to be arranged in a similar manner.**

- At least three independent position reference systems, of which two may operate on the same measurement principle, and **three sets of gyro compasses** must be fitted. Two wind sensors are required in the Rules, however, the requirements for motion reference units are not stated. **The third reference system and one of the gyros must be located at the backup control station.**

- The specified maximum environmental conditions are given in the Rules as "the specified wind speed, current and wave height under which the vessel is designed to carry out intended operations. The specified maximum environmental conditions for each Class notation can be different.

3. DP (AA) and DP (AAA) Class Notations From Lloyd's Register Rules

The basic requirements for LR Class notation DP(AA) are as follows:

- All systems necessary for the correct functioning of the DP system are to be configured such that a fault in any active component or system will not result in a loss of position.
- Passive components such as cables and pipes are to be located and protected such that the risk of fire or mechanical damage is minimized.
- No single fault in the generation and distribution systems is to result in the loss of more than 50 per cent of the generating capacity.
- Two independent automatic control systems are to be provided and arranged such that no single fault will cause loss of both systems, a fault in one causing automatic bumpless transfer to the backup system.
- At least three position reference systems incorporating at least two different measurement techniques are to be provided and are to be arranged so that a failure in one system will not render the other systems inoperative.
- At least three gyrocompasses and three vertical reference units, if necessary, are to be provided.

The basic requirements for LR Class notation DP(AAA) are as follows (where they differ from those of Class DP(AA)):

- The DP system is to be arranged such that failure of any component or system necessary for the continuing correct functioning of the DP system, or the loss of any one compartment as a result of fire or flooding will not result in a loss of position.
- Thruster units are to be installed in separate machinery compartments, separated by a watertight A-60 class division. Generating sets, switchboards and associated equipment are to be located in at least two compartments separated by an A-60 class division and, if located below the waterline, the division is also to be watertight. There is to be provision to connect the switchboard sections together by means of circuit breakers.
- Duplicated cables and pipes for services essential for the correct functioning of the DP system are not to be routed through the same compartments.
- In addition to the two independent automatic DP control systems, an independent backup control station is to be provided in a compartment separate from that for the main control station.
- One of the position reference systems and one of the gyrocompasses are to be located at the backup control station and the signals repeated into both main and backup DP control systems.
- The backup control system is to be supplied from its own independent UPS.

Note: For assignment of DP(AA) or DP(AAA) notation, a Failure Mode and Effect Analysis (FMEA) is to be submitted.

4. AUTR and AUTRO Class Notations From DnV Rules

The basic requirements for DnV Class notation AUTR are as follows:

- Loss of position is not to occur in the event of a single failure in any active component or system. Normally static components will not be considered to fail if adequate protection is provided. Single failure criteria for AUTR include:
  - 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.
- Flooding and fire are not to be considered beyond main class requirements. Failure of non-moving components, e.g. pipes, manual valves, cables etc. may not need to be considered if adequate reliability of a single component can be documented, and the part is protected from mechanical damage.
- An automatic position control mode consisting of at least two mutually independent control systems Failure of the on-line system is to cause automatic changeover to the off-line system.
- An independent joystick
- Manual levers for each thruster.
- Where more than one positioning reference system is required, at least two are to be based on different principles.
- A main bus-bar system consisting of at least two sections, with bus-tie or inter-connector breaker(s), are to be arranged. The switchboard arrangement is to be such that no single equipment failure, including short-circuit of the bus-bars, will give a total black-out. Bus-bar sections can be arranged in one switchboard.

The basic requirements for DnV Class notation AUTRO are as follows (where they differ from those of Class AUTR):

- Loss of position is not to occur in the event of a single failure in any active component or system. A single failure includes:
  - items listed for AUTR and failure of static components
  - all components in any one watertight compartment, from fire or flooding
  - all components in any one fire sub-division, from fire or flooding.
- Redundant equipment is to be separated by bulkheads that are to be fire-insulated by A-60 class division, and in addition are to be watertight if below the damage water line.
- Cabling to equipment that forms part of the designed redundancy requirement is to neither run along the same route, nor in the same compartment as the cabling for other parts of the designed redundancy. When this is practically unavoidable, the

use of an A-60 cable duct or equivalent is acceptable but not in high fire risk areas, e.g. enginerooms and fuel treatment rooms.

- In addition to the two mutually independent control systems, a back-up DP-control system is to be arranged in an emergency DP-control station, separated from the main centre by an A-60 division.

- The back-up system is to include an automatic position control mode, and is to be interfaced with a position reference that may operate independently of the main system.

- At least one of the positioning reference systems is to be connected directly to the back-up control system and separated by the A-60 class division from the other positioning reference systems.

- Sensors connected directly to the back-up positioning control system are to be installed in the same A-60 fire zone as the back-up control system.

- The switchboard arrangement is to be such that loss of all equipment in a fire and watertight subdivision will not give a total black-out. It is therefore required that each bus-bar section is isolated from the other(s) by watertight A-60 divisions. There is to be a bus-tie breaker on each side of this division.

Appendix 3, Table 1 - ***Summary of IMO, ABS, DnV & LR Equipment Classes***

Subsystems or Components	**IMO Equipment Classes/ System Configuration**			**ABS Equipment Classes/ System Configuration**		**DnV Equipment Classes/ System Configuration**		**LRS Equipment Classes/ System Configuration**	
Notation:	**IMO Class 2**	**IMO Class 3**		**DPS-2**	**DPS-3**	**AUTR**	**AUTRO**	**DP (AA)**	**DP (AAA)**
Power System: Generators	Redundant	Redundant - separate rooms		Redundant	Redundant - separate rooms	Redundant	Redundant - separate rooms	Redundant	Redundant - separate rooms
Main Switchboard	1 split with bus-tie	2 with bus-ties (normally open) Separate rooms		1 split with bus-tie	2 with bus-ties Separate rooms	1 split with bus-tie	2 with bus-ties Separate rooms	1 split with bus-tie	2 bus-ties Separate rooms
Bus Tiebreaker	1	2		1	2	1	2 - normally open	1	2
Distribution System	Redundant	Redundant - separate rooms		Redundant	Redundant - separate rooms	Redundant	Redundant - separate rooms	Redundant	Redundant - separate rooms
Power Management	Yes	Yes		Yes	Yes	Yes	Yes	Yes	Yes
Thruster System: Arrangements of thrusters	Redundant	Redundant - separate rooms		Redundant	Redundant - separate rooms	Redundant	Redundant - separate rooms	Redundant	Redundant - separate rooms
DP Control System: Auto control: No. of control computers	2	3, with 1 in backup control station		2	3, with 1 in backup control station	2	3, with 1 in backup control station	2 - independent operation	3, with 1 in backup control station
Man. control: Joystick with auto heading	Yes	Yes		Yes	Yes	Yes	Yes	Yes	Yes
Single man. control each thruster	Yes	Yes		Yes	Yes	Yes	Yes	Yes	Yes
Position ref. systems	3	3, with 1 in backup control station		3	3, with 1 in backup control station	3	3, with 1 in backup control station	3	3, with 1 in backup control station
Ext. sensors:									
- Wind	2	3	1 each in backup control station	2	2	2	2	At least 2	At least 2
- Vertical Ref. Syst.	2	3		Not specified	Not specified	2/3	3	3	3
- Gyro	3	3		2	3, with 1 in backup control station	3	3	3	3, with 1 in backup control station
UPS (Uninterruptible Power Supply/Battery System)	2	2, with 1 UPS in backup control station		UPS system specified	UPS system specified, plus 1 UPS in backup control station	2 UPS	2 UPS, plus 1 UPS in separate compartment	UPS system specified	UPS system specified, plus 1 UPS in backup control station
Backup control system in separate control station	No	Yes		No	Yes	No	Yes	No	Yes
Printer for register and explaining alarms	Yes	Yes		Yes	Yes	Yes	Yes	Yes	Yes

APPENDIX 4: TYPES OF DP FAILURE MODE UNCOVERED BY FMEAS

Single Point Failures:

"Common mode failures" or "single point failures" occur when some external factor defeats redundancy. The most common example, in general terms, is the failure of a common power supply to two redundant elements. Any system which has an identical standby is open to the possibility of common mode failures that were not considered in the reliability study. For example, a nuclear accident in the USA is believed to have been initiated by the simultaneous failure of two valves, due to them having both been wrongly maintained by the same team of fitters.

Areas for Special Consideration:

From the IMCA reference document for station keeping incidents (IMCA M 157), statistical data for DP incidents over the period from 1990 to 1999 show that the main causes of incidents are due to failures of reference systems, thrusters and computers and operator error. Whilst the most incidents over this period are attributed to computers, and the trend appears to be towards rising failure rates, attention to design and reliability of computers has caused the failure rates to fall in recent years. However, reference systems and thruster systems in particular still give rise for concern.

Reference systems continue to provide a significant contribution to the number of reported incidents. Reliance is put on redundant DGPS systems, for example, but it has been shown that all DGPS systems can be susceptible to common atmospheric effects such as scintillation. For drilling vessels, a recent study showed that a combination of at least two separate DGPS systems and two long base line hydroacoustic position reference systems is the best scenario when drilling in deep water (IMCA Publication "Reliability of Position Reference Systems for Deepwater Drilling" (IMCA Document M 160 January 2001).

Where thruster incidents are concerned, about a third are serious and usually an incident concerns one thruster only. Typically, if there is a thruster problem, the DPO will put it down as a DP computer problem, so these types of incidents require some investigation.

These are areas which should receive special consideration, but this is not to say that all of the other areas should receive less attention.

A considerable amount of attention appears to have been given to the design of electrical systems, as the trend of electrical incidents appears to be downwards. However, potential electrical failures are the most difficult to spot from design drawings, due to the complexity of some systems and the fact that the consequences of small electrical failures, such as loose connections, are almost impossible to determine without lengthy and costly investigations. Power management has recently been highlighted as an area for special consideration as, with the progress in technology and the increase in complexity of the systems, it becomes more difficult to identify certain failure modes, and hence

reveal their insidious effects. (IMCA Publication "Power Management System Study" (IMCA Document M 154 January 2000)

Where machinery systems are concerned, fuel oil system problems are potentially the most dangerous, as any fracture in the piping system can lead to fire. Any fuel problems such as a broken pipe, a valve malfunction, or water in the fuel could cause loss of all generating engines if redundancy is not built into the system.

Single Point Failures Revealed in Service:

Insidious failures have been uncovered, sometimes only as a result of in service failures.

- Recently, a failure of a redundant computer system having two communication networks is believed to have failed owing to the identical interface units on the two nets being affected by a high ambient temperature in the console in they were situated.

- On a different vessel, the output of each of three gyros froze, one at a time over a period of 24 hours. As the weather conditions were calm and the vessel's heading did not change outside of the dead band, no alarms were generated and only after all three had frozen did the heading alter and an excursion result. There was no software in the DP control computers to detect a non-changing signal. This was recommended, along with a study as to why the gyro outputs froze. Operational measures also included an occasional small heading change to check the changing gyro outputs. Interestingly, a "fixed gyro output" alarm had been included in earlier generations of the DP system but was, presumably, removed in recent years because its purpose was thought to be superfluous.

Unacceptable Failure Modes Uncovered by FMEAs:

Potential failure modes have been uncovered using FMEA techniques that could have caused significant downtime or, worse, loss of critical position, if the FMEA had not been carried out.

- On one vessel, all DP computers were located in the same cubicle. Difficulties in restructuring the wiring meant that physical divisions were put in and heat sources such as the power supplies were relocated to adjacent cubicles.

- Often it is found that fuse failure alarms are not present on essential circuits supplied by redundant power supplies. Loss of one supply if not alarmed is a hidden failure and will mean that a failure of the other supply will result in a total failure of the system being supplied.

- The ESD on one vessel with two enginerooms comprised a single pushbutton to activate a complete shutdown of the power system. Whilst the loop was monitored, it was possible for a fault in the pushbutton to cause a

total blackout. The switch contact arrangement was revised so that a single contact short circuit would only shutdown one engineroom and not two.

- The analysis of a thruster drive system showed that the thruster drives had a shut down on loss of cooling water flow. Lack of redundancy in the forward cooling system to all thrusters forward gave the possibility that all thruster drives would shut down if the pump stopped. The system was modified to alarm on loss of cooling water flow and trip on high temperature only. Also, additional redundancy in the cooling system was built in later.

- Sometimes it is found that there is a lack of fire detection and protection in spaces containing essential DP related equipment.

- The FMEA on one vessel showed that there were common power supplies to duplicated control consoles at a primary control station. Both consoles would fail if the power supply was lost. Each console was given a segregated power supply.

- On one distributed control system it was found that there were dual power supplies to dual process CPUs but a common power supply to the I/O. A system providing an alternative power supply to the I/O should the main supply fail was installed.

- A vessel had two enginerooms each provided with its own fuel system but no crossover. A modification to the design will enable a cross connection between port and starboard fuel supply systems so that one service tank could be taken out of service if required.

- An example of systems being designed in isolation involved the UPS battery system of one vessel. The air supply to the dampers in the UPS battery rooms port and starboard was on a single supply line. When the damper shut on loss of air, interlocks made the fan trip. Loss of the fan then caused both of the UPS chargers to trip through further interlocking.

- Common power supplies to the engine governor control system meant that loss of power resulted in loss of half the available power. Whilst this did not exceed the worst case failure criteria, modifications were made such that a loss of power would affect only one engine.

- Both of the network interface units in a bridge console were supplied from the same fuse. This was changed so that each network interface unit was supplied from a separate supply.

- During FMEA testing it was found that the UPS distribution did not agree with the drawings used in the paper analysis. In one case, the doppler log and a network distribution unit interfacing with one of the dual networks were fed from the same fuse. This meant that, unknown to the Instrument Technician, removal of the fuse to work on the doppler log would result in loss of redundancy in the dual network. Many other anomalies were found in the UPS distribution demonstrating the benefit of FMEA testing.

- As a result of carrying out an FMEA on a cable ship, fitted with a simplex (single) DP computer, a problem was identified with the power supply changeover relay that would have prevented a changeover from the DP computer to the independent joystick in the event of a computer failure.

The above failures are dangerous for any DP vessels and safety of personnel is always of the utmost importance. For drilling vessels and shuttle tankers the economic consequences of failure could also be dire.

These examples serve to illustrate how a detailed FMEA and subsequent FMEA proving trials can minimise, if not eliminate, the above failures.

Examples of Common Mode Failures:

The examples of common mode failures outlined below are taken from audits on existing vessels and from FMEAs on new vessels or conversions. The examples from the audits of existing vessels are intended to illustrate the type of mistakes that have been made in design in the past which would be highlighted in today's indepth FMEA. Some of the problems caused incidents, or were caught before an incident was allowed to occur. The problems would have been identified at a much earlier stage using FMEA techniques, either during the analysis of the drawings or during the FMEA sea trials.

Electrical Problems:

- One incident involved a Class 2 vessel in which all online generator circuit breakers tripped causing a total blackout. All diesels continued to run and the automation system reclosed two circuit breakers to restore main power. But the momentary blackout stopped the thrusters which were fixed pitch propellers driven by SCR controlled main motors. Two problems were revealed. The first problem was that the blackout was caused by the over-excitation of one generator with the protection system failing to clear the fault. This generator took the entire load whilst the others shed load to maintain frequency. When the overloaded generator eventually tripped, the low system voltage caused tripping of the other generator breakers. The second problem was that the resulting low voltage also caused the thruster drive protection systems to switch off the thruster drives. The SCRs had to be reset locally and this took time.

- The power management system for the generators and high voltage equipment of one vessel depended upon two basic sources of supply. One was from 48V DC, provided from a common bus bar by battery and parallel connected float chargers, and the other from 220V AC, provided from a common bus bar by inverters supplied from the 48V DC source. The FMEA showed that total loss of either source effectively blacked out the ship.

- Sometimes, UPS failure alarms are not generated at the DP console.

- Frequently, the UPS distribution is found not to be as per the design drawings. One wiring fault in particular was that the two DP computers on one vessel were wired incorrectly; in this case, if there had been a problem

with one of the computers, this could have had the effect of the wrong computer being switched off, thereby losing both (all) computers.

- A fault that is found frequently is the lack of a power monitoring alarm on loss of a redundant power supply. Redundancy can be provided by two power supplies, each from a separate source. However, if one is lost and it is not alarmed, the operator does not know that redundancy is impaired. Loss of the other power supply sometime later will mean loss of the equipment being supplied by the two redundant power supplies, and possible loss of DP.

- Another fault found is common power supplies being provided for redundant displays.

- Sometimes a common transfer switch is used for switching control power to essential equipment, e.g. a main switchboard. A problem with the transfer switch would mean possible loss of control or complete loss of the essential equipment.

Fuel Problems:

- A fire was reported in a vessel with two enginerooms. A low pressure fuel oil pipe fractured and sprayed fuel droplets over a hot manifold. The fire was only noticed when smoke started to come from the engineroom ducts. It was found that the fire detection system had not activated, as the detectors had been sited near the ventilation blowers and had fresh air flowing over them. No one was hurt but the engineroom was destroyed. The vessel stayed on station because the power demand was within the capability of the generators running in the other engineroom, which continued to supply power. For some critical operations it is requested that all generators are on line.

Cooling Water Problems:

- Sometimes temperature or pressure control valves will adopt a non-fail safe mode, e.g. temperature control valves shutting on loss of actuator power air, restricting cooling water flow to coolers.

- Insufficient redundancy in the thruster cooling water supply to one group of redundant thrusters. A recommendation was made to increase security of the system by splitting the system and providing additional pumping capacity.

Control Air Problem:

- On a twin screw vessel, with the main engine coupled to each shaft via a clutch, it was found that the control air to both clutches was common and loss of air pressure caused the engines to declutch. Separate supplies were arranged so that loss of both clutches could not happen simultaneously.

Lubrication Problems:

- On one vessel, poor security of valve arrangement would have allowed the purification of one running engine sump oil into another engine sump.

Thruster Problems:

- Crossovers in the wiring of alarms and thruster control circuits were found during DP trials on one vessel, amongst other potential thruster problems.

- Another vessel had been working for several years with a serious failure mode in which loss of thruster pitch feedback caused the pitch to travel to maximum.

DP Control System Problems:

- On one occasion, following sea trials, a newly commissioned vessel was to undertake follow-sub operations. The centre of rotation of the vessel was chosen at a point away from the centre of gravity and the vessel set up on DP. As soon as the DPO entered the follow-sub mode, the centre of rotation jumped back to the centre of gravity, giving a 15 metre drive off. Builder's and Owner's sea trials, which should include FMEA tests, should be exhaustive and include a demonstration of every function built into the control strategy. The one that is missed could be the one that causes an incident. Designers must be aware of what the operator may want to do during the execution of specific workscopes.

DP Computer Problems:

- On one vessel that had been operating for many years, the power supplies to the computers were common, the thinking being that "belt and braces" would provide redundancy. But a fault on the resulting cable loop between both computers would have caused a power failure to both computers and loss of all automatic positioning control.

- Thruster command signals for one redundant group of thrusters were controlled by the same output card, which was supplied by one fuse. Modifications were made to enhance the redundancy by rewiring the command signals so that a failure of one single fuse or card did not result in loss of all thrusters in the redundant group.

- Problems are not necessarily confined to vessels incorporating full redundancy. FMEA tests were carried out on a simplex vessel with a single DP computer and computerised joystick, with functions including automatic heading control. It was noticed that a fuse was critical to the changeover between automatic DP and joystick. Loss of this fuse was not alarmed and, with the vessel on automatic DP, it was proved that, with loss of this fuse remaining hidden, should the automatic DP be lost, then transfer of control to the joystick was impossible. Fuse failure monitoring was introduced in this case to cure the problem. It should be established what fuses are critical to DP and arrange an alarm to warn of failure.

Note: This is a similar situation to the power failure monitoring alarm mentioned above.

Generator Control Problems:

- One vessel had two separate governor systems, one for the generators in each engineroom. Data connections were provided between the two systems to enable load balancing when the two sections of main switchboard were connected. Failure of the data connections caused imbalance and total blackout. Loss of these interconnections were not alarmed.

- On one vessel, the power supplies to all governors were common.

Ventilation Problems:

- Machinery space dampers (or rig saver dampers) failing to the shut position starving engines of combustion air.

- Ducting common to redundant spaces.

APPENDIX 5: REFERENCES

- American Bureau Of Shipping - ABS Rules for Building and Classing Steel Vessels 2001 - Part 4, Chapter 3, Section 5, 15 Dynamic Positioning Systems
- Analysis techniques for system reliability - Procedure for failure modes and effects analysis (FMEA) - CEI/IEC 812:1985
- BSI Standard, BS 5760-5:1991: 'Reliability of Systems, Equipment and Components', Part 5: 'Guide to Failure Modes, Effects and Criticality Analysis (FMEA and FMECA)
- Det Norske Veritas - Rules for the Classification of Steel Ships - Part 6, Chapter 7, Dynamic Positioning Systems - July 2001
- CEI/IEC812 – Analysis techniques for system reliability - Procedure for failure modes and effects analysis (FMEA)
- IEC Standard, IEC 60812: 'Analysis Techniques for System Reliability - Procedure for Failure Mode and Effects Analysis (FMEA)'
- IMCA Publication "Guidelines for the Design and Operation of Dynamically Positioned Vessels" (IMCA Document M 103 February 1999)
- IMCA – The IMCA Database IMCA M 156: Dynamic Positioning Incidents 1990-99
- IMCA Publication "Reliability of Position Reference Systems for Deepwater Drilling" (IMCA Document M 160 January 2001)
- IMCA Publication "Power Management System Study" (IMCA Document M 154 January 2000)
- IMCA Publication "Proceedings of the 2001 IMCA Marine Division Annual Seminar and Workshops" (IMCA Document M 164 October 2001)
- IMO - Guidelines for Vessels with Dynamic Positioning Systems – MSC/Circ 645 6th June 1994
- IMO MSC Resolution 36(63) Annex 4 – Procedures for Failure Mode and Effects Analysis (HSC Code)
- Lloyds Register - Rules and Regulations for the Classification of Ships, v8.1 July 2000
- US Department of Defense MIL-STD-1629A