Guidance on
Failure Modes and Effects Analysis (FMEA)

International Marine Contractors Association

www.imca-int.com

IMCA M 166 Rev. 1
April 2016

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 activities that relate to all members:
- Competence & Training
- Safety, Environment & Legislation

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 five regional sections which facilitate work on issues affecting members in their local geographic area – Asia-Pacific, Central & North America, Europe & Africa, Middle East & India and South America.

IMCA M 166 Rev. 1

ABB, DNV GL, ENSCO, Global Marine Consultants and Surveyors, Global Maritime, Haarseth DP & Marine Services, M3 Marine, Maritime Assurance & Consulting, Marine Cybernetics, Noble Drilling Services, OCIMF, Saipem, Shell, Subsea 7, Teekay and Transocean assisted in the review of this document.

www.imca-int.com/marine

If you have any comments on this document, please click the feedback button below:

feedback@imca-int.com

Date	Reason	Revision
April 2002	Initial publication	
April 2016	Full rewrite	Rev. 1

Guidance on Failure Modes and Effects Analysis (FMEA)

IMCA M 166 Rev. 1 – April 2016

1 Introduction to FMEA 1-1

1.1 Introduction 1-3
1.2 The Failure Modes and Effects Analysis (FMEA) 1-3
1.3 The Beginnings of FMEA 1-4
1.4 FMEA Methods of Analysis 1-5
1.5 Level of FMEA Analysis 1-6
1.6 Limitations of FMEA 1-6
1.7 The Uses of an FMEA 1-7
1.8 Meeting FMEA Standards 1-8
1.9 Industry Guidance on FMEA 1-9
1.10 IMCA Safety Flashes 1-10
1.11 Classification Societies and their Requirements for FMEA 1-10
1.12 Background and Explanations behind DP Class 2 and DP Class 3 1-11
1.13 DNV GL Notations DPS 2 and DPS 3 1-13
1.14 Enhanced DP Notations 1-13
1.15 Worst Case Failure Design Intent and Worst Case Failure 1-14
1.16 Redundancy 1-14
1.17 Mal-operation Defeating Redundancy 1-16
1.18 Hidden Failures 1-17
1.19 System Configuration 1-17
1.20 System Modification 1-17
1.21 DP Operations with Closed Main Bus Tiebreakers 1-17
1.22 DP 3 and the Backup DP System 1-18
1.23 The DP Vessel and the Mission 1-18
1.24 Software FMEA 1-19
1.25 Hardware-in-the-Loop (HIL) Testing 1-20
1.26 Interactive FMEAs and other Decision Support Tools 1-21
1.27 FMEAs of Non-Redundant Systems 1-21

2 Specifying an FMEA 2-1

2.1 Prequalification 2-3
2.2 Baseline of Specification 2-3
2.3 Overview 2-4
2.4 Depth of the FMEA 2-4
2.5 Objective of FMEA 2-5
2.6 Prerequisites of an FMEA 2-5
2.7 FMEA Proving Trials Plan 2-6
2.8 FMEA Management 2-6
2.9 Vendor FMEA Documents 2-7

2.10 Failure Modes, Effects and Criticality Analysis (FMECA) 2-7
2.11 Final Documentation Required 2-8
2.12 Example of a Specification for an FMEA for a DP Vessel 2-8

3 DP FMEA Methodology 3-1

3.1 The FMEA Process 3-3
3.2 FMEA Objective 3-5
3.3 FMEA Methodology 3-5
3.4 The FMEA Report 3-21
3.5 FMEA Management Guidance 3-31
3.6 FMEA Verification 3-38
3.7 Updating of an FMEA 3-40
3.8 DP Incident Follow-up 3-41
3.9 Additional Studies to Complement the FMEA Process 3-42

4 DP FMEA Proving Trials 4-1

4.1 Introduction 4-3
4.2 Reasons for FMEA Testing 4-3
4.3 DP FMEA Proving Trials 4-3
4.4 Annual DP Trials and Five-Yearly Trials 4-5
4.5 Customer Acceptance Test (CAT) and Shipyard Trials Tests 4-6
4.6 Classification Society Requirements for Testing 4-7
4.7 Prerequisites for FMEA Testing 4-7
4.8 FMEA Trials Team 4-8
4.9 DP FMEA Proving Trials Test Programme 4-8
4.10 Use of Gap Analysis Tool 4-10
4.11 FMEA Test Programme for Alongside and At Sea 4-11
4.12 Cross Component Groups (X Group) Testing 4-11
4.13 FMEA Trials Management 4-12
4.14 Pre- and Post-Trials Meetings 4-13
4.15 Deviations from Trial Prerequisites 4-14
4.16 Conduct of the FMEA Trials 4-14
4.17 Testing On and Off DP 4-15
4.18 FMEA Test Results 4-15
4.19 Concerns 4-16
4.20 Guidance on Handling Disputes 4-16
4.21 Pre-FMEA Trials Tests 4-17
4.22 Post FMEA Trials Retesting 4-17
4.23 Electrical Testing and Safety 4-18
4.24 Electrical Testing of Closed Bus Tie Operational Mode 4-18
4.25 Advanced Test Methods 4-20
4.26 Hardware-in-the-Loop (HIL) Testing 4-20
4.27 MODU Tests 4-23

Appendices

1 The Requirements for Compliance with IMO DP Class 1-1

2 Example List of DP System Components for Analysis with Guidance in Analysis 2-1

3 The IMCA DP Station Keeping Incident Database..... 3-1

4 Types of Failures Uncovered by FMEAs 4-1

5 DP FMEA Reference Documents..... 5-1

6 Glossary and Abbreviations..... 6-1

Introduction to FMEA

Introduction to FMEA 1-1

1.1 Introduction 1-3
1.2 The Failure Modes and Effects Analysis (FMEA) 1-3
1.3 The Beginnings of FMEA 1-4
1.4 FMEA Methods of Analysis 1-5
1.5 Level of FMEA Analysis 1-6
1.6 Limitations of FMEA 1-6
1.7 The Uses of an FMEA 1-7
1.8 Meeting FMEA Standards 1-8
1.9 Industry Guidance on FMEA 1-9
1.10 IMCA Safety Flashes 1-10
1.11 Classification Societies and their Requirements for FMEA 1-10
1.12 Background and Explanations behind DP Class 2 and DP Class 3 1-11
1.13 DNV GL Notations DPS 2 and DPS 3 1-13
1.14 Enhanced DP Notations 1-13
1.15 Worst Case Failure Design Intent and Worst Case Failure 1-14
1.16 Redundancy 1-14
1.17 Mal-operation Defeating Redundancy 1-16
1.18 Hidden Failures 1-17
1.19 System Configuration 1-17
1.20 System Modification 1-17
1.21 DP Operations with Closed Main Bus Tiebreakers 1-17
1.22 DP 3 and the Backup DP System 1-18
1.23 The DP Vessel and the Mission 1-18
1.24 Software FMEA 1-19
1.25 Hardware-in-the-Loop (HIL) Testing 1-20
1.26 Interactive FMEAs and other Decision Support Tools 1-21
1.27 FMEAs of Non-Redundant Systems 1-21

1.1 Introduction

This guidance document was commissioned by IMCA to highlight industry good practice in the use of failure modes and effects analysis (FMEA) techniques when applied to the technical systems associated with offshore vessels, in particular dynamic positioning (DP) systems. It is an update of the original document IMCA M 166 which was published in 2002. The four sections and appendices are designed to be read separately or as a single document. If read as a single document, the reader will find some repetition in the text.

Standards, guidelines and class rules are referenced throughout this document. These may be updated/ changed at regular intervals. It is incumbent on all persons specifying, carrying out FMEAs or carrying out FMEA reviews to ensure that the standards, guidelines and class rules they are using are the ones in current use and are applicable for their specific project.

An FMEA is an easy to use yet powerful proactive engineering quality tool that assists in the identification and removal of weak points in the early design phase of products and processes. It is a technical document and a statement of fact and not opinion.

When reading this guidance 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. A team of analysts expert in the FMEA technique and fully conversant in the architecture and operation of the systems or processes to be analysed is essential to ensure a comprehensive final product. This document is intended to guide the reader through the FMEA process. It is not intended to teach the skills necessary to analyse the systems and sub-systems comprising a DP system. The assumption is that the members of the FMEA team already have the in-depth knowledge of their specialist discipline or disciplines and the skills necessary to analyse the relevant systems.

Whilst the emphasis of this document is on DP systems, FMEA techniques can be applied to any system, whether applied to land, sea or air based equipment or systems, which require that 'no single failure should cause a total failure of the system or process'.

The document explains the history and development of FMEA and the role of FMEA in classification. Specifying an FMEA, the depth of FMEA reporting, the procedures used and the format of the final FMEA report are discussed. The additions to the FMEA process which can complement the analysis and the benefits of subjecting non-redundant systems to FMEA are briefly explored.

It is anticipated that these guidelines should assist in producing more consistent and thorough FMEAs.

1.2 The Failure Modes and Effects Analysis (FMEA)

Why do we need an FMEA? Murphy's Law states that 'Everything that can fail, will fail', 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!' Unfortunately, what is not known is when it will fail. Consequently, during the design of a system or product, the designer should 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?

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.

In the case of a DP vessel, the FMEA is part of the vessel's assurance programme. This is a product of international regulations, IMCA guidance, other relevant standards and company procedures which are based on established reliability engineering standards and could demonstrate the vessel's compliance with the identified requirements[1].

1 IMCA M 204 – *Vessel assurance*

The FMEA should be viewed, first and foremost, as a safety item necessary for the assessment of a vessel's capability to perform its function in a safe and proper manner. It can only be used as such if it has been continuously reviewed and updated to include all changes and modifications to the vessel's systems throughout its life cycle. Management of the FMEA is discussed in section 3.

When assessing the charter or purchase of an existing DP vessel, it is essential that the FMEA is viewed as a critical item and placed high on any vessel pre-charter or pre-purchase checklist.

The findings of the FMEA should be incorporated into the operations, emergency and maintenance manuals. These findings can then be fed into the risk assessment for each vessel task and 'standing orders'. It is necessary, for example, that:

- The DP operators (DPOs) and engineering staff need to know what corrective actions are required should the vessel's DP system be subjected to a specific failure.
- The maintenance supervisor needs to know what the impact on redundancy is if an item of equipment is taken out of service. Therefore, it would be beneficial to cross-reference the FMEA with the planned maintenance system.
- The risk assessment meetings have the right marine expertise present that is fully conversant with the FMEA contents.

It is necessary to provide sufficient detailed description of the vessel's systems to allow the FMEA practitioner to understand how the systems work at a level that allows them to correctly assess their failure modes. It is not necessary to detail materials, dimensions, etc. except when describing the systems and the redundancy concept. The description of the systems provides a certain amount of training information for ship's staff and improves operator understanding. Additionally, any findings arising from the FMEA process which have an impact on operations should be included in the operations manual as well as the training manual.

1.3 The Beginnings of FMEA

The FMEA discipline was originally developed in the United States military. Military Procedure MIL-P-1629, *Procedures for Performing a Failure Modes, Effects and Criticality Analysis*, is dated November 9, 1949. It was used as a reliability valuation 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 FMEA to complement their design processes, notably the automotive industry.

Dynamic positioning (DP) started to be applied to offshore oil industry assets on a large scale in the early 1980s, particularly with the exploration of the North Sea and deeper water oil and gas fields world-wide. The initial DP system development had begun in the USA with drilling ships in the late 1960s and early 1970s.

The offshore industry first began using the FMEA technique in the 1970s and 1980s. Current requirements for redundancy demonstrations on DP vessels derive from an approach developed during the mid-1980s for the Norwegian Maritime Directorate (NMD), intended to improve the classification rules dating from the mid-1970s. The NMD approach was adopted by the DP Vessel Owners Association (DPVOA) in 1991, introducing the annual audit. The DPVOA was a trade organisation which merged with the Association of Offshore Diving Companies to form IMCA. The NMD document was developed into an international standard by the International Maritime Organization (IMO) in 1994 (IMO MSC Circular 645 – *Guidelines for Vessels with Dynamic Positioning Systems*). Classification society requirements have since been adjusted for consistency with this IMO document, including the later requirement for FMEA.

Although the influence of auditing initially (in the 1980s) rapidly reduced the number of DP incidents, particularly serious ones, it was found that very little on-going improvement occurred after the annual audit was introduced. A series of incidents in 2002 (all in the UK sector of the North Sea) brought the matter to the attention of the UK's Health, Safety and Environment (HSE) Agency, which commissioned a study from Det Norske Veritas (DNV), suggesting that errors were not being designed out of the vessel systems by shipyards, contractors and suppliers.

The HSE/DNV *Review of Methods for Demonstrating Redundancy in Dynamic Positioning Systems for the Offshore Industry* (2004) confirmed this, concluding that vessel operators and managers were not always applying the guidance available and, in many cases, were not even aware of it. It also stated that the perceived weaknesses in the FMEA technique were mainly as a result of:

- lack of application of adequate FMEA expertise;
- failure to follow a systematic procedure, i.e. weakness in the procedures for specifying, conducting and verifying the FMEA;
- being commissioned too late to influence design;
- failure to outline all operating modes when specifying the FMEA.

The FMEA technique clearly needs to be applied correctly. This can be achieved to some extent by:

- putting in place the verifiable systems to ensure that the FMEA practitioners are suitably qualified;
- updating and revising guidance documents where necessary and ensuring that they are complied with; and
- improving the specification of an FMEA as to what has to be covered, including all of the vessel operating modes.

Many issues with weak FMEAs can be avoided at the initial stage by a much more detailed FMEA specification. Specifications for FMEA should be sufficiently comprehensive to ensure that any information provided by manufacturers' FMEAs is detailed and useful, and that the information can be easily integrated into the overall FMEA for the vessel's DP system – see section 2.

Whilst FMEAs have improved through more industry guidance and through greater scrutiny by owners and class, some of these weaknesses still persist. One of the aims of this guidance document is to bring together the guidance within the industry, and to improve the management, performance and verification of FMEA.

1.4 FMEA Methods of Analysis

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 hugely time consuming and has now been all but abandoned, even by the US Military.

A top down FMEA starts from the overall system level and progresses to the next level down, or sub-system level, and so on down to the equipment item and component level. However, if it can be 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 sub-system 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 as thorough as the bottom up method, but is obviously less time consuming.

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.

1.5 Level of FMEA Analysis

It is frequently asked how deep into the system the FMEA needs to progress to achieve a thorough analysis, i.e. to system level, sub-system level, and so on down to component level. The answer to this question is, basically, 'as far as it takes', meaning that the FMEA analysts should pursue their investigations until completely satisfied that all possible failure modes and system responses to those failures are identified and confirmed.

The analysis should proceed by identifying all systems and sub-systems relating to, or potentially influencing, the vessel's DP system that are likely to suffer a failure which could lead to a loss of DP. It should continue by identifying all weaknesses in each of these systems and analyse how each identified weakness is managed.

This can only be achieved by using a multi-disciplined team of skilled FMEA practitioners with considerable experience of carrying out FMEAs of DP systems using a structured analysis procedure. The success of the analysis relies on the judgement of these FMEA practitioners as to how far the analysis should proceed such that all exposure to risk of DP failure has been identified and minimised as far as is reasonably practicable.

The depth of analysis of the system interfaces should also be sufficient to ensure the FMEA objectives are met, and again this is up to the judgement of the FMEA team.

A gap analysis can be carried out on the FMEA to ensure all aspects of the system being subjected to FMEA have been properly covered (see section 3.5.1). Industry guidance also contains gap analysis methodology[2].

1.6 Limitations of FMEA

Although the FMEA methodology is highly effective in analysing various system failure modes, this technique has several limitations:

Human error: The analysis of human error is limited. A traditional FMEA uses potential equipment failures as the basis for the analysis. All of the questions focus on how equipment functional failures can occur. A typical FMEA addresses potential human errors only to the extent that human errors produce equipment failures of interest. Mal-operations that do not cause equipment failures are often overlooked in an FMEA. A combination of both can lead to a significant failure mode.

Single failures: A traditional FMEA tries to predict the potential effects of specific equipment failures. These equipment failures are generally analysed one by one, which means that important combinations of equipment failures may be overlooked.

External influences: A typical FMEA addresses potential external influences (environmental conditions, system contamination, external impacts, etc.) only to the extent that these events produce equipment failures of interest. External influences that directly affect vessel safety and crew safety are often overlooked in an FMEA if they do not cause equipment failures.

Risk analysis: An FMEA is not in itself a risk analysis. The results of the FMEA are dependent on the configuration of the system. The effects of certain equipment failure modes will vary widely depending on the configuration of the system. An FMEA generally accounts for the possible effects of equipment failures during one mode of operation only or a few closely related modes of operation. It has been known for a system configuration that has not been considered in the analysis to permit a serious incident. In analysing a system, the FMEA should therefore take into account every operational mode in which the DP system is intended to be operated.

Software: System software may be seen as a common mode failure as the same software is used in redundant systems. Where FMEA is concerned, analysis of the control software is not normally carried out. Only practical failure testing of the system, either during factory tests using the actual hardware, or during shipboard commissioning and DP proving trials at sea, is used to prove the software. Success in determining every system response to failure is dependent on the extent of the practical testing and on occasion this has been insufficient to reveal serious software errors.

2 MTS *Technical and operational guidance* – TECHOP ODP 04 (D) (FMEA Gap Analysis), September 2012

1.7 The Uses of an FMEA

Whenever the function of an item of equipment or system requires it to work in an environment in which any failure has the potential to have a catastrophic effect on the process, it is responsible design practice to carry out an FMEA as part of an operations and maintenance strategy. Consequently, a number of people, organisations, bodies, etc., are very interested in the findings of an FMEA. These include:

Classification Societies: The classification societies such as Lloyd's Register (LR), DNV GL, American Bureau of Shipping (ABS) and Bureau Veritas (BV) all issue requirements in the form of class notations for DP vessels. These implement the IMO guidelines (refer to IMO MSC/Circ.645 1994; and subsequent amendments) with more specific requirements. The classification societies also specify the documentation that must be provided for approval and the scope of testing.

An FMEA is one of the documents required for DP vessels with class notations equivalent to IMO equipment classes 2 and 3 for compliance with the acceptance criteria. These DP classes will be discussed later in this document. FMEAs of DP vessels with class notation equivalent to IMO equipment class 1 are covered in section 1.27.

Task Risk Assessors: The FMEA is used as part of the overall risk based assessment carried out prior to critical DP operations, such as drilling, diving and working close to fixed structures. IMO MSC/Circ.645 states: 'The equipment class of the vessel required for a particular operation should be agreed between the owner of the vessel and the customer based on a risk analysis of the consequence of a loss of position. Else, the Administration or coastal State may decide the equipment class for the particular operation.'

In order to assess the risk of a certain task a vessel is to accomplish, the task risk assessors may use documentation such as CAMOs, TAMs, ASOGs, WSOGs and FSOGs.

The critical activity mode of operation (CAMO) sets out the most fault tolerant configuration for the DP system and associated plant and equipment. The CAMO should be implemented for all critical activities undertaken by the vessel. For DP class 2/3 vessels the CAMO usually defines the most robust fault tolerant configuration of the DP system ensuring that the effects of a single point failure do not exceed the vessel's worst case failure as identified in the FMEA[3].

In order for the CAMO to be determined, the worst case failure should be fully understood. As the FMEA objective is to determine the worst case failure, the vessel's FMEA is reviewed in producing the CAMO. It is usually presented in tabulated form. IMCA M 220 – *Guidance on operational activity planning* – gives guidance on the items typically contained in the CAMO and an example of a CAMO table. References to the safest mode of operation (SMO), which is synonymous with CAMO, may be found in various industry documents, however, this term is being replaced by CAMO.

The CAMO may be replaced by the task appropriate mode (TAM) where it is considered acceptable to operate with the vessel's DP system and equipment configured to a lower level standard of fault tolerance. TAM is a risk-based operating mode in which the DP vessel may be set up and operated, accepting that a single point failure could exceed the vessel's identified worst case failure. TAM is usually applied to less critical activities where a risk assessment determines that the consequences of exceeding the vessel's identified worst case failure are acceptable[3].

The vessel's FMEA is also reviewed when a vessel is being considered for a certain task so that the operational guidelines can be prepared prior to it commencing work. The operational guidelines are termed activity specific operational guidelines (ASOG), well specific operational guidelines (WSOG) and field specific operational guidelines (FSOG)[4].

The ASOG sets out the operational, environmental and equipment performance limits considered necessary for safe DP operations while carrying out a specific activity. The ASOG will vary depending on the activity and is unique to that activity[5]. For example, the type of activity could be diving, pipelay, heavy lift, construction, supply, etc. The WSOG is specific to drilling operations and, in particular, the actual well the vessel is to drill. The FSOG is specific to the special requirements of the field in which the vessel is to work.

3 IMCA M 220 – *Guidance on operational activity planning*
4 Marine Technology Society (MTS) DP Technical Committee DP (Dynamic Positioning) *DP operations guidance*
5 DNV GL Recommended Practice (RP), DNV-RP-E307 – *Dynamic positioning vessel operation guidance*, January 2011

ASOG, WSOG and FSOG are also generally presented in tabulated format. The tables set out various levels of operator action as these limits are approached or exceeded. IMCA M 220 gives guidance on the items typically contained in the ASOG and an example of an ASOG table.

DP Operations Manual: The vessel's DP operations manual should refer to the FMEA. It should give a précis of the findings of the FMEA such that the DPOs and engineering staff are fully aware of the vessel's limitations under failure conditions. It should give guidance on the actions to be taken in the event of such failures.

Crew Training: The crew should have access to and become familiar with the FMEA to increase their knowledge of the operation of their vessel over and above that contained within the DP operations manual. Interactive FMEA guides are available which have integral training facilities which are intended to make the learning process more user friendly.

Maintenance Personnel: Maintenance personnel require knowledge of the FMEA so that they are aware of any critical areas which could potentially give rise to a serious problem in the event of a failure. Prior to any vessel maintenance, this knowledge can be incorporated into effective maintenance planning.

Shore Personnel: The FMEA should be made available to all those in the shore base who have a responsibility for the operation and maintenance of the DP system.

Safety: As mentioned above, the FMEA should be part of the pre-setting-to-work risk assessment. As the FMEA is considered a safety related document, safety personnel involved in risk analysis should have some knowledge of the contents, in particular the limitations of the DP system and actions to be taken in the event of a failure.

Builder: In the case of a new build vessel, the builder should act upon any findings from the FMEA which may require a modification to the system, in particular, those which may contravene class requirements, guidelines or which have the potential to have a detrimental effect on the safety of personnel, assets or environment.

Vessel Owners/Operators: Vessel owners/operators require an FMEA to satisfy their clients chartering a vessel that the vessel complies with specified requirements. It is also good practice for an owner to have a thorough FMEA carried out on their vessels as it provides the assurance that any potential risk has been identified. The FMEA provides the necessary input so that mitigation measures and procedures can be developed to mitigate the effects of any failure mode. The FMEA will assist in development of the operations manuals and training programmes. The FMEA should be one of the inputs to the CAMO for a DP vessel.

Charterer: The charterer will review the FMEA to ensure that the vessel will fulfil the contractual requirements. Together with the ASOG, WSOG or FSOG, the FMEA is part of the vessel acceptance criteria such that the charterer 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 risk.

Regulatory Authorities: National regulatory authorities, such as the UK Health & Safety Executive (HSE), often require an FMEA as part of the safety case for an offshore installation or DP vessel. 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.

1.8 Meeting FMEA Standards

If an FMEA is to meet its purpose, and not be just an academic exercise to meet class and flag state requirements, it should be carried out to a rigorous standard. It is the owner's responsibility to ensure this is achieved.

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 fit for purpose and will be accepted by all parties who have an interest in it.

Section 3.3.4 sets out the standards that may be used in compiling an FMEA. Appendix 5 sets out the documents which should be consulted by the different participants and responsible persons who contribute to maintaining a valid and up to date FMEA.

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

- 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)*;
- 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);
- US Department of Defense military standard MIL-STD-1629A (1980) has since been withdrawn but is still quoted and used occasionally.

1.9 Industry Guidance on FMEA

Whilst sound guidance can be obtained from IMCA (refer to section 3.3.6) in varying forms on the design and operation of DP vessels, training and certification can also be obtained from government and regulatory bodies such as:

- International Maritime Organization (IMO);
- UK Health & Safety Executive (HSE);
- UK Department of Energy (DEn);
- Oil & Gas UK (formerly UKOOA);
- Norwegian Maritime Directorate (NMD) (NMA);
- Classification societies;
- US Coast Guard (USCG);
- Nautical Institute (NI);
- Marine Safety Forum (MSF);
- Maritime & Coastguard Agency (MCA).

Additionally, international companies such as oil majors produce their own guidance documents concerning the system verification and operation of DP vessels.

IMO: A most important guideline and one that is most frequently quoted is IMO MSC/Circ.645, *Guidelines for Vessels with Dynamic Positioning Systems*, 1994, also published as IMCA 113 IMO. Whilst it has been in the industry domain for a long time and is still as valid now as it was in 1994, readers should be aware that IMO MSC/Circ.645 is currently under review at the time of revising IMCA M 166 in order to reflect advances in technology and operations[6].

The Annex to information note IMCA M 04/04 – *Methods of establishing the safety and reliability of DP systems* – provides guidance on the IMO guidelines in IMO MSC/Circ.645 1994. IMCA M 04/04 in itself is extremely detailed and comprehensive but, as no document can be inclusive of all potential single point failures, it should be used as guidance.

The IMO High Speed Craft (HSC) Code addresses FMEA issues for compliance purposes and is a useful descriptive document for reference purposes in understanding the FMEA process.

Flag State: The flag state has to fulfil certain obligations regarding safety of navigation and seaworthiness of the ship when allowing ships to fly its flag, in particular with respect to:

- construction and equipment of the ship – Art. 94(3)(a);
- pre-registration and post registration surveys of ships by approved surveyors – Art. 94(4)(a)

However, flag states tend to delegate their technical duties to Recognised Organisations (ROs); these ROs are usually classification societies. Recognised Organisation is a legally defined term.

6 International Maritime Organization MSC 90/25/17 *Proposed amendments to the guidelines for vessels with dynamic positioning (DP) systems* (IMO MSC/Circ.645) 2012

US Coast Guard: The US Federal Register states that: 'Failure of a DP system on a vessel conducting critical operations such as oil exploration and production could have severe consequences including loss of life, pollution, and property damage. This is particularly true for Mobile Offshore Drilling Units (MODUs), where a loss of position could result in a subsea spill and potentially catastrophic environmental consequences'[7].

In response to certain incidents in the US Gulf and following public consultation, the USCG has adopted the DP operations guidance which was prepared through the Dynamic Positioning Committee of the Marine Technology Society (MTS)[8]. Note that this MTS DP operations guidance document was also the basis of DNV GL's recommended practice on DP vessel operations guidance[9].

The US Coast Guard Supplemental Requirements for Qualitative Failure Analyses (QFA) require that US flagged vessels must have an FMEA or 'qualitative failure analysis' for many of the same systems for which classification societies require FMEAs, e.g. propulsion controls, microprocessor-based system hardware, safety controls, automated electric power management, automation required to be independent that is not physically separate, and any other automation that potentially constitutes a safety hazard to the vessel or personnel in case of failure[10]. The QFA should enable the designer to eliminate single points of failure. An FMEA will be accepted by the Coast Guard as a QFA if a qualitative analysis is included. The QFA is required to be submitted to the USCG for approval, or to a classification society authorised to carry out such reviews of these systems on behalf of the USCG.

The vital automation systems of these vessels, including the DP system plans, must also undergo a USCG review called the design verification test procedure (DVTP)[11]. The DVTP specifies the methods used to validate the automation system failure modes and effects and receives final USCG approval only after satisfactory completion of testing and incorporation of any changes found necessary.

1.10 IMCA Safety Flashes

IMCA safety flashes are an important way of communicating problems to look out for in the offshore industry including DP incidents. They assist owners/operators to be more aware of how serious incidents can occur. However, how many owners/operators read them and think 'Hey, that was bad luck' and then file them away, or how many think 'Could that happen on any of my vessels?' and then investigate? FMEA practitioners should read all safety flashes concerning DP incidents to increase their knowledge base and thus input more value into the FMEA.

The IMCA DP station keeping incident reporting scheme has provided the DP industry with an important source of safety information over many years. Annual reviews of DP incidents are compiled using anonymous event trees and lessons can be learnt from the reported initiating event and causes of the DP event.

The reporting scheme name has changed to remove the word 'incident' and has been replaced with 'event' to encourage reporting of more minor events that could potentially lead to major incidents. From 2016, IMCA will provide industry with opportunities to learn from reported DP station keeping events received. DP safety flashes are issued on a periodic basis and presented as anonymous event trees with a summary compiled by IMCA's DP Focused Workgroup to provide opportunities to learn from the event. In addition, and included in the yearly review of DP station keeping events will be initiating events and causes which will be compiled into a gap analysis tool so that individual vessels will be able to easily view the information. It is intended that this tool will be used by vessel owners/operators and crew to assess whether a reported DP event could happen on their vessel.

1.11 Classification Societies and their Requirements for FMEA

Most classification societies have rules for DP vessels and requirements for FMEA. The classification societies also specify the documentation that must be provided for approval and the scope of testing. Amongst the documentation required for DP vessel compliance with the class notations equivalent to DP class 2 and DP class 3 is an FMEA. There is no requirement for DP system FMEAs for DP class 0

7 Federal Register/Vol. 77, No. 87 2012
8 Marine Technology Society (MTS) DP Technical Committee DP (Dynamic Positioning) *DP operations guidance*
9 DNV GL Recommended Practice (RP), DNV-RP-E307 – *Dynamic positioning vessel operation guidance*, January 2011
10 US Code of Federal Regulations (46 CFR 62.20-3); USCG MSC *Guidelines for qualitative failure analysis* Procedure Number E2-18 also refer
11 USCG Marine Technical Notice 02-11 – *Review of vital system automation dynamic positioning system plans*

and DP class 1 vessels. Class rules and guidelines are referenced throughout this document. As these may be updated/changed at regular intervals, all persons involved with FMEAs of DP vessels should ensure that they are familiar with those rules and guidelines in current use and applicable for their specific project.

In terms of rules and regulations, in general there is increasing reference to the International Standard ISO 31010 'Risk Management, Risk Assessment Techniques' which includes FMEA. Lloyd's Register in particular makes such a reference in its *Rules and regulations*, leaving it up to the designer to select and justify the technique used. Note: ISO 31000 represents the risk management standard whilst ISO 31010 is guidance on various risk assessment techniques.

Whomever has the contract with the classification society to provide the FMEA (e.g. the shipyard or the vessel owner) has the responsibility for making sure the FMEA reports are submitted to the relevant class. Class review requires time, therefore the FMEA for a new DP vessel should be completed in sufficient time to allow class to review it without causing undue risk of delay to vessel delivery. As part of the FMEA process, any concerns arising from the analysis that may have an impact on DP class should be discussed with the shipyard.

Once the FMEA has shown the vessel meets the specified criteria, with respect to the DP system, (design/survey/test/review) the FMEA is approved and the vessel is assigned its notation after rules approval and survey. The FMEA is then archived. However, there is a mechanism whereby the ship owner needs to inform class and regulatory authorities of any changes to the vessel's systems and class will then assess whether or not the notation is affected. Any modifications to the DP system that relate to a class requirement should result in the submission of a revised FMEA report to class.

1.12 Background and Explanations behind DP Class 2 and DP Class 3

The location in which a DP vessel is allowed to work and the scope of the work it is going to carry out is governed by the degree of fault tolerance required and by the failure modes identified in the analysis of the DP system. This was originally addressed by the Norwegian Maritime Directorate (NMD) and IMO and led to the introduction of 'consequence classes'[12] and 'equipment classes'.

The 'consequence' of failure was grouped 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.

Consequence class 0 and consequence class 1 operations were operations where the vessel would be in open water, or in a position where the combined effects of wind and current would take the vessel away from any nearby structure or other vessel should it suffer a failure in the DP system. Operations such as these would be carried out by a vessel with little or no redundancy in the DP system. These vessels were termed by IMO as equipment class 0 and equipment class 1 vessels or DP class 0 and DP class 1 vessels, defining the requirements of the DP system.

Consequence class 2 and consequence class 3 operations were operations where the vessel would be in a position where the combined effects of wind and current would take the vessel toward any nearby structure or other vessel should it suffer a failure in the DP system or when undertaking critical operations such as diving operations with the divers working in enclosed subsea structures. Vessels carrying out class 2 and class 3 operations were termed equipment class 2 and equipment class 3 vessels, or DP class 2 and DP class 3 vessels. These required more redundancy in their DP systems as the consequences of system failure and resulting loss of position when carrying out DP critical operations could be considerably more than when carrying out consequence class 0 and consequence class 1 operations.

12 IMO Sub Committee on Ship Design and Equipment 33rd Session Agenda Item 17 *Guidelines on dynamic positioning systems*, submitted by Norway, January 1990

IMO defines the vessel 'equipment' classes by their worst case failure modes[13]. IMO MSC/Circ.645 1994 defines three equipment classes; class 1, class 2 and class 3.

For equipment class 1, a loss of position may occur in the event of a single fault.

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 or passive 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 their reliability is proven. Single failure criteria include any active component or system, e.g. 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 2, a single inadvertent act is classed as a single failure if such an act is reasonably probable.

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 static components (cables, pipelines, manual valves, etc.) in any one watertight compartment are assumed to fail due to the effects of fire or flooding and all static components in any one fire subdivision are assumed to fail due to the effects of fire or flood. Equipment class 3 also classes a single inadvertent act 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 engine rooms each separated by an A-60 bulkhead. In the case of a two engine room system, typically half of the generating capacity would be located in one engine room and the other half in the other engine room. In other cases, the requirement is that the vessel is not operated in conditions where the loss of the engine room with the largest capacity would lead to a loss of position. The switchboard room would similarly be split into two rooms each separated by an A-60 bulkhead 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 directly from both sections of switchboard. With the effect of fire being considered, a backup DP control station would be located in a compartment separated from that in which the main control station is located by an A-60 bulkhead. Cabling to items of redundant equipment would not be run through the same compartment, but be run segregated such that a cable failure or a fire would not affect both units. This implies that loss of all systems in relevant fire zones should be tested.

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.

Classification societies require FMEAs for DP class 2 and DP class 3 vessels. There is no requirement for FMEAs for DP class 0 and DP class 1 vessels. However, owners of these vessels have commissioned FMEAs in order to learn more about the weaknesses inherent in their vessels. In this way, more comprehensive guidance can be given in the DP operations manuals and emergency procedures manuals and the DPOs will be better prepared in the event of an emergency. An example of the worth of an FMEA of a DP vessel is that the FMEA of one DP vessel revealed that a hidden fuse failure would prevent changeover to joystick on loss of the simplex DP system. The fuse failure was subsequently alarmed.

IMO equipment class 2 is generally consistent with ABS DPS-2, DNV GL DYNPOS AUTR and LR (AA) and IMO equipment class 3 is generally consistent with ABS DPS-3, DNV GL DYNPOS AUTRO and LR (AAA).

13 IMO MSC/Circ.645 – *Guidelines for vessels with dynamic positioning systems*, June 1994 (also IMCA 113 IMO)

Some DP vessel owners require their vessels to have DP systems that lie somewhere between the IMO class 2 and class 3 requirements. 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 is as the owner intended. This is best included in an FMEA of the overall system.

Further guidance on design and operation can be found in IMCA M 103 – *Guidelines for the design and operation of dynamically positioned vessels*.

1.13 DNV GL Notations DPS 2 and DPS 3

DNV GL have issued DP notations which are less stringent than DYNPOS-AUTR and DYNPOS-AUTRO. These are DPS 2 and DPS 3 respectively. The DNV GL rules also include DPS 0 and DPS 1 which are less stringent than DYNPOS-AUTS and DYNPOS-AUT.

DYNPOS-AUTRO, DYNPOS-AUTR, DYNPOS-AUT and DYNPOS-AUTS all have additional requirements to achieve higher availability and robustness as compared to DPS 3, DPS 2, DPS 1 and DPS 0 respectively.

DNV GL rules require that redundancy shall be based upon running machinery. For example, a changeover of a single stern thruster from a failed power source to a healthy one would constitute a loss of power during changeover, i.e. stop before restart. An arrangement such as this would not be allowed in the design of a vessel classed DYNPOS-AUTR, however, it would be allowed under DPS 2 notation.

For DPS 2, where necessary for correct functioning of position reference systems, at least three vertical reference sensors (VRS) are to be provided for corrections. If VRS corrections are not required, then two VRS can be provided. Three must be provided for DYNPOS-AUTR.

1.14 Enhanced DP Notations

DNV GL and ABS have extended their DP notations. DNV GL has the additional notation DYNPOS-E/ER[14], and ABS has extended the DPS-2 and DPS-3 notations with EHS-C (control)[15]. Both notations are introduced in order to achieve enhanced reliability in DP control systems that utilise the technology within modern marine power plants. The new notations will have an impact on both the DP control system arrangement and the functionality in the DP control system. The DP control system must be designed with more separation on the communication links, as for a main DP control system and an independent joystick system.

The main objectives for the DNV DYNPOS-ER notation are to provide a dynamic positioning system with the following properties:

- redundancy in technical design;
- A-60 separation between redundancy groups in high fire risk area;
- A-0 separation between redundancy groups in other areas;
- watertight separation between redundancy groups below damage waterline;
- redundant main DP-control system;
- independent single alternative DP-control system;
- operator stations for main and alternative DP-control systems placed in the same space (e.g. the bridge);
- flexibility and increased availability of power and thrust by use of connected power systems, standby start and change-over.

A qualifier (A), if requested by the vessel owner, can be assigned, DYNPOS ER (A), which requires the vessel to undergo an annual survey according to the applicable five-yearly complete survey.

14 DNV GL *Rules for the classification of ships, newbuildings, special equipment and systems, Additional Class*, Part 6 Chapter 26 Dynamic Positioning Systems – Enhanced Reliability DYNPOS-ER, July 2010

15 ABS *Guide for dynamic positioning systems*, November 2013, updated July 2014

ABS enhanced system (EHS) notations recognise design features beyond current DPS-series notations. EHS-C notation for example requires enhanced reliability in the following equipment:

- DP control station and DP controller;
- DP data logger;
- capability plot;
- UPS.

For a vessel with a DPS-2 notation, the enhanced power and thruster system notation (EHS-P), the enhanced control system notation (EHS-C), fire and flood protection notation (EHS-F) or any combination may be assigned, though not EHS-F for DPS-3 as this is already addressed.

1.15 Worst Case Failure Design Intent and Worst Case Failure

Worst case failure design intent: The worst case failure design intent (WCFDI) is the basis for the design and operational criteria set out for the vessel at the concept stage. It is the single failure mode that can be tolerated which has the maximum effect on DP capability were it to occur. It usually relates to the number of thrusters, generators and control equipment that can simultaneously fail and reduce positioning capability following the single failure. The WCFDI should be specified in the contract/ specification for the DP vessel and the FMEA specification where the redundancy design intentions and the intended post failure DP capability in relation to worst case failures (WCF) should be described. It should be referenced in the FMEA. The WCFDI may also form part of the information submitted to class as part of the approval process. Post failure DP capability is the remaining DP capability following any failure. In addition, it should be specified for which technical system configuration(s) (system setup) the intended integrity should be in place.

Worst case failure: The worst case failure (WCF) is the identified single failure mode in the DP system resulting in the maximum detrimental effect on DP capability as confirmed by the FMEA study. It should, of course, not exceed the WCFDI unless it is proven that the vessel has an accepted post failure DP capability after the WCF identified in the FMEA has occurred.

1.16 Redundancy

Redundancy is the ability of a component or system to maintain or restore its function when a single failure has occurred. Redundancy can be achieved, for instance, by installation of multiple components, systems or alternative means of performing the function.

Redundant component: A redundant component is one of a number of components performing the same or similar function. Should any one component become unavailable when subjected to a single failure, the overall system function will not be lost.

Redundant equipment groups: A redundant equipment group is one of a number of groups of components performing the same or similar function. Should any one group become unavailable when subjected to a single failure, the overall function will not be lost.

With regard to position keeping, each redundant equipment group will include elements to control surge, sway and yaw, such that if one group is lost the remaining group or groups will still be able to continue to control surge, sway and yaw.

As stated above, worst case failure (WCF) is defined as the identified single failure mode in the DP system resulting in maximum effect on DP capability as determined through FMEA study[16]. Redundancy groups will be identified as a consequence of the single WCF.

There are no limits (above two) to the number of redundancy groups within an overall system, however, the groups will be identified in the FMEA and confirmed by FMEA testing. Each redundancy group should be analysed with the aim to prevent a propagation of a failure from one redundancy group to another.

Redundancy groups are described in depth in industry guidance documents[17]. These guidelines set out the application, objective, and contents of FMEA for redundant systems.

16 DNV GL Recommended Practice (RP), DNV-RP-E307 – *Dynamic positioning vessel operation guidance*, January 2011
17 ABS *Guidance notes on failure modes and effects analysis for class*, May 2015

They state that the objective of the redundancy design intention is to describe at a high level the distribution of systems and components into redundant equipment groups. Redundant equipment groups in a DP system require identifying, such that it can be established that each group is capable of controlling surge, sway and yaw forces. Refer to Figure 1-1.

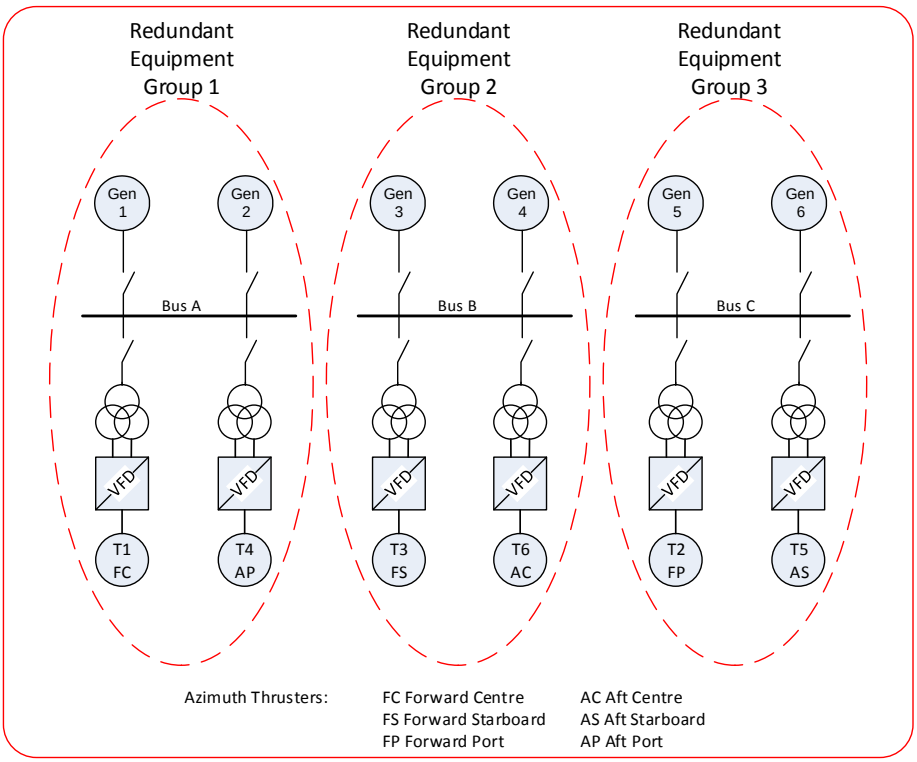


Figure 1-1 – Example of redundant equipment groups

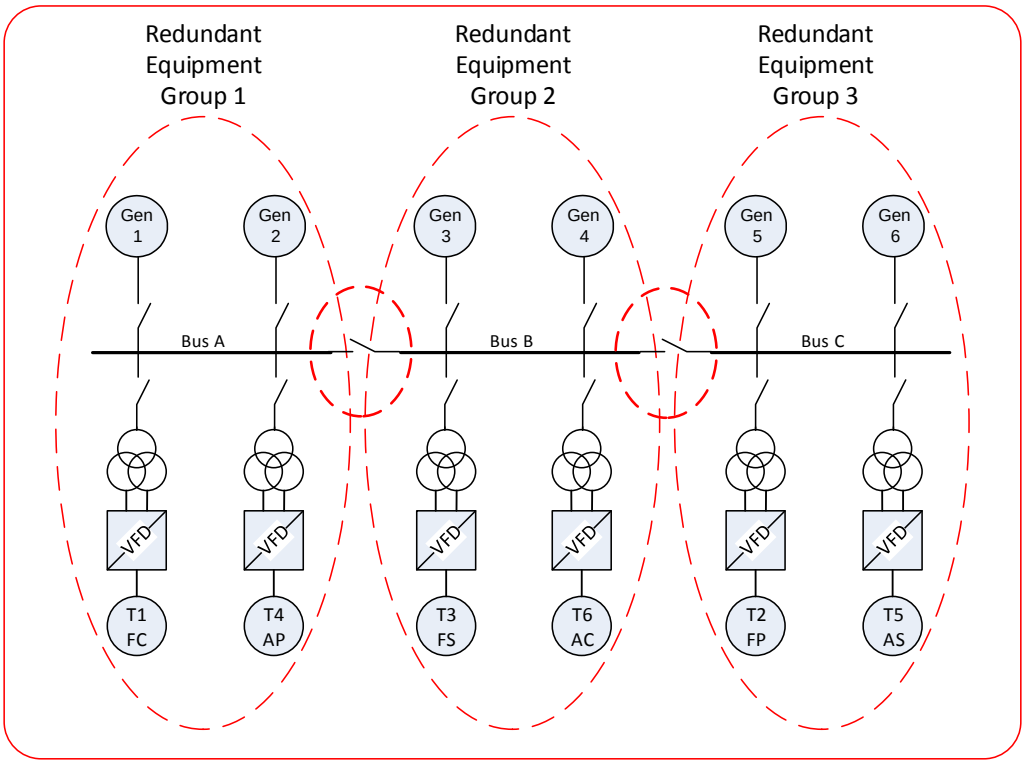


Figure 1-2 – Example of redundant equipment groups with cross connections

It is accepted that redundant component groups in a unit can either have no intersection, some common components, or be related by connecting components[18]. For example, normally the arrangement in Figure 1-1 would have bus tiebreakers connecting the three switchboard busses as in Figure 1-2.

Where cross connections between redundant groups exist, fault tolerance, fault resistance and the potential for fault propagation should be analysed by the FMEA and proven by testing. Refer also to section 4.12.

Should any connecting components be identified between redundant groups in the FMEA, emphasis is placed on the importance of analysing cross-connections and identifying the protective functions upon which redundancy depends. Dual supplied and changeover systems associated with more than one redundancy group can, in particular, prove problematical in that faults may have the potential to affect both redundancy groups.

An example is in the case of a DP 3 vessel where a thruster drive is capable of being dual supplied by power from more than one redundancy group. Consider the arrangement in Figure 1-3 with T3 and T5 drives (VFD) each being supplied simultaneously by both main switchboards. A potential problem for this type of arrangement is that a fire in either of the compartments containing T3 or T5 could affect the port side and starboard side cabling to the thrusters and propagate back to both main switchboards causing a total blackout. If the design is such that it cannot satisfy all requirements for DP class 3 with both feeds energised, T3 and T5 should be isolated completely with respect to power and auxiliaries from one of the redundancy groups.

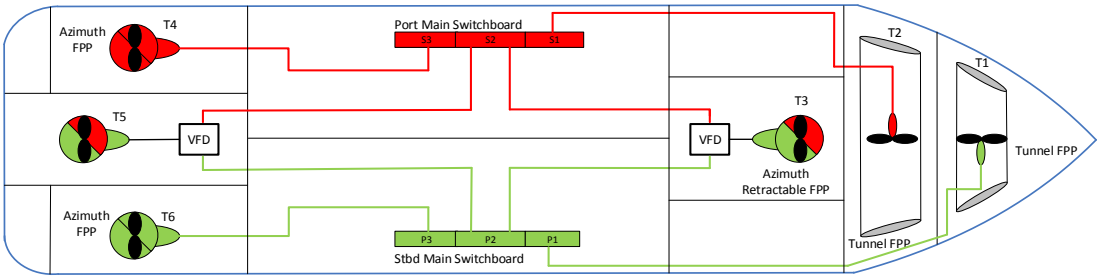


Figure 1-3 – Typical arrangement with dual supplied thrusters

Whilst the above example is confined to thrusters, there are other types of faults involving cranes or other mission equipment powered from redundant sources that may have the potential to affect more than one redundancy group.

For more details on the redundancy concept, refer to IMCA M 225 – *Example redundancy concept and annual DP trials for a DP class 3 construction vessel* – which describes the DP redundancy concept for a fictitious project and construction (P&C) vessel.

1.17 Mal-operation Defeating Redundancy

The FMEA technique does have limitations; for example, a traditional FMEA focuses on the effects of equipment functional failures. There is a need to identify credible acts of mal-operation that may defeat redundancy. Equipment mal-operations due to human error are more often overlooked in an FMEA. Therefore, a HAZID/HAZOP would provide a valuable supplement.

18 *Reference DNV GL Recommended Practice (RP) DNV-RP-D102 – Failure mode and effect analysis (FMEA) of redundant systems, January 2012*

1.18 Hidden Failures

Hidden failures are systematic failures or faults that can be hidden until a new fault appears. The possibility for hidden failures causing loss of a change-over function, for example, or the possibility for single failures rendering more than one redundancy group unavailable should be carefully considered in order to minimise the possibility of such failures. This is discussed further in section 3.3.11.

1.19 System Configuration

It is essential to ensure correct system configuration for each DP operational mode and to identify and mitigate any configuration errors. Interlocks and other features should be used in the design to prevent the DP system being configured in a manner that could defeat or degrade the redundancy concept. The FMEA should take this into consideration.

1.20 System Modification

Following any DP system modification, it is important that the modification should undergo further FMEA. However, it should not be reanalysed in isolation, but reanalysed as part of the whole system to ensure that any failure within the modified equipment does not have a failure mode which is in excess of that which would have occurred prior to the modification.

1.21 DP Operations with Closed Main Bus Tiebreakers

When generators in different redundancy groups are running in parallel, this will introduce the possibility that a single failure may propagate between systems. In such cases, it is required that protective measures are implemented in the system in order to ensure the required integrity between the redundancy groups. In the past, because such protective measures could not be shown to be effective, before undertaking critical DP operations, it was known for charterers of DP 2 vessels to request that the bus tiebreaker between the main switchboards be opened.

Operating with the bus tiebreakers open has the benefit that a failure in one main switchboard will not propagate to the other main switchboard via the bus tie, resulting in a partial blackout rather than a full blackout. Positioning capability would still be available, albeit reduced, usually by as much as 50%.

However, operating with the bus tiebreakers open also has some downsides, notably an increase in the amount of generating capacity required on line and hence an increase in fuel consumption and emissions and the amount of maintenance required and an increase in operating costs.

For DP 2 and DP 3 vessels it is required by all of the classification societies that analysis of the relevant failure modes associated with closed bus tiebreaker operation are addressed in the FMEA,

In the case of DP 3 operations, traditionally these have been carried out with the power plant in split mode, i.e. with the bus tiebreakers between main switchboards open, in line with IMO guidelines. IMO MSC/Circ.645 states that '*bus tiebreakers should be open during equipment class 3 operations unless equivalent integrity of power operation can be accepted*.' DP 3 vessels carrying out long term contracts requiring continuous DP 3 system set up with the bus tiebreakers open, such as drilling vessels, are particularly affected by an increase in operating costs.

In view of the benefits in operating DP 3 vessels with the bus tiebreakers closed, this naturally raises questions such as: How can it be assured that the main bus tiebreakers will open under all fault conditions? Additionally, how can it be ensured that, should a short circuit fault and/or earth fault occur on one section of main switchboard, the tiebreakers will open in sufficient time such that all equipment sensitive to voltage transients, including thruster VFDs and other auxiliary DP systems, do not trip on under voltage?[19]

19 DNV GL Offshore Technical Guidance (OTG), DNV GL-OTG-10 – DP-classed vessels with closed bus tie(s), April 2015.

1.22 DP 3 and the Backup DP System

The FMEA should identify the backup systems remaining available in the event of failure of the main system. With the effect of fire being considered for DP 3 vessels, a backup DP control station is located in a compartment separated from the main DP control station on the bridge or CCR by an A-60 bulkhead, i.e. within a separate fire zone. The backup DP control system is used in cases where the main DP control station has failed or must be evacuated due to fire. The backup DP system may share a communication link or network with the main DP control system, but it should not rely on any messages or data from the main DP control system. The backup DP system will rely on sensors and reference systems located in its own fire zone. The operator station for the backup DP system should also be in a different fire zone than the main DP control system, and is often located in a space with little or no overview of the ongoing DP operation. The backup DP system should be capable of being set up in a 'hot backup' standby mode, in such a way that the positioning is not affected when command is transferred to it via the backup DP selector switch.

Backup DP selector switch: In the event of fire in the main DP control station, control is transferred to the backup DP system via the backup DP selector switch. This is usually located on the backup DP system operator console under a cover to prevent inadvertent operation. The switch circuit is usually monitored in some way such as line monitoring to provide protection against faults such as short or open circuit inadvertently taking control away from the main DP control system.

In the event of a fire in the backup DP room, it is possible that a meltdown of the backup DP selector switch and the cables may occur and change the main DP/backup DP status of a number of thrusters or all thrusters. The backup DP selector switch cannot be segregated between thrusters as the switch needs to be located at the relevant control location in the backup DP room. The FMEA should confirm that the switch and the cables are designed with sufficient integrity against fire and flooding to avoid hidden failure. They could be provided with protection, such as thermal fuses in the vicinity of the backup DP selector switch in the backup DP room together with loop monitoring of the cables, to prevent inadvertent changeover.

1.23 The DP Vessel and the Mission

In section 1.3, it was stated that originally failures were classified according to their impact on mission success and personnel/equipment safety. The FMEA should be used as a part of a design review to identify those failure modes in the design which could impact on mission success and personnel/ equipment safety. The failures identified by the FMEA should then be eliminated or mitigated until there are no failure modes that present a high risk of failure to the vessel's mission. The FMEA should be an iterative process such that at the end no significant risk to the vessel's mission remains.

The industrial mission of a DP vessel varies. Examples are as follows:

- DP MODUs;
- project construction vessels;
- logistics vessels.

Class rules do not address the industrial mission of a DP vessel or the overall performance and operational capability. Consequently, vessels designed to obtain a DP class notation alone may not achieve the desired DP capability following worst case failure (WCF). The FMEA should determine the WCF and then it should be assessed what impact this WCF has on the vessel's mission.

The Marine Technology Society (MTS) published a DP vessel design philosophy document which is a compilation of experiences, practices and information gleaned from various sources in industry, some of which are not in the public domain[20]. This document was produced in co-operation with DNV GL who issued its own version[21]. It is intended to aid in the design of a fault tolerant, fault resistant DP vessel and to apply to any class of DP vessel operating in support of offshore oil and gas activities.

20 Marine Technology Society (MTS) DP Technical Committee, *DP (dynamic positioning) design philosophy guidelines*
21 DNV GL Recommended Practice (RP), DNV-RP-E306 – *Dynamic positioning vessel design philosophy guidelines*, September 2012

1.24 Software FMEA

Dynamic positioning and active mooring systems, and most position measurement equipment, are software based systems on which safety of life and vessel is often dependent. It is therefore essential, and should be considered mandatory, for the manufacturers of such systems to have comprehensive, efficient, highly developed and accredited quality assurance procedures.

Software has a potential for common mode failure as normally there are redundant DP computers in the system each running the same software. A software fault could therefore affect all DP computers. Whilst most developers assume that 'software doesn't fail,' things sometimes do go wrong as a processor executes its code. Structured testing such as FAT and on site commissioning is itself not sufficient to fully test software because no set of tests can address all permutations of transactions among software units under test and the outside world. Testing cannot address the handling of all unexpected internal values and events due to programming and algorithmic errors, inadequate exception processing, timing or scheduling errors, hardware and I/O failures, bad input data, disturbances on power lines, electromagnetic interference, and many others.

Software analysis, as well as hardware analysis, is therefore key to the robustness of the system. However, typically, the FMEA of the DP control system does not extend to carrying out an analysis of the software. Software functions should therefore be rigorously exercised as a matter of course during FMEA proving trials tests and also during factory acceptance tests.

IMCA M 163 – *Guidelines for the quality assurance and quality control of software* – is a document intended to provide guidance for the management of software for use in dynamic positioning systems, active mooring systems and position measurement equipment. It is not intended to give guidance on how to carry out a software FMEA.

IMCA M 163 covers software management in areas such as:

- management;
- quality assurance;
- design control;
- document and data control;
- process control;
- verification and validation testing;
- access to software;
- corrective and preventive action;
- data control and control of quality records;
- change procedures;
- software maintenance procedures and upgrades;
- training.

Specially tailored database tools can make the software FMEA process feasible, highly accurate and very thorough, however it is hugely time consuming, intrinsically tedious and potentially confusing so a structured approach is essential. It also requires input from specialist software engineers.

Software FMEA does not predict software reliability, but aims to determine whether a single failure can cause specific catastrophic events or other serious effects. At the same time, the analysis can identify possibilities of less serious consequence so that source code can be made more robust in specific places. Hardware-in-the-loop (HIL) testing is not a software FMEA but goes some way to exercising the software in order to identify faults which have the potential to cause loss of position. Refer to section 1.25.

DNV GL guidelines do not set out any guidance to FMEA of software. However, they do require testing and verification of how the software responds to relevant failures in the system subject to verification[22].

22 *DNV Recommended Practice DNV- RP-D102 Failure mode and effect analysis (FMEA) of redundant systems, January 2012*

1.25 Hardware-in-the-Loop (HIL) Testing

The DP system FMEA of the various software components, on which the overall vessel FMEA analysis relies, is usually undertaken by the control system vendors without third-party testing and verification. Also, in the FMEA proving trials, which constitute an important part of the sea trials for a new-build vessel, focus is put on the hardware components and the I/O layer of the computer systems. The software functionality of the computer systems is only superficially tested, mainly due to a lack of appropriate testing tools and the limited time available for testing every operational scenario that the control system could possibly encounter.

For FMEAs, the ability to verify failure handling in control system software is limited. HIL failure testing helps to address these issues by systematically testing the system response to a large number of failure modes.

HIL testing is a well proven test methodology from automotive, avionics, space, and other industries, targeting the software part of the control system. The HIL test process has many similarities with the FMEA process however the main difference is that the HIL test process does not normally need access to the vessel which makes it possible to perform testing earlier in the vessel new build project. While the FMEA process needs access to the vessel (dock and sea trial), the HIL test process uses a simulator without the need for access to the vessel.

The HIL test is not just a 'test', it is a verification process, interacting with the clients and getting feedback both from the client and from the class society on the process documentation.

As FMEA and HIL testing deal with different aspects regarding the above, co-ordination between FMEA and HIL testing will increase the quality of the station keeping ability verification required by the class societies. FMEA and HIL testing are complementary verification methods and both can be used to verify the DP system's ability to maintain position after a single failure. However, there are some aspects of FMEA testing which are similar, if not identical, to HIL testing. If HIL and FMEA are to be used in conjunction, the test procedures for each should be cross referenced to ensure that there is no duplication.

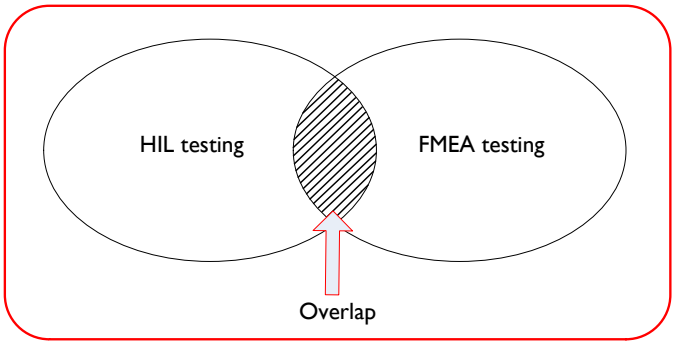


Figure 1-4 – Overlap between HIL and FMEA testing

HIL testing only superficially tests hardware and redundancy since the main test target is software. HIL testing is accomplished by isolating the control system and its operator stations from its surroundings and replacing all actual I/O with simulated I/O from an HIL simulator in real time.

In addition to testing the DP control system, the power management system (PMS) and the thruster control system (TCS) also need to be tested. Both are computer based control systems and therefore contain control system software. As these computer systems are part of the redundancy design intent, a software failure, or an inadequate failure handling within these control systems, may compromise the redundancy intent, with a possible loss of position as the result.

Many more operating scenarios can be tested than can otherwise be tested using FMEA techniques during sea trials. Currently, HIL cannot be used exclusively for FMEA testing such as annual trials. Further details on HIL testing can be found in section 4.26.

Both DNV GL and ABS have issued class notations focusing on the HIL test process; these being DNV GL's ESV[23] and ABS's ISQM and SV guides[24]. Note that, in some cases, a sea trial is only required for HIL tests on DP control systems in DNV GL's ESV (enhanced system verification), e.g. notation ESV-DP [HIL-IS].

1.26 Interactive FMEAs and other Decision Support Tools

Interactive FMEAs and other decision support tools could be developed to extend the usefulness of the FMEA throughout the vessel's operational phase. An interactive FMEA in which the user selects items to fail and the failure mode and its effects are automatically displayed would be more user friendly in today's digital age.

The FMEA could also be developed further to assist maintenance routines during normal DP operations, as it can be used to assess the potential effect on the DP system if an item of equipment is taken out of service for maintenance and a subsequent failure occurs. 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 following should therefore be considered:

- 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?

The FMEA can therefore assist in the decision making process prior to DP related equipment being taken out of service.

1.27 FMEAs of Non-Redundant Systems

1.27.1 Non-Redundant Systems

Redundancy improves the reliability and availability of a system but adding redundancy increases the cost and complexity of system design. However, due to increased reliability of system components, many systems do not need redundancy to function successfully. Notwithstanding, components within a non-redundant system can still fail and the effects of failure should be assessed. FMEAs are applied in the verification of redundant systems for the purposes of proving that they are fault tolerant. However, the FMEA process can be applied to any system whether it is intended to be fault tolerant or not. The benefits of carrying out an FMEA on a non-redundant system should not be overlooked.

Present industry practice is based around using HAZID/HAZOP techniques. Although such techniques are valuable, they are not a substitute for an in-depth engineering analysis of the failure modes and effects of a system and rely heavily on experience and probability to reach conclusions. Consequently, clients and regulators are increasingly requesting FMEAs for existing or new non-redundant equipment, including DP systems.

The classification societies do not have a requirement for FMEAs for non-redundant DP systems, i.e. DP class 0 and DP class 1 vessels. However, failures are not confined to vessels incorporating full redundancy.

Operational procedures should prevent a DP class 0 or a DP class 1 vessel being used for tasks where a loss of position could cause unacceptable consequences. Provided these procedures are adhered to then a loss of position should not cause injury to personnel or significant damage to an asset or the environment. However, a failure can give rise to vessel downtime. An FMEA may be able to indicate where modifications to the design will improve overall vessel availability thus reducing down time which should make an FMEA more cost effective.

23 DNV GL *Rules for the classification of ships* Part 6 Chapter 22 Enhanced System Verification, July 2013. In addition to the class rule, DNV GL has also issued a *Standard for certification for HIL testing* – SfC 2.24, July 2011

24 ABS *Guide for systems verification (SV)*, July 2014 and ABS *Guide for integrated software quality management (ISQM)* September 2012, updated July 2014

182 MSF – *International guidelines for the safe operation of dynamically positioned offshore supply vessels* – states that: 'Although classification societies do not require DP FMEAs for an equipment class 1 vessel, there may be occasions when charterers will require a DP FMEA to ensure the quality of the system design and operation and to identify the effects of single failure on the operation of the vessel'[25].

1.27.2 Objectives

Non redundant systems can still have failures within the system. The objective of an FMEA of a non-redundant system is to establish whether or not in the case of a single failure the system function is still available and operations can still proceed without any restriction. If in the case of a failure, the system function is restricted or, in the worst case, lost, it should be determined what the effect is on the vessel's mission and if there are alternative ways of carrying out the system function.

The FMEA of a non-redundant system should determine where the weaknesses lie in the system due to these failures so that:

- procedures can be formulated in case of a failure;
- system reliability can be improved by selection of more robust equipment or by adding redundant elements;
- maintenance routines can be changed to reduce the numbers of failures in service; and
- the causes of vessel downtime can be reduced.

The FMEA procedure may be summarised as follows:

- A comprehensive analysis of all systems, sub-systems, and their main components necessary for the system under analysis;
- Analysing design and redundancy tolerance where this is incorporated (it is usual to find some redundancy within the system but the system in itself is not redundant);
- Analysing the failure modes and effects for each component of the system through a detailed analysis of drawings and related specifications; making documentation which contains functional descriptions and block diagrams for all the equipment and systems relating to and affecting the system function;
- Implementation of a test and trials programme in a simulated operational state to determine and confirm particular failure modes and effects where necessary;
- Reporting any weakness of a serious nature when identified to enable corrective measures to be taken at the time of identification;
- Detailing which major component and equipment failures will result in a critical situation or catastrophic loss of system function;
- Reviewing the cause and consequence of any such failures, and propose any obvious actions or changes to procedures which can be taken to mitigate the effects of failure;
- Updating the operations manual for the operators to include changes to procedures as determined by the FMEA.

1.27.3 Types of Non-Redundant Systems

Typical examples of non-redundant systems include the DP systems of DP class 0 and DP class 1 vessels, drilling systems, motion compensated hydraulic accommodation vessel gangways, dive systems, single screw MEGI (slow speed gas injection) engines and the propulsion systems of non-DP vessels.

In the case of an auto/manual system, the FMEA should ensure that if auto control is lost manual control is still available and not inhibited. The following is an example of the benefits of carrying out an FMEA of a non-redundant auto/manual DP system.

25 182 MSF – *International guidelines for the safe operation of dynamically positioned offshore supply vessels*

An FMEA was carried out on a simplex DP vessel with a single DP computer and independent computerised joystick with functions including automatic heading control. During the FMEA it was noticed that a fuse was critical to the changeover between automatic DP and joystick. Failure of this fuse was not alarmed and, with the vessel on automatic DP, it was proved from practical tests at sea that, with failure of this fuse remaining hidden, should the automatic DP fail then transfer of control to the joystick was impossible and position was lost. Fuse failure monitoring was introduced in this case to mitigate the problem.

The National Hyperbaric Centre states that: 'FMEA/FMECA of a saturation diving system is now considered a mandatory requirement within the industry and is highlighted as such in the International Association of Oil & Gas Producers (IOGP) Diving Recommended Practice Report No: 411, dated June 2008. Furthermore it is also considered a requirement under class and would be submitted to the classification society for review prior to the award of class certification'[26].

It goes on further to state that: 'The purpose of a diving system FMEA/FMECA is to ensure a systematic assessment is carried out on all diving system equipment, and the support vessel interfaces to identify any areas where the system or vessel interfaces may fail due to equipment operational reliability as well as inadequate operational procedures, lack of redundancy and critical spares required for safe operation'.

IMCA D 039 – *FMEA guide for diving systems* – gives guidance of how a diving system FMEA should be carried out.

Where engines incorporate electronic control systems (e.g. those without camshafts), the International Association of Classification Societies (IACS) requires an FMEA of the electronic control system to show that a single failure will not cause loss of essential services for the operation of the engine and that engine operation will not be lost or its performance degraded more than that which is acceptable[27].

In the case of non DP vessels, owners of LNG vessels are requesting FMEAs of the propulsion systems to include fuel gas systems. A risk analysis is required by class.

Lloyd's Register requires that: 'A failure modes, effects and criticality analysis (FMECA) may be undertaken as part of the RCM process'[28]. Gas turbine systems will require an FMEA in areas such as starting and stopping, oil fuel supplies, LO, air induction, exhaust, control and monitoring and electrical power supplies.

In order to gain Lloyd's Register notations such as ICC (integrated computer control), IFP (integrated fire protection), PES (programmable electronic systems) and WIG (wing in ground-effect), an FMEA is mandatory. Electronically controlled engines (e.g. those without camshafts) will also require an FMEA.

1.27.4 Standards and Guidelines

There are industry standards and guidelines and also relevant class rules relating to non-redundant industrial equipment (rules for lifting equipment for example) some of which have requirements for FMEAs. These include documents such as:

- IMCA M 171 – *Crane specification document*
- IMCA D 039 – *FMEA guide for diving systems*
- DNV GL Offshore Standard DNV-OS-E402 – *Offshore standard for diving systems*

26 National Hyperbaric Centre Website 2012
27 International Association of Classification Societies (IACS) UR M44 *Documents for the Approval of Diesel Engines* 2015
28 ShipRight Design and Construction *Machinery Planned Maintenance and Condition Monitoring* March 2013

Specifying an FMEA

Specifying an FMEA 2-1

2.1 Prequalification 2-3
2.2 Baseline of Specification 2-3
2.3 Overview 2-4
2.4 Depth of the FMEA 2-4
2.5 Objective of FMEA 2-5
2.6 Prerequisites of an FMEA 2-5
2.7 FMEA Proving Trials Plan 2-6
2.8 FMEA Management 2-6
2.9 Vendor FMEA Documents 2-7
2.10 Failure Modes, Effects and Criticality Analysis (FMECA) 2-7
2.11 Final Documentation Required 2-8
2.12 Example of a Specification for an FMEA for a DP Vessel 2-8

2.1 Prequalification

Companies carrying out FMEAs will on occasion have to undergo a prequalification process, part of which will involve completion of a questionnaire set by the owner of the FMEA. This covers both technical and commercial issues.

For those requesting an FMEA to be produced by a non-qualified company, the issues listed below are a guidance as to those issues to be raised during the prequalification process.

For those being subjected to the prequalification process, the issues listed below are a guidance as to what responses are useful to have in place at the commencement of prequalification.

The following issues are therefore those which are likely to be raised during the prequalification process. Guidance as to how to prepare and respond to most of these issues can be found in the later chapters in this document.

2.1.1 Technical Issues

- The requirement for a multi-discipline team;
- Declaration as to which FMEA standards and guides are used;
- How the FMEA project is managed to a deadline;
- Explanation of how deep to go in the FMEA on specific equipment;
- How DP/PMS manufacturers' standard FMEAs are handled in the FMEA;
- How the analytic work of the team is managed to ensure complete coverage of the technical issues, and that specific equipment is looked at by the right members of the team;
- How new team member resources are qualified for the right discipline expertise and how contract or temporary help is integrated into the FMEA team;
- How the analysis of network technology is handled;
- How the analysis for 'common cause' faults is performed and managed and how are these tested in the FMEA trials;
- How the identification of 'hidden faults' is managed and performed;
- How the identification of a 'single inadvertent act' is managed and performed;
- How the scope of the FMEA trials is determined;
- Provision of a sample of an FMEA report produced by the non-qualified company;
- Is there a programme in place to systematically evaluate and improve the FMEA product?

2.1.2 Commercial Issues

- Provision of references, including individual name, title, organisation and contact information;
- Details of experience of carrying out FMEAs or FMECAs on the type of subject vessel in compliance with the scope of work as outlined in the FMEA specification.

Other commercial issues will be covered but these will be specific and it is not appropriate to give guidance on these issues in this document.

2.1.3 Safety Management System (SMS)

An FMEA is a critical safety item on a vessel, and kept as part of the safety management system documents (SMS). The FMEA specification should state that it is regarded as such to ensure that sufficient attention is paid to it by the key personnel.

2.2 Baseline of Specification

The FMEA specification should reference all relevant local, national and international rules and guidelines, including IMCA documentation, used to produce the FMEA so that the FMEA practitioners bidding for the work are fully aware of the FMEA process they should follow. This should prevent competitive bids

from adopting short cuts in an attempt to win the bid by offering an incomplete FMEA. Good examples of documentation, in particular, are IMO MSC/Circ.645 and IEC 60812.

The building contract should specify that input from the FMEA should be taken into consideration, and the FMEA should be commissioned as early as possible in the project. It is advisable that a high level analysis at the design outline stage is specified, so that the initial FMEA output can be used as guidance in the pre-engineering phase (new builds).

The class rules used for adjustments/edits or changes to an existing vessel's FMEA should be clearly stated in the FMEA where applicable and recorded in the revision history section of the document. For an existing vessel, company management needs to be aware that changes to the system may be required as a result of the concerns arising from the FMEA and that sufficient funds should be made available to meet the changes. The FMEA should be viewed as a critical item in the purchasing process (existing FMEA documents).

Other international rules and guidelines used to produce the FMEA should also be quoted in the FMEA if applicable.

The FMEA should clearly state the class notation of the vessel, the year of the class rules applicable for the vessel, the DP system configurations to be analysed and the vessel's worst case failure design intent.

For the FMEA to be useful, relevant and acceptable to all parties it should be performed by competent personnel (see section 3.3.3), properly managed (see section 3.5) and be executed to a sufficient level of detail to demonstrate all requirements of the specification. It needs to satisfy the nominated classification society and other regulatory requirements, and should be suitable for use as a training reference document for the vessel's staff and onshore backup team.

2.3 Overview

The FMEA should be a comprehensive systematic investigation that establishes the failure conditions of the DP system. Primarily, it is an analytical process that takes advantage of experience where possible. For guidance, the DP system includes the equipment and systems shown in information note IMCA M 04/04 – *Methods of establishing the safety and reliability of DP systems* – and its Annex (2004). This should be referenced as part of the specification (see section 2.12).

2.4 Depth of the FMEA

The depth of analysis on equipment systems will be left to the judgment of the approved FMEA team such that the FMEA objectives are met. The owner of the FMEA may require an extended depth of work on specific systems if the FMEA team cannot demonstrate that the initial depth chosen was appropriate.

The FMEA should be a comprehensive analysis of all systems and sub-systems necessary for, or potentially, impacting the station keeping of the vessel and should be carried out by:

- establishing the main system components which are fundamental to position keeping;
- analysing the failure modes and effects for each of the systems;
- reviewing the causes of any critical failures (see 3.3);
- detailing any potential major component and equipment failures which would result in a loss of position;
- identifying any tests and trials necessary to determine and confirm particular failure modes and effects where necessary;
- reporting any weakness of a serious nature to the client, vessel owner and classification society to enable corrective measures to be taken at the time of identification by way of an auditable report that will be retained as a part of the FMEA documentation;
- implementation of a full test and trials programme while the vessel is operating on DP.

2.5 Objective of FMEA

The main objective of the DP FMEA is to identify the single point failures in any part of the vessel's DP system and/or its sub-systems which, if they were to occur, would cause loss of the position keeping capability of the vessel. The causes and consequences of any such failures should be noted and obvious corrective actions which can be taken to avoid such failures should be described in the final FMEA report. The FMEA should also prove that the requirements with respect to redundancy, independency and separation are achieved in the design.

The objectives of the FMEA should be clearly stated when specifying an FMEA. For example, the specification should state that the FMEA is to achieve the following:

- identify, with a view to elimination or mitigation, the effects of all single point failures and common mode failures in the vessel DP equipment which, if any occur, would cause total or partial loss of position keeping capability;
- demonstrate effective redundancy;
- demonstrate that each DP related system is single-fault tolerant with no adverse loss of functionality in the event of failure;
- identify potential hidden failures and determine the effects of a second failure after the hidden failure has been exposed;
- identify the effect these failures and hidden failures will have on the system;
- describe the design safeguards that minimise the risk of failure and any operational procedures required to ensure the design safeguards remain in place;
- prove that control circuit and interface equipment faults, including failures should not result in an unsafe condition to personnel or cause damage to equipment.

It is vital that the term 'single point failure' is defined in the document and, more importantly, understood when defining the objectives.

2.6 Prerequisites of an FMEA

When planning an FMEA, a timescale should be agreed and adequate time should be allowed for each part of the FMEA process. Deadlines should be drawn up for issue of the preliminary FMEA report, including any concerns and necessary sea trials tests, and closing out of those concerns made as a result of the FMEA process.

Reporting procedures (communications) outside of the FMEA process as described in this document should be defined.

All DP operating and design philosophies or modes of the vessel should be identified so that each associated system configuration can be outlined in the FMEA specification and addressed by the FMEA, for example, a class 2 or 3 DP vessel operating with open and closed main switchboard bus tiebreakers.

The specified rules/regulations (e.g. class notation) with which the vessel is to comply should be stated.

With regard to operational boundaries, the vessel functional design specification should define the environments in which the vessel is expected to operate, and the performance level expected in each. The vessel functional design specification should also define the WCFDI. The FMEA should address anticipated 'worse case' ambient conditions (e.g. temperature and humidity) as these could produce common mode failures in equipment hardware if no forced cooling has been applied.

With regard to physical boundaries, the first stage of the FMEA process should be to define the boundaries of the equipment to be assessed as part of the DP system. Guidance on the sub-systems to be analysed can be found in IMCA M 04/04.

There is a requirement in the FMEA for conclusions at sub-system level and overall system (vessel) level. In addition, the FMEA should list and categorise any concerns raised during the analysis. The levels of categorisation of concerns should be defined, which could be as follows:

- Category A – Concerns which address potentially serious failure modes which are in excess of WCFDI or raise safety issues or do not comply with class requirements;

- Category B – Concerns which address failure modes which are not in excess of WCFDI, do not raise safety issues or are in compliance with class requirements but are considered important enough to make the system more robust, such as additional redundancy in key areas;
- Category C – Concerns which, if addressed, are designed to improve system operation. These are suggestions and not essential to the process.

Note: All concerns raised during the FMEA and during the proving trials tests should be addressed and the action taken recorded in the final FMEA report, even if a decision is made not to take action.

Guidance on the categorisation and handling of concerns can be found later in this document.

2.7 FMEA Proving Trials Plan

Ultimately the responsibility for ensuring that safe, productive and informative FMEA proving trials are carried out lies either with the shipyard, in the case of new build vessels, or the vessel owner's nominated responsible person, such as the master, in the case of an operational vessel. If for any reason a test should be rejected by any party, the reasons for the rejection should be recorded in the FMEA and a suitable alternative test, formatted to achieve a satisfactory result, agreed by all parties.

Trial plans and test procedures should be provided to the class society as early as possible in the vessel's building phase to prevent any delay. Once accepted by class it is unacceptable to remove or change any test for any reason (with the most common reasons being to save cost and time) unless agreed between the FMEA vendor and class society. Depending on contractual arrangements and obligations, the FMEA vendor's reporting line with the class society is most likely to be via the shipyard for a new build vessel or the owner if an existing vessel.

Changes in design or the installation equipment could possibly mean a test may need to be altered; the new test sheet should be appended to the original sheet to be part of the trial.

The test/trial plan should be agreed (and preferably signed for) by all parties at the kick off meeting held before trials begin with a view to avoiding ad hoc short cuts and preferential engineering solutions.

Each FMEA proving trials test procedure should include the test method, any changes to normal equipment set up, results expected, actual results, comments and witness verification of the test results.

Should any test give a result that is not satisfactory or expose an unexpected result all relevant parties need to consult and agree whether to repeat the test, or edit the test sheet accordingly. It should be recognised that simply because a test result was not as expected, does not mean that it is wrong. All actions taken in this instance should be recorded and form part of the FMEA documentation with the original test sheet for reference.

It is imperative that the actual FMEA proving trial results are fed back into the FMEA itself to produce the final document.

FMEA proving trials procedures and reporting are further covered in section 4 of this document.

2.8 FMEA Management

The FMEA report should be revisited as a result of changes made to the system during the life of the vessel and in the light of any information gathered at a later date that was not available at the time of the FMEA. Any DP related equipment changes to the vessel should be analysed to identify whether they have an impact on the FMEA. Any identified changes should be addressed on an on-going basis but not later than the next DP annual trial. The FMEA report is therefore to be regarded as a 'living, working document'.

The FMEA format should allow the document to be easily updated. Section 3 of the document gives clear guidelines on how to manage the FMEA with sample documents to keep an easy auditable trail of any changes either major or minor to the document. The flow diagrams in section 3.5 suggest an easy method to manage the changes in the FMEA whilst keeping the auditable trail intact.

Recording changes in an existing vessel's FMEA can be done by an amendment to the existing FMEA, an addendum to an existing FMEA, a section rewrite of an existing FMEA, or the existing document may need to be fully renewed.

2.9 Vendor FMEA Documents

Most vendors produce an FMEA specific only to the equipment they are contracted to supply. This type of FMEA can be a useful document but it is restricted to one piece of equipment or control system only and should not be confused with the full DP FMEA that incorporates all the DP related systems and sub-systems and information from several vendors' FMEA documents. Although items of equipment will meet their class notation when analysed individually, when they are interfaced with each other to complete the installation, single failures are often identified when carrying out the full DP FMEA using the block diagram methodology as described in section 3 of this document.

Vendor FMEAs can be used as guidance or for incorporation into the overall FMEA. Specifying 'manufacturers' or 'vendors' FMEAs of DP related equipment are typically:

- DP control system;
- vessel management and power management systems, IAS/PMS FMEAs;
- F&G and ESD (particularly where MODU code appears to be in conflict with DP requirements);
- thruster control systems;
- advanced protection systems;
- engine control systems FMEAs/governor and AVRs;
- power plant FMEAs by electrical system contractor.

Guidance on engineering studies to be performed to support the FMEA includes:

- short circuit withstand;
- electrical system harmonic analysis in the intact and post failure conditions;
- electrical systems resonance;
- transient stability following short circuit;
- effects of crash synchronisation of generators and power systems;
- voltage dip analysis associated with fault clearance;
- influence of unbalanced and arcing faults;
- load balance analysis for each DP mode of operation;
- protection co-ordination study.

Where the vendor FMEA reports are not available, it should be recommended that the failure tests be carried out by the key vendors on their equipment at the FAT. The results of these failure tests should be witnessed by the relevant FMEA team member or be available to the FMEA vendor in writing and recorded as part of the FMEA audit process.

2.10 Failure Modes, Effects and Criticality Analysis (FMECA)

International Standard IEC 60812 describes failure modes and effects analysis (FMEA) and failure modes, effects and criticality analysis (FMECA), and gives guidance as to how they may be applied to achieve various objectives by:

- providing the procedural steps necessary to perform an analysis;
- identifying appropriate terms, assumptions, criticality measures, failure modes;
- defining basic principles and providing examples of the necessary worksheets or other tabular forms.

All the general qualitative considerations presented for FMEA will apply to FMECA, since the latter is an extension of the other.

Both the FMEA and the FMECA are carried out in a similar fashion as described in section 3 of this document. The FMECA will attempt to measure the criticality each failure mode has on the system itself.

2.11 Final Documentation Required

The final FMEA report after the DP FMEA proving trials should be supplied with its companion documents. The companion documents should include the completed registers and documentation to demonstrate and verify that all recorded technical queries both historically and currently have been effectively closed out and the method of close out recorded, together with the preliminary annual trials document as required. Refer to IMCA M 212 – *Example of an annual DP trials report* – and IMCA M 225 – *Example redundancy concept and annual DP trials for a DP class 3 construction vessel* – for examples of an annual trials document.

2.12 Example of a Specification for an FMEA for a DP Vessel

The following is one example of a specification for an FMEA for a DP vessel. This example is indicative and does not preclude alternative specifications. Actual specifications should be specific to each individual project.

Introduction

The vessel owner is responsible for the vessel and for the FMEA, and is the 'owner' of the FMEA.

It is intended that the FMEA be true and accurate, therefore it must be performed by qualified resources, properly managed and be executed to sufficient level of detail to demonstrate all requirements of this specification. The FMEA must be to a standard that will satisfy class and regulatory requirements, and be a training reference for operators and maintenance staff of the vessel.

The FMEA should be a comprehensive systematic investigation that establishes the failure conditions of the DP system. It should be primarily an analytic process but take advantage of experience where possible.

The FMEA should be structured and documented to allow easy verification of the FMEA and easy updating for changes to the vessel.

Scope

The FMEA contractor is to:

1. *Perform a DP FMEA study of the vessel that meets the owner's referenced standards and guidelines and this specification.*
2. *Include a specific review for 'single inadvertent act' by any person on board the DP vessel.*
3. *Co-ordinate with equipment manufacturers for provision of their FMEA documents. These are to be reviewed, commented and referenced in the overall FMEA.*
4. *Produce and maintain registers, with supporting documentation, for operational and technical assumptions, technical queries, concerns and document review. These should be issued as part of the periodic progress reports and as part of the final documentation.*
5. *The FMEA is to consider all intended DP operational modes of the vessel, such as operation with bus ties closed and bus ties open.*
6. *The FMEA is to consider the effects on the DP system of failures in the equipment associated with the vessel's industrial function and with the equipment associated with the vessel's safety systems.*
7. *Prepare a preliminary FMEA report for comment prior to DP FMEA proving trials taking place.*
8. *Prepare a DP FMEA proving trials programme to prove the content and conclusions of the FMEA. The trials will demonstrate compliance with the worst case failure design intent (WCFDI). The FMEA team will participate in such trials and prepare a trial report that is to include the results for each test.*
9. *Prepare and issue a final FMEA report to reflect the DP FMEA proving trials findings and any corrective action taken for any concerns recorded. This should also include the registers, with supporting documentation.*

10. *Prepare a draft annual trials document as an inventory of the trials that will be performed on a continual basis during the lifetime of the vessel.*

Summary Objectives of the FMEA

The objectives of the FMEA are:

1. *To identify any single failure, in any system of the vessel, which may cause a loss of position keeping capability if that failure occurred.*
2. *To ensure that all possible failure modes are defined, including identification of the 'worst possible' single point failure.*
3. *To detect common mode/common cause failures. Examples are:*
   - *Main power plant protection design that can trigger shutdown of the system, such as under voltage (UV), over voltage (OV), under frequency (UF), over frequency (OF) and earth fault*
   - *A transformer fault might be cleared successfully by the main switchboard protective design but the resulting momentary voltage dip could trigger shutdown of other critical equipment, including thrusters, because of their own protective device settings*
   - *Common heating and cooling systems for redundant equipment*
   - *Network faults that might delay or compromise power management functions or thruster response.*
4. *To demonstrate effective equipment redundancy.*
5. *To identify potential 'hidden' failures and determine the effects of a second failure.*
6. *To describe the design safeguards that minimise the risk of failure and any operational procedures required to ensure the design safeguards remain in place.*
7. *To provide a clear description of the DP system with its failure modes to be used for operator and maintainer training purposes.*
8. *To review the manufacturers' FMEAs, including revisions, for the DP control, power, propulsion and power management system (including proprietary systems). There must be a specific review for networks and serial interfaces unless addressed specifically in the manufacturers' FMEAs.*
9. *To indicate critical maintenance requirements for DP related equipment.*

FMEA Team

The discipline makeup and individual qualifications of the FMEA team of practitioners who will be carrying out the FMEA must be reviewed and approved by the FMEA owner. CVs of FMEA team members are to be provided. Substitutions also require the same treatment.

Technical resource expectations are for the team members to have a minimum of the following three disciplines:

- *marine/mechanical engineer;*
- *electrical engineer;*
- *control/automation engineer.*

Other additional specialists may be introduced to the project as needed and agreed.

The team leader and principal author may be any one of these discipline engineers or another suitably qualified individual.

The FMEA owner will appoint a project engineer who will be the only interface or focal point between the FMEA team and all other interested parties.

Depth of Equipment Review

The review is to be appropriate to the DP class of the vessel. The depth of review on equipment systems will be left to the judgment of the FMEA team providing the FMEA objectives are met. The FMEA owner reserves the right to require within the project scope an extended depth of work on specific systems if the FMEA team cannot demonstrate the initial depth chosen was appropriate.

For DP 2/DP 3 vessels items covered in the FMEA as a minimum requirement are as follows:

- *bilge and ballast systems (DP 3)*
- *passive and active components (DP 3)*
- *cable routing and equipment segregation (DP 3)*
- *fuel systems*
- *lube oil systems*
- *all safety systems including emergency shutdown (ESD) fire and gas detection systems*
- *remote valves and hydraulic and pneumatic systems*
- *all control systems*
- *heating and ventilation systems (HVAC)*
- *power and generation systems*
- *main and emergency power systems*
- *electrical power distribution systems*
- *IAS/PMS systems*
- *thruster and propulsion systems*
- *DP control systems*
- *DP position and reference sensors*
- *network(s) and communication*
- *human-machine interface (human factors)*
- *anchor or mooring lines (POSMOOR FMEA).*

Generally the equipment systems to be evaluated include those shown in Appendix D of the Annex to IMCA M 04/04.

Steps in the FMEA

The FMEA is to break the overall system down into logical systems and include descriptive and tabular analysis of each system in addition to system block diagrams to show functional interdependence of components.

The FMEA should include the following steps:

1. *Define each system to be analysed, dividing the overall DP system into systems, sub-systems and components.*
2. *Include a functional description and tabular analysis (worksheets) for each system and sub-system, descriptive and tabular analysis of each system.*
3. *Illustrate the interrelationships of functional elements of the system by means of block diagrams.*
4. *Define the interfaces between each block.*
5. *Identify all potential failure modes and their causes.*
6. *Evaluate the effects on the system of each failure mode.*
7. *Identify failure detection methods.*
8. *Identify corrective measures for failure modes.*
9. *Fully document the analysis.*
10. *Maintain a technical query (TQ) register to record queries raised during the analysis, the response to the query and the status of each query (either open/closed).*
11. *Develop a test programme.*
12. *Prepare final FMEA report.*

Initial Project Details

The following project details are to be provided:

- *contractor organisational chart;*
- *CVs of FMEA team members;*
- *project schedule;*
- *work location proposal:*
  - *work at site*
  - *work in contractor's office;*
- *communication and reporting channels;*
- *FMEA contractor focal point;*
- *list of documentation/drawings for analysis submitted by contractor;*
- *frequency of periodic progress reviews.*

The project schedule above should include:

- *project start date;*
- *kick off meeting;*
- *documentation/drawings delivery to FMEA team;*
- *initial analysis work based on the drawings;*
- *site visit if appropriate;*
- *preliminary report submittal;*
- *FMEA proving trial attendance;*
- *final report submittal.*

FMEA Guidelines and Standards

The following standards and guidelines (as appropriate) are to be consulted in the preparation of the FMEA:

- *Class rules for the classification of ships (class rules as appropriate);*
- *ABS Guidance notes on failure modes and effects analysis for class, May 2015;*
- *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);*
- *DNV GL Recommended Practice (RP) DNV-RP-D102 – Failure mode and effect analysis (FMEA) of redundant systems, January 2012;*
- *IEC Standard, IEC 60812: Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA) Second Edition 2006-01;*
- *IMCA M 04/04 – Methods of establishing the safety and reliability of DP systems – and its Annex (2004);*
- *IMCA M 103 – Guidelines for the design and operation of dynamically positioned vessels;*
- *113 IMO – Guidelines for vessels with dynamic positioning systems (MSC Circular 645);*
- *IMCA M 166 – Guidance on failure modes and effects analyses (FMEAs);*
- *182 MSF – International guidelines for the safe operation of dynamically positioned offshore supply vessels;*
- *IMCA M 190 – Guidance for developing and conducting annual DP trials programmes for DP vessels;*
- *IMCA M 190A – Guidance for developing and conducting annual DP trials programmes for DP vessels: Executive summary;*
- *IMCA M 191 – Guidelines for annual DP trials for DP mobile offshore drilling units;*
- *IMCA M 212 – Example of an annual DP trials report;*
- *IMO MSC Resolution 36(63) Annex 4 Procedures for failure mode and effects analysis (HSC Code).*

FMEA Deliverables

A preliminary DP FMEA report for approval and a DP FMEA proving trials test schedule for class review to be submitted at least six weeks prior to DP FMEA proving trials taking place.

The final version of the DP FMEA report is to incorporate the results and feedback from the DP FMEA proving trials.

The FMEA report is expected to contain the following:

- *Executive Summary (to include a summary of the findings of the analysis and an assessment of the vessel's compliance with the nominal DP class notation);*
- *Introduction:*
  - *FMEA introduction*
  - *scope of work and objective (to include a description of the WCFDI and WCF)*
  - *FMEA procedure or methodology (including standards and guidelines to be applied)*
  - *vessel application and particulars*
  - *any assumptions made in the analysis, e.g. the vessel's operational mode/s when the analysis is carried out*
  - *documentation;*
- *Method of Analysis:*
  - *Block diagrams and descriptive narrative for each system or sub-system*
  - *FMEA worksheet including format, description of fields, definitions of severity levels for each system or sub-system*
  - *FMEA corrective action report form produced and submitted in the event of any serious failure modes being revealed;*
- *Description of Systems, for example:*
  - *DP control system*
  - *power generation system*
  - *electrical distribution system*
  - *auxiliary machinery systems*
  - *propulsion systems*
  - *safety systems;*
- *Concise summary of FMEA concerns and actions to be taken. Each concern to be assigned a category, e.g.:*
  - *Category A – Concerns which address potentially serious failure modes which are in excess of WCFDI or raise safety issues*
  - *Category B – Concerns which address failure modes which are not in excess of WCFDI or raise safety issues but are considered important enough to make the system more robust, such as additional redundancy in key areas*
  - *Category C – Concerns which, if addressed, are designed to improve system operation. These are suggestions and not essential to the process;*
- *Conclusions, including with respect to objectives;*
- *Appendices:*
  - *trials test sheets with results and a report on any concerns raised*
  - *FMEA report sheets recording any Category A concerns found*
  - *list of vessel/shipyard and vendor drawings received and reviewed*
  - *list of other working documents*
- *DP FMEA proving trial report document;*
- *Draft annual (continuous) trials document if required.*

All of the deliverables must be supplied as protected PDF files or equivalent.

DP FMEA Proving Trials

The FMEA proving trials procedures are to be submitted for approval. Each test procedure is to be provided in an individual work pack format which should include the following:

- *title;*
- *test reference;*
- *test objective;*
- *changes to normal equipment set up;*
- *test method;*
- *results expected;*
- *actual results;*
- *comments;*
- *test specific system drawing/s where appropriate;*
- *witness verification (signature and date of test).*

Guidance on how FMEA testing may be used to validate engineering models that may then be used to explore failure modes that are more difficult to test or which carry a higher risk of equipment damage. Arcing faults for example.

DP FMEA Methodology

DP FMEA Methodology 3-1

3.1 The FMEA Process 3-3

3.2 FMEA Objective 3-5

3.3 FMEA Methodology 3-5

3.4 The FMEA Report 3-21

3.5 FMEA Management Guidance 3-31

3.6 FMEA Verification 3-38

3.7 Updating of an FMEA 3-40

3.8 DP Incident Follow-up 3-41

3.9 Additional Studies to Complement the FMEA Process 3-42

3.1 The FMEA Process

This section describes the method by which an FMEA is carried out from the start of the FMEA process to the ongoing FMEA management during the life of the vessel after the final FMEA has been issued.

At the beginning of an FMEA, it is necessary to:

- Clearly understand and define the objectives of the analysis;
- Adopt a method suited to achieve the desired result;
- Select the FMEA team;
- Define the standard or standards with which the FMEA is to be in compliance;
- Define the boundaries of the system to be analysed;
- Define the reporting procedures;
- Organise system design information.

During the FMEA, the process includes:

- Identify the system or sub-system, mode of operation and the associated equipment or components that make up the system or sub-system;
- Identify the potential failure modes and their causes;
- Evaluating the effects of each failure mode on the system;
- Identify measures for mitigating the risks associated with each failure mode;
- Identifying failure detection methods/corrective actions;
- Arranging vessel audits as required;
- Producing a preliminary FMEA report;
- Identify the trials and testing necessary to prove the FMEA conclusions and producing an FMEA proving trials test programme;
- Arranging practical FMEA tests, dockside/at sea/on full DP;
- Advising of any concerns.

Completion of the FMEA entails:

- Producing the final FMEA report.

After the FMEA, the following should be addressed:

- Ensure the operators understand the capabilities and limitations of the system so as to achieve best performance;
- FMEA documentation and ongoing QA (FMEA management).

Figure 3-1 contains an FMEA process flowsheet. Whilst it is a good overview of the process, it is viewed from the perspective of the FMEA team carrying out the FMEA, not, for example, from the perspective of a ship owner requiring an FMEA.

The key stages will be discussed later in this document.

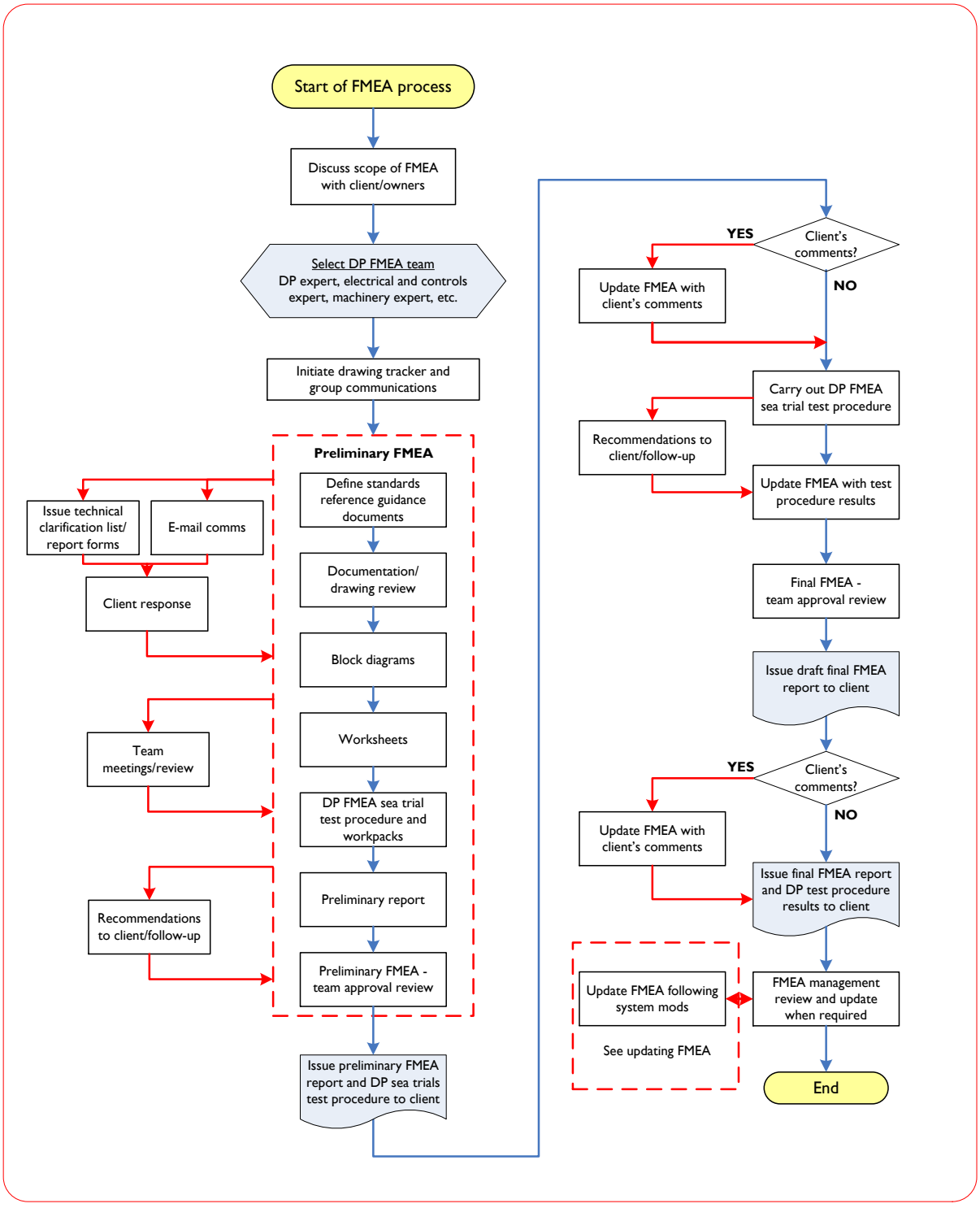


Figure 3-1 – The FMEA process flowsheet

3.2 FMEA Objective

The objective of an FMEA is to identify the potential design and process failures which will cause the system under analysis to fail to perform its intended function.

In the case of a DP system, the objective of the FMEA is to assist in developing a fault tolerant system by identifying and analysing the consequences of any single point failure in any DP related system on the vessel to ensure that, if it were to occur, it would not cause any failure in excess of worst case failure design intent (WCFDI) or cause a significant loss of position by 'drift off' or 'drive off'. It is expected that loss of position will occur if the operational limits of DP capability for the vessel are exceeded. It is the responsibility of the vessel operator to ensure that the vessel is operated within the conditions of approval. The FMEA should also prove that the requirements with respect to redundancy, independency and separation are achieved in the design.

The FMEA considers the vessel to be in the DP configuration, or configurations, identified for analysis, e.g. redundant automatic DP operation, main switchboard bus ties open or closed, etc., and a single failure occurs.

Throughout the FMEA, the FMEA analyst should not lose sight of the objective of the FMEA with respect to the WCFDI and the required level of redundancy and separation intent in the design. The redundancy concept is discussed in section 1 of this document. For more details on the redundancy concept, refer to IMCA M 225 – *Example redundancy concept and annual DP trials for a DP class 3 construction vessel* – which describes the DP redundancy concept for a fictitious project and construction (P&C) vessel.

3.3 FMEA Methodology

The following is an overview of the FMEA methodology. The points raised in this overview will be discussed in more detail as the section progresses.

FMEA methodology follows a 'top down' approach that is recognised as ensuring that all relevant systems on the vessel, including those that may not immediately appear to interface with the DP aspects of the vessel, are considered and evaluated.

It is important that all components essential to the operation of the system are identified. It should be understood how each component is functionally related and dependent on each of the other components.

The methodology requires the appointment of a team of specialists each having expertise in one or more of the different systems that make up the overall DP system and each having previous experience performing an FMEA.

Areas of uncertainty, such as in detailed equipment design, failure mode uncertainty or operational uncertainty should be highlighted in an FMEA trials list so that actual tests can be undertaken in due course to identify them (refer to section 4). This ensures that a full audit trail of the FMEA process is maintained throughout and is available subsequent to the vessel's delivery.

Initially, a preliminary FMEA report is issued with a related list of questions and requests for clarifications to assist in final completion of the document. The report is updated when these are known. The process should ensure the resolution of any concerns made as a result of the analysis. (Note: It is essential that every concern is addressed and the action taken is recorded, even if a decision is taken not to take action.)

The methodology of the FMEA can be summarised as follows:

1. A comprehensive analysis of all systems, sub-systems, and their main components necessary for the position keeping of the vessel.
2. Analysing the design and its tolerance to failure as well as analysing the design against the applicable class rules, class notations and standards.
3. Analysing the failure modes and effects for each of the systems through a detailed review of DP design philosophy documents (stating the WCFDI and operational modes), drawings and related specifications; making documentation which contains functional descriptions and uses tools such as block-diagrams for all the equipment and systems relating to and affecting the DP operation of the vessel.

4. Identifying the causes of any critical failures.
5. Detailing which major component and equipment failures will result in a loss of position.
6. Noting the cause and consequence of any such failures.
7. Timely reporting of any concerns to the client by detailing any fault identified which is not compliant with WCFDI so as to enable corrective measures to be taken at the earliest opportunity. Reanalysis of any modifications will be required.
8. Identifying any tests and trials necessary to determine and confirm particular failure modes and effects where necessary.
9. Implementation of a test and trials programme in a representative DP operational state.
10. Providing the basis of a training manual for all crew members as well as the onshore and offshore maintenance engineers.

Items 8 and 9 are necessary when the failure modes still cannot be fully determined by the desktop analysis.

With the above methodology, all catastrophic and critical failure possibilities can be identified and then eliminated at an early stage through design correction or introducing operational procedures. The causes and consequences of any such failures should be noted and the severity[1] of each failure recorded. The failure severity levels should be defined at the start of the FMEA, for example:

- Severity Class 1: Catastrophic – A 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 position keeping ability leading to an excursion, drive off, or drift off from position resulting in possible asset loss or major environmental impact and which will lead to an emergency termination of the operation.
- Severity Class 2: Critical – A 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 result in loss of position, necessitating a controlled termination of the operation, e.g. loss of a main switchboard, and results in an extended period of shut down of operations.
- Severity Class 3: Serious – A failure resulting in a temporary loss of availability or degradation of DP operational capability but does not require termination of the operation, e.g. loss of a generator.
- Severity Class 4: Minor – A failure which has negligible effect on the DP system or sub-system level, generally at component level, and results in minor unscheduled maintenance or repair.

Any concerns the FMEA team has regarding failure modes which may have a detrimental impact on the DP system and its operation should be raised. Refer to sections 3.3.18 and 4.19 for further information on how concerns should be managed.

3.3.1 Performing the FMEA

The FMEA does not quantify the probability of failures or the reliability level of systems and components on the vessel. These assessments are excluded for the purposes of simplicity. It is necessary to know whether the vessel will or will not lose position and not how often. Where the FMEA indicates that a critical single point failure exists which cannot be overcome by the introduction of a backup system, a detailed reliability analysis, such as a failure modes effects and criticality analysis (FMECA), could be undertaken as a separate work-scope. Areas identified as being affected are listed and reported.

Software is not normally analysed as part of the FMEA. However, during the DP FMEA proving trials, tests are carried out which will determine the system's capability to withstand a single failure. These tests, and also the factory acceptance tests, should be sufficiently detailed to rigorously test the software functions.

1 IEC Standard, IEC 60812: *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*

3.3.2 The FMEA Team

Prior to commencement of the analysis, a team of specialists should be appointed each having a discipline in each of the systems and each having previous experience performing an FMEA.

Whilst all team members should have knowledge of FMEA procedures, it is unrealistic to expect that one individual person will have all the technical knowledge of all the systems on the vessel. A team approach with multi-disciplined members is essential for identifying all FMEA elements. Each member should be competent and have previous experience in carrying out FMEAs. The team should consist of competent individuals with expertise relating to machinery, control and electrical systems. If fire and flooding is to be considered, as in an FMEA for DP 3, a specialist in naval architecture may be consulted regarding the structural element of the analysis.

Each team member should have not just the in-depth knowledge of the system relating to their specific discipline but also the analytical skills needed to determine the failure modes and their effects within their system. They should also have some knowledge of design, manufacturing, assembly, service, quality and reliability. Each individual member should add to the process their own expertise and each should be responsible for document preparation and data input to the FMEA. The company carrying out the FMEA should make the qualifications of the team members available for scrutiny by the client.

A qualified lead 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.

FMEA team members on a specific contract should work as a team, but need not necessarily be in the same location or from the same company provided good communications are in place. Team competency and skills should be matched with the level of technology within the DP system being analysed. For existing vessels, one of the vessel's experienced DP staff could be appointed to the FMEA team, i.e. someone who knows where to source the information and understands why it is required. For new vessels, a company representative experienced in DP vessel operation could be appointed to the team.

3.3.3 Selecting the FMEA Team Members

The FMEA should be carried out by 'competent' FMEA team members. Competence is defined by the UK Health & Safety Executive (HSE) as *'the ability to undertake responsibilities and perform activities to a recognised standard on a regular basis. It combines practical and thinking skills, knowledge and experience'*.

When assessing the competency of an organisation it may be useful to consider the qualifications, activity specific training, procedures and experience of their staff. Adherence to the requirements of a certified quality management system and the use of IMCA or other standard industry guidelines and materials could also be taken into consideration.[2]

Whilst IMCA M 190 lists the following qualifications and experience that might be expected to apply to individuals involved in the preparation of an annual trials programme, they would also be appropriate for FMEA:

- *qualified engineer (STCW III/2 – chief engineer, electrical engineer with relevant degree or other equivalent qualification) or a qualified mariner (STCW II/2 – master);*
- *part of a team responsible for the production of at least one DP FMEA for a vessel of a similar type;*
- *witnessed at least three annual DP trials;*
- *has a thorough knowledge of all applicable class rules and IMO/IMCA guidelines;*
- *is familiar with the IMCA station keeping incident database;*
- *has knowledge of the operational or industrial function of the vessel and any relevant interfaces between the DP system and specialised equipment. [IMCA M 190]*

2 IMCA M 190 – *Guidance for developing and conducting annual DP trials programmes for DP vessels*

The FMEA team should be independent of the designers and be fully aware of all available IMCA documentation. The company and its personnel should be able to demonstrate a track record or reference list relating to previous FMEA work and DP expertise.

3.3.4 Defining the Standards

It is important to specify a standard to which the FMEA is to be carried out. Any deviations from the standard that may be needed should also be defined.

The use of a clearly defined methodology for carrying out the FMEA should allow the required in-depth study to be attained without the uncertainty of a less structured approach. Consequently, whoever requires the analysis to be undertaken will be confident that it was performed in a structured manner. They should also have increased confidence that all interested parties will accept the FMEA.

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

- 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)*;
- 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);
- US Department of Defense military standard MIL-STD-1629A (1980) has since been withdrawn but is still quoted and used occasionally.

These standards are general standards for FMEA and not DP FMEA specific. There are other standards, such as SAE J1739, which use similar techniques but the ones above are sufficient for reference purposes. It should be acknowledged that the medical device and the automotive industries are very intense users of FMEAs.

Specifying a standard may not guarantee an acceptable FMEA but it should guarantee an acceptable procedure and format. It will not dictate what areas should be analysed in a particular system or to what level of detail those areas 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.

Specifying an FMEA standard should not limit design innovation. 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.

3.3.5 Class Rules and the FMEA

Class rules are mandatory requirements in the design and build of a vessel. When carrying out an FMEA for a particular vessel, the rules in force at the time of signing of the vessel contract should be consulted. It is important that the FMEA team is using the class rules that are applicable for their specific project.

In the case of a major upgrade taking place on an existing vessel, the rules governing the upgrade should be consulted, unless decided otherwise by class.

The classification societies, American Bureau of Shipping (ABS), DNV GL and Lloyd's Register (LR), issue requirements in the form of class notations for DP vessels. These implement the IMO guidelines (refer to IMO MSC/Circ.645) with more specific requirements. The classification societies also specify the documentation that should be provided for approval and the scope of testing. An FMEA is required for compliance with class notations equivalent to DP 2 and DP 3.

The classification society issuing the DP notation can form part of the FMEA team subject to rigid and independently auditable segregation. Class review requires time (typically a minimum

of six weeks); therefore, the FMEA for a new DP vessel needs to be submitted to class as early as possible.

Class rules consulted in the preparation of DP system FMEAs include:

- *ABS Guide for dynamic positioning systems* – November 2013. (This guide replaces ABS DP system requirements previously included in the ABS *Rules for building and classing steel vessels (steel vessel rules)* and the ABS *Rules for building and classing offshore support vessels (OSV rules)*;
- DNV GL *Rules for classification of ships*, Part 6 Chapter 3;
- Lloyd's Register *Rules and regulations for the classification of ships*, July 2015, Part 7 Chapter 4.

3.3.6 Guidelines

The FMEA team should make use of all current DP related guidelines that can assist in achieving the desired redundancy and operability of a DP vessel. They give a good guide as to which shipboard systems relating to DP need to be covered.

Note: Where references below contain dates current to publishing of this guide, the reader should ensure that they have the correct revision of the documents relevant to their subject vessel.

IMCA Guidelines

The main IMCA guidelines recommended in the preparation of DP system FMEAs are:

- IMCA M 103 – *Guidelines for the design and operation of dynamically positioned vessels* – 2014;
- 113 IMO – *Guidelines for vessels with dynamic positioning systems (MSC Circular 645)* –1994;
- IMCA M 206 – *A guide to DP electrical power and control systems* – 2010;
- Information note IMCA M 04/04 – *Methods of establishing the safety and reliability of DP systems* – 2004. This is a very comprehensive and detailed guide to the systems and their boundaries, particularly Appendices D and E of the Annex which include guidance on the IMO guidelines in IMO MSC/Circ.645 (113 IMO).

The IMO HSC Code addresses FMEA issues for compliance purposes and is a relevant descriptive document for reference purposes in understanding the FMEA process.[3]

Although the FMEA team member needs to be familiar with all the guidance documents and the relevant standards for DP class vessels, those concerned with the management of the vessels need not concern themselves with having to read all of them.

Table 3-1 gives an indication of IMCA documents with which individual members in the ship operator's team (and others) should be familiar.

Responsible Person	**IMCA M 166** (*this document*)	**IMCA M 103**	**IMCA M 04/04**	**113 IMO**
Ship Manager				
Ship Superintendent	X	X	X	X
Master/OIM		X	X	X
DPO		X	X	X
Chief Engineer	X	X	X	
ET/ETO/Electrician	X	X	X	
FMEA Team Member	X	X	X	X
System Designers	X	X	X	X

Table 3-1 – Matrix of IMCA documents

3 IMO *International Code of Safety for High-Speed Craft*, 2000 (2000 HSC Code) with amendments

Other reference material that can be consulted in the preparation of DP system FMEAs include that produced by the classification societies, the Marine Technology Society and various documents relating to specific systems such as MODU and mooring systems.

Oil Majors

Some oil majors have their own guidelines on FMEA/FMECA.

For example, the BP *Shipping offshore assurance guidelines on FMEA and FMECA* dated 5 April 2006 state that the guideline *'affects all existing and new construction vessels on hire or coming on hire required to have an FMEA and/or FMECA provided, i.e. DP-2/DP-3 class drillships and semi-submersibles, dive support vessels, derrick barges, etc.'*

3.3.7 Defining the Reporting Procedures

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. A point of contact should be appointed in both the FMEA team and in the client's or FMEA owner's team. Figure 3-2 shows the reporting flow.

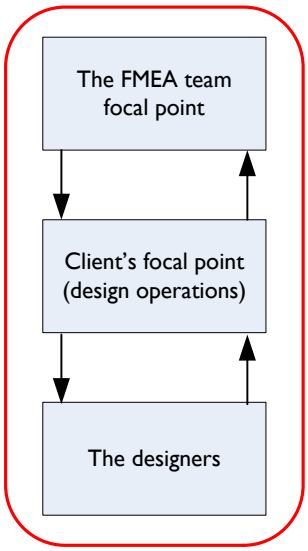


Figure 3-2 – Reporting flow

It should be stressed that the designers and FMEA team should work together and not operate in an isolated manner. Provided the designers carry out the design with failure in mind, then the FMEA is a double check on the process. Following the initial analysis, the designers should consider the findings of the FMEA team and any subsequent modifications made to the design should be reanalysed.

3.3.8 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 configurations the system is expected to perform.

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

A list of the components to be analysed by the FMEA can be found in Appendix D to the Annex of IMCA M 04/04. This list should be used only as a guide, as DP systems can be configured differently and may include additional items to those on the list or exclude some of those items on the list.

The boundaries of the system consist of the following:

- the physical boundaries, and
- the operational boundaries.

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 analysed, it is not necessary to analyse systems such as, for example, domestic hot water, if they do not have any direct or indirect effect on the DP system should they fail. However, if a system is analysed and found to have no impact on the vessel's station keeping ability, it is good practice to include that system in the FMEA analysis stating the findings. This is to avoid doubt on whether the system had been covered or not in the FMEA.

Techniques such as reliability block diagrams or fault trees can be helpful when defining the boundaries of the system. These are graphic methods which help to break the main system down from a high system level to lower system levels to ensure that no critical element is overlooked. They can be used to illustrate the interdependence between elements and how each system level interacts with another. Alternative techniques may be used where it can be demonstrated that these are suitable and sufficient.

The IEC standard 60812 requires that the FMEA should *'illustrate the interrelationships of functional elements of the system by means of block diagrams'* and *'develop block diagram(s) showing the functional flow sequence of the system, both for technical understanding of the functions and operation of the system and for the subsequent analysis'*.

The reliability block diagrams of all major equipment groups are developed from the top level design, i.e. from the single line drawings or P&IDs (process and instrument diagrams). They are often used to categorise and identify the equipment analysed during the FMEA process.

Functional block diagrams are simplified system diagrams, showing the interrelationships of major components. When describing the part of the system under analysis, the system description should include a functional block diagram which is a simplified version of the single line system diagram or P&ID.

The examples below show a reliability block diagram (Figure 3-3) and a functional block diagram (Figure 3-4).

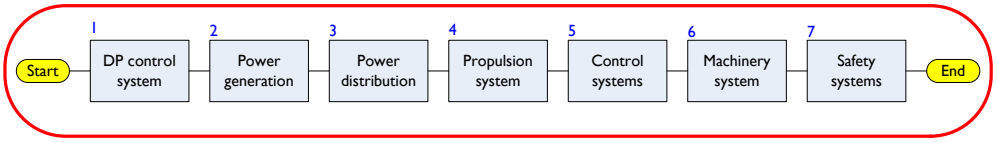


Figure 3-3 – Basic RBD of the DP system

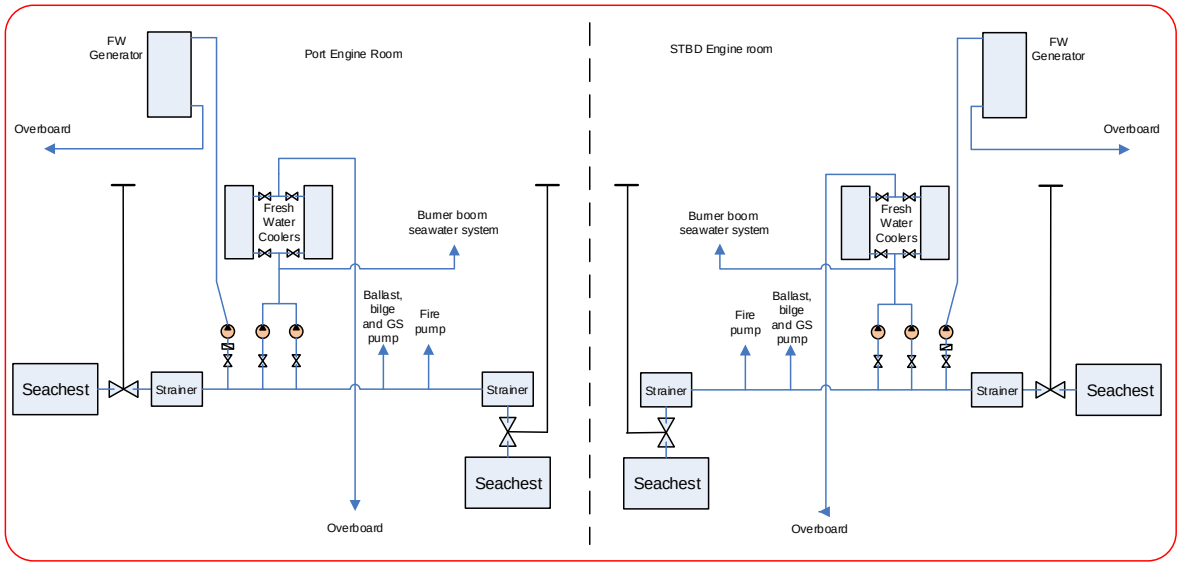


Figure 3-4 – Example functional block diagram of seawater cooling system

Major DP equipment grouping can be organised as follows (refer to the Annex to IMCA M 04/04:

- DP control system, including computers and consoles, networks, hardware architecture, changeover switches, position reference systems, gyros, vertical reference sensors and wind sensors;
- Power generation, including generators, voltage regulators, governors, generator and bus bar protection systems;
- Power distribution, including high, medium and low voltage AC distribution systems, emergency systems configuration and distribution, UPS systems configuration and distribution, low voltage DC distribution systems and control power supplies, bus tiebreakers and breaker interlocks;
- Propulsion system, including main propellers and/or thrusters and their drives, hydraulic systems, lubrication systems, emergency stops, steering gear, gearboxes, cooling system, control loops, manual, joystick and DP interfaces;
- Control systems, including integrated control system, thruster control systems, vessel management system, power management system (including load sharing, load shedding, load reduction, and black out recovery), data networks and hardware architecture;
- Machinery systems, including prime movers, fuel system, freshwater and seawater cooling systems, lubrication systems, compressed air systems, remote controlled valve systems, heating, ventilation, and air conditioning;
- Safety systems, including fire and gas detection systems, fire extinguishing systems, emergency shutdown system and quick closing valves.

Block diagrams would be developed for each of these groups, breaking each group down into sub sections. For a full description of how the RBDs are developed, refer to section 3.4.2.

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, i.e. the WCFDI, 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 vessel's capability plots which should include the worst case failure condition.

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 e.g. if two redundant items are placed in same location where temperature and humidity are high, the temperature, humidity ratings should be reviewed (refer to section 3.3.10). Other consideration should be given to ergonomics and factors which affect human performance.

3.3.9 Active and Static (Passive) Components

FMEAs, such as those required for DP systems, use the concept of static (or passive) and active components when deciding what types of failures will be included in the FMEA.

Active components refer to machinery that moves and rotates during operation (e.g. pumps, compressors, generators, thrusters, remote controlled valves, etc.). For electrical/electronic systems, active equipment refers to those that require being powered in some way to make them work (e.g. integrated circuits, PLCs, switchboards, etc.).

Static components refer to machinery having parts that normally do not move (e.g. pipes, tanks, vessels, shell-and-tube heat exchanger, manual valves, etc.). For electrical/electronic systems, passive components are those that do not require energy to make them work (e.g. electrical cables, resistors, capacitors, etc.).

IMO MSC Circular 645 states that "*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 will not be considered to fail where adequate protection from damage is demonstrated, and reliability is to the satisfaction of the Administration*." For equipment class 3, IMO MSC Circular 645 states that: "*Items listed above for class 2, and any normally static component is assumed to fail*". Hence, for DP 2 vessels, the FMEA should determine whether or not a static component has suitable reliability and is protected from damage.

Static components are, in general, considered to be of higher reliability, whereas active components have a lower reliability. However, even static components can have a significant probability of failure in mechanical systems (e.g. small diameter pipes, gaskets, flanged connections in the pipe, heat exchanger tube ends, etc.) and in electrical systems (e.g. capacitors failing very rapidly when exposed to a voltage above their rating). Failures such as these should be considered in the FMEA and demonstrated to be mitigated to an acceptable level[4].

3.3.10 Common Mode and Common Cause Failures

There are two cases when more than one failure should be considered in the FMEA:

- when two or more systems or components can fail due to a single specific event or cause (common mode and common cause failures);
- when one of the failures can be latent, undetected or hidden (see section 3.3.11).

DNV-RP-D102 – *Failure mode and effect analysis (FMEA) of redundant systems* – January 2012 states that: *Common mode failures should not be confused with common cause failures as the common mode failures may result from differing causes*.

A 'Common mode' failure is the failure of two or more systems or components in the same manner or mode due to a single event or cause. Any two identical elements have the potential to fail in the same manner; therefore any system which has identical redundant elements is open to the possibility of common mode failures. The most common example would be the failure of two identical redundant elements due to the failure of a common power supply. Load sharing failure between generators or a single heat exchanger for the cooling of two redundant systems would also be considered to be common mode failures.

4 ABS *Guidance notes on failure modes and effects analysis for class*, May 2015

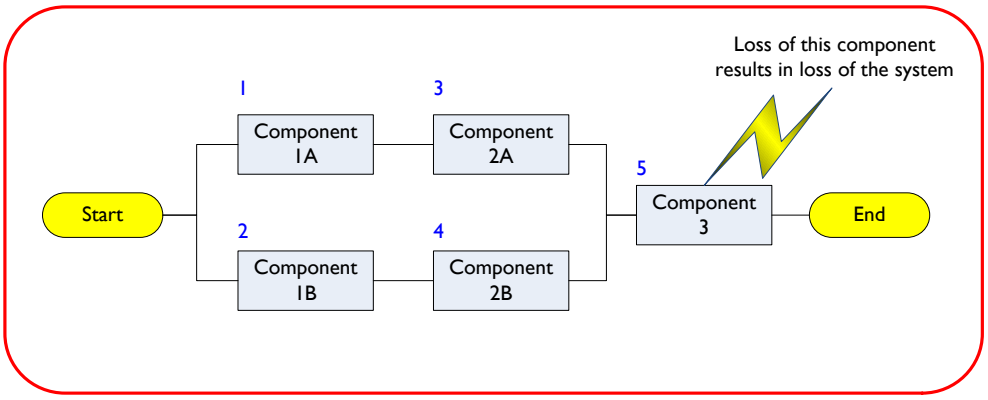


Figure 3-5 – Example of common mode failure

A 'common cause' failure is one in which a single failure or condition affects the operation of multiple redundant elements that would otherwise be considered to be independent. The redundant elements that have failed may have different failure modes. Common cause failures are generally those due to high ambient temperature, humidity, vibration, voltage transients, contaminants and improper maintenance affecting redundant items of hardware. Operation and maintenance errors are often reported to be common cause failures (carelessness, miscalibrations, erroneous procedures). The most common type of common cause failure is software. More specifically to DP vessels, common cause failures affecting redundant systems could be due to fire, flooding, external EMC, scintillation affecting GPS and extreme movements of the vessel.

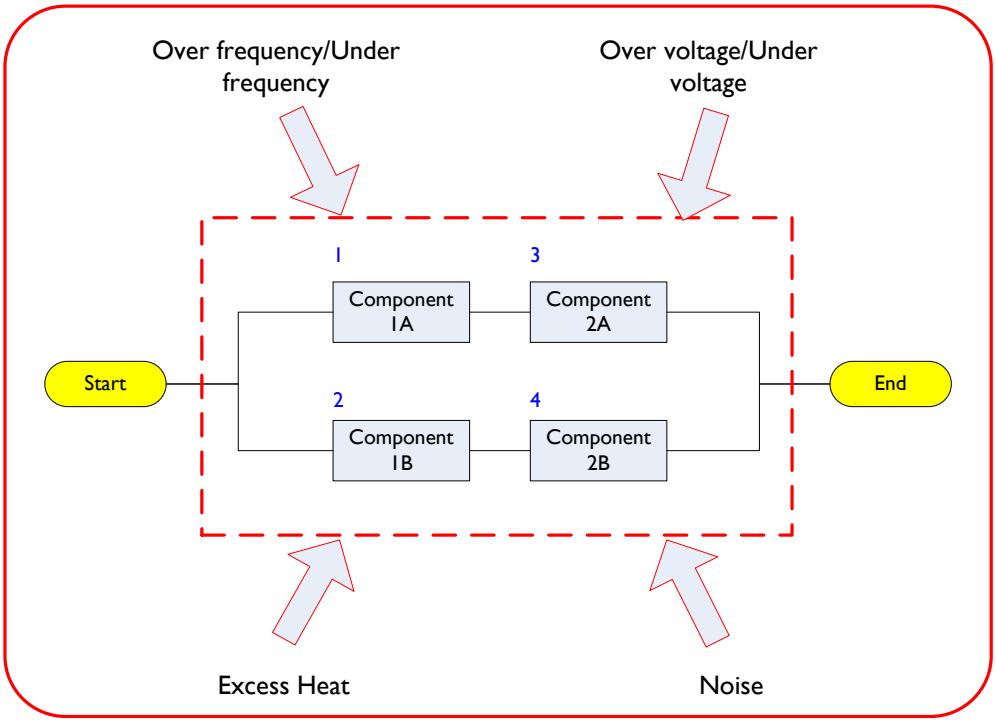


Figure 3-6 – Example of common cause failures acting on a redundant system

Prevention measures include:

- monitoring, testing and inspection (including dedicated tests performed on redundant components following observed failures);
- redundancy using redundant elements of differing design;
- design and equipment selection;

- preventive maintenance;
- personnel training (ensure that procedures are followed in all operation conditions).

A common mode and common cause failure analysis should be incorporated into the descriptive section for each system in the FMEA report to define the areas where a common effect could cause redundant equipment to fail. The PMS/DP failure/maintenance records and existing records of non-conformity (NCRs) should be reviewed to identify if there is any historical evidence of these types of failure.

3.3.11 Hidden Failures

The FMEA should consider hidden failures which are capable of defeating or degrading redundancy. These are failures in which a failure of a backup or standby item of equipment is not alarmed so that a first failure is not realised until the initiating second failure has occurred.

For instance, a fault on a standby pump which is not alarmed will fail to warn the operator that the pump will be unavailable when the duty pump fails, or a UPS having a faulty battery which, if not alarmed, will fail to warn the operator that the UPS will not be able to take load when required. Typical of this type of failure are fuses to the standby equipment which would require fuse failure monitoring.

Hidden failures should therefore be revealed by appropriate alarms. When carrying out the analysis, it should be considered what alarms are generated on failure of equipment, such that even if the item of equipment is on standby, it is monitored for failure. Where it is not practical to have an alarm and a DP failure will result if the item of equipment fails, then the system will require modification or measures put in place for mitigating the risk of the hidden failure by periodic testing.

A statement regarding hidden failures should be incorporated into the descriptive section for each system in the FMEA report advising the FMEA owner that the problem of hidden failures has been properly addressed in the FMEA.

3.3.12 Inadvertent Acts

An inadvertent act is an action taken by an operator which is carried out in an unintentional manner. No single inadvertent act should lead to a loss of position or heading. Suitable measures should be provided to mitigate such risks where they are found to exist. The potential for an inadvertent act to occur is part of the scope of an FMEA.

Systems such as a DP control system should ensure that more than one step is required to carry out an action. For example, after the request to carry out the action, it should ask the operator to confirm on the screen that the action is to be carried out. Similarly, other systems may require two actions to take place, for example, in the case of quick closing valve activation, the opening of a cabinet door and activation of a lever. Some systems will not have this type of feature and if the action can occur without a confirmation then the design should be such that a known worst case failure cannot be exceeded.

3.3.13 Transfer of Fault

Particular attention should be paid in the design to removing any fault path which can allow failure effects to be transferred from one redundant element of a pair to the other. Common connections should be minimised but where such connections are necessary or cannot be removed there should be automatic protective functions to prevent fault transfer. Operator intervention to prevent fault transfer should only be accepted where there is adequate time for such intervention before plant stability is lost and there are sufficient alarm and indications to reveal the fault.

3.3.14 Assumptions and System Configurations in the Analysis

The FMEA should state the assumptions made in the analysis and the system configuration. For example, from an operational point of view, it would be assumed that the vessel is operating in DP mode and with all equipment available for use (though, if relevant, consideration could be given to a main diesel generator set being unavailable due to maintenance).

When analysing the drawings and specifications, the normal configuration and all alternate configurations of the DP system should be stated, for example:

- all vessel equipment relating to DP should be functional and running with no alarms;
- main switchboard configurations, i.e.
  - closed ring with all tiebreakers closed
  - open ring mode with the main switchboards coupled and one set of tiebreakers open
  - all main switchboards operated isolated;
- lower voltage switchboard configuration;
- emergency switchboard configuration;
- arrangement of generators connected to each switchboard;
- all generators available and selected to PMS control;
- all cooling systems operating in split mode with lead pump running and standby pump selected to auto;
- all thrusters operational and selected for use by the DP;
- thruster servo hydraulic backup pumps available and set to auto;
- a minimum of three position reference systems, using at least two different measuring principles, selected for use by the DP;
- all vessel reference systems (wind, gyro, and VRSs) available for use by the DP;
- FO system operated split;
- all FO and LO pumps set to normal automatic operation.

The equipment configuration for DP operations during trials where it deviates from the normal configuration should be stated for each individual test.

3.3.15 Organising System Design Information

A considerable amount of correspondence and design information, including drawings, will need to be studied during an FMEA. This information may be received in a single package but it is more likely to be received in stages over the course of the analysis.

It is therefore important that, from the outset, each item of information is documented so that it can be retrieved easily. To assist in this part of the process, the following areas require addressing:

- document tracking database;
- technical query (TQ) list;
- 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.

The strategy for carrying out an FMEA on an existing vessel should be no different from that for carrying out an FMEA on a new vessel. Both cases require good documentation. If drawings are not available for existing vessels then, if necessary, the vessel owner should arrange for the systems to be traced (e.g. cables and pipelines) to enable accurate drawings to be produced.

Document tracking 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 identify the drawings that are needed for the analysis and send a requested drawing list to the client's focal point who will arrange for these to be sent to the FMEA team. When received, the drawings should be logged into a document tracking database so that any revisions will be highlighted. In this way it will be ensured that the FMEA team is using the latest drawing revisions.

The database could be extended to log all in and out correspondence and design information received. Separate databases can be used, if necessary, to record the technical query list, FMEA worksheets and FMEA corrective action report forms (see below).

Technical query (TQ) list: During the course of the FMEA, technical questions will inevitably be raised. These will in turn generate answers. In order to ensure that all questions and their responses are fully documented, a technical query list 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 technical query list for the question or item number, the question, the response or answer, and whether the item has been closed out or not. It is also helpful to have fields identifying who is responsible for the question and who is responsible for answering. The technical query list should form part of the FMEA documentation.

FMEA corrective action report form: Whenever a potential problem is identified, particularly one which has the potential to compromise the worst case failure design intent (WCFDI) or the DP notation, or have a safety implication, the designers should be made aware of this at the earliest possible moment as it is easier to change a drawing than make physical modifications to the installation.

In order to do this, an FMEA corrective action report form should be completed as soon as possible and forwarded to the designers via the client's point of contact. In this way the designers are notified at an early stage such that remedial design work can be undertaken.

Corrective action report forms should be 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. An example can be found in Table 3-2. To complete the loop, the designers return the updated drawing with a revised arrangement and, subject to a satisfactory reanalysis, the corrective actions taken are indicated on the corrective action report form.

Essentially, the items on the corrective action report forms are concerns which are to be listed in the report. As with the technical query list, it should be recorded which concerns have been addressed and closed out during the analysis and which items are still outstanding. The corrective action report forms can be stored in a database for ease of retrieval, sorting, and digital transmission.

3.3.16 Evaluating the Effects of each Failure Mode on the System

Once the system requirements have been defined and the functional analysis commenced, the failure modes are identified and the failure effects and severity of each failure mode evaluated.

Initially, when analysing a system, it should be understood how it works before it can be understood how it fails. One method of ensuring this is to represent the system as reliability block diagrams (RBDs). RBDs are a key tool in assessing the interaction between systems and components, identifying the potential single point failures and establishing design redundancy levels. Refer to section 3.4.2.

Client Name/ABC DP Engineering **DP FMEA Type Vessel 'Vessel Name'** **FMEA CORRECTIVE ACTION REPORT FORM**		
FROM:	ABC DP Engineering	ISSUE DATE:
TO:	Client Name (Addressee)	REPORT FORM No.:
REFERENCE DWG No.: REFERENCE DWG TITLE: REFERENCE FMEA FORM/WORKSHEET No.:		
The following concern has been identified during the course of the analysis: CONCERN:		
Have hidden failures been taken into consideration (yes/no/not applicable):		
CORRECTIVE ACTIONS TAKEN: SIGNATURE: DATE:		

Table 3-2 – Corrective action report form

The failure effect is the consequence of the failure mode on the operation, function, or status of an item of equipment or a system. The effect should consider conditions that influence the system operability. The effects are generally classified into three levels: local, system and global effect. Failure effects on a specific item of equipment or sub-system under consideration is the local effect, the failure effects on the system itself is the system effect and the impact on the overall system function such as the position keeping of the vessel is the global effect.

The FMEA study analyses the effects of a single failure only in the system and therefore a means of detection to warn the operator of that failure, such as visual or audible warning devices,

automatic sensing devices, sensing instrumentation or other specific indications, should be identified.

The response of any backup equipment, or any corrective action initiated at a given system level to prevent or reduce the effect of the failure mode of a system element or equipment, should also be identified and evaluated. These are termed 'compensating provisions'.

The results for each failure mode of each component, with its assigned severity level, the identified failure detection method, e.g. alarm, and the compensating provisions should be recorded by the FMEA team in a structured manner such as on a worksheet. Refer to section 3.4.3.

An attempt should be made to correct a failure or provide a backup system (redundancy) to reduce the effect of fault propagation to the rest of the system. If this is not possible, procedures should be developed for reducing the effect of the failure mode through operator actions, maintenance, and/or inspection provided they are accepted as mitigation of failure effects under the relevant notation.

Figure 3-7 is an example of the failure evaluation process.

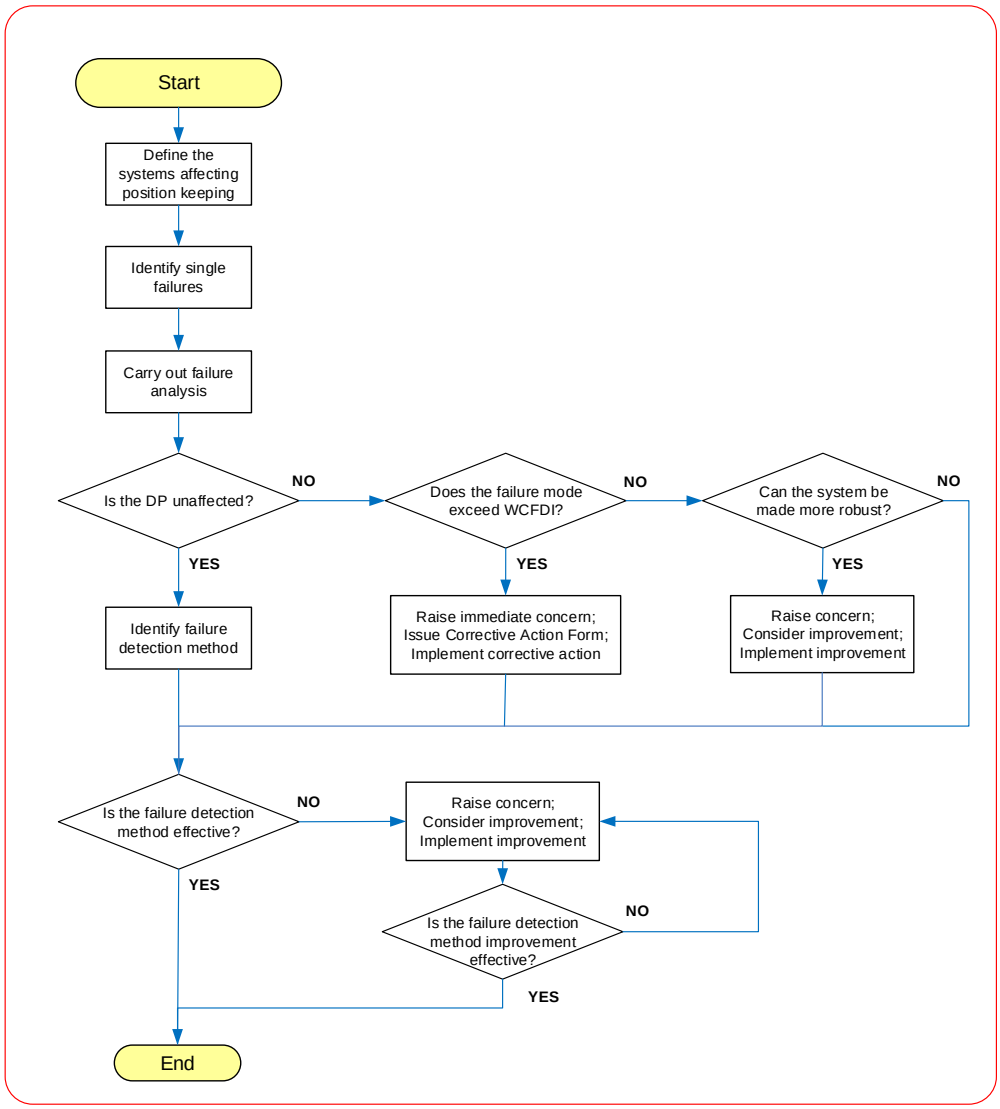


Figure 3-7 – Failure evaluation process flowsheet

When evaluating the effects of each failure mode on the system, the effectiveness of this part of the process is related to the technical strength of the team members in their respective disciplines. 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 analyst's knowledge base should be kept updated. This can be extended to include advice from manufacturers' representatives, shipyard specialists and designers.

3.3.17 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.

In reality, it is impractical to have an alarm for every failure that may remain hidden in a redundant system. Alarms can also fail. In the case of a DP system it is accepted that periodic testing such as annual DP trials plays a part in detecting hidden failures.

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. Any design modifications should result in a failure having less impact on a system if it occurs.

3.3.18 Concerns

This section gives guidance on how to administer any concerns arising from the FMEA. During the course of the analysis, any concerns the FMEA team has regarding failure modes which may have a detrimental impact on the DP system and its operation should be raised. The FMEA team should be at liberty to put forward any suggestions to improve the design features of the system.

Administration of the items for concern involves actions with respect to raising, categorising and 'closing out' of the items.

The FMEA should list any concerns under categories recommended as follows:

- Category A – Concerns which address potentially serious failure modes which are in excess of WCFDI, raise safety issues or do not comply with class requirements;
- Category B – Concerns which address failure modes which are not in excess of WCFDI, do not raise safety issues or are in compliance with class requirements but are considered important enough to make the system more robust, such as additional redundancy in key areas;
- Category C – Concerns which, if addressed, are designed to improve system operation. These are suggestions and not essential to the process.

When a failure mode is analysed and it is revealed that a potentially serious effect on the system could result if it occurs, i.e. a Category A concern, then this should be notified immediately to the client and the designers so that measures can be taken at the earliest opportunity to make design corrections. This can be done using the FMEA corrective action report form. A possible solution for corrective action could be offered. Refer to section 3.3.15.

A successful completion or 'close out' of the concern should be recorded, as well as a decision not to take action. It should be noted that agreement on an action does not, in itself, constitute 'close out', as 'close out' requires a verification of the effectiveness of the action.

Those concerns that have been actioned or not actioned during the course of the FMEA should be highlighted in the final report. The concerns and the method by which the concerns are closed out should be included in both the final FMEA report and the FMEA proving trials report where appropriate and not in separate documentation. Effective follow-up programmes are essential as the purpose of the FMEA is defeated if any Category A or Category B concerns are left unaddressed.

3.4 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 standards and guidelines followed during the analysis together with the class rules applicable to the vessel should be stated. The worst case failure design intent (WCFDI) should also be specified. 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.

Two levels of reporting are recommended; a comprehensive executive summary (or management overview) and a main report (with building blocks or subsections relating to each discipline). Operational assumptions should be included in the top level executive summary, together with a summary of the conclusions which should state the worst case failure determined from the analysis.

Each section should include a description of the system under analysis, including simplified system drawings developed from the system P&IDs. It should include the operating configuration/ configurations or set up of each system when the vessel is on DP and details of any significant failure modes identified together with any concerns raised. It should also include an analysis to show that the potential problems of hidden failures and common mode failures have been properly addressed in the FMEA.

The report should contain a summary of conclusions and concerns 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 should be included in the report to substantiate what has been done during the analysis and how the findings were achieved.

The FMEA report is a technical document and a statement of fact so it should avoid ambiguous statements, for example, when describing a particular failure or test, words like 'should happen', 'may happen', 'could happen', 'might happen' or 'possibly happen', etc. should be avoided. Therefore, where ambiguity exists and the FMEA seems to be undecided, actual FMEA proving trial tests should be carried out to obtain a satisfactory and positive result.

The FMEA report should be kept up to date to reflect any changes made to the system, hardware or software, during the life cycle of the vessel and in the light of any information gathered at a later date that was not available at the time of the FMEA. The FMEA should have a revision history section and be fully auditable with changes properly recorded during the process.

One purpose of the FMEA document is to assist in the training of crew and maintenance engineers; therefore, it is vital that all changes and modifications to the systems are analysed by the FMEA practitioner to determine any changes to post failure DP capability and updated in the document as and when they occur.

Following issue of the final revision of the FMEA, management of the FMEA should be based on IMCA guidelines. For these, refer to section 3.5.

3.4.1 FMEA Report Structure

The FMEA report would be expected to contain the following:

- Executive summary;
- Introduction:
  - FMEA Introduction
  - Glossary and/or list of abbreviations
  - Scope of work
  - FMEA procedure or methodology, including standards and guidelines
  - Vessel application and particulars
  - Any assumptions made in the analysis and the vessel equipment configuration/s analysed, e.g. the operational mode/s the vessel is in when the analysis is carried out
  - Documentation;
- Methodology of analysis:
  - Block diagrams
  - FMEA worksheet: Format, description of fields, definitions of severity levels
  - FMEA corrective action report form: Format;
- Description and analysis of Systems, including simplified system drawings, for example:
  - DP control system
  - Power generation
  - Automated control and monitoring systems
  - Power distribution systems
  - Machinery systems
  - Safety systems;
  - Fire and flood (DP 3)
- Concerns:
  - Summary of concerns and actions;
- Conclusions;
- Appendices:
  - Trials test sheets
  - Technical query list
  - FMEA corrective action report sheets
  - List of vessel/shipyard and vendor drawings received and reviewed.

3.4.2 Reliability Block Diagrams (RBDs)

Reliability block diagrams (RBDs) are also known as inter-dependability block diagrams as the RBD is a graphical representation of how each sub-system is dependent upon each other. They are not 'one line' system diagrams or process and instrumentation diagrams (P&IDs) and the blocks are not necessarily in any particular order. The RBD graphically illustrates how a system functions and shows the effect on the system of the loss of any one sub-system or component in the diagram. The thought processes involved in producing the RBDs aid the FMEA team member in analysing the system under review. It also significantly helps to reduce the risk that some parts of the system have been overlooked in the analysis.

Block diagrams are referenced in industry standard guidelines, e.g. IEC 60812. They should be provided for each system and/or sub-system unless alternative techniques are used where it can be demonstrated that these are suitable and sufficient. IEC 60812 states that:

'As a minimum, the block diagram should contain the following:

a) breakdown of the system into major sub-systems including functional relationships;

b) all appropriately labelled inputs and outputs and identification numbers by which each sub-system is consistently referenced;

c) all redundancies, alternative signal paths and other engineering features which provide protection against system failures.'

The examples of block diagrams below serve to illustrate how the system under analysis is broken down into its different levels. Figure 3-8 shows an RBD 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.

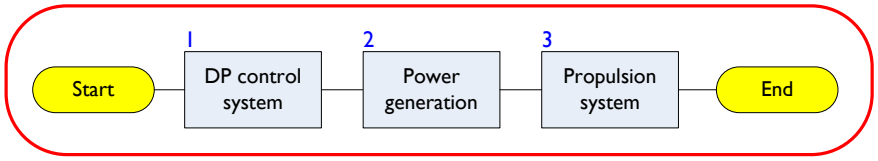


Figure 3-8 – Basic block diagram of the DP system

Figure 3-9 shows the DP control system block from Figure 3-8 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.

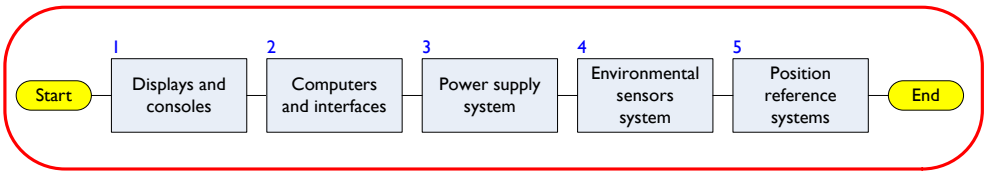


Figure 3-9 – Block diagram of DP control system

Figure 3-10 shows an example of how the position reference system block, Block 5, from Figure 3-9 can be broken down into its component parts. In this case, there are four position reference systems each carrying out the same task, two DGPS and two hydroacoustic systems, but as there are two power supplies, there are two parallel paths. Should one of the parallel paths fail, then the system is still operational as the other path is still available.

One way to understand the RBD is to 'fail' any one single block by covering it up. If a path can be traced from 'Start' to 'End', the process still functions using the blocks that are still in the path from 'Start' to End', with either loss of redundancy or reduced redundancy. In the example in Figure 3-10, loss of a DGPS would be reduced redundancy and loss of a PSU would be loss of redundancy.

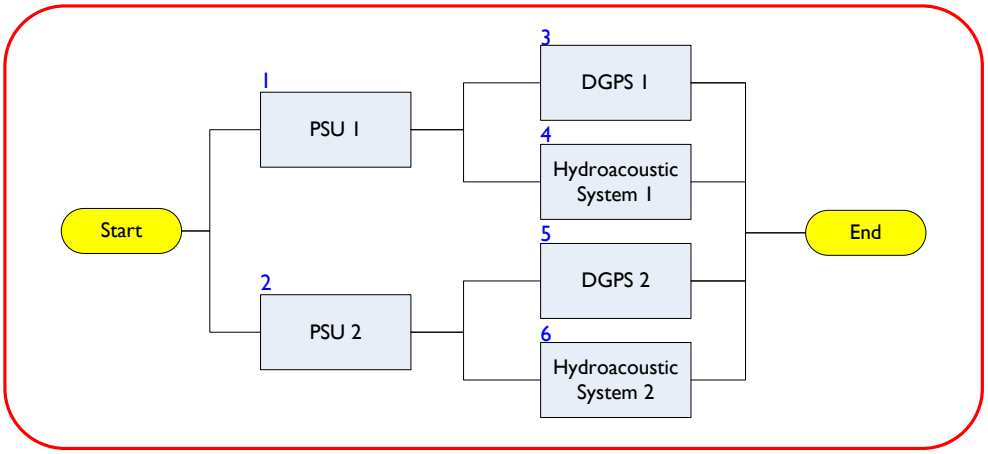


Figure 3-10 – Block diagram of position reference systems

Figures 3-11 and 3-12 show how the RBD for the seawater system is developed from the P&ID.

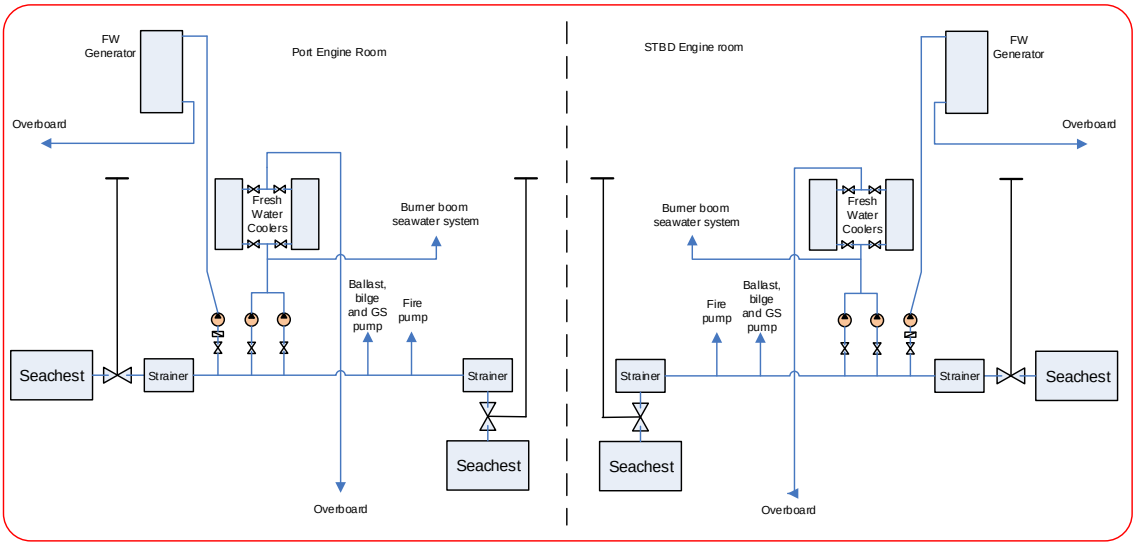


Figure 3-11 – Seawater system P&ID

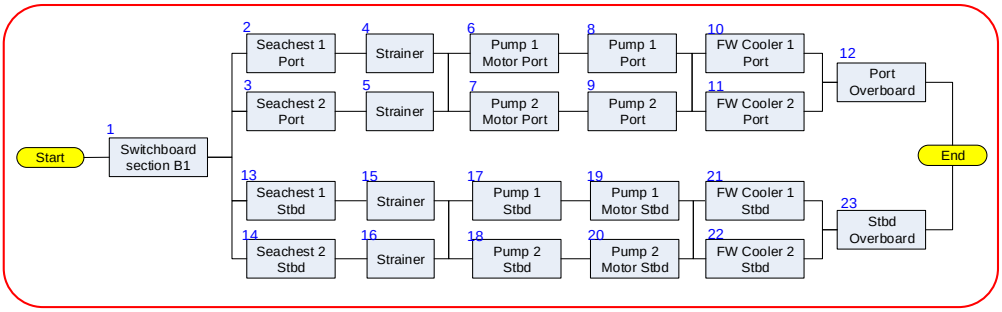


Figure 3-12 – Seawater system RBD

The FMEA team member will usually try to lay out the block diagram in a logical order to improve readability but this is not always possible. In the example of a seawater system in Figure 3-12, the order for the port and starboard system has been changed, but both are logically correct for this system.

This example also includes a 'common mode failure'. If the 'Switchboard section B1' block is covered, the entire process is lost.

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 3.9.4). Furthermore, the RBDs can be used at a later date to input information into a reliability, availability and maintainability (RAM) analysis if required.

3.4.3 FMEA Worksheet

The failure mode of each component and the effects of failure should be categorised by reference to the severity of the failure effects in relation to the worst case failure design intent. This should be recorded in a structured form such as in an FMEA worksheet.

A worksheet is a form of tabulated report and compiled for each equipment system and/or sub-system, with each worksheet containing an entry for each component, detailing the component function and its failure assessment. Each worksheet should have a unique number for traceability purposes. Worksheets are required by industry standard guidelines (e.g. IEC 60812).

The fields expected in the FMEA worksheet are as follows:

- **ID/component**: A discrete number and name or nomenclature of the item or system function being analysed for failure mode and effects is listed.
- **Function**: A concise statement of the function performed by the hardware item is listed.
- **Failure mode and failure cause**: The predictable failure modes for each systems level analysed are identified and described. Potential failure modes are determined by examination of item outputs and functional outputs identified in applicable block diagrams and schematics. The most probable causes associated with the postulated failure mode is identified and described. Since a failure mode could have more than one cause, all probable independent causes for each failure mode are identified and described.
- **Failure effect consequences**: The consequences of each assumed failure mode on item operation, function, or status is identified, evaluated, and recorded. Failure effects should focus on the specific element which is affected by the failure under consideration. The failure under consideration could affect several systems levels in addition to the systems level under analysis; therefore, 'local consequences', 'system consequences', and 'global consequences' should be evaluated.
- **Local consequences**: Local consequences 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 postulated failure affecting the item are described along with any second-order effects which result. It is possible for the 'local' effect to be the failure mode itself.
- **System consequences**: System consequences 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 postulated failure affecting the next higher systems level should be described.
- **Global consequences**: System consequences evaluate and define the total effect an assumed failure has on the operation, function, or status of the main system, i.e. whether or not DP is lost, redundancy is lost (i.e. reduced to simplex system), redundancy is impaired, or redundancy is still intact.
- **Failure detection method**: A description of the methods by which occurrence of the failure mode is detected by the operator is recorded. The failure detection means, such as visual, alarm devices, or none, is identified.
- **Compensating provisions**: The compensating provisions, either design provisions or operator actions, which circumvent or mitigate the effect of the failure are identified and evaluated.
- **Severity/risk**: For an FMEA, each failure mode should be assigned a value for the 'severity' or 'consequence' of the failure occurring. A definition of the severity categories used should be included.

The following are examples of the definitions of the severity categories in the case of a DP system:

- Severity Class 1: Catastrophic – A 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 position keeping ability leading to an excursion, drive off, or drift off from position resulting in possible asset loss or major environmental impact and which will lead to an emergency termination of the operation.
- Severity Class 2: Critical – A 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 result in loss of position, necessitating a controlled termination of the operation, e.g. loss of a main switchboard, and results in an extended period of shut down of operations.
- Severity Class 3: Serious – A failure resulting in a temporary loss of availability or degradation of DP operational capability but does not require termination of the operation, e.g. loss of a generator.
- Severity Class 4: Minor – A failure which has negligible effect on the DP system or sub-system level, generally at component level, and results in minor unscheduled maintenance or repair.

- **Test Reference**: Cross reference to the relevant test in the DP FMEA proving trials.

The worksheets form part of the FMEA final report. They verify that each sub-system or component part of the system has been analysed and document the results of the analysis. An example of a worksheet is shown in Table 3-3.

FMEA Worksheet			
System:	Power Distribution	Compiled by:	
Sub-system:	490V Switchboards Control Power	Date:	
Drawings used:			

ID	Component	Function	Failure mode	Failure cause	Failure effect consequence			Failure detection	Compensating provisions	Severity	Test ref
					Local	System	Global				
24Vdc Control Power											
1	Bus transformer	Supply power	No power	Open/short circuit	Loss of one or two supplies	Reduced redundancy	No effect on position keeping	Alarm	UPS used	3	n/a
2											
3											
4											

Table 3-3 – Example of an FMEA worksheet

3.4.4 Fire and Flood Assessment

DP 3 vessel single point failure criteria includes the loss of a watertight space due to flooding or the loss of a space contained within an A-60 fire protected area due to fire. To this end, it is expected that the FMEA will contain a descriptive text of the means used to achieve this and some form of tabulated analysis of each fire and flood protected space. This tabulation should include all DP relevant equipment, including cables, piping and conduit, in each fire and flood protected space. An assessment is made of the resources that remain following a fire or flood and that these remaining resources are sufficient for the vessel to maintain position following the loss of any single fire/flood protected space.

Fire and flood assessment can be a difficult part of the analysis, even if the cable and pipe routing drawings are available. It can be time consuming as it may take a review of several drawings to be able to trace, for example, a single cable run between one item of equipment in one compartment to another item of equipment in another compartment.

For a DP 3 vessel, shipyards may produce routing drawings for power and control cabling and piping, showing on the general arrangement drawings the redundant paths the cables and pipes take. Where fire and flood assessment is required, routing drawings should be specified at the contract stage. For an existing DP 3 vessel, where these drawings are not available, it may be necessary to physically trace each cable and pipe route.

Below is an example of a fire/flood assessment for an imaginary DP 3 vessel. The assessment will require some descriptive text, for example "… *A fire in the engine room work shop will propagate to port FO separator room. This will result in loss of FO service and settling tanks for port engine room, eventually resulting in …*"

Tabulation of the Effect of Fire and/or Flood

Effect on DP System	Severity
Severe loss of DP capability exceeding the WCFDI or no DP capability. Probable loss of position.	1
Reduced to simplex system. Loss of redundancy in the main DP system or loss of redundancy exceeding loss of backup DP system. Possible reduction in DP capability.	2
Duplex system. Possible reduction in DP capability.	3
No effect on redundancy or DP capability.	4

Table 3-4 – Definitions of severity levels

Compartment	DP resources including piping and cabling lost due to fire/flood in compartment	Result	Severity after fire/flooding of compartment
Wheelhouse (Deck H)	DP OS 1. DP OS 2. DGPS No. 1. DP Alert Panel and Switch. Wind display No. 1 Wind display No. 2.	Loss of main DP. Control to be transferred over to backup DP.	2
Electric Room 1 (Deck G)	DP controller cabinet. Control cables Thr 1, 3 and 5.	Loss of main DP. Control to be transferred over to backup DP. Reduced thruster capacity	2
Backup DP Room	Back up DP console Wind display 3 MRU 3	Loss of backup DP control. Control continues with main DP	3
Engine room Port	Diesel generators 1, 2 and 3	Loss of 50% generating capacity	2

Table 3-5 – Worksheet example

3.4.5 Manufacturers' FMEAs

Some manufacturers produce an FMEA of the vessel sub-system they provide which forms part of the complete DP system as they are required and approved by the classification society. The standard of information about failure modes provided by manufacturers can be variable and generally it is not possible to successfully integrate these sub-system FMEAs into the main FMEA.

Whilst the manufacturers' FMEAs tend to be generic, they should be reviewed and the results verified as being compatible with the overall redundancy design intent before being included in the main FMEA.

Any areas of weakness identified should be readdressed, with the manufacturer providing relevant data. Owners or shipyards commissioning the FMEA should ensure sufficient detailed information is made available to the FMEA team.

The overall FMEA should not include manufacturers' FMEAs unless they have been tightly specified so as to be compatible with the overall FMEA. Manufacturers should be encouraged to follow the same guidelines and format used for the main FMEA to assist in possible integration if found appropriate.

3.4.6 FMEA Proving Trials Test Programme

The FMEA proving trials are generally devised to confirm, in a practical manner, the conclusions of the FMEA desktop analysis and failure modes that cannot be confirmed during the analysis of design drawings and other design information. However, class in particular have extended this to require the FMEA proving trials to test performance related functions.

The FMEA tests are developed as the desktop analysis progresses. The FMEA trials document should form part of the FMEA report and the results of the trials fed back into the FMEA. The trials test sheets are generally developed from the FMEA worksheets so there is a strong link between the two. The trials test sheets may include a reference to the relevant section of the FMEA report.

The trials equipment configuration, or set up, that will be used in the test programme should be described in a section in the FMEA proving trials report. It should be stated that, for each specific test, if there is any deviation from this set up, it will be shown on the relevant test sheet. The relevant test sheet should therefore detail any differences in set up that will be required.

For each test it is helpful to attach a copy of the relevant part of the 'as built' drawing showing the item of equipment under test or the cabinet and terminations where a control loop is being failed. These comprise the 'workpacks' referred to in Figure 3-1. The workpacks help to save time during the sea trials as, should there be any doubt about a particular test, the information is immediately to hand.

The tests can be categorised on the basis that they can be conducted on 'full auto DP' or alternatively with the vessel in an operational configuration other than 'full auto DP' such that there is acceptable confidence that this will have no effect on the test result. The location will depend on where the tests can be performed safely and efficiently. The tests can be divided into three categories as defined below. The test categories can be changed by those witnessing the tests upon analysing the onsite survey of the situation at the time of the test.

Alongside tests: As the name suggests, the 'Alongside' tests can be done alongside. It should be made sure that the equipment or the system under test is fully operational and should have been commissioned prior to the FMEA test.

At sea tests: The tests categorised as 'at sea' can be done at sea without the vessel being on DP. In these tests different switchboard configurations may be required or extra load may be required which may not be achievable when the vessel is alongside.

On DP tests: The tests categorised as 'on DP' have to be done in full DP condition with the vessel's systems set up for normal DP operations and all reference systems, sensors and thrusters selected in DP.

3.4.7 Preliminary Report

Prior to the FMEA proving trials, the trials programme should be issued with the preliminary FMEA report. If they are to be submitted to class, they will require to be issued at least six weeks prior to the proving trials.

Class reviews frequently find problems in FMEAs when they are submitted for approval. However, whilst this guidance document is intended to avoid those problems, it is of benefit to carry out an internal review of the FMEA prior to submittal to ensure these problems do not exist. A list of common problems is as follows[5]:

- parts of the system omitted in the analysis;
- critical operations omitted in the analysis;
- incomplete failure list;
- no consideration of common-cause failures;
- no consideration of hidden failures;
- global end effects not addressed;
- no consideration of hidden failures on existing controls;
- failure of or delayed follow through of corrective actions;
- insufficient descriptions in the worksheets to understand the failure scenarios;
- insufficient information in FMEA report;
- FMEAs not matching the latest design or off-the shelf FMEAs;
- submittals too late.

5 ABS *Guidance notes on failure modes and effects analysis for class*, May 2015

3.4.8 FMEA Proving Trials

The FMEA confirms that the design of the vessel in compliance with the redundancy concept. The FMEA proving trials are drawn up to prove the conclusions of the FMEA in a practical manner and to confirm that the construction of the vessel is in compliance with the design.

The FMEA proving trials tests determine the dynamic response to failure rather than reliance being placed upon the static desktop analysis of the FMEA. The tests are also intended to confirm hardware redundancy and DP capability after failures and should also prove some aspects of software control.

Refer to section 4 for more details of FMEA testing.

If required, the annual trials checklist can be developed from the FMEA trials checklist, incorporating tests that demonstrate and confirm redundancy and show the system response to failure to the DP operators, some of whom may be new to the vessel. Refer to IMCA M 212 – *Example of an annual DP trials report* – and IMCA M 225 – *Example redundancy concept and annual DP trials for a DP class 3 construction vessel* – for examples of annual trials reports with checklists.

3.4.9 Final Report

Following the completion of the FMEA sea trials, the results should be incorporated into the preliminary FMEA report and the FMEA issued as a final FMEA report.

3.5 FMEA Management Guidance

3.5.1 FMEA Management and Ongoing QA

During the life of a vessel, inevitably modifications will be made to either improve the system operation or alter it to provide additional or different functions. The FMEA should be kept on board for reference and review by the vessel's staff on a regular basis so that any modifications to the vessel's system will prompt the need for a possible update of the FMEA. Such modifications may include hardware and/or software changes.

In order for DP related modifications to be managed, an FMEA management procedure should be put in place so that any changes are recorded and analysed and the FMEA updated where appropriate.

The vessel's FMEA should be identified as a controlled document which is part of the quality management system of the vessel so any changes to the FMEA contents will be identified through the audit trail.

The responsibility or ownership of the FMEA should be with the vessel operating company that is responsible for the safe operation of the vessel. The vessel holds the FMEA but the vessel management team ashore owns the FMEA and should be the responsible point for changes.

A focal point in the management team should be designated who should have a thorough understanding of the FMEA management process. The vessel's key personnel have the responsibility to make the vessel management team aware of any deficiencies or inaccuracies in the FMEA as they themselves become aware of them. The vessel management team is responsible for ensuring that any such deficiencies or inaccuracies are corrected in a timely manner.

The FMEA documentation consists of the FMEA report and supporting documentation such as the trials report, the technical query list and corrective action report forms. 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 vessel acceptance criteria during pre-charter audits.

As modifications are made to a vessel that may have a bearing on its DP system, the FMEA should be reviewed and updated to reflect the changes. It may not be necessary to update the FMEA formally on a regular basis, provided that any changes that are made during the life cycle of the vessel are properly analysed, recorded and acted upon accordingly. This would depend on the extent of the changes made to the system. From a safety point of view, the danger in not analysing the changes is that a number of small changes over a period of time may combine later to cause an incident. Should it be determined that the number and nature of the changes to the system have caused the FMEA to become out of date, the FMEA should be updated following the change control management procedure (see below).

The FMEA should contain references to any changes which have affected the FMEA since its original version. The FMEA should give guidance to ship operators as to when a change to the FMEA has no effect (low level) or has an effect (high level) on operations, emergency and maintenance operations and manuals.

It is important to have an effective follow-up FMEA management programme in place to ensure that all questions during the analysis are satisfactorily closed out, any corrective actions required or concerns raised are followed up and any modifications made are reanalysed and retested. In this way the FMEA will be kept up to date.

Following the FMEA, on an annual basis and assuming it is possible, workscope and worksite permitting, the vessel should be put through a series of DP tests, called annual DP trials, using a test plan developed from the FMEA proving trials test sheets. These tests should also prove the continued functionality of the system in addition to confirming the system's continued response to failure as concluded by the FMEA. Refer to the following IMCA reference documents:

- IMCA M 190A – *Guidance for developing and conducting annual DP trials programmes for DP vessels: Executive summary*;
- IMCA M 191 – *Guidelines for annual DP trials for DP mobile offshore drilling units* (continuous programme);
- IMCA M 212 – *Example of an annual DP trials report.*

These tests should 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.

Classification societies require notification of any changes made that may affect the basis of the classification requirements. It then depends on the society surveyor reviewing the changes whether or not a revised FMEA will be required. If the FMEA report is required to be updated it should be resubmitted to demonstrate that the system is still in compliance with the design philosophy and is then to be kept onboard the vessel[6].

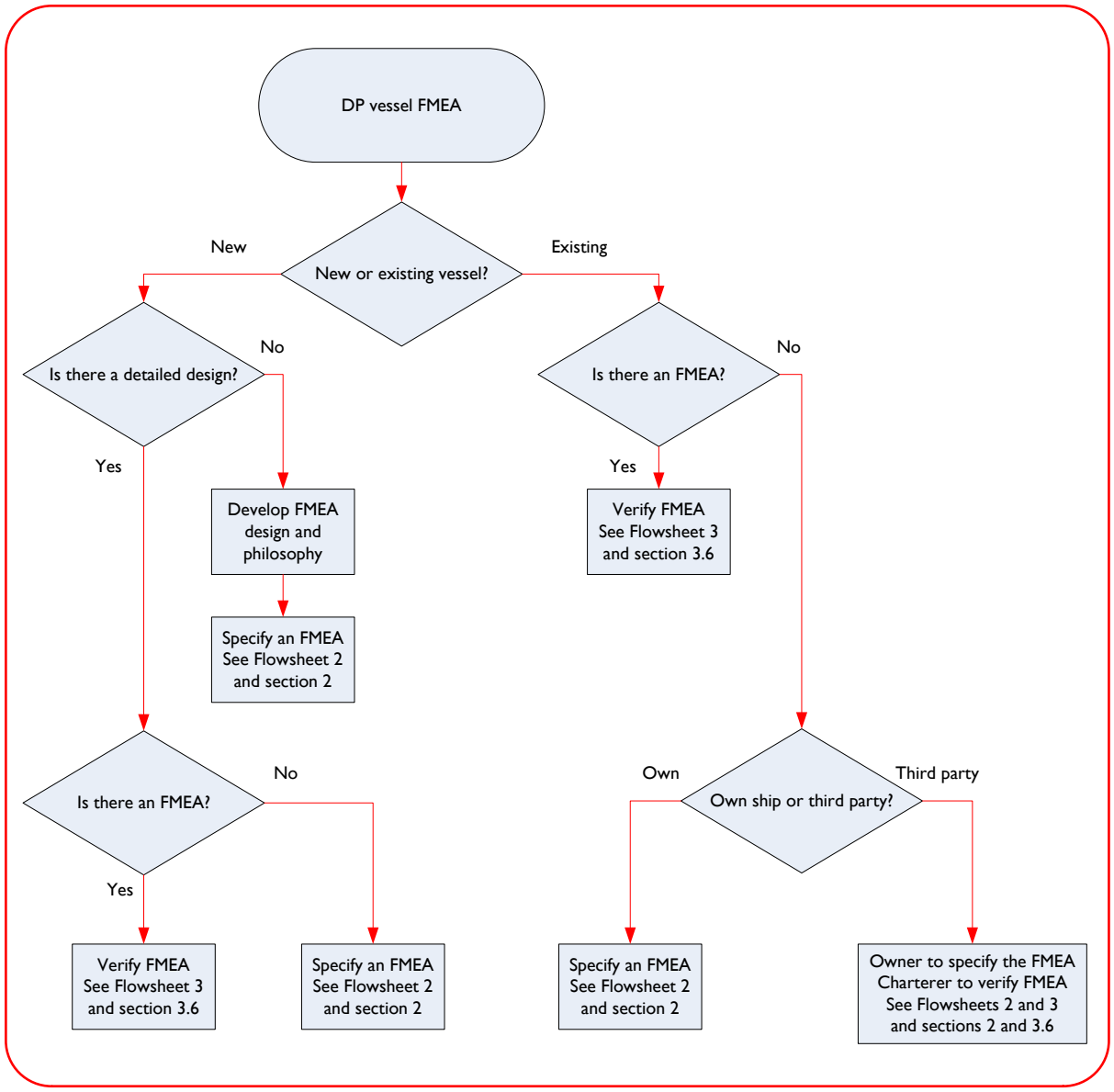
3.5.2 FMEA Management Guidance Flowsheets

Minor system modifications can be analysed and, together with any concerns 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 concerns and follow-up, presented in a new revised final report.

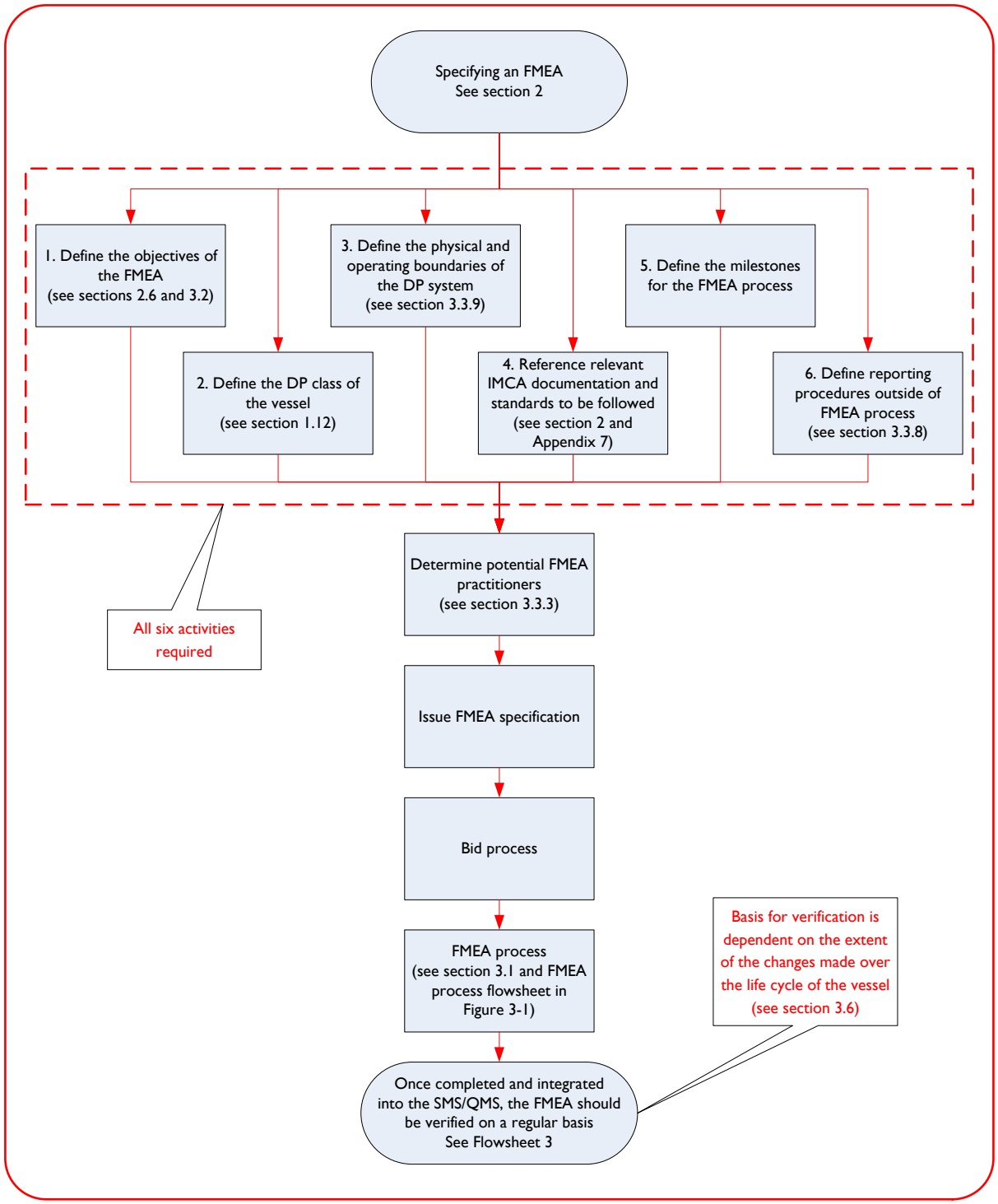
This FMEA management guidance starts at Flowsheet 1. This guides the reader in determining whether or not a new FMEA should be specified (using Flowsheet 2) or an existing FMEA should be verified (using Flowsheet 3).

Flowsheet 3 also assists in determining whether an existing FMEA requires updating (using Flowsheet 4). The flowsheets give reference to where guidance and explanation can be found.

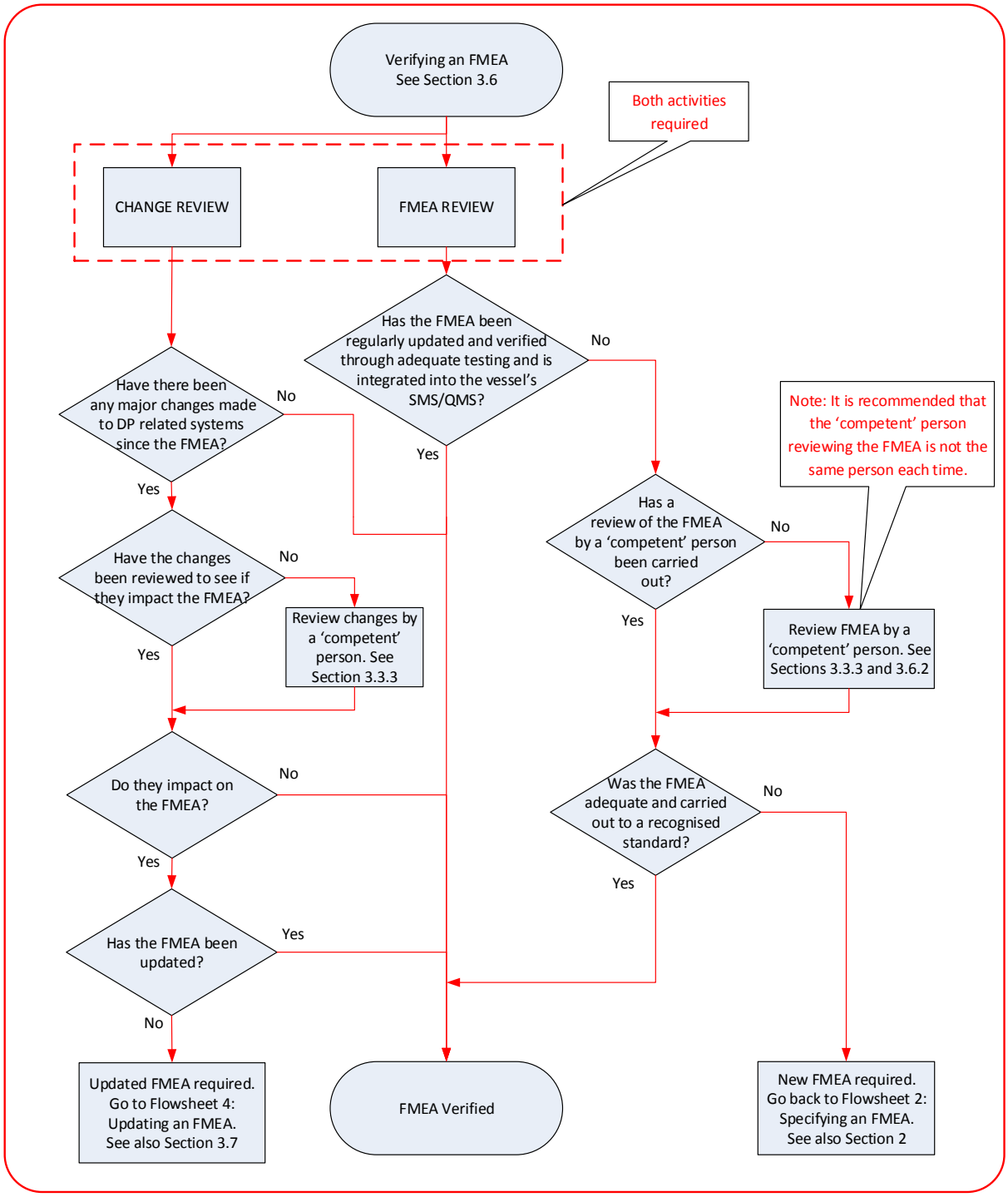
6 ABS *Guidance notes on failure modes and effects analysis for class*, May 2015 [Lifecycle Management]



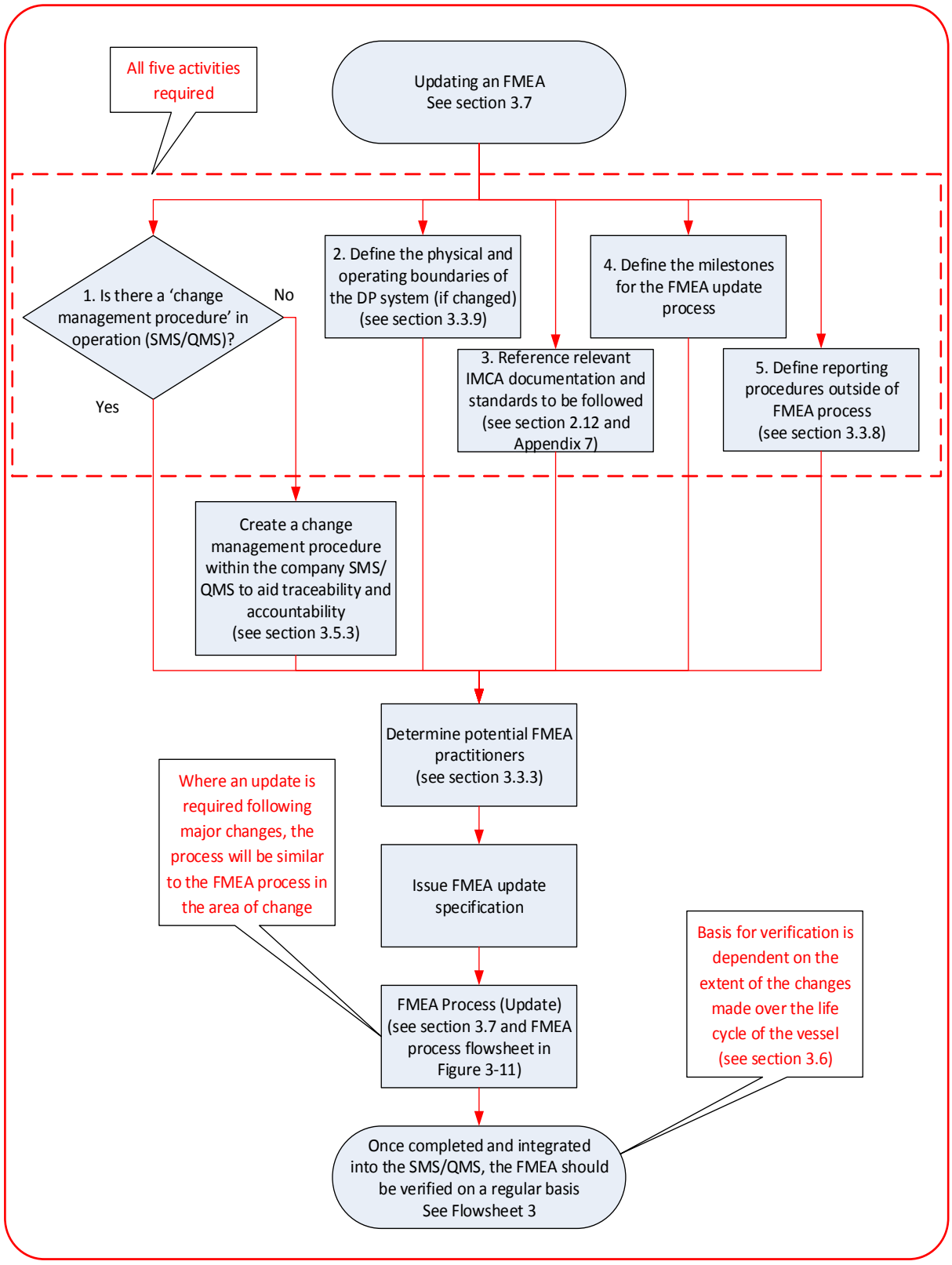
Flowsheet 1 – Initial FMEA management



Flowsheet 2 – Specifying an FMEA



Flowsheet 3 – Verifying an FMEA



Flowsheet 4 – Updating an FMEA

DP Company Limited		
FMEA Change Control Management Procedure		
Date	3 January 2015	
Vessel	DP Explorer	
FMEA CCMP Ref No	CCMP DPEX 001	
System(s) affected	DP control system	
Item(s) affected	DP computer backplane	
Is this change a result of an incident?	Y ☒ N ☐	
If yes, date and description of incident (details as given in incident report from vessel)	22 December 2014 Backplane failure causing erroneous data to both computers. Loss of thrusters and vessel position. No damage to client assets or company property. No injury to personnel or loss of life	
Reason for and description of change (operational or technical)	Technical change: Upgrade of DP computer to new model	
What effect does the change have on the DP system:	No change as DP control system is changed for new model, i.e. like for like	
Does it affect the FMEA?	Y ☒ N ☐	
Has the FMEA been modified?	Y ☒ N ☐	
If yes, how has the FMEA been modified?	Worksheets and FMEA report updated in line with new system. FMEA now version 2400-95-0040 v4	
If no, why not	N/A	
Has a function test been carried out?	Y ☒ N ☐	
If yes, reference FMEA trials test sheet number:	Refer to FMEA test sheet number 45A	
Does this change also affect:	1. Operations manual 2. Emergency operations manual 3. Maintenance manual	Y ☐ N ☒ Y ☐ N ☒ Y ☒ N ☐
If yes, have the following documents been changed?	1. Operations manual 2. Emergency operations manual 3. Maintenance manual	Y ☐ N ☐ Y ☐ N ☐ Y ☒ N ☐
If no, why not?	N/A	
Does this change also apply to other company vessels?	Y ☒ N ☐	
If yes, what action has been taken?	Inspection of backplanes on every company vessel by manufacturer's technician. No similar problem found	
Vessel circulation list: **Master** **First Officer** **Senior DPO** **Senior DPO** **Chief Engineer** **Electrical/Electronics Engineer**	**(Signed):** _	**Date:** _
Vessel Supervisor	_ **(Signed)**	
Vessel Manager	_ **(Signed)**	
Date	_ _	

Table 3-6 – Example change control management form

3.5.1 Change Control Management

In order to keep a DP FMEA up to date and applicable to the vessel to which it refers, it should be ensured that any changes in the vessel's DP related systems are tracked and decisions are captured, recorded and fed back to the vessel for the implementation of corrective action.

Management of the changes is the key issue. This can be achieved by the adoption of a change control management procedure. The change control mechanism should be the responsibility of both the company's shore based and shipboard management to ensure that it is followed and kept up to date. The change control mechanism should form an audit trail to aid traceability and accountability of FMEA system updates (see section 3.6.1).

A suggested format for an FMEA change control management form, which can be tailored to the company's SMS/QMS, can be found in Table 3-6. This is intended to document the reasons for change, the change made and whether or not it affects the FMEA and the relevant vessel DP/operations, emergency and maintenance manuals.

3.6 FMEA Verification

3.6.1 Verifying an FMEA

From the definitions, 'Validation' is concerned with checking that the system will meet the customer's actual needs, i.e. is the right product being produced? 'Verification' is concerned with whether or not the system is well-engineered and error-free, i.e. is the product being produced right?

As an FMEA has been produced, it is assumed that it should have been validated, i.e. it has been confirmed that an FMEA is the correct method to analyse the system for its fault tolerance.

Once the FMEA has been produced it should be verified, i.e. ensured that it has been executed properly.

In verifying an FMEA, it should be ensured that the analysis:

- has covered all DP related systems and sub-systems in sufficient depth;
- has covered all systems not related directly to DP but which may cause the DP system to malfunction;
- has confirmed the WCF redundancy design intent and class notation;
- has been confirmed through adequate annual DP trials;
- has been reviewed and updated if necessary whenever ANY change to DP related equipment has occurred on the vessel;
- is regularly consulted by ship's staff or independent auditors to confirm accuracy (see Flowsheet 3).

Successive verifications should be undertaken on a regular basis, if deemed necessary, and additional tests drawn up to be performed during the annual trials. The annual trials results may then indicate if an update of the FMEA is required.

Verification should be an iterative process, thereby raising the quality of the FMEA and leading to an improvement in the integrity and robustness of the system. The basis for verification would be dependent on the degree of system change. The FMEA should be reviewed by competent FMEA specialists. Any areas not covered or inadequately covered should be subjected to a paper review and additional tests formulated where necessary to be performed during the annual trials.

DPOs and engineers need to identify and investigate unexpected events. A process should be put in place where unexpected events are logged, and then analysed to see if there is a trend which would indicate a future problem. In the case of a DP incident, when the investigation is completed, the IMCA DP incident reporting system should be followed as one of the control mechanisms.

Verification of an FMEA should be based on a comprehensive checklist. This should identify the areas the FMEA has covered and identify those areas that have been overlooked and then categorise each one to the level to which they have been analysed (refer to the list of DP components in the Annex to IMCA M 04/04). This should reflect the DP class of the vessel in question.

An example of a checklist can be found in Table 3-7 in section 3.6.2. This is referred to as a gap analysis. The gap analysis checklist should also cover a list of drawings that would be affected if the DP system were to be modified, e.g. single line system drawings, electrical distribution diagrams, etc.

3.6.2 Gap Analysis

A gap analysis is 'a methodical investigation throughout the whole area of a given technology to identify 'gaps', thus highlighting those areas in existing technology that are inadequate and open to speculation, with a view to improvement'. The 'most useful time to carry out a gap analysis is on the draft revision of the FMEA when it is submitted to the vessel owner for review prior to class for approval'[7].

However, although checklists will highlight if a particular item is covered or not covered, they will not always identify a missing item which should be checked. This is where the experience of a competent FMEA specialist is essential.

The gap analysis lists those component parts that comprise the typical DP system. It then establishes which items apply to the subject vessel and goes on to determine if the FMEA being reviewed has covered them in sufficient depth. Each item is assigned a category. For example, the categories could be:

- Category A: Analysis incomplete. Further assessment required as a failure could have a significant impact on class notation or WCFDI;
- Category B: Analysis incomplete. Further assessment required, though a failure is unlikely to have an impact on class notation or WCFDI;
- Category C: Analysis satisfactory, no further assessment required.

The gap analysis is not intended to be a repeat FMEA. It is intended only to review the FMEA so as to identify those areas not covered or covered inadequately. It should assume that the information given in the FMEA is accurate. Those areas identified for further analysis should be addressed by performing either a new FMEA or an updated FMEA (see section 3.5).

The example table below is intended to give an indication of the areas to be covered in the gap analysis when reviewing the machinery section of an FMEA. The table is based on the Annex to IMCA M 04/04.

7 MTS *Technical and operational guidance* – TECHOP ODP 04 (D) (FMEA Gap Analysis) September 2012

1. Main and Auxiliary Engines			
1.1 Fuel			
	Applies to this vessel?	**Assessed by the FMEA?**	**Category**
1. Storage tanks	Yes	Yes	C
2. Fuel transfer	Yes	Yes	C
3. Control of containment	Yes	Yes	C
4. Day tank level alarms	Yes	Yes	C
5. Quick closing valves	Yes	Yes	C
6. Automated valves	Yes	Yes	C
7. Pumps and filters	Yes	Yes	C
8. Pressure alarms	Yes	Yes	C
9. Supply and return lines	Yes	Yes	C
10. Coolers	Yes	Yes	C
11. Electrical supplies to pumps and automation	Yes	Yes	C
12. Leak protection	Yes	Yes	C
13. Hot surface protection	Yes	No	B
14. Flexible pipes for vibration absorbance	Yes	No	B
15. Fuel system changeovers	Yes	Yes	C
Notes:			
Category Key: A Analysis incomplete. Further assessment required as a failure could have a significant impact on class notation or WCFDI; B Analysis incomplete. Further assessment required, though a failure is unlikely to have an impact on class notation or WCFDI; C Analysis satisfactory, no further assessment required.			

Table 3-7 – Gap analysis table for main and auxiliary engines

3.7 Updating of an FMEA

The FMEA will become out of date if it is not maintained regularly and systematically, due to changes in operating procedures, modifications to DP hardware and software, etc., over the life cycle of the vessel. If this happens, it is likely that another FMEA revision will be incurred later. A systematic FMEA review through the vessel's life cycle should be an ongoing process which should be formally completed at least once every five years.

The FMEA is strongly related to the vessel's DP operations manual. DNV GL Recommended Practice (RP), DNV-RP-E307 – *Dynamic positioning systems operations guidance* dated January 2011 states that *'The provision and development of the manual* (DP operations manual) *is the responsibility of the DP vessel owner or manager and should be incorporated in the company's SMS and, where relevant, developed and managed in accordance with Requirement 7 of the ISM Code'*.

A failure to maintain the FMEA would therefore result in an ISM Code 2010 non-conformance.

Flowsheet 4 describes the process to be followed when it is decided that system modifications require an update, whether a revised FMEA (large system modifications) or an update (small system modifications).

Large hardware/software system modifications would be considered to be those which have a significant impact on the redundancy concept and/or DP configuration. Included in this category would be major modifications to equipment essential to position keeping such as the DP control system, thruster control system, power management and switchboards.

Small hardware/software system modifications would be considered to be those which have minor impact on the redundancy concept and/or DP configuration. These would include modifications such as the addition of a position reference system, which would increase redundancy rather than reduce redundancy.

Modifications which do not have an impact on the FMEA other than minor editing, such as a change to equipment make, model, size following a 'like for like' replacement could be recorded and the FMEA revised at the next update.

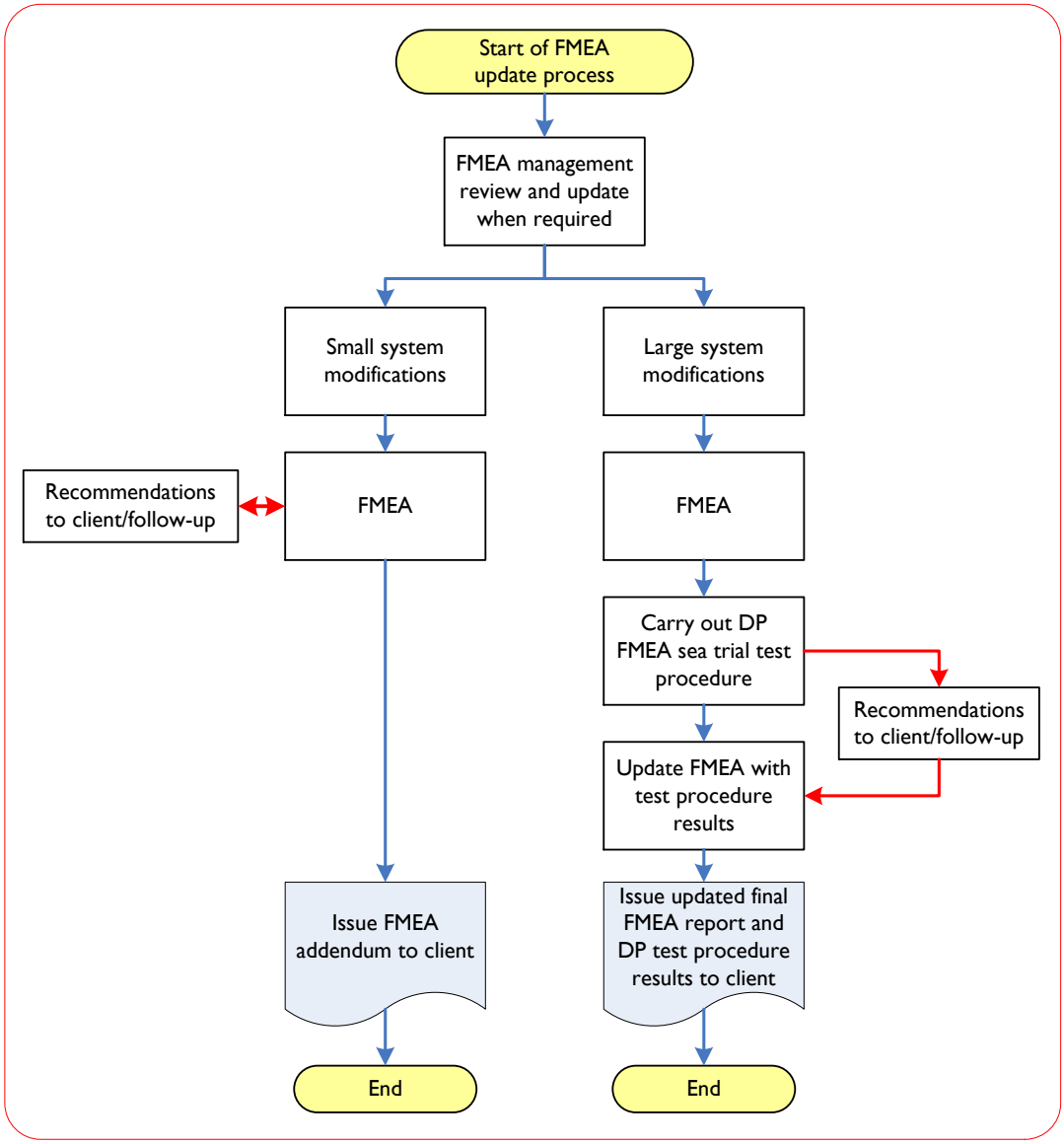


Figure 3-13 – FMEA update process

3.8 DP Incident Follow-up

In the event of the occurrence of a DP incident relating to the vessel's configuration as described in the DP FMEA and other documents, the FMEA provider should be involved in the incident investigation. This will facilitate lessons learnt to be implemented into the DP FMEA and in future trials programmes.

3.9 Additional Studies to Complement the FMEA Process

If required, the FMEA process can be complemented by including appropriate studies usually involving some type of risk analysis. IEC[8] and HSE[9] both give guidance on risk assessment techniques.

Types of risk assessment techniques that could be utilised include:

- hazard identification and operability studies (HAZID/HAZOP);
- structured 'what if?' (SWIFT) analysis;
- qualitative and quantitative risk assessment (QRA);
- failure modes effects and criticality analysis (FMECA);
- fault tree analysis;
- event tree analysis.

These are briefly described below.

Other types of risk assessment techniques are also available but are used to a lesser extent. They include:

- root cause analysis;
- Monte Carlo simulation;
- cause-consequence analysis;
- Ishikawa or fishbone analysis;
- bow tie analysis;
- Markov analysis.

Reliability, availability and maintainability (RAM) analysis, reliability centred maintenance (RCM) and risk based inspection (RBI) are also techniques which can analyse the system beyond the FMEA process.

One technique may not work well in every situation. Some techniques are better suited for some activities or systems than for others. Furthermore, some techniques are specifically designed to analyse complex systems, activities or problems, while others focus on particular types of systems and risks. For example, the FMEA technique is best suited for the analysis of the risks in well-defined systems, such as electronic control or mechanical systems, whilst the HAZOP technique often does not work very well for these types of systems as it is more suited to the analysing of fluid and thermal systems and sequential procedures or operations.

Whilst HAZID/HAZOP and fault tree analysis are often used, from the list above the only ones that are 'strongly applicable' and satisfy all of the criteria for risk analysis, i.e. risk identification, risk analysis (consequence, probability and level of risk) and risk evaluation, are FMEA and SWIFT[10].

3.9.1 HAZID/HAZOP

HAZOP/HAZID is a widely used technique in risk assessment. It is similar to FMEA in that it identifies failure modes of a process, system or procedure and their causes and consequences. However, it works in the opposite direction by firstly considering undesirable outcomes and then working towards the likely causes and failure modes whilst the FMEA starts by identifying the failure modes. The analysis uses a team review in a workshop style format overseen by a facilitator who is an expert in the technique, is fully familiar with the system being analysed and has good communication skills.

It uses a formal, structured and systematic team review of a system or process to:

- identify possible deviations from normal operations and their causes and consequences;
- show what safeguards are in place;
- recommend appropriate measure to prevent accidents.

8 IEC/FDIS 31010:2009(E) – *Risk management, risk assessment techniques*
9 HSE guidance document *Marine risk assessment*, HSE Offshore Technology Report 2001/063
10 MTS *Technical and operational guidance* – TECHOP ODP 04 (D) (FMEA Gap Analysis) September 2012

During the HAZID/HAZOP session, information is recorded systematically on a dedicated worksheet. Where appropriate, recommendations are generated to address critical issues and/or to assure that areas which need to be investigated further are recorded. The following information is documented in the worksheets: section, intention, deviation, causes, accidents, consequences, safeguards, and concerns.

The analysis is usually split into sessions, each one covering section of the DP system, i.e. machinery, thrusters, electrical system, safety, etc., and the designers and specialists of each would be present at the relevant session. The sessions would generally be facilitated by a third party. In addition to the independent HAZOP/HAZID leader, these participants would include the project team, the technical operations team, the shipyard and the vendors. Class may also be present.

The HAZOP/HAZID requires a high degree of procedure specification and documentation. The list of documents relating to each system or equipment required for the HAZOP/HAZID sessions will typically include; a complete set of GA drawings, shipyard contract technical specification, functional design specification, all applicable system and equipment documents, applicable regulations and standards (class, flag state, IEC, etc.), vessel owner company policies, maintenance and downtime information and technical queries (TQs).

This method is increasingly being used to analyse the DP system, particularly by shipyards, as they have the means to gather all the relevant specialists together for each session. As the sessions are usually segregated into separate systems or parts within the overall process, the analysis does not view the process as a whole or consider how each separate system or part can affect another following failure. The sessions are sometimes called FMEA or FMECA sessions, erroneously because the output is usually only a set of worksheets, there is no report structure and no block diagrams or descriptions of systems and sub-systems.

3.9.2 SWIFT Analysis

The SWIFT analysis is a structured form of the 'what-if analysis' technique. The SWIFT technique is used to identify hazards based on brainstorming and checklists. The discussion systematically addresses the system elements and/or operations in order to determine what things can go wrong and to assess the likelihood and severity of those situations occurring. During the brainstorming, the questions 'What if?', 'How could this happen?' or 'Is it possible?' are posed. The acceptability of the risks is then determined and a recommended course of action is planned for those risks judged to be unacceptable.

SWIFT analysis is usually performed by a team of experts familiar with the system and system operations, under the supervision of a SWIFT technique specialist. Personnel experienced in the design, operation, and servicing of the equipment under analysis or similar equipment are essential. Additionally, piping and instrument diagrams, design documents, operational procedures, and maintenance procedures are essential information for the review team.

'What if?' questions can be formulated around human errors, system faults and equipment failures. These errors and failures can be considered during normal operations, during maintenance activities, as well as during debugging situations. The questions could address any of the following situations:

- failure to follow procedures or procedures followed incorrectly;
- procedures incorrect or latest procedures not used;
- operator inattentive or operator not trained;
- procedures modified due to upset;
- process conditions upsets;
- equipment failure;
- instrumentation miscalibrated;
- debugging errors;
- utility failures such as power, fuel, cooling water, etc.;
- external influences such as weather, vandalism, fire;

- combination of events such as multiple equipment failures.

The procedures and results of the analysis are documented in standard SWIFT worksheets. A simple example of a bilge and ballast system SWIFT analysis is shown in Table 3-8.

No.	What If	Cause	Consequences	Safe Guards	Concerns
1	Ballast tank leaks	Hole in side shell	Filling/emptying of ballast tank. Affect stability	Tanks internal coating in good order	
2	Ballast tank over pressurised	Mal-operation by operator. Blocked vent. Faulty tank gauging.	Possible rupture of tank. Affect stability	Ballast tank gauging Dual vents	
3	Ballast tank under pressurised	Blocked vent.	Possible rupture of tank. Affect stability	Ballast tank gauging Dual vents	
4					

Table 3-8 – Example of bilge and ballast system SWIFT analysis

Whilst the SWIFT type analysis is rarely used offshore, it is flexible and applicable to any type of installation, operation or process, at any stage of the life cycle.

3.9.3 Qualitative and Quantitative Risk Assessment (QRA)

QRA is intended to give an idea of the frequency of an event occurring (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 risks the event 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 extensions 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 cause extensions to a project.

3.9.4 Criticality Analysis (FMECA)

With respect to criticality and probability, it is the responsibility of the FMEA team to determine whether or not the FMEA technique is sufficiently stringent for the complete analysis. More critical systems and sub-systems within the overall DP system, such as interfaces, software and power management, may require the use of other analysis tools.

If, when analysing a system, a single point failure is identified in a sub-system and the design cannot be modified to eliminate it, the FMEA can be extended to include a criticality analysis to indicate how often it will fail (FMECA). 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 sub-system can be either overhauled or replaced. During normal operations, procedures would have to be drawn up to ensure the effects of failure are mitigated.

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, TR, in hours-to-repair, which will indicate how long it will take to recover the intact system after repair, can further extend the analysis.

This requires that the reliability data will need to be accessed, this 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). If the failure rates are not available, they are estimated, which may dilute the credibility of the final figure.

Very few classification requirements specifically request an FMECA. As detailed in ABS guidance[11], ISQM and system verification do explicitly require an FMECA. However, classification will accept any voluntary submission of an FMECA instead of an FMEA.

3.9.5 Consequence and Frequency

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

The analysis would use a standard type risk matrix with the levels of consequence and frequency defined. The FMEA worksheet would have a column with heading 'consequence' and the addition of a further column with heading 'frequency' and each failure mode entry would be assigned a defined consequence and a frequency value to enable the level of risk to be determined.

Risk

Each failure mode should be assigned a value for frequency of the failure occurring and a value for the consequence, or severity, of each failure, such that:

Risk = Frequency x Consequence

For example, each failure mode is assigned a value of 1-5 for frequency of the failure occurring and the consequence of the failure, as given in Table 3-9.

Frequency	**Frequent**	**5**	Medium 5	Moderate 10	High 15	High 20	High 25
	Probable	**4**	Low 4	Medium 8	High 12	High 16	High 20
	Occasional	**3**	Low 3	Medium 6	Medium 9	High 12	High 15
	Remote	**2**	Low 2	Low 4	Medium 6	Medium 8	Medium 10
	Improbable	**1**	Low 1	Low 2	Low 3	Low 4	Medium 5
Risk = Frequency x Consequence			**1**	**2**	**3**	**4**	**5**
			Minor	**Marginal**	**Serious**	**Critical**	**C'trophic**
			Consequence				

Table 3-9 – Risk matrix

11 ABS *Guidance notes on failure modes and effects analysis for class*, May 2015

Definitions

Definitions of the frequency and consequence values used should be included. Table 3-11 gives examples of how they can be defined.

5	Frequent – likely to occur frequently	$1x10^{-1}$
4	Probable – may occur several times in the life of an item	$1x10^{-2}$
3	Occasional – may occur sometime in the life of an item	$1x10^{-3}$
2	Remote – unlikely to occur but possible	$1x10^{-4}$
1	Improbable – unlikely to occur at all	$1x10^{-5}$

Table 3-10 – Frequency definition – DP related

5	Catastrophic – A major system failure which will cause total loss of DP capability regardless of any limitations put on the vessel and which will lead to an immediate termination of the operation.
4	Critical – A failure of a redundant item which, in itself, will not cause loss of position but loss of position will result should a further failure of its redundant twin occur (e.g. loss of one of two engine rooms). Requires immediate controlled termination of the operation.
3	Serious – A failure of a redundant item which, in itself, will not cause loss of position and where a further failure of its redundant twin will not cause loss of position if operational limitations are adhered to (e.g. loss of a duty generator fuel pump supplying one engine room). Does not require immediate termination of the operation.
2	Marginal – A failure which will have an effect on operational capability but does not result in termination of the operation if operational limitations are adhered to (e.g. loss of one generator in a multi generator installation).
1	Minor – A failure which has negligible effect on system or sub-system level generally at component level and results in minor unscheduled repair (e.g. duty generator LO pump).

Table 3-11 – Consequence of failure definition – DP related

3.9.6 Fault Tree Analysis and Event Tree Analysis

A fault tree analysis (FTA) is a logical, 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 logical functions. 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 function, 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 function. 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 IMCA M 160 – *Reliability of position reference systems for deepwater drilling*.

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).

Event trees are used in the IMCA database of station keeping incidents (IMCA M 228 – *DP incidents reported for 2012* – and earlier). This is a collection of real DP incidents reported to IMCA, which are represented as event trees.

3.9.7 RAM (Reliability, Availability and Maintainability)

RAM is a methodical process to improve the performance of a system or equipment for a given configuration in terms of reliability, availability and maintainability.

Reliability is the measure of the probability that a system or equipment will perform a required function under stated conditions for a defined period of time. It quantifies what fails and how often.

Availability is the probability that a system or equipment is performing its required function at a given point in time or over a stated period of time when operated and maintained in a prescribed manner. It is often defined as 'the proportion of time for which the item is working or fit for work'.

Maintainability is the probability that a failed system or equipment will be restored or repaired to a specified condition within a specified period of time when maintenance is performed in accordance with prescribed procedures.

RAM analysis addresses the following issues:

- system or equipment performance and availability;
- the potential critical system components and process bottlenecks;
- the equipment which has the highest risk of operational failures;
- the operational improvement of the system for acquiring spare parts;
- the 'what-if' scenarios and their predictions;
- the potential single points failure;
- the impact on system reliability and availability of varying duty cycles, service-life limitations, wear out items, or environments and conditions.

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 centred 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.

3.9.8 Control of Software

Where software functions for control systems are being considered in the FMEA, for example, DP. PMS, thruster control systems, it has been generally sufficient for the failure of the software function to be considered rather than a specific analysis of the software code itself. Traditionally, only extensive testing of the system, either during factory tests using the actual hardware, or during shipboard commissioning and sea trials, has been used to reveal any serious failure modes within the software that would have a detrimental effect on the position keeping system of the vessel.

System software is traditionally assumed to be of adequate design and therefore not analysed in the FMEA. However, it may be seen as a common mode failure as the same software is used across redundant systems. Hardware-in-the-loop (HIL) testing is seen as a method to reduce the potential for software to cause an undesirable system failure.

Software changes after the vessel is in service should also be tested.

IMCA M 163 – *Guidelines for the quality assurance and quality control of software* – gives guidance on quality assurance and quality control of software used by vessel owner/operators and manufacturers in computerised control systems including DP computers. The principles set out in this document can equally be applied to the QA/QC of all software applications.

Whilst manufacturers are expected to have comprehensive, efficient, highly developed and accredited QA/QC procedures, the owners/operators should also have a compatible quality procedure as the way they use the system can have a significant impact on its 'fitness for purpose'. Without these controls, the problems and difficulties that have arisen in the past will continue, for example:

- issue of software which is incompatible with the hardware;
- presence of two different master copies;
- introduction of malfunctions by upgrade/update of software;
- uncontrolled changes to software;
- inadequately trained operators;
- incorrect and/or incomplete manuals.

With regard to testing, IMCA M 163 does not describe how to analyse or test software. It states that: *'Verification and validation are the responsibility of the manufacturer and should be carried out throughout the development process, see ISO 9000-3 clauses 4.4.7 and 4.4.8 (Ref. 2) using a verification and validation test plan based on the requirements definition. The results and any perceived consequences should be monitored during the design review stages.*

'Onboard verification and validation should be carried out by the manufacturer to a plan agreed with the vessel owner/operator and should be under the control of the vessel owner/operator. This verification and validation test programme should be realistic and viable, and be based on the vessel's future anticipated work scope.'

The FMEA should address software as a common mode failure.

Software testing is dependent on thorough practical trials such that all envisaged operational modes are tested. Once the program has been finalised and tested after commissioning by practical trials, master copies should be made and two kept on board, one for use and one in a secure location as backup.

IMCA M 163 also gives guidance on establishing a planned and systematic approach to mitigating the risks when upgrading and installing new system software. Any changes should be fully documented. Proper procedures should be drawn up for reloading software and making changes.

DNV GL's offshore standard DNV-OS-D203 December 2012 details the requirements for assigning an integrated software dependent system (ISDS) class notation to an offshore unit in order to prove compliance with the standard. The standard does not describe how to analyse or test software but contains the requirements and guidance on the process of design, construction, commissioning and operation of ISDS which are integrated systems where the overall behaviour depends on the behaviour of the systems' software components. DNV-OS-D203 requires that the verification and validation strategies be defined and documented.

3.9.9 Hardware-in-the-Loop (HIL) Testing

HIL testing is a proven test methodology from automotive, avionics, space, and other industries, targeting the software part of the control system. HIL testing is accomplished by isolating the control system and its operator stations from the systems being controlled and replacing all actual inputs/outputs (I/O) with simulated I/O from an HIL simulator in real time. The control system cannot sense any difference between the real world and the virtual world in the HIL simulator. This facilitates systematic testing of control system design philosophy, functionality, performance, and failure handling capability, both in normal and off-design operating conditions. HIL testing only superficially tests hardware and redundancy, since the main test target is software.

The main common objective of both FMEA and DP HIL testing is to verify the vessel's ability to keep position after a single failure. Another important objective of HIL testing is to verify the control system software functionality as specified by the supplier and possibly the end user of the DP system.

As FMEA and HIL testing deals with different aspects, i.e. hardware and software respectively, co-ordination between FMEA and HIL testing has the potential to increase the robustness of position keeping.

The FMEA study may be updated based on HIL test results and HIL test programs may be updated based on issues identified in the FMEA study.

FMEA and HIL testing are therefore complementary verification methods so, ideally, both could be used to verify the DP system's ability to maintain position after a single failure. HIL testing is further discussed in section 4.26.

DP FMEA Proving Trials

DP FMEA Proving Trials 4-1

4.1 Introduction 4-3
4.2 Reasons for FMEA Testing 4-3
4.3 DP FMEA Proving Trials 4-3
4.4 Annual DP Trials and Five-Yearly Trials 4-5
4.5 Customer Acceptance Test (CAT) and Shipyard Trials Tests 4-6
4.6 Classification Society Requirements for Testing 4-7
4.7 Prerequisites for FMEA Testing 4-7
4.8 FMEA Trials Team 4-8
4.9 DP FMEA Proving Trials Test Programme 4-8
4.10 Use of Gap Analysis Tool 4-10
4.11 FMEA Test Programme for Alongside and At Sea 4-11
4.12 Cross Component Groups (X Group) Testing 4-11
4.13 FMEA Trials Management 4-12
4.14 Pre- and Post-Trials Meetings 4-13
4.15 Deviations from Trial Prerequisites 4-14
4.16 Conduct of the FMEA Trials 4-14
4.17 Testing On and Off DP 4-15
4.18 FMEA Test Results 4-15
4.19 Concerns 4-16
4.20 Guidance on Handling Disputes 4-16
4.21 Pre-FMEA Trials Tests 4-17
4.22 Post FMEA Trials Retesting 4-17
4.23 Electrical Testing and Safety 4-18
4.24 Electrical Testing of Closed Bus Tie Operational Mode 4-18
4.25 Advanced Test Methods 4-20
4.26 Hardware-in-the-Loop (HIL) Testing 4-20
4.27 MODU Tests 4-23

4.1 Introduction

The DP system of a vessel is a dynamic system, made up of sub-systems that dynamically interact with each other. Commissioning and testing normally carried out by shipyards, equipment vendors or other third party suppliers tends to test their equipment in isolation or at the sub-system level without fully testing the complete, integrated DP system. Also, vendor commissioning and customer acceptance tests (CATs) are primarily focused on demonstrating that the systems function correctly in the fully operational (i.e. no fault) condition. DP FMEA proving trials tests are intended to confirm system redundancy and fault tolerance to failures of individual pieces of equipment in the various sub-systems that make up the complete DP system that could or will cause the system to fail completely.

DP FMEA proving trials are an important part of the FMEA process. Initially the FMEA is a paperwork theoretical analysis; however, to be assured that the theoretical analysis is correct, the DP FMEA proving trials have to be conducted on the vessel to verify the findings of the theoretical FMEA.

4.2 Reasons for FMEA Testing

FMEA testing is a part of the overall vessel test process. Essentially, the DP FMEA proving trials tests are designed to test the robustness of the overall system's response to failure by ensuring full redundancy has been installed to meet the vessel's DP class notation requirements. They are necessary to prove the key principles of a fault tolerant DP system including performance, protection and detection; proving the performance of each redundant equipment group, testing any protective functions intended to prevent fault propagation between redundant groups and testing all necessary alarm and indications used to detect and reveal hidden failures.

FMEA testing has multiple benefits:

- The findings of the 'desktop' FMEA are confirmed to be true and accurate (or otherwise);
- The failure modes and effects of 'grey areas' (i.e. areas which could not be adequately analysed by desktop study of system drawings and vendor documentation) are established, e.g. the behaviour of any interlocks that may inhibit operation of essential systems;
- Areas where the FMEA has proved to be undecided are confirmed and recorded by testing;
- Testing can identify incorrect system wiring;
- Normally the FMEA concentrates on analysing hardware failures only, however, the tests can also demonstrate and verify the response of control software that contributes to the correction of a hardware failure;
- Operational personnel can witness first-hand the effects of failures enhancing their knowledge of the systems;
- Information is gathered to allow updating of the FMEA database to reflect the 'as built' configuration of the vessel;
- The FMEA test plan should be used as the basis of an annual DP trials programme that requires function tests and failure modes on an annual basis to confirm correct system operation as part of the vessel's ongoing QA;
- Similarly, the FMEA test plan should be used as the basis of the five-yearly trials programme.

4.3 DP FMEA Proving Trials

The DP FMEA proving trials are a series of controlled failure mode tests which are intended to prove the findings of the desktop FMEA and, where there are any doubts about any failure modes from the desktop analysis, eliminate these doubts by carrying out onboard testing in a safe and practical manner.

FMEA testing should be a structured and well co-ordinated exercise to demonstrate:

- the redundancy concept;
- the effectiveness of system protection functions;
- stability of the system under the full range of load/operational conditions;

- monitoring functions;
- degraded and failure conditions.

For this to be achievable, the complete system should have undergone full commissioning test process and be fully operational, particularly alarm and event logging. A suitable number of qualified personnel need to be present for witnessing the tests. All participants should review the test procedures so that the method and expected failure effects are well understood beforehand. It is not acceptable for changes to be made to the DP or DP related systems during or immediately after the DP FMEA proving trials tests unless a relevant follow up test has been reformatted, agreed, carried out, witnessed and recorded in the FMEA document.

The DP FMEA proving trials are normally carried out on 'full auto DP' but can be carried out with the vessel in an operational configuration other than 'full auto DP' (e.g. alongside or at sea) provided there is an acceptable confidence that this will have no effect on the test result.

This part of the FMEA process requires:

- That a DP FMEA proving trials test document is prepared to confirm, by practical testing, the system response to failure;
- Provision of hard copies of drawings with failure test points highlighted should be included with the actual test sheets. This will save time spent accessing drawings during the trials;
- Participation by members of the FMEA team in the DP FMEA proving trials to independently witness and record the results of each test;
- Assessment of any findings or concerns during the trials and discussion of these during or following the trials with the shipyard, vessel owner, class and vendors as appropriate;
- Retesting if alterations are found to be necessary to any part of the DP installation following the original test;
- Ensuring that the DP FMEA proving trials results are properly recorded and fed back into the FMEA document to reflect the trial findings where applicable.

The scope of the FMEA testing should be determined by the need to prove the conclusions of the FMEA. The FMEA team should generate the DP FMEA proving trials test list and corresponding test procedures, with tests being developed as the FMEA progresses. If the analysis determines that a failure mode and its effect are inconclusive, a test should be formulated.

In addition to the FMEA trials team, the tests should be independently witnessed by officers of the flag state administration, or delegated to Recognised Organisations such as classification societies.

For a new build vessel, the tests should be co-ordinated with the owner and shipyard test teams well before the trials commence. Those tests that can be carried out dockside should be identified and agreed with the remainder being integrated into the sea trials testing.

If the vessel is an existing operational vessel, FMEA testing should be carried out in much the same way during down times between contracts.

The DP FMEA proving trials test procedure describes the purpose of the test, the vessel and equipment configuration or set up 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 should be provided for documenting the actual test results.

The test procedure should detail the DP equipment set up that will be used during the tests. The set up should be described in a section in the DP FMEA proving trials report and it should be stated that, if there is any deviation from the normal set up, it will be shown on the relevant test sheet. The relevant test sheet should therefore detail the differences in set up that will be required.

The tests are part of the FMEA process and should not be treated in isolation. The results of the tests will be used in the FMEA final analysis and it is good practice to include the test sheets in the final report.

It is important that practical testing is thorough. It is better that any unacceptable failure mode is revealed during trials rather than later when the vessel is working. There is no intention of causing damage to equipment during testing. Any risk of damage should be determined by the experience of

the FMEA team, in conjunction with the responsible person or trials co-ordinator from the owner or shipyard overseeing the trials. If any risk of damage is determined, the test should be modified such that any damage is prevented and there is an acceptable confidence that the original objective of the test will be achieved.

4.4 Annual DP Trials and Five-Yearly Trials

IMO DP Guidelines (MSC Circular 645 June 1994) require the following tests of the DP systems:

- An initial complete test of all systems and components and the ability to keep position after single failures (i.e. DP FMEA proving trials);
- An annual test of all important systems and components to document the ability to keep position after single failures (i.e. annual trials);
- A periodical complete test at intervals not exceeding five years;
- Tests after a defect is discovered or an accident occurs, to demonstrate full compliance with the applicable provisions of the guidelines.

DP FMEA proving trials: As described in this document, the DP FMEA proving trials are a component part of the FMEA. For a new build vessel, commissioning tests should be carried out prior to the DP FMEA proving trials tests. The system should be fully commissioned prior to the DP FMEA proving trials tests as all parts of the system need to be functioning as designed, otherwise the system's response to a failure during FMEA testing cannot be determined with certainty.

Annual DP trials: Annual DP trials should be performed once a year within three months before or after each anniversary date of the initial survey (IMO MSC Circular 645). Although there are many similarities there are some key differences between the annual trials and the DP FMEA proving trials.

FMEA proving trials are focused on verifying the failure effects outlined in the FMEA and demonstrating the system's response to failure and the effectiveness of the designed redundancy concept. Annual DP trials are more inclined towards uncovering areas of performance deterioration or deficient maintenance and demonstrating that the redundancy concept is still intact.

The annual DP trials should be developed utilising the DP FMEA proving trials where necessary, incorporating tests that demonstrate and confirm redundancy. The annual DP trials combine these failure tests with function tests which are intended to confirm that the DP system is continuing to function as intended. Annual DP trials may be conducted as a single, separate event, or as part of a rolling test programme over the year, possibly as part of the vessel's planned maintenance programme. This is elaborated on in IMCA M 190 – *Guidance for developing and conducting annual DP trials programmes for DP vessels* – and other industry documents[1]. There should be a clear link between the failure modes in the FMEA and the tests in the annual trials to ensure that the trials programme and FMEA are comprehensive and co-ordinated[2]. There should be evidence that the FMEA has been modified following the trials if this is the case.

Annual DP trials also provide an opportunity for training of the vessel's crew, some of whom may be new to the vessel, particularly with respect to the effects of failures within the system and the actions to be taken in the event of those failures occurring.

Annual DP trials tests should be created specifically for the vessel under test but there are many tests which are common to all DP vessels. Section 5.11 – *Practical guidance on carrying out tests and recording the results* – in IMCA M 190 gives details of the type of tests to be carried out and provides hints and tips on carrying these out, whether they are part of the annual trials or planned maintenance.

As part of the annual trials, operational and maintenance records together with test schedules are examined to ensure that the DP control system and associated machinery has operated satisfactorily during the previous year. A general visual examination of the equipment is also carried out.

1 Refer also to IMCA M 191 – *Guidelines for annual DP trials for DP mobile offshore drilling units*, IMCA M 225 – *Example redundancy concept and annual DP trials for a DP class 3 construction vessel* and MTS TECHOP FMEA Testing

2 Review of methods for demonstrating redundancy in dynamic positioning systems for the offshore industry. Prepared by DNV Consulting for the Health and Safety Executive 2004; Research Report 195

Due to the difficulty in interrupting drilling operations, DP MODUs are not usually able to carry out annual DP trials at a specific time once a year. Guidance relating to the carrying out of annual DP trials for DP MODUs is given in IMCA M 191 – *Guidelines for annual DP trials for DP mobile offshore drilling units*.

Five-yearly trials: IMO requires that a complete test of the DP system at intervals should be carried out periodically, but not exceeding a period of five years. Some classification societies recommend that the DP FMEA proving trials should be repeated every five years[3]. Other societies require that the five year tests validate the redundancy concept that is established during the initial proving trials[4], but allow for a shortened test schedule when compared with the initial proving trials. It should be noted that often tests completed during the initial proving trials were designed to answer a particular question the FMEA practitioner may have raised. Therefore, re-testing the complete proving trials every five years may not be necessary, unless it is required by class. It is recommended that the five yearly trials programme is carefully planned, the intent clearly specified and then verified through testing.

Five years is generally accepted as a reasonable period within which to carry out an extended test which is focused on, firstly, demonstrating and confirming the level of redundancy that was established in the FMEA and, secondly, demonstrating the continued functionality of the DP system.

Five-yearly trials are, therefore, an extension to the annual trials and can include tests from the initial DP FMEA proving trials which are designed to prove the original redundancy design intent of the DP system.

Retesting: Following a defect being discovered or an accident occurring, in order to demonstrate full compliance with the applicable provisions of the guidelines retesting will be required. Modifications to the system design may have been made which may have an effect on the whole system. Consequently, when retesting, the system should be set up as it was when tested originally. If this required the vessel to be at sea and on auto DP, then these should be the conditions under which the system is tested.

4.5 Customer Acceptance Test (CAT) and Shipyard Trials Tests

Customer acceptance test (CAT): During sea trials it is likely that there will be a need for various systems vendors, such as the PMS/VMS system and DP control system manufacturers, to carry out a CAT for the client. The CAT is designed to verify that the equipment delivered by the vendor is in accordance with the requirements stated in the (approved) functional description and according to classification society requirements. The CAT procedure typically contains a number of tests which either aim to demonstrate particular functionality of the system or confirm the system's response to a failure. The latter tests, in particular, should be included in the DP FMEA proving trials programme.

Unless specifically requested otherwise by the trials co-ordinator, the FMEA trials team may elect to witness and record the results from those CATs which duplicate or overlap with their own DP proving trials programme provided that they, or a class representative, have witnessed the test executed appropriately. This will reduce duplicate testing and save valuable testing time at sea.

Should the CAT not cover all aspects of the associated DP proving trials tests, the FMEA trials team may accept those parts of the test based upon the CAT and indicate to the trials co-ordinator that the remaining DP proving trials tests where the outcomes have not been ascertained from the CAT should be carried out.

Shipyard trials tests: For a new build vessel, the shipyard will produce the schedule for the sea trials of the vessel which could include the DP FMEA proving trials. The shipyard will normally request the DP proving trials document several weeks prior to the sea trials taking place so that they can be introduced into the overall sea trials programme in a logical manner. In order to schedule the sea trials, the shipyard will request that each DP proving trials test be allocated an estimated time to completion. It is to be expected that the test programme will be fragmented as there are other test activities being carried out on the vessel that are not DP related.

If DP FMEA proving trials tests are carried out concurrently with other non DP related tests, conflicts may occur that may invalidate the test results. All parties involved in the DP FMEA proving trials should therefore have a good understanding of the sea trials schedule such that any conflicts are avoided.

3 DNV GL Recommended Practice (RP), DNV-RP-E307 – *Dynamic positioning systems operational guidance*, January 20114
4 ABS Rules for Survey After Construction, 2016 - 7/9/6-3.5

4.6 Classification Society Requirements for Testing

Following production of the DP FMEA proving trials programme, the test programme should be submitted to the relevant classification society for approval to ensure that it contains all the tests that the classification society requires. It should be submitted in sufficient time for class to review and make comment and request any further tests to suit their purpose. In addition to the required failure tests, when reviewing the test documentation, class now expects to see tests incorporated in the test programme to demonstrate DP system functions. The results of test procedures are to be retained aboard the vessel.

According to ABS, the techniques used in the test method should not simulate monitored system conditions by maladjustment, artificial signals, improper wiring, tampering, or revision of the system unless the test could damage equipment or endanger personnel[5]. Should any of these techniques be used, it needs to be on a case by case basis. It should be explained why it is being used and how it complies with the purpose of the test.

Following the review of the DP system design and survey during manufacture and the FMEA with subsequent testing by class engineers, a classification society will assign its requested DP notation provided the DP system is in compliance with the appropriate rules. In particular, classification societies will require FMEA testing to verify system redundancy for DP class 2 or 3 vessels.

The classification societies are not, however, obligated or desirous to carry out any FMEA testing beyond what is required by class rules. The DP FMEA proving trials programme may include tests that are not required by class. Class may not be present when these tests are carried out.

If the owner's design philosophy/specification has redundancy features in excess of the class rules to be applied to the vessel, then the required classification society failure mode testing may not adequately test the complete system. For example, it may be that a vessel is specified to have a DP class 2 notation, but is designed to have redundancy over and above DP class 2 requirements (i.e. an enhanced DP class 2). It is up to the owner to ensure that additional adequate FMEA testing demonstrates and validates the enhanced features of the system.

4.7 Prerequisites for FMEA Testing

Prior to FMEA testing, it is imperative the system has been installed, commissioned and function tested thoroughly, otherwise it cannot be determined with certainty that the systems response to failure will be as per design. Any modifications to the original design that may arise from the DP FMEA proving trial results will require a further testing. All documentation with regards to alterations from the original design should form a part of the FMEA and be properly recorded.

Where testing is concerned for a new build vessel, there are five distinct sequential phases in the project cycle[6]. These are:

- Factory acceptance test (FAT), normally carried out by the equipment vendor and usually witnessed by representatives of class and owner;
- Mechanical completion in which the equipment is installed by the vessel builder and confirmed that it is installed as per design;
- Pre-commissioning, which is carried out with the equipment set up in the defined operational configurations and should include loop testing;
- Commissioning of equipment which is validated following tuning and load testing. Accurate tuning is a precursor to effective commissioning;
- Testing which confirms that the equipment has been commissioned correctly, such that performance meets specifications and tuning is consistently effective across a representative range of conditions, and proving of the FMEA.

5 ABS *Guidance notes on failure modes and effects analysis for class*, May 2015
6 DNV GL Recommended Practice (RP), DNV-RP-E306 – *Dynamic positioning vessel design philosophy guidelines*, September 2012

4.8 FMEA Trials Team

If a vessel is to be thoroughly tested, the FMEA team members present at the trials to witness the tests should have as wide a scope of knowledge as possible. As these specialists will have been part of the FMEA team that prepared the test procedure, they will have a sound knowledge of the concept of redundancy and a good overall knowledge of the whole DP system. Section 3 refers to the makeup of the FMEA team.

Whilst it is important that members of the FMEA team who have carried out the desktop analysis are present to witness the tests making it easier to insert the actual test results into the final document, in the case that they are not available, the test procedures need to be sufficiently comprehensive such that an FMEA practitioner of equivalent experience can follow the objective and method of each test.

4.9 DP FMEA Proving Trials Test Programme

The DP FMEA proving trials test programme should be accurate, valid and of sufficient depth to demonstrate the performance, protection and fault detection methods of the vessel's DP system. Vessels operating in compliance with IMO DP equipment class 2 or 3 need to have redundancy central to the design concept. Each redundancy group needs to be capable of independently maintaining vessel position within the design's post worst case failure capability envelope and this should be evident from the trials.

In addition to the test programme itself, a good DP FMEA proving trials report should cover the following sections:

1. Classification and guidelines
   - Outlining the classification society to which the vessel is classed, the applicable rule year and notations
   - The flag administrations' applicable guidelines;
2. Trials vessel configuration
   - In which configuration all DP sub-systems should be for DP operations, and hence the setup before each test (unless otherwise stated on the individual test sheet)
   - The FMEA specification may have requested analysis of different configurations, e.g. for critical and non-critical operations (CAMO and TAM). These should both be described;
3. Redundancy concept overview
   - A description of the different redundancy groups and the worst case failure of each group;
4. WCFDI
   - A statement of the worst case failure design intent to which the FMEA analysis and trials is based;
5. Description of DP sub-systems
   - Each sub-system should be given an overview description and could contain an accompanying figure, to provide the reader a high level understanding;
6. Test list
   - Containing a list of all tests to be completed
   - Stating whether each individual test is to be carried out only on DP or may be done alongside
   - Estimation of the time to carry out each test (if requested by shipyard or owner);
7. Concerns
   - This section should state the rules and guidelines by which the DP system analysis is based
   - Concern levels should be categorised by severity with respect to the defined class rules and redundancy concept
   - There should not be a time constraint
   - There should not be any recommendations made, simply statements of fact.

Ultimately the DP proving trials are used to demonstrate and give confidence that the vessel will not lose position keeping ability due to a single point of failure in any active (or including passive for DP 3)

component resulting in drift off or drive off from location. The fault tolerance of the DP system should be fully examined and equipment inspected to determine a fail-safe condition.

The DP FMEA proving trials test programme should demonstrate the **performance** of the power system and thruster ability to sustain position both with the system fully functional and post worst case failure.

The test programme should cover the DP system **protective** installations and fail safe failure effects. For an open bus tie configuration, failure of the protective system to perform as expected is unlikely to have an effect exceeding that of the WCFDI. However, it could lead to expensive or life threatening consequences, for example an engine's overspeed protective trip not functioning. For closed bus tie configuration, the protective systems in place are fundamental to the redundancy concept and should be fully tested to give confidence that the WCFDI cannot be exceeded. It is to be expected that additional technical measures will be required for closed bus tie DP designs compared to open bus tie designs and these will require rigorous testing. Refer to section 4.24 for further guidance.

The test programme should demonstrate and confirm the appropriate **detection** or warnings to personnel on board the vessel that a fault has occurred on some piece of machinery/equipment. This is typically achieved using audible and visual alarms. The DPO will be alerted at the DP desk and/or (depending on the category of equipment fault) the engineers in the ECR. Testing should cover alarms for all DP equipment on which the redundancy concept is dependent – this includes both running and standby machinery from which the lack of alarm may create a hidden fault.

Hidden failures can exist in DP systems and the trials should aim to uncover these where practicable. Where the redundancy concept is based on standby machinery, failure to start is a hidden failure which could defeat the redundancy concept or inability to alarm on fault whilst in standby mode. Running machinery may also possess hidden faults which may only manifest itself in times of high demand, for example a thruster's inability to deliver rated thrust and hence impacting on the position keeping abilities of the vessel. The trials programme should test both running and standby machines. Generators should be proven to be capable of delivering to the rated maximum of their power and thrusters capable of delivering to the rated maximum of their thrust.

The test programme should be valid and appropriate for the classification society's rules and guidelines as per the vessel's notation (DP 2 or 3) and switchboard configuration (open or closed bus tiebreaker) for DP operations.

Fields for the objective of the test, the method for carrying out the test safely, the expected and actual tests results should be included in each test sheet. The expected results are determined from the FMEA desktop analysis using analytical techniques and experience.

Key components of an individual test are:

- a clear, concise description of the purpose of the test;
- a link between test and FMEA reference;
- a statement of system configuration required for test validity;
- if testing off DP mode may be completed without compromise;
- a step-by-step breakdown of the test procedure, including terminal/cable tags where applicable;
- a section stating the *expected* outcomes for each step in the test procedure;
- a section stating the *actual* outcomes for each step in the test procedure;
- a section for comments and analysis of unexpected actual results, test procedure, concerns, supplementary information etc.;
- a dated signature of the witnessing surveyor.

An example of a test sheet can be found in Table 4-1.

System	
Test no.	**Test name**
Purpose:	The purpose of the test and reference to FMEA analysis
Configuration:	Alongside/at sea/on DP: Any test specific configurations of equipment in order to setup for the test procedure effectively to demonstrate realistic outcomes
Method: The method of executing the test, broken down into single action instructions. The stages involved in carrying out the test should be as comprehensive and free from ambiguity as possible including terminal/cable numbers where applicable 1. 2. 3. 4.	
Expected results: Individual outcomes expected for each of the stages stated in the 'Method' section, based upon desktop FMEA analysis and acceptance criteria. If the results following proving trials differ, but are acceptable, then this section should be updated for subsequent annual trials 1. 2. 3. 4.	
Actual results: Document the results of each stage of the test procedure, stating any observations differing from the 'Expected results'. When appropriate, results may be documented in tabular format for ease of understanding. Figures, photos and evidence of this like, should be appended to the report and simply referenced here accordingly 1. 2. 3. 4.	
Comments: The comments section offers the surveyor an area to make notes and/or observations on the test, for example: 1. Further descriptive text to expand on any 'Actual results' where the result was not as expected; 2. Reasoning for why a test, wholly or partly, was not carried out or where the actual test method differed from that on the 'Method' section; 3. Highlight and describe any concern(s) which has arisen from the test; 4. Helpful information regarding the setup/configuration of the test for subsequent annual trials; 5. Reference to any picture taken relevant to the test that shows evidence of a test result, e.g. alarm screens.	
Witnessed by:	**Date:**

Table 4-1 – Example FMEA test sheet

4.10 Use of Gap Analysis Tool

Any opportunity to further verify the DP FMEA proving trials document and improve the quality and increasing confidence in the proving trials depth and accuracy should be embraced. This includes the use of a gap analysis. Refer to section 3.5.1.

The gap analysis is used to review the FMEA so as to identify those areas not covered or covered inadequately, in particular those relevant to the vessel's DP notation. It is not intended to be a repeat FMEA. Any areas identified for further analysis should be addressed at a later date. In carrying out the gap analysis it has to be assumed that the information given in the FMEA is accurate. The gap analysis can be consulted to ensure that the test has covered all areas.

Reference may be made to the MTS FMEA testing TECHOP document[7] to aid the FMEA practitioner in developing a DP FMEA proving trials test programme to a standardised level, based on industry recommended practice, for both IMO DP equipment class 2 or 3 and open/closed bus tie configuration.

IMCA M 04/04 Annex Appendices D and E can be used as a checklist to determine whether the scope of the DP proving trials are adequate and provides guidance on the types of failure modes in each system.

4.11 FMEA Test Programme for Alongside and At Sea

The majority of the DP FMEA proving trials test programme is carried out with the vessel in a fully operational DP condition. There are, however, a number of FMEA tests that can be carried out either in 'alongside' or 'at sea' modes. There may be some FMEA tests that can be carried out with the vessel not on DP, i.e. on DP related equipment which operates regardless of whether or not the vessel is on DP or not, provided there is an acceptable confidence that this will have no effect on the test result. However, FMEA tests demonstrating redundancy and DP function/capability need to be carried out with a fully intact DP system and whilst operating on DP.

Guidance found in IMCA M 190 highlights tests that can be meaningfully carried out with the vessel alongside or in transit to the sea trials location. Whilst this guidance is for annual trials, it is still relevant for FMEA proving trials. These tests may include:

- battery endurance;
- generator performance tests;
- thruster performance tests;
- pump changeovers, e.g. confirmation of cooling water pump duty/standby changeover on loss of pressure or flow;
- low level alarms on fuel oil service tanks;
- selected safety tests;
- communications and DP alert.

Each test in the DP FMEA proving trials test programme should be clearly indicated to the respective authorities for approval if it is to be carried out alongside or at sea whilst operating on automatic DP.

4.12 Cross Component Groups (X Group) Testing

On occasion there may be some equipment which is common to both redundant groups, and which represent the means for propagating failure effects from one redundant group to the corresponding redundant group. Such connections between redundant groups are termed cross component groups or X groups[8] and include equipment such as fuel line crossovers, connected cooling water, governors (over fuel), AVRs (over excitation), a single router to which redundant networks connect or common software modules. It is important that these are not overlooked and the trials programme fully proves the redundancy concept as outlined in the FMEA.

The diagrams in Figure 4-1 illustrate the ways in which redundant groups (A and B) containing DP equipment can be dependent or independent.

If this is part of the design, fail safe tests should be included in the trials programme to prove that a fault within one redundant group may not propagate to another via this common equipment (e.g. network storm test).

7 MTS *Technical and operational guidance* – TECHOP ODP 01 (D) (FMEA Testing) September 2012
8 DNV GL Recommended Practice (RP), DNV-RP-D102 – *Failure mode and effect analysis (FMEA) of redundant systems*, January 2012

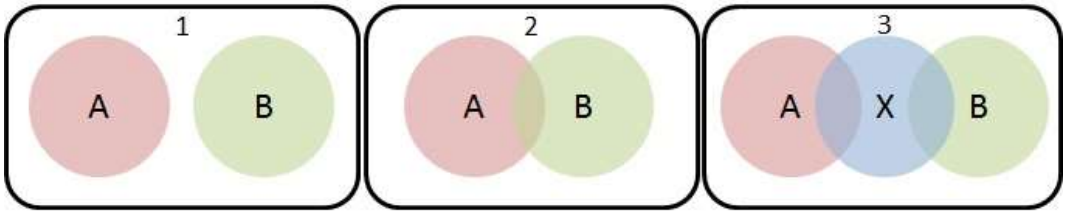


Diagram 1 – Both groups are totally independent of one another

Diagram 2 – There is equipment common to both redundant groups

Diagram 3 – There is some equipment connecting the otherwise independent redundant groups

Figure 4-1 – Illustration of redundant groups

The example in diagram 3 reflects a design concept of a two switchboard configuration (A and B) with the bus tiebreaker forming the X group, bridging between the redundant groups. Testing for this particular configuration is required to prove, as far as practicably possible, that the protection system is adequate to prevent transient faults between the two groups. Such tests should include, but not be limited to:

- short circuit current protection;
- voltage dip ride through;
- reactive power imbalance;
- active power imbalance;
- power management system closed and open bus functionality;
- under voltage (UV), over voltage (OV);
- under frequency (UF), over frequency (OF);
- earth fault.

4.13 FMEA Trials Management

4.13.1 New Build Vessel

For a new build vessel, the shipyard normally controls the schedule for the sea trials of the vessel which will include the DP FMEA proving trials.

Present for the trials should be representatives from the shipyard, the flag administration or Recognised Organisation (RO), the owner, classification society, vendors and the FMEA team. Ideally, the vessel's crew who are to operate the vessel after delivery should also be present during the trials so that they have time to familiarise themselves with the vessel and its operation. They may not operate the vessel during trials in the case of a new building as they may be relegated to the role of observers until delivery.

A trials co-ordinator should be appointed by the shipyard who is normally a senior member of the commissioning team who has a good understanding of the DP system topology and the class requirements of the DP notation to be assigned to the vessel. There will be other test activities carried out on the vessel during sea trials that are not DP related, so the trials co-ordinator should also have a good understanding of the sea trials schedule such that there should be no conflicts with the other tests that may invalidate the FMEA test results. The trials co-ordinator will be responsible for ensuring that the tests are carried out safely. The vendors should be available for advice on safety issues relevant to their equipment.

Usually prior to the DP FMEA proving trials, the vendors will have made final commissioning adjustments of systems such as thrusters, i.e. thruster tuning. FMEA testing of these systems should not proceed until these are finalised. Once these adjustments are finalised, the trials co-ordinator should give permission for FMEA testing to proceed. The vendors will be present in case there are any test results that are not as expected.

Members of the crew such as the DPOs, engineers, electrical/electronic officers should be familiar with the test methods so that they can be involved with carrying out the tests. Having the vessel's operations/maintenance crew in attendance at the trials is of great benefit to them as it is probably their only opportunity, other than during annual trials, to witness the effects of the failures and learn of the procedures for corrective action that may have to be put into place to mitigate the failures. Generally, the only time many personnel will see a major failure with the DP system is when the failure is simulated during FMEA testing. This makes it an essential part of the training process for the ship's crew, helping them to increase their knowledge of their vessel.

4.13.2 Existing Vessel

For an existing vessel, the owner will dictate the schedule for the FMEA tests. Present for the trials should be representatives from the vessel's owner, the FMEA team and possibly class and vendors. Also present will be the vessel's crew who, as it is an existing vessel, should have considerable knowledge of the vessel but will not necessarily have had past experience of witnessing the failure modes that will be carried out during the trials. The owner should appoint a trials co-ordinator. This is often the vessel's technical superintendent.

Prior to the tests, crew members including, in particular, the electrical/electronic officers should be familiar with the test methods so that they can assist with carrying out the tests. This helps to increase their knowledge of their vessel. If they know exactly where the failure is to be made then this can dramatically reduce the time taken to complete the tests.

4.14 Pre- and Post-Trials Meetings

4.14.1 Pre-Trials Meeting

Prior to the trials commencing, and usually on board the vessel, it is imperative that a pre-trials meeting take place between all parties that have an interest in the outcome of the trials. At the meeting, the trials programme should be discussed and agreed by all parties before the trials commence. Those parties should include the vessel superintendent, class representatives, master/OIM, chief engineer, electronics/electrical engineer and the FMEA trials team. Representatives from vendors such as the DP and VMS/PMS manufacturers, and representatives from the charterers may also be present. It is important that all interested parties have reviewed the trials programme and made comments before the pre-trials meeting takes place. Suggested items for the pre-trial meeting would be:

1. Identify the trials co-ordinator and responsibilities
2. Trials safety in general, including the personnel carrying out the testing
3. Focus on keeping the integrity of the power plant intact
4. Agree how each individual test will be carried out. (Questions with regard to the method in which the test is carried out can be clarified or adjusted by agreement at this stage)
5. How to deal with short cuts during the trials should they be suggested
6. How to deal with genuine further tests should they be identified
7. How to deal with ad hoc suggestions and variations to the test programme during the actual FMEA trials
8. Consolidation of the test programme with the various vendors.

4.14.2 Post-Trials Meeting

The post-trials meeting or close out meeting should be held following the trials to review the results of the tests and to agree the actions to be taken regarding any concerns raised. As for the pre-trials meeting, all parties that have an interest in the outcome of the trials should be present, together with any party that can be of assistance in resolving any issues which have arisen during the trials.

Suggestions for further tests can be considered, recorded and planned at the close out meeting that should take into consideration the following:

- the benefit of the test;
- the impact on the FMEA;
- any tests that for certain reasons could not be completed during the main set of tests;
- any unacceptable failure modes found and require a retest;
- any equipment that has been replaced following the main set of tests and require retest.

4.15 Deviations from Trial Prerequisites

It is important that, prior to FMEA testing, the system has been fully designed, installed, commissioned and function tested to confirm that it works as per design. There may be occasions when items of equipment are not available at the time of the trials due to various reasons. It could be that an item has been taken out of service for maintenance or an item has failed and the owner is awaiting the necessary spares.

In this case, it should be determined what the effect the unavailability of the item of equipment would have on the test procedure, whether or not testing can continue and, if it does, whether or not any retesting is required after the reason for any deviation from the test method is removed.

For example, in the case of generator unavailability, if one of a multiple of engines is unavailable for partial blackout testing then it is possible that the test will be unaffected. In the case of a DP 2 or DP 3 vessel with four thrusters and one is out of service due to a fault, thruster redundancy tests cannot proceed until the faulty thruster is made available for DP.

Any known deviations from the trial prerequisites need to be discussed at the time of the pre-trials meeting.

4.16 Conduct of the FMEA Trials

During the FMEA tests in DP mode, all relevant shipboard equipment needs to be fully operational. In particular, all propulsion units and their controls, both manual and automatic, all power generation equipment, all computer systems and all position reference systems should be fully functional, including their alarms, stand-by units, battery backups, shutdowns, trips, etc.

During the pre-trials meeting, the trials test procedure and their scheduling should have been discussed and agreed by all parties. This will prevent any potentially unhelpful disagreements arising and testing time being wasted once the trials have commenced.

The tests should then be able to continue as the schedule allows unless, for example, a serious safety concern is raised.

All tests should be co-ordinated by a designated responsible person and with full regard to the safe navigation of the vessel. Whilst each test procedure should have been reviewed by all interested parties, if, prior to carrying out any test, a safety issue has been overlooked which, as a result of the test, may cause injury or damage to equipment, the test should be halted and reconfigured to achieve the aims of the test but prevent such injury or damage. The designated responsible person needs to have the final decision.

Testing that has not been carried out in port or at sea (see section 3.4.6) should be carried out on full DP, in realistic environmental conditions or with some varying load on the system induced by movements of the vessel.

During the tests, assistance will be required in recording alarms and failures locally. Locally means not only at the relevant bridge/CCR operating console but also at the monitoring and control stations in the ECR, machinery space, etc.

During the failure tests, the system should not be reinstated until all parties are satisfied that they understand the full effects of the failure and that all the information or indicators to show what has occurred have been noted.

When reinstating systems after failure simulations, all parties need to be satisfied that the system has been reset and is stabilised before the trials continue.

If there are any doubts about a test, it should be repeated. If test results are unexpected or if results of the same failure tests differ across identical equipment, e.g. when different failure modes are found between two individual thrusters, the tests should be repeated to determine where the discrepancies lie within that system. Any changes to the test programme or retesting in case of an unsatisfactory result should be carefully considered before the test is carried out again. It should be noted that seemingly small or spurious faults in DP control systems may be the first manifestation of a more serious problem.

Tests should continue only when all those involved have been informed and (where necessary) suitable communications have been set up, e.g. DP console to switchboard rooms.

4.17 Testing On and Off DP

During the proving trials there are likely to be periods of DP downtime during which DP testing is not possible whilst work from other vendors, transiting, etc. is taking place. During these periods it may be acceptable to complete tests within the programme which are not reliant on the vessel operating on DP.

Tests, either whole or partial, which the FMEA practitioner considers acceptable and which retain their validity if completed off DP mode, should be clearly outlined in the test procedure.

The validity of the test being completed off DP, during transit or alongside, should be stated in the trials programme and agreed upon by class and the client prior to commencement of the trials. The default position should always be to choose testing in full DP mode when there is any doubt.

Once the trials document has been finalised and prior to the trials taking place, it should be reviewed by those parties with an interest in the execution and outcome of the trials, particularly the client and the classification society. It should be agreed by all parties witnessing the tests that the test procedures in the document are able to achieve the required objectives.

4.18 FMEA Test Results

As each test is conducted, it will be necessary for the results to be recorded. Depending on where the failure is to be made, it is probable that the effect of failure will manifest in more locations than one. For example, the effect of failure of a UPS distribution will be noticed in areas such as the UPS room where the failure may be taking place, in the ECR for alarms, on the bridge by the loss of DP control equipment and by alarms on the DP consoles. It is therefore necessary to have personnel recording alarms and the loss of equipment in more than one location. It is also necessary to have complete co-ordination between the recorders in these locations.

Assistance in recording the effects of failure can be made by consulting the alarm printers in the ECR and on the bridge. It should be confirmed that these printers are synchronised from the point of view of time so there is no dispute over the chronological issuing of alarms and events.

When carrying out the test practically, it may be found that the actual result of a test does not coincide with the expected results. This can occur for a number of reasons:

- invalid test procedure;
- test execution deviating from procedure;
- incorrect system configuration;
- fault active in the system before the commencement of the test.

It may be found that the test method used has not complied with the test method in the test sheet, for example, the wrong wire has been removed in a wire break scenario. If the test method has diligently been followed, then it needs to be determined whether or not the actual results are more severe than those expected. If the failure mode of the actual test is in excess of worst case failure, it needs to be addressed as soon as possible, a modification made and a retest carried out. If it cannot be addressed until later then it should be recorded as a Category A concern (see section 4.19).

What is important is that the actual result is recorded such that it can be further analysed. For any of the above factors, the reason should be rectified and the test repeated. If, upon repetition of the test, the result is no longer unexpected but that which the test sheet predicted, then the previous result may be discarded, and the most recent result accepted as the test outcome. The exception to this is if an incorrectly performed test has a result exceeding that of the WCFDI. In this case, the result should be retained and a Category A concern given regardless.

Occasionally there may be a circumstance whereby the unexpected result cannot be explained and/or remains unresolved. In this case, the result should be documented and, depending on its impact on the redundancy concept, a concern raised and categorised accordingly.

4.19 Concerns

All parties should be made aware of concerns as they arise throughout the DP FMEA proving trials. The concerns should be brought to light during frequent meetings to discuss the progress of the trials, usually at the end of each day. This helps facilitate the speedy resolution of concerns.

Any concerns arising from the trials should be addressed. These concerns should be free of ambiguity, subjectivity and recommendation, stating only facts as observed during the test procedure. They may be of varying significance so they should be categorised. Section 3 refers to the categorisation of the concerns. These could be as follows:

- Category A – Concerns which address potentially serious failure modes which are in excess of WCFDI, raise safety issues or do not comply with class requirements;
- Category B – Concerns which address failure modes which are not in excess of WCFDI or raise safety issues but are considered important enough to make the system more robust, such as additional redundancy in key areas;
- Category C – Concerns which, if addressed, are designed to improve system operation. These are suggestions and not essential to the process.

A concern in Category A indicates that the vessel does not comply with the redundancy requirements, raises safety issues or does not comply with class requirements and so requires immediate action. Category B concerns identify deficiencies within non-critical redundancies. Finally, Category C concerns are for future attention or consideration, and can be somewhat subjective.

Should concerns be raised following the trials, as with other IMCA inspection documentation concerns, there should be a clear indication of what is required to be remedied and then it is up to the shipyard or vessel owner, if a new build vessel or an existing vessel respectively, to decide how this is going to be closed out. The shipyard or vessel owner may do this in discussion with other parties such as class and the FMEA team.

Based on the compilation of concerns post trials, the FMEA should include a governing, summary statement on the vessel's compliance with the rules and guidelines for the notation of the classification society. Such a statement may read: 'The vessel shall be considered fit to perform DP operations under the assigned notation, when operating in the tested power system configuration, **if and only if**, there are no Category A concerns outstanding'.

Once the trials are complete, the results of each test should be reviewed to see if they have any effect on what has been written in the FMEA report. If so, the FMEA report should be revised to reflect the trials results.

4.20 Guidance on Handling Disputes

It is possible that disputes will arise as to how any concerns from the DP FMEA or DP FMEA proving trials are categorised. Category A concerns are infrequent and if any are raised there is usually no dispute as to the categorisation.

It is the categorisation of Category B and Category C concerns that cause the most disputes. Any issues that compromise safety are usually not in dispute but those raised by the FMEA team which are considered important enough to make the system more robust give rise to most dispute. These are usually resolved by the shipyard or vessel owner, depending on the design requirements.

Disputes may arise as to how any concerns are to be addressed. Clearly, any failure mode that compromises class rules needs to be addressed immediately. Modifications proposed to mitigate the failure mode should be agreed by class. Any modifications should be retested and witnessed by class and other interested parties to ensure that the DP notation is not affected.

Other failure modes and effects that do not exceed class requirements but may be in excess of those expected will cause discussion and it is up to the relevant parties to come to agreement as to the best course of action, assuming action is required.

Based on the compilation of concerns outstanding post trials, the surveyor should give a governing, summary statement on the vessel's compliance with the rules and guidelines for the notation of the classification society.

4.21 Pre-FMEA Trials Tests

Any advanced FMEA testing that can be carried out to give advanced warning of any potentially detrimental failure effects would have the considerable benefit of allowing more time for remedial work or redesign.

It is very rare for FMEA to be involved during an FAT unless the vendor is to produce an FMEA on their equipment. However, whilst an FAT means that vendor equipment will be tested only at the sub-system level and in isolation from the complete integrated DP system, equipment vendors have been known to programme FMEA tests into the FAT. Where possible, the relevant member of the FMEA team should be present to witness these tests.

4.22 Post FMEA Trials Retesting

Should an FMEA test reveal a failure mode which could possibly contravene guidelines, modifications will be needed to eliminate or reduce the effect of the failure mode. As some modifications may have an effect on the whole system, when retesting the completed modification, the system should be set up as it was when original testing revealed the failure mode in question. If this required the vessel to be at sea and on auto DP, then these should be the conditions under which the modification is tested.

If the necessary modifications to the system can be made during the trials, the FMEA team should be present to witness the retesting and record the new results. However, this may not always be possible. In the case that a redesign is found necessary and new hardware or parts are required which are not currently available, it is likely that the modifications will not be completed until sometime after the trials. In this case, a concern should be identified at the end of the trials period.

If the modifications affect the FMEA and the test procedure, revised drawings would need to be produced and forwarded to the FMEA team for reanalysis and the test procedure updated. It is essential that the builder or owner ensures these modifications are captured in revised drawings to provide proof as to how the system is modified. This can sometimes get overlooked in the haste to get the vessel working.

In order to close out the concern, retesting will be required once the modifications are completed. In the event that the trials team is not present to observe any remedial work and witness subsequent retesting, it should be agreed how to close out the concern.

If the concern is a Category A concern which affects class notation, class should be notified and attend if required, otherwise either a competent independent witness or member of the ship's staff can witness the retesting. In any case, the test results should be forwarded to the FMEA team for inclusion in the FMEA DP proving trials document.

If the modification requires a software revision change then it is highly likely that CAT testing will be required with a complete FMEA retest of the relevant computer system to follow. Depending on the significance of the subject computer system within the DP system, it may be that the FMEA team will require to be present for the retest.

Should any equipment be unavailable during FMEA testing due to operational reasons such as, in the case of an accommodation unit, the gangway not being deployed due to no fixed structure at the trials location, then these tests can be witnessed by a member of the ship's staff once the equipment is available and the results forwarded to the FMEA team for assessment and inclusion in the trials document.

4.23 Electrical Testing and Safety

A vessel's personnel, electrical plant and machines along with the distribution systems needs to be protected against damage that may occur through abnormal conditions.

Abnormal conditions may be grouped into two types:

a) Operation outside the designed ratings due to overloading or incorrect functioning of the system;

b) Fault conditions due usually to breakdown of some part of the system.

Condition (a) is usually 'chronic' that is it may persist for some time and is often acceptable for a limited period. It may give rise to temperatures outside the design limit of the machines and equipment, but unless these are excessive or very prolonged it seldom causes sudden or catastrophic failure. It can usually be corrected before it leads to breakdown of machinery or equipment.

Condition (b) would be described as 'acute' and will arise from electrical or mechanical failure which once established produces a condition beyond control. Usually it gives rise to very severe excess currents which could cause catastrophic failure of other electrical and mechanical equipment in the system unless the fault is rapidly isolated. It may be caused by a breakdown of insulation due to a material failure, overheating or physical damage to an item of plant or cable.

Automatic protection of an electrical system against conditions (a) and (b) is possible because it is easy to measure various parameters to detect abnormalities and to set in motion the protective action the instant an abnormality arises.

Protection of an electrical system is provided for one or more reasons:

- to maintain electrical supplies to as much of the system as possible after a fault has been isolated;
- to protect the generators and other plant against damage due to abnormal conditions and faults;
- to protect the consumer equipment against damage due to abnormal conditions such as overload of the complete system;
- to isolate the faulty equipment and to reduce the risk of fire locally;
- to limit damage to the installation including the cable system resulting from a fault.

Transient disturbances are liable to occur on most electrical systems for many reasons connected directly with operations and most electrical plant is capable of operating safely with moderate overloads for short periods. However, during an acute fault, such as a short circuit on any part of the main electrical installation, the excessive current that will be induced into that fault by the running generators will cause a severe voltage dip (zero in the worst case) on the whole power distribution system. This is especially so when the system is configured operating as one system, i.e. bus tiebreakers closed and not in an open bus tie split configuration where only one part of the installation would be affected by the same fault.

Further information on electrical testing can also be found in MTS TECHOP documentation.[9]

4.24 Electrical Testing of Closed Bus Tie Operational Mode

If an owner or operator wishes to operate a vessel with equipment class 2 or 3 during critical DP operations with the bus ties closed, class, flag state and the charterer will want verification that the DP system has the same safety, reliability and performance as it would have had if operating with the bus ties open. Therefore, it should be demonstrated that the power network survives the effects of a fault that could propagate across switchboards, resulting in a full blackout.

9 MTS *Technical and operational guidance* – TECHOP ODP 01 (D) (FMEA Testing) September 2012

Advanced power system protection systems based on substantial monitoring systems and algorithms have been developed to detect the early onset of electrical faults which have the potential to propagate across switchboards. It should be well understood and clearly identified which faults are primarily protected against by either the advanced protection system or by the conventional protection systems. It is a challenging but highly valuable exercise, to verify design against final installation and commissioning. Any additional protective functions should be considered in the protection co-ordination study.

It has long been considered that:

- open bus ties = less chance of total blackout but more chance for partial blackout;
- closed bus ties = less chance of partial blackout but more chance for total blackout.

IMO MSC/Circ 645, part 3.2.4, for equipment class 3 states: *'… Bus tie breakers should be open during equipment class 3 operations unless equivalent integrity of power operations can be accepted according to 3.1.3.'*

'3.1.3 … Non-redundant connections between otherwise redundant and separated systems may be accepted provided that it is documented to give clear safety advantages and that their reliability can be demonstrated and documented to the satisfaction of the Administration.'

A short circuit across the main bus bars has been identified as one of the most severe faults that can occur on a vessel designed for closed bus tie operation. However, there are multiple other faults in the power system which can quickly propagate, resulting in a full blackout. Each potential electrical fault and its effect should be studied, and protective system(s) clearly identified for each of these faults.

4.24.1 Voltage Dip Ride Through Capability

Currently there are two different approaches to this issue:

1. Simulating the effect of a short circuit to prove the directional protection and the ability of the system to ride through the brief voltage dip.
2. Develop a mathematical model of the power system then apply a conductor across the bus bars and energise the conductors to develop a controlled short circuit. The test is designed to limit the purposefully induced fault current to 10% of the switchboard rated current. This test can be used as part of the validation process for a model which can then verify that the switchboard would have behaved correctly with a short circuit which induced fault current. The validated model can then be used to confirm correct operation of the protection devices and control systems in more diverse configurations and failure scenarios.

All test equipment should be removed and any temporary connections points restored and made safe on completion of testing. Keeping a log of the test connections will reduce the risk of inadvertently leaving something connected.

All protection settings should be confirmed as having been returned to the correct values as per the approved protection co-ordination study. If the testing suggests that changes should be made to protection co-ordination values, then any such changes should be subject to a suitable and sufficient management of change process.

Both methods have advantages and disadvantages.

Simulating the effects of a short circuit avoids the risks of a full short circuit and the attendant risk to personnel and equipment. However, it requires temporary modification of the directional protection settings for the duration of the test which then have to be restored to the original settings on completion of testing.

Applying a conductor across the bus bars and then energising the circuit is contrary to normal industry practice and HSE policy. A deviation from the predicted fault current may have significant consequences, both for the personnel and the vessel. This type of testing requires a comprehensive risk analysis and accurate modelling of the system. The veracity of the result is dependent on both the accuracy of the model and an assumption that the short circuit condition is the one most likely to cause loss of power, both of which may be questionable.

IMCA recommends that IEC standards regarding breaker loading should be followed.

DNV GL asserts that it is necessary to carry out live short circuit and live earth fault testing[10] on DP 3 equipment class vessels that have their equipment designed in order to have confidence in the behaviour of the HV system in the event of a fault. Other classification societies are applying a risk based philosophy for the applicant to demonstrate the suitability of their proposed testing method(s).

There may be a situation in the future where test methods yet to be determined supersede those currently in existence or new designs render these tests unnecessary.

4.25 Advanced Test Methods

Regardless of which is the best method of testing the DP system, either primitive or advanced, the outcome of the test should be the same, i.e. it should meet the objectives of the test.

Any advanced test method shown to assist or replace FMEA testing needs to be:

- approved by class and national authorities;
- shown not to cause damage to personnel, environment and asset;
- shown to have advantages over any current means of testing.

4.26 Hardware-in-the-Loop (HIL) Testing

HIL testing and modelling techniques for short circuit testing are techniques for consideration.

Whilst the FMEA is a powerful tool for assessing the impact of failures on the operation of a DP system, unless all failure modes and their effects are identified and confirmed by practical testing during DP FMEA trials and all possible functions of the DP are rigorously exercised, it can be difficult to reveal all software errors.

HIL testing has the objective of verifying the control system software functionality as specified by the supplier and possibly the end user of the DP system. The HIL test is not just a 'test', it is a verification process. It provides interaction with the clients, getting feedback both from the customers and from the class society on the process documentation.

Some of the advantages of HIL testing are:

- facilitates early testing of the software;
- facilitates thorough and extensive testing, since most of the testing can be done outside the critical timeline for vessel construction;
- facilitates testing of failures and off-design situations that would be difficult, dangerous, or costly to test onboard the vessel;
- facilitates testing on similar replica hardware at a laboratory or at the vendor's site when the actual hardware onboard the vessel is not available;
- facilitates integration testing of control systems from several vendors;
- facilitates third-party testing, since no detailed design knowledge about the control system software is needed for testing;
- facilitates tests that could harm the equipment if tested onboard the vessel.

HIL testing tests the failure handling and alarm functions of control systems by using a real time vessel simulator interfaced to the computer system. It is therefore a powerful tool to uncover any software weaknesses within the DP control system, PMS or thruster control systems.

10 DNV GL, DP Asia Conference, 2015

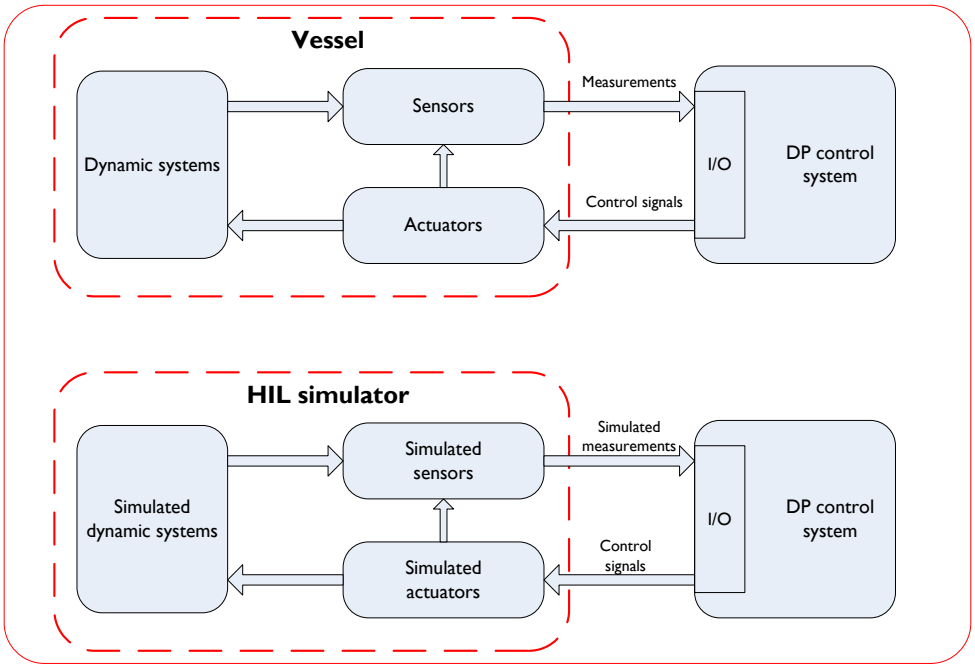


Figure 4-2 – Arrangement of DP HIL simulator

A modern DP vessel is equipped with a multitude of computer-based automation systems that are essential for the safety, reliability and performance of the vessel. The control systems that are relevant for HIL testing are, for example:

- dynamic positioning (DP) control systems;
- power management systems (PMS);
- thruster control systems;
- integrated automation systems (IAS);
- drill-floor control systems;
- drilling control/safety systems;
- BOP control systems;
- well control systems;
- crane control systems;
- offloading systems;
- diving control systems;
- pipe-laying systems;
- ballast systems.

The DP system comprises several interconnected control systems, the most prominent being the DP computer system, the PMS, and the thruster control systems.

There are multiple key problem areas related to the integrated DP system, including but not limited to:

- understanding of the worst case single failure and associated implementation of the consequence analysis for all different power modes and system setups;
- common understanding of functionality and signals related to load limitation;
- blackout prevention and local load reduction;
- common understanding of reserved power functionality and signals;
- thrust allocation and implementation of forbidden/restricted zones including fix/zone release;
- common understanding of pitch/rpm/azimuth response in different operational modes.

An HIL test of a DP system would typically target all the interconnected control systems, both individually and as an integrated whole.

For the HIL test of the DP computer system, the HIL simulator includes mathematical models of:

- the vessel itself;
- environment (wind, current, waves);
- the vessel motion due to environmental loads and thruster action;
- the thrusters;
- the power system;
- all position reference systems (such as GNSS, HPR, taut wire, Artemis, and relative reference systems);
- all relevant sensors (including gyrocompasses, MRUs, wind sensors, draught sensors, and riser angle sensors);
- mooring line forces (for a semisubmersible with thruster-assisted position mooring).

The HIL simulator includes the physical interaction between all these components. During HIL testing the DP computer system commands the simulated thrusters and receives measurements from the simulated position reference systems, sensors and equipment. The DP computer system does not see any difference from being in actual operation onboard the vessel. Functionality, performance, and failure handling capability can then be tested systematically in a controlled environment.

For the HIL test of the PMS, the HIL simulator includes models of:

- prime movers;
- generators;
- power distribution;
- thrusters; and
- circuit breakers and bus ties.

Load sharing and synchronising functions are included if the PMS is not responsible for load sharing and synchronising.

For testing of the thruster control systems, the HIL simulator includes models of:

- propellers;
- motors;
- drives;
- pitch and azimuth hydraulics;
- relevant auxiliary equipment.

The interfaces and commonalities that are networked together can be thoroughly verified during testing of the entire system. An HIL test of the integrated DP system is possible with all sub-systems connected and operating simultaneously to verify integrity of the interfaces between the individual systems and their shared functionality.

Depth of HIL testing depends on how the simulator is connected to the control system. If part of the control system software performs the I/O signal processing before it is used by the station keeping algorithm and the simulator is only connected to the station keeping software, the I/O signal processing part of the software will not be tested by the HIL test. In this case, however, the FMEA trial tests will target the I/O software because the test is done on the real system with the interconnected sensors and actuators. The failure modes, however, are often limited to 'loss of signal', while the HIL test will test many types of fault modes, like signal noise, signal bias, signal freeze, signal to maximum/minimum, slow/fast signal drift, etc. Otherwise, the simulator is hardwired to the control system and the complete control system computer software is within the scope of the HIL test.

FMEA simulation by HIL and practical testing by FMEA are therefore complementary. HIL testing should be complemented by conventional FMEA testing that is more ideally suited for testing of integrated hardware functions and confirmation of physical segregation. Co-ordination between the DP system FMEA testing and HIL testing will result in an increased level of verification. More information will be gained from the system, more safety critical functions and failure modes will be tested, and the verification efficiency will increase.

The FMEA desktop study will reveal possible weak points in the physical design, and point to critical software functions that deserve increased attention. This provides important input to the HIL testing, which in turn will provide essential information on the functionality and failure handling capabilities of the control system software that may be included in the FMEA.

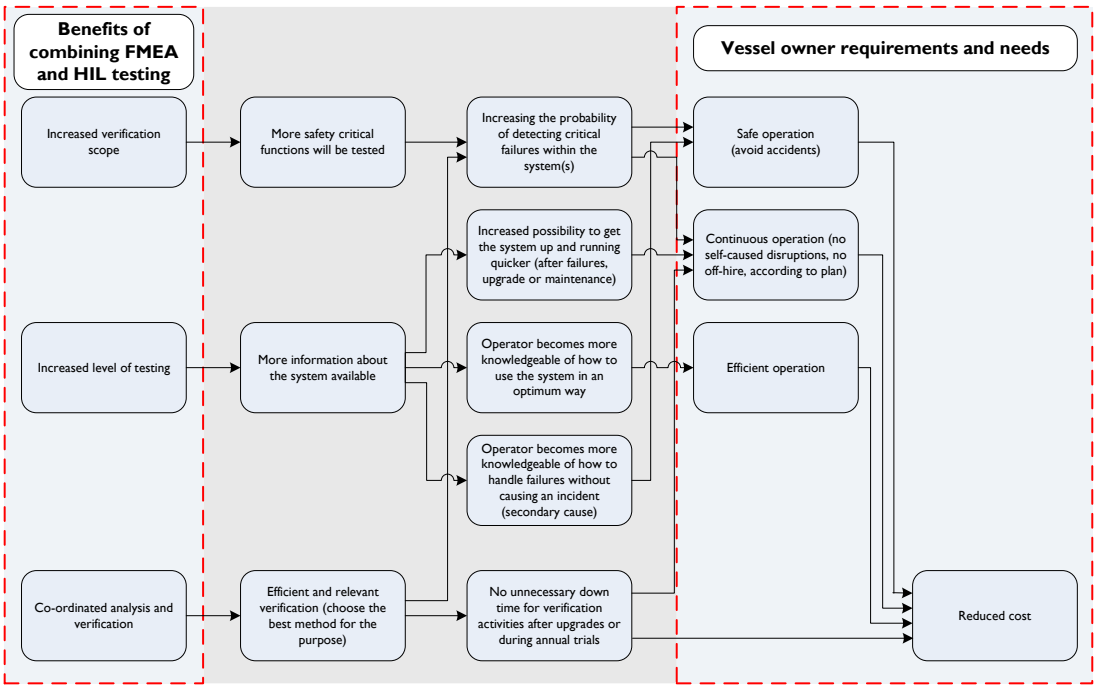


Figure 4-3 – Benefits of combining HIL and FMEA testing[11]

HIL cannot be used exclusively for FMEA testing such as for annual trials as there are many failures that can occur outside of the DP system computers and their software.

Both DNV GL and ABS have issued class notations focusing on the HIL test process; these being DNV GL's ESV[12] and ABS's ISQM and SV guides[13]. Note that, in some cases, a sea trial is only required for HIL tests on DP control systems, e.g. notation ESV-DP [HIL-IS] in DNV GL's enhanced system verification.

Other systems classed by DNV GL that have successfully undergone HIL testing in compliance with the requirements of specification DNV Standard for Certification No.2.24 may be assigned an HIL test certificate which identifies the systems that have been tested, lists the specific HW type, serial numbers and specific SW version identification and references the specific HIL test package used and the HIL test report.

4.27 MODU Tests

Mobile offshore drilling units are often on location for a period greater than the interval between consecutive annual DP trials renewal dates, so it is problematical for annual trials to be programmed on a consistent basis.

11 Marine Cybernetics White Paper DP system HIL vs. DP system FMEA 06.02.2012
12 DNV GL *Rules for the classification of ships* Part 6 Chapter 22 Enhanced System Verification, July 2013. In addition to the class rule, DNV GL has also issued a *Standard for certification for HIL testing* – SfC 2.24, July 2011
13 ABS *Guide for systems verification (SV)*, July 2014 and ABS *Guide for integrated software quality management (ISQM)* September 2012, updated July 2014

To help overcome this problem of the vessel not being available for the conduct of these trials, a system, similar to the continuous inspection of machinery space equipment operated by classification societies, was developed. This allowed for the annual DP trials to be carried out as tests over the course of the year, between the previous trials date and the renewal date.

Naturally, if the charterer of the MODU is prepared to release it for annual trials or the vessel is between charters, it would still be acceptable to carry out the trials as a single event. But normally release of the vessel is rarely achievable. This has resulted in the development and issue of appropriate guidance contained in IMCA M 191 – *Guidelines for annual DP trials for DP mobile offshore drilling units*.

The Requirements for Compliance with IMO DP Class

IMO MSC Circular 645

MSC/Circ.645 6 June 1994

System Arrangement

Subsystem or Component			Minimum Requirements for Equipment Class		
			DP Class 1	**DP Class 2**	**DP Class 3**
Electrical power system	Electrical system		No redundancy	Redundancy in technical design	Redundancy in technical design and physical separation (separate compartments)
	Main switchboard		1	1(1)	2 in separate compartments
	Bus tiebreaker		0	2(2)	2(3)
	Distribution system		No redundancy	Redundant	Redundant, through separate compartments(4)
	Power management		Not specified	Not specified	Not specified
Thrusters	Arrangement of thrusters		No redundancy	Redundancy in technical design	Redundancy in technical design
	Single levers for each thruster at main DP control centre		Yes	Yes	Yes
Positioning control systems	Automatic control; number of computer systems		1	2	2 + 1 in alternate control centre
	Manual control; independent joystick system with automatic heading control		Yes(5)	Yes	Yes
Sensors	Position reference systems		2(6)	3(6)	3(6) whereof 1 in alternate control centre
	External sensors	Wind	1	3(7)	3(7) whereof 1 in alternate control centre
		Gyro compass	1	3(7)	3(7) whereof 1 in alternate control centre
		Vertical reference sensor (VRS)	1	3(7)	3(7) whereof 1 in emergency control centre
UPS			1	2	3
Printer			Not specified(8)	Not specified(8)	Not specified(8)
Alternate control centre for backup DP control			No	No	Yes
FMEA			Not specified	Not specified	Not specified
DP Operations Manual			Not specified	Not specified	Not specified
Consequence Analysis			Not specified	Yes	Yes

Comments:

(1) At least two sections of main switchboard coupled by tiebreakers. Can be located in one switchboard room.
(2) Detailed as 'bus tiebreakers' (plural).
(3) Bus tiebreakers should be open during equipment class 3 operations unless their reliability can be demonstrated and documented to the satisfaction of the Administration such that equivalent integrity of power operation is provided.
(4) Separate cable routes for essential redundant cables with A-60 protection.
(5) Common joystick specified.
(6) Based on at least two different measuring techniques.
(7) Based on three systems serving the same purpose.
(8) A permanent record of the occurrence of alarms and warnings for failures in systems and of status changes should be provided together with any necessary explanations.

Example List of DP System Components for Analysis with Guidance in Analysis

The following is an example listing of the parts making up a DP system. It is based on the Annex to information note IMCA M 04/04 – *Methods of establishing the safety and reliability of DP systems*. Each part is made up of a series of components, each of which requires analysis. Guidance is given in what the analyst needs to look for within each part. When analysing each part of the system the analyst should not lose sight of the objective of the FMEA with respect to the worst case failure design intent (WCFDI) and the required level of redundancy and separation intent in the design.

FMEA objectives [as given in section 2.5]:

- Identify, with a view to elimination or mitigation, the effects of all single point failures and common mode failures in the vessel DP equipment which, if any occur, would cause total or partial loss of position keeping capability.
- demonstrate effective redundancy;
- demonstrate that each DP related system is single-fault tolerant with no adverse loss of functionality in the event of failure;
- identify potential hidden failures and determine the effects of a second failure after the hidden failure has been exposed;
- identify the effect these failures and hidden failures will have on the system;
- describe the design safeguards that minimise the risk of failure and any operational procedures required to ensure the design safeguards remain in place;
- prove that control circuit and interface equipment faults, including failures should not result in an unsafe condition to personnel or cause damage to equipment.

Typical failures to be considered when determining failure modes and causes are:

- Failure to operate when required;
- Intermittent or spurious operation;
- Failure to stop operating when required;
- Loss of output or failure during operation;
- Degraded output or degraded operational capability.

Items to be addressed when analysing each component:

- Position of the component in the system configuration;
- The component's dependence on other components and vice versa;
- Compliance with redundancy concept;
- Identification of which redundant group the component resides in and is it common to other redundant groups;
- Physical location of the component in a compartment with respect to fire and flood, e.g. A-60 separation (to Class 3 standard);
- Protective functions, means of preventing fault propagation between redundant groups, identification of hidden failures, common cause failures and configuration errors.

Section	Components for Analysis	Guidance in Analysis
1 Main, Auxiliary and Thruster Engines		
1.1 Fuel Oil	Storage tanks; fuel transfer facilities including pumps; purifiers; safety shutdowns and procedures; day tanks including service tanks; setting tanks and buffer (or header) tanks; day tank level (remote and local) indication; level alarms; water detection; sludge cocks; QCVs (quick closing valves); automated valves; pumps; mechanical and electrical; flowmeters (supply and return); filters (suction and discharge); differential alarms on filters; pressure alarms; leakage alarms; supply lines; return lines with valves; fuel coolers; electrical supplies to pumps and automation; air or hydraulics for valve actuation; HO/DO changeover; HO heating; purifiers; distillate cooling	Fuel transfer arrangements; failures which would prevent the transfer of fuel from bunkers to settling tank, from settling tank to service tank and service tank to engines; duty/standby arrangement of pumps; control of water and microbiological contamination; changeover between DO and HO fuel modules. Possibility of LNG as fuel and failures within gas valve units, failure modes of automated remote control valves; redundancy in electric supplies; effects of most common leaks (to class 3 standard); leak protection; hot surface protection; flexible pipes for vibration absorbance.
1.2 Lubricating Oil	Storage tanks; pumps (mechanical and electrical); level alarms; pressure alarms and shutdowns; alternator bearing pumps; suction and discharge filters; coolers; automatic valves; purifiers; oil mist detectors (OMDs); priming pumps and readiness for standby starts; electrical supplies to pumps and automation	LO transfer arrangements; filling; sump arrangement; alarm and shutdown modes; purification and cross connection; OMDs – alarm or shutdown; priming pump and generator bearing pump readiness for generator standby starts; pre-lubrication overrides.
1.3 Seawater Cooling	Sea chests; filters; pressure and flow alarms; remotely operated or automated valves including actuation and control power; bulkhead isolation valves; emergency shell isolation valves including actuation and control power; pumps (mechanical and electrical); coolers	Failure modes of automated remote control valves; redundancy in electric supplies; cross connections; duty/standby arrangement of pumps; biocide treatment; recirculation valves and temperature control; emergency cross connections; common overboard valves; effects of most common leaks (class 3 standard).
1.4 Freshwater Cooling	LTFW; HTFW; pumps (mechanical and electrical); thermostatic valves and controllers; bulkhead isolation valves; coolers; freshwater generators; remotely operated or automated valves; header tanks; header tank level alarms; temperature alarms; alarms and shutdowns; emergency cross connection	Temperature control (running and on standby); temperature control valve controller sensors; duty/standby arrangement of pumps; electrical power supplies for pumps and temperature control; air or hydraulic power for temperature control valves; system cross connections; effects of most common leaks (class 3 standard); use of flexible pipes.
1.5 Charge Air	Turbochargers; ducting, dampers, coolers; air temperature controllers; control valves (including actuation and control power); rig savers; dump valves; jet assist	Temperature control system; damper redundancy and failure modes; failure modes of control valves and rig savers.

Section	Components for Analysis	Guidance in Analysis
1.6 Compressed Air Systems – Start Air; Work Air and Control Air	Start air/work air/control air; compressors; receivers; driers; operating modes; cross connections; bulkhead isolation valves; reducing valves for DP related use; other non-DP users; pressure alarms; emergency start air	Compressor operating modes; lead/lag; cross connections; failure modes of control valves; electrical power supplies; compressor automation; effects of most common leaks; leaks for class 3.
1.7 Emergency Generator	Generator and engine; starting methods including batteries	Starting methods; indication of start status; indication of mode – emergency/ harbour, any DP dependency on emergency generator; blackout recovery.
1.8 Engine Management or Safety Systems	Engine manufacturer's engine safety system; engine E-stops	Power supply segregation; interface to power management system and vessel management system; power management system supervision; engine protection; shutdowns – compatible with worst-case failure design intent; cross connections between safety systems; interface to switchboards – open circuit breakers on engine shutdown; time on hot standby; start interlocks; maintenance of readiness to start – lube oil priming; starting time – slow turning; engine response of failure of engine management safety system; load up ramps; engine E-stop circuits; wire break effects.
1.9 Emergency Shutdown Systems	ESDs	Split along lines of redundancy concept; isolation of batteries; failure modes of control system; protection against inadvertent operation
	Thruster Emergency Stops	Hardwired; available within easy reach of DPO; layout of push-buttons representative of thruster locations; over network (not recommended); wire break protection alarm.
	Group Emergency Stop Systems	Split along lines of redundancy concept; failure modes of actuators and valves; failure modes of control system; cabling route considerations for DP class 3; protection against inadvertent operation; cause and effects (if available; for fans and flaps).
	Fans	Effect on loss of ventilation; ventilation provided along lines of redundancy concept; alarms for compartment temperature if no redundancy in ventilation.
	Flaps	Actuation power and control power; remote indication; protection against inadvertent operation.
	Watertight Doors	Actuation power and control power; remote indication.
	Fire Fighting Systems	Control system – failure modes; pipe work and valves – failure modes; division between engine rooms, switchboard rooms and other compartments; protection against inadvertent operation.
	Quick Closing Valves	See also 'Fuel': Fuel system and valves split along lines of redundancy concept; failure mode of valves; protection of valves; protection against inadvertent operation.
1.10 Bilge & Ballast System	Ballast system (as appropriate); ballast pumps and valves, ballast control system, anti-heeling system, HPU for solenoid valve control	Ballast valve failure modes; manual backup; HPU redundancy; control system operations, failures which would render the ballast system uncontrollable from remote control position
1.11 Remote Valve Control	Location; power supplies; hydraulic power – pumps; accumulators; valve actuators; valve duty	Redundancy concept; actuation and control power; remote indication; failure mode of valves.

Section	Components for Analysis	Guidance in Analysis
2 Power Generation		
2.1 Generators	High voltage; low voltage; AC or DC; coolers; bearings; bearing LO systems	Ratings; separation between redundant systems; independence/commonality; intent of single failure – defined loss of generators – worst-case failure; typical power plant configuration for DP operations; power plant configurations to allow maintenance activities; effectiveness of fault clearing; current – not to exceed rated value; voltage – not to exceed rated value or fall below set limits – voltage dip effect on consumers – ride through capability; power – active and reactive to be shared in proportion to generator size; frequency – to be maintained within defined limits – engine load acceptance; harmonics to be maintained within defined limits; power factor – aware of effects on governor failures; NETs; NERs; earth system – low resistance/high resistance – operation with earth fault v tripping; type of alternator/generator; control by power management or other systems; environmental/temperature control – compatible with redundancy concept; bearing LO pressure/flow interlocks; manual controls and synchronising – effect of crash synchronisation; dead bus connection; interlocks – earth switches – hardware – software – possibility of conflict; bus ties/tie lines – class 3 considerations; transfer of fault – particularly in class 3.
2.2 Generator Protection System	Protection relays; protection functions; power supplies; AGPS	Protection scheme supports worst case failure design intent philosophy; failure modes of protection systems compatible with declared worst case failure; vendor support – planned maintenance; switchgear – circuit breakers and contactors; differential protection – trip incomer and de-excite alternator; over current protection – short circuit – thermal; over voltage/under voltage protection; over frequency/under frequency; reverse power protection; negative sequence protection – overheating; temperature alarms – shutdowns; lube oil pressure alarms – shutdowns; directional earth fault protection and zero sequence protection; over/under excitation protection – VAr imbalance; load sharing imbalance protection; signal monitoring – redundant signals mismatch alarm; frozen signals; transducer failures; self-monitoring; communication.
2.3 Governors	Type of governor and rack actuation; load sharing methods	Isochronous/speed droop electronic mode for speed control and load sharing – increased commonality; connection to or interface with PMS; PMS control (compensated droop); overload protection; over/under fuel; over/under frequency; speed pick-up failures; actuator failures; hunting; mechanical default control – interaction with electrical system – failure modes; rack position indication; interaction with thrust limitation or blackout prevention systems; load sharing lines (analogue/digital) – possibility to split; default to droop on load share line fault.

Section	Components for Analysis	Guidance in Analysis
2.4 Automatic Voltage Regulators	Automatic Voltage Regulators (AVR); type of regulator and exciter	AVR failure mode; control by power management or other system; interface with generator protection; reactive power sharing; excitation alarms; excitation protection; loss of excitation current – field failure; over/under voltage; loss of sensing; hunting; monitoring of field current; droop characteristics; current boost systems; cross current compensation.
3 Power Management		
3.1 Scope of Power Management	Design specification	Conditions; Prime objective – maintain continuity of electrical power under all defined load and failure Secondary objective – restore propulsion capability if fails in prime directive; alarms for failure of redundant components; spinning reserve – adequate to cope with worst-case failure of generators – load acceptance limitations; efficient management of generators; diesel automation; control of engine starting requirements – pre-lube – pre heating; control of engine specific requirements – time on hot standby – slow turning – load up; selection of generator running order – alarm on incorrect selection – effect of incorrect selection; load dependent starting of generators – preservation of spinning reserve; load dependent stop; blackout prevention system – thrust limitation/ thrusters tripping – preferential tripping; auto reconfiguration of circuit breakers – alternative supply routes for DP essential consumers; advanced power reservation – make available sufficient generators to cope with large consumer starting demands – avoid blackout; interface with electronic governor or external load sharing; interface with AVR or external VAr sharing; interface with engine management and safety system; load sharing – each generator to carry equal/proportionate share of load – prevent cascade failures; reactive power sharing – each generator to carry equal/proportionate share of current; net frequency control – if not under governor control; asymmetric load sharing to compensate for the effects of low load running on medium speed engines; protective functions – load sharing alarm – generator tripping – bus tie tripping; maintain harmonics within set levels by switching in and out harmonic filters; control of switchboard fault levels – bus tie control; power regeneration; analogue/digital communication links; unintended operations; signal validation, faulty signal, loss of signal.
3.2 Architecture	Operator stations; field stations; controllers; networks, hubs, stars, NDUs; power supply units	Hierarchy; redundancy concept; integration; power supplies; centralised or distributed; system segregation – also class 3 requirements; system independence and duplication; switching and protective functions; common mode failures; hidden failures; multiple independent failures; barriers to prevent operator error; I/O allocation across redundant groups; analogue/digital communication links; unintended operations; unintended automatic actions (e.g. actions which could result in unnecessary blackout, partial blackout, lack of power or unintentional power reduction); signal validation, faulty signal, loss of signal – transducer failures.

Section	Components for Analysis	Guidance in Analysis
3.3 PMS Functions	Load Dependent Starting	Start/stop/running order; spinning reserve; interface with engine protection systems.
	Synchronising	Connection of synchronous generators in phase with network – separate module; voltage/frequency control; synchroniser failure; crash synchronising; check synch.
	Load Sharing	Speed droop; compensated droop; isochronous – increased commonality between systems – class 3 requirements; each generator to carry a share of the load in proportion to its rating; avoid cascade failure – effect of load sharing imbalance; load sharing failure active/reactive power; failure of load share lines.
	Blackout Prevention	Load dependent start protection of spinning reserve; start blocking – advanced power reservation heavy consumer protection; heavy consumer protection; load limitation – load shedding; thrust limitation/reduction; thruster tripping; thruster priority; heading priority; preferential tripping; interfaces with other blackout protection systems – DP control system; interaction with other systems – governors, AVRs; process/drilling priority; locked to bottom; process phase-back; e.g. rotary table or top drive; crane/pipelay priorities.
	Blackout Restart	Generator starting sequence, dead bus connection; staged reconnection of consumers; protection against reconnection of faulty generator; protection against simultaneous connection of generators; lockouts – which may prevent reconnection of healthy generators.
	Static Power Estimate	Normal power plant configurations for DP – bus ties open – bus ties closed; normal power plant configuration for transit (optional); after defined worst case failure; after defined worst case loss of generators without loss of load; after defined worst case failure – one generator down for maintenance; active power; reactive power; current and power factor; load acceptance – step load; DP configurations – CAM and TAM.

Section	Components for Analysis	Guidance in Analysis
4 Power Distribution		
4.1 HV/LV Distribution	High voltage, medium voltage and low voltage AC distribution systems, emergency systems; switchboards; type of power system (e.g. three wire, three phase); bus bars; switchgear; circuit breakers; contactors; arc detection (optical/pressure); number of bus ties (master/slave); open/closed bus tiebreaker operation; interlocks; short circuit and breaker discrimination analyses – selectivity/co-ordination study; load balance; harmonic analysis; transformers – power distribution – cooling fan supplies; transducers and control power supplies, interfaces; reference to short circuit and earth fault test of main switchboard; shore power/emergency generator interlocks and intertripping; emergency generator backfeeding	HV/LV configuration and distribution; A-60 and watertight separation of redundant groups; compare worst-case failure at all levels; protection philosophy; switchgear – fault levels; bus tiebreakers and tie lines – particularly open/closed bus tiebreakers for class 2 and 3 – potential for unscheduled closing – potential for crash synchronising; closed ring bus; breaking capacity and selectivity/ discrimination; verification of system parameters; short circuit faults – protection – current limiting breakers; earth faults – protection; control power supplies, interfaces; overload; governor/ AVR failures; interface to PMS/VMS; PMS and active load share failures; effect of voltage transients (dips); worst-case voltage dip (depth and duration) on healthy bus after short-circuit on other bus (in closed tie-breaker operation); cable routes – particularly for class 3 but obvious hazards for class 2; cross connections; interlocks (electrical/ mechanical) – inter tripping; motor starting and protection; tables of DP related consumers – check against all utilities; list MCCs and distribution boards; common backup systems – common mode failures; reliance on switching of power to switchboards – auto reconfiguration; reliance on switching of power to MCCs or distribution boards; thrusters – maintaining DP ready signals during switching; interface to ESD, emergency stop and F&G systems; DP configurations – CAM and TAM.
4.2 110V/24VDC	Location; charger; batteries; power distribution boards	Alarms; consumer distribution; segregation; diode cross connections; prevention of transfer of faults.
4.3 UPS	Location; type; charger; rectifier; batteries; power distribution boards	Power supplies; alarms; consumer distribution; segregation; diode cross connections; bypass arrangements; prevention of transfer of faults.
4.4 Module Power Supplies	Power for drilling, cranes, ROVs, pipe lay, cable lay, survey, etc., (as appropriate)	Effect of failure within power supplies to module spread – fault propagation back to DP switchboards.
5 Propulsion and Thrusters		
5.1 General	Redundancy concept; location; type (e.g. main propeller, tunnel, azimuth, gill jet, combinatory, Voith Schneider, FPP, CPP); specification; prime movers; main power; auxiliary power; utilities; control stations and backup control stations; FU and NFU control; thrust/power curves; barred zones; emergency stops	Describe DP system redundancy concept; operating modes; surge, sway and yaw analysis (intact and post failure conditions); redundancy; power supplies, main, auxiliary and backup pumps – changeover systems, hydraulics, cooling, main, alternative and backup controls, control power supplies, protections, angle indications, alarms, DP ready signal requirements; alarms; effect of loss of cooling, hydraulics, lubrication and power supplies; interlocks; emergency stops – independent of control system, hardwired, loop monitored, easily accessed by DPO, alarm on loss of power.
5.2 Main Propellers	Mechanical components; seals; gearbox; clutch (including actuating medium and power supplies); CPP; speed control; pumps; hydraulics; lube oil; cooling; control stations (alternative controls, emergency controls)	Interfaces with switchboards and PMS; thrust limitation and reduction signals; interaction of variable speed control with power system; power supplies (main, auxiliary and backup); operating modes; combinatory pitch/speed control; signal failure; control loop protection (speed and pitch); interface with rudder.

Section	Components for Analysis	Guidance in Analysis
5.3 Azimuth Thrusters	Mechanical components; seals; variable frequency drive (VFD); drive transformers; motors; azimuth/pitch hydraulic systems; lube oil; cooling; seal air pressure	Azimuth control modes; azimuth control loop protection; pitch control modes; pitch control loop protection; signal failures; VFD speed control loop protection (speed and/or pitch and azimuth); interfaces with switchboards and PMS; thrust limitation and reduction signals; defaults, e.g. on loss of hydraulic pressure.
5.4 Tunnel Thrusters	Mechanical components; seals; variable frequency drive (VFD); drive transformers; motors; pitch hydraulic systems; lube oil; cooling; seal air pressure	Pitch control modes; pitch control loop protection; VFD speed control loop protection; interfaces with switchboards and PMS; thrust limitation and reduction signals; defaults, e.g. on loss of hydraulic pressure.
5.5 Steering Gear	Power supplies (main, auxiliary and backup); control power supplies; pumps; hydraulics; cooling; control stations; alternative controls; emergency controls; mechanically linked rudders; high lift rudders	Operating modes (mechanically linked, independent, push/pull, set at zero, hydraulic locking); control power supplies; ready signal requirements; control loop protection; angle indication; alarms; defaults, e.g. on loss of propulsion; failure modes including 'hard over'.
5.6 Propulsion/ Thruster Control Systems	Operator stations; field stations; controllers; networks, hubs, stars, NDUs; power supply units; independent joystick	Interfaces with PMS and DP; DP/manual/joystick changeover; power supplies redundancy; thruster control unit segregation; network segregation.
6 Vessel Management Systems and Networks		
6.1 Architecture	System architecture; operator stations; field stations; controllers; networks, hubs, stars, NDUs; power supply units	System architecture; integration; redundancy concept; system segregation; system independence and duplication; power supplies – normal and/or UPS; switching and protective functions; common mode failures – network storms; hidden failures; multiple independent failures; operator error; allocation of signals to field station I/O modules; remote access for diagnostics.
6.2 Communication with Switchboard PLCs for Engines	Data links between switchboard PLCs and engine controllers	Reaction of engines to PLC failures.
6.3 Air Conditioning and Forced Ventilation	Main AC units; packaged AC units; location of units; fan coil units; backup units	Susceptibility of controllers, hubs, stars, process stations, outstations, etc. to overheating; alarms on AC failure and temperature increase; provision of A/C redundancy in critical DP equipment spaces; provision of alternative ventilation for critical spaces; time before a critical situation develops if non-redundant; failure effects of condensation.

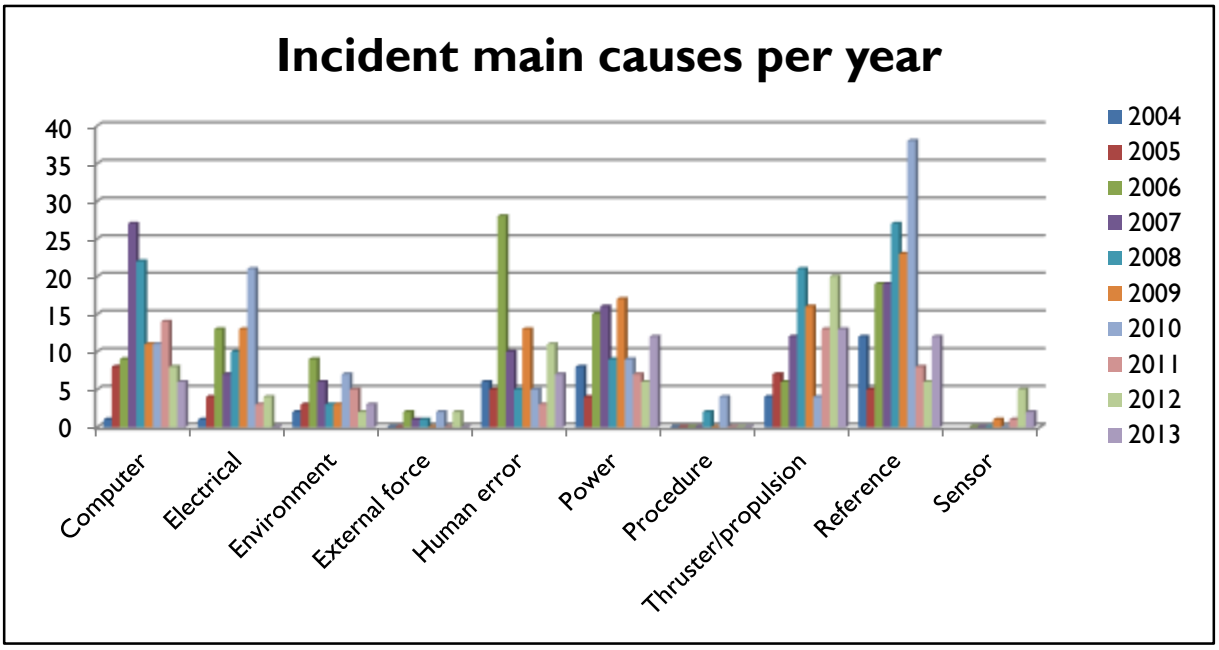
Section	Components for Analysis	Guidance in Analysis
7 DP Control Systems		
7.1 System Architecture	Manufacturer – type and model (simplex, duplex, triplex); operator stations; field stations; controllers; networks, hubs, stars, NDUs; power supply units; backup DP control station (DP 3); isolation box for shared vessel sensors and position reference systems; independent joystick (IJS)	Layout; redundancy concept; configuration for DP; integration; network; communication; separation; independence; duplication; switching; interfaces with vessel equipment, e.g. riser system, cranes, pipelay spread, survey equipment; common mode failures; hidden failures, multiple independent failures; operator error – means to prevent inadvertent operation; I/O allocation (complies with redundancy concept); mode selector switches between DP and manual control; mode selector switch between main and backup DP – 'Fire backup switch' (DP 3); no inhibiting of manual control or failure in excess of WCFDI on failure of a mode selector switch; backup DP system independent and isolated from main DP control (A-60 segregation); backup DP system failure modes; vendor FMEA; transfer to IJS on loss of main DP; alarm on loss of IJS when on auto DP; confirm independence of IJS from the main DP control; thruster control modes (bias, fixed, variable); emergency thruster stops – normal thruster stops – see also shutdowns.
7.2 Vessel Sensors	Gyros; motion reference units (MRU); vertical reference sensors (VRS); wind sensors; draft sensors	Compliance with class rules; redundancy; segregation; power supplies; data links; boosters; wind sensor masking by ship's structure; rejection of faulty data.
7.3 Position Reference Sensors	As appropriate: DGPS/GLONASS; antenna array – correction data; hydro acoustic (HPR, HiPAP); taut wire; microwave (RADius, Artemis); laser (Fan beam, Cyscan); riser angle; pipe tension: crane angle; survey package; INS; power supplies; transmitters; receivers; survey package	Compliance with class rules; redundancy. As appropriate: Segregation in power supplies, receivers, transmitters and correction data; antenna array separation and masking by ship's structure; scintillation (DGPS); data links; boosters; serial interface failure; rejection of faulty data (including from false targets); radar, radio and acoustic interference; range restrictions; riser angle input to DP but as indication and not control; pipe tension – auto or manual input.
7.4 DP Alert and Other Communication Functions	DP status lights and switches	Provision of DP status lights and switches; hard wired or over a network; location of alarms and indication (e.g. dive spread, ROV control, pipe lay control, drill floor); automatic functions related to position failure (e.g. auto riser disconnect, etc.).
7.5 Cable Routes (DP 3)	Cable routing drawings	For Class 3: HV cable routes for generators and thrusters; cable routes for thruster control and feedback signals also thruster start and stop; philosophy of cable routing in respect of fire – possibility of fire causing loss of thrusters exceeding the worst case failure; cable routes to vessel sensors and reference systems; Possible visual inspection required.

Section	Components for Analysis	Guidance in Analysis
7.6 Fire and Flooding Analysis (DP 3)	Layout drawings including structural fire protection drawings showing fire rated divisions (A-60); list of DP related equipment and their locations; cable routing drawings (power and control); pipework routing drawings; figures; tables; watertight door system	Verification of provision of appropriate fire and watertight sub-divisions between redundant equipment. Location of redundant component groups in separated zones with fire and flooding protection. Analysis of all pipework and cable routes in zones, spaces and cable trays where the pipes and cables are run and DP related equipment is installed to ensure that fire or flooding will not cause fault propagation from one compartment/system to another or between redundancy groups; possible visual inspection required of pipework and cable routing; watertight door analysis to confirm separation of all the DP related rooms after flooding of compartments.
8 Safety Systems		
8.1 Fire & Gas	Fire and Gas system; main panel; repeater panels; alarms. Cause and Effect diagram	Redundancy concept; extent of coverage; types of detector; interfaces with VMS and ESD; auto shutdowns or alarm only; effect of smoke or gas intake.
8.2 Fire extinguishing systems	Fire extinguishing systems (water based, CO_2 based, smothering gas based, etc.); control system; pipework and valves; activation mechanism; alarms	Division between compartments; inadvertent discharge of fire extinguishing medium into critical spaces, e.g. engine rooms.
8.3 ESD systems	ESD system philosophy; Cause and Effect diagram; location of ESD panels; switches; circuits	Redundancy concept; shutdown levels (ESD 1, ESD 2, ESD 3, etc.), commonality in shutdown of redundant equipment; effect of shutdown on DP; loop monitoring; I/O allocation; isolation of batteries; prevention of inadvertent operation (no single button), interfaces with ESD and F&G
8.4 Group Emergency Stops	Power supplies; arrangement of control boxes and stop loops; actuators and valves; cause and effects	Redundancy concept; cable routing; prevention of inadvertent operation; loss of power to actuators and valves; interfaces with ESD and F&G
8.5 Ventilation	Dampers; type (electrical, pneumatic, manual); fans; power supplies; ventilation backup	Effect of loss of ventilation; damper redundancy and failure modes; fan power supply redundancy; compartment temperature monitoring
8.6 Quick Closing Valves	Location; power supplies; hydraulic power, valve actuators	Redundancy concept; actuation and control power; remote indication; failure mode of valves, commonality between engine rooms, valve protection; means to prevent inadvertent operation.
8.7Watertight Doors	Location; power supplies; hydraulic power	Actuation and control power; remote indication.

The IMCA DP Station Keeping Incident Database

During the period 2004 to 2013, 749 accounts of DP incidents were received by IMCA 264 different vessels provided data. The received DP incident reports are anonymised and reviewed annually in a report produced by IMCA. The data contained from these ten annual reviews has been combined to produce the report for this document.

The largest percentage (23%) of incidents had 'references' as their main cause. 'Thruster/propulsion' and 'computer' problems (16%) were the next highest scorers. 'Power' (14%), 'human error' (12%), 'electrical' (10%) and 'environment' (6%) were significant causes. The least of the main causes of incidents over the ten year period were caused by 'sensor' (1%), 'procedure' (1%) and 'external force' (1%).



Analysis of the incidents involving references as the main cause revealed that over half involved DGNS systems. This is not surprising when considering its wide use within the industry and the flexibility this position reference gives operators. When considering position reference systems, it has been shown that all DGNS systems can be susceptible to common atmospheric effects such as scintillation. Microwave and hydroacoustic position reference systems made up the bulk of the other systems that were recorded as the main cause of an incident. This does not necessarily reflect the unreliability of these systems. It is thought this higher number of reported incidents is more likely to reflect the greater use being made of these systems, in particular microwave systems as relative position reference systems and hydro acoustic systems being used in deep water situations.

It is still considered that for drilling vessels working in deep water, the best scenario is a combination of at least two separate DGNS systems and two long base line hydroacoustic position reference systems (see IMCA M 160 – *Reliability of position reference systems for deepwater drilling*).

The vast majority of DP incidents involving thruster or propulsion as the main cause of the incident did not result in a major incident. This is because these incidents usually concerned one thruster only and, as each vessel was working within its WCFDI, there was no subsequent loss of position. However, operations had to be interrupted whilst the thruster fault was investigated and corrected.

Where computer incidents are concerned, a significant number involve software issues and faulty operator stations. Often the problem is solved by 'rebooting' the computer system. As software forms a part of so many systems, it is likely to be a factor in categories other than computer systems.

Reasons behind the computer related incidents recorded on the IMCA incident report forms are as follows:

- Software did not meet industry reliability requirements;
- Network problems;
- Operator station not communicating;
- Virus on systems – transferring data by USB device;
- Operator station motherboard failure;
- Software error;

- Loss of DP main controller;
- Software issue;
- Operator station computer shutdown;
- Operator stations stopped responding.

Power management has 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 (see IMCA M 206 – *A guide to DP electrical power and control systems*).

Human error still contrives to play its part in DP incidents. It is thought that the number of incidents recorded as having human error as the main cause is possibly higher than that recorded in the received DP incident reports. Whilst it is easy to identify pressing the wrong button or shutting the wrong valve as a human error, it is not always as easy to attribute it to an incident when, for instance, there has been a lack of maintenance or operations continue despite increasing environmental conditions.

Since 2010 there have been very few recordings of electrical faults being the main cause of DP incidents. It is difficult to draw a conclusion from this however it could be due to better design. Equally it could also be due to electrical failures being 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.

Where machinery systems are concerned, fuel oil system problems are potentially the most dangerous, as any fracture in the piping system could 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.

Types of Failures Uncovered by FMEAs

The failures illustrated below can be dangerous for any DP vessel and safety of personnel is always of the utmost importance. A DP incident has the potential for serious injury or death to personnel and significant damage to assets and environment with dire economic consequences.

The examples below serve to illustrate how a detailed FMEA and subsequent FMEA proving trials can minimise the effect, if not eliminate, of failures in a vessel's DP system. These are areas which should receive special consideration, but this is not to say that other areas should receive less attention.

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. Examples of these and other failure modes either revealed in service or uncovered by FMEA can be found below.

Failures Revealed in Service:

Insidious failures have been uncovered, sometimes only as a result of in service failures. Most of these failures would be revealed by a thorough FMEA, however, it may require other techniques such as HIL to reveal embedded software problems.

- Failure of a DP control system electronic module caused it to keep sending superfluous data onto both networks overloading them both and causing a failure of position.
- 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.

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 had to be 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.
- Problems are not necessarily confined to vessels incorporating full redundancy. FMEA tests were carried out on a simplex DP vessel with a single DP computer and independent computerised joystick, with functions including automatic heading control. It was noticed that a fuse was critical to the changeover between automatic DP and joystick. Failure of this fuse was not alarmed and, with the vessel on automatic DP, it was proved from practical tests at sea that, with failure of this fuse remaining hidden, should the automatic DP fail then transfer of control to the joystick was impossible and position was lost. Fuse failure monitoring was introduced in this case to mitigate the problem. It should be established what fuses are critical to DP and arrange an alarm to warn of failure.
- The ESD on one vessel with two engine rooms 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 engine room 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 engine rooms 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 room's 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.
- During FMEA testing it was found that a fault on the generator engine governor analogue load share lines whilst running in isochronous mode would cause a severe disturbance on the electrical distribution network. In order to mitigate these effects, the engine governors are now operated in droop mode.

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 in-depth 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 VFD 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 voltage. 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 VFDs 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 engine rooms. 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 engine room 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 engine room was destroyed. The vessel stayed on station because the power demand was within the capability of the generators running in the other engine room, which continued to supply power. Detector siting should be reviewed to ensure activation in the event of fire. For some critical operations it is requested that all generators are on line.
- An investigation following a blackout incident on a DP 2 vessel revealed that redundant fuel pump power supplies were found to be cross connected. The incident was triggered by the accidental tripping of a QCV and resulted in loss of fuel supplies to all generators. Modifications had been made during an upgrade to increase the redundancy in the system but pressure to get the vessel to work had caused a weakness in FMEA testing.

Cooling Water Problems:

- Sometimes temperature or pressure control valves will adopt a non-fail safe mode, e.g. temperature control bypass valves opening 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 suggestion 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 both 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 trials on one vessel revealed that loss of the DP Request signal into the thruster control system caused all thrusters to adopt zero pitch and azimuth settings. It was found that these were the settings from the manual bridge levers. There was no alarm to warn the operator of the changeover from auto DP to manual levers. There was an eventual loss of DP and control had to be taken over on the bridge remote joystick.

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 should be aware of what the operator may want to do during the execution of specific workscopes, and operators should be aware of what they cannot do due to limitations in design.

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.

Generator Control Problems:

- One vessel had two separate governor systems, one for the generators in each engine room. 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 was 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.

DP FMEA Reference Documents

Note: Some of the following documents are subject to continual change. The reader should verify the latest revision for any specific case.

IMCA DP related documents relevant to FMEA:

- The Annex to information note IMCA M 04/04 – *Methods of establishing the safety and reliability of DP systems*
- IMCA M 103 – *Guidelines for the design and operation of dynamically positioned vessels*
- IMCA M 109 – *A guide to DP-related documentation for DP vessels*
- 113 IMO – *Guidelines for vessels with dynamic positioning systems (MSC Circular 645)*
- IMCA M 117 – *The training and experience of key DP personnel*
- IMCA M 140 – *Specification for DP capability plots*
- IMCA M 160 – *Reliability of position reference systems for deepwater drilling*
- IMCA M 162 – *Failure modes of variable speed thrusters*
- IMCA M 163 – *Guidelines for the quality assurance and quality control of software*
- IMCA M 173 – *Station keeping incidents reported for 2002*
- 182 MSF – *International guidelines for the safe operation of dynamically positioned offshore supply vessels*
- IMCA M 190 – *Guidance for developing and conducting annual DP trials programmes for DP vessels*
- IMCA M 190A – *Guidance for developing and conducting annual DP trials programmes for DP vessels: Executive summary*
- IMCA M 191 – *Guidelines for annual DP trials for DP mobile offshore drilling units*
- IMCA M 206 – *A guide to DP electrical power and control systems*
- IMCA M 212 – *Example of an annual DP trials report*
- IMCA M 220 – *Guidance on operational activity planning*
- IMCA M 225 – *Example redundancy concept and annual DP trials for a DP class 3 construction vessel*

Other DP related documents relevant to FMEA:

- ABS *Guidance notes on failure modes and effects analysis for class*, May 2015
- ABS *Guide for dynamic positioning systems*; November 2013, updated July 2014
- ABS *Guide for systems verification (SV)*, July 2014
- ABS *Guide for integrated software quality management (ISQM)*; September 2012, updated July 2014
- ABS *Rules for building and classing steel vessels*, Part 4 Vessel Systems and Machinery, Chapter 3 – Propulsion and Maneuvering Machinery, Section 5 Thrusters, 2013
- 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)
- DNV GL *Rules for the classification of steel ships* – Part 6 Chapter 7 – Dynamic Positioning Systems, July 2011, amended January 2012
- DNV GL *Rules for the classification of ships, newbuildings, special equipment and systems*, Additional Class, Part 6 Chapter 26 – Dynamic Positioning Systems – Enhanced Reliability DYNPOS-ER, July 2010
- DNV GL Recommended Practice (RP), DNV-RP-D102 – *Failure mode and effect analysis (FMEA) of redundant systems*, January 2012
- DNV GL *Rules for the classification of ships* Part 6 Chapter 22 – *Enhanced System Verification*; July 2013
- DNV GL Recommended Practice (RP), DNV-RP-E306 – *Dynamic positioning vessel design philosophy guidelines*, September 2012
- DNV GL Recommended Practice (RP), DNV-RP-E307 – *Dynamic positioning vessel operation guidance*, January 2011
- DNV GL Offshore Technical Guidance (OTG), DNVGL-OTG-10 – *DP-classed vessels with closed bus tie(s)*, April 2015
- DNV GL *Standard for certification for HIL testing* – SfC 2.24, July 2011

- GL *Rules for Classification and Construction, Ship Technology, 1 Seagoing Ships, 15 Dynamic Positioning Systems*, Edition 2013
- HSE *Review of methods for demonstrating redundancy in dynamic positioning systems for the offshore industry*, Prepared by DNV Consulting for the Health and Safety Executive 2004
- IEC Standard, IEC 60812: *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)* Second Edition 2006-01
- IEC Standard IEC/FDIS 31010 *Risk management — Risk assessment techniques* 2009
- IMO MSC Resolution 36(63) Annex 4 *Procedures for failure mode and effects analysis (HSC Code)*
- IMO *Guidelines for vessels with dynamic positioning systems* MSC Circular 645, dated 6 June 1994 (also issued as IMCA document 113 IMO)
- Lloyd's Register *Rules and regulations for the classification of ships*, July 2015
- Marine Technology Society (MTS) DP Technical Committee *DP (Dynamic Positioning) Design Philosophy Guidelines*
- Marine Technology Society (MTS) DP Technical Committee *DP (Dynamic Positioning) DP Operations Guidance*
- Marine Technology Society (MTS) Various TECHOP documents
- US Department of Defense MIL-STD-1629A (now obsolete)

Glossary and Abbreviations

Glossary

Initially, it is important to understand the meanings of some of the terms used in the FMEA process. The following are terms commonly used during the FMEA process together with their explanations.

Active component	A component or system which requires an external source for operation and contributes in a dynamic manner by modifying system behaviour in some way, e.g. pumps, fans, generators, thrusters, switchboards, remote controlled valves, etc.
Active redundancy	The use of redundant elements operating simultaneously to prevent failure or permit recovery from failures
Availability	The degree to which a system or component is operational and accessible when required for use. Often expressed as a probability. It combines the ideas of reliability and maintainability
Backup	A system or component available to replace or help restore a primary item in the event of failure
Block diagram	[IEEE 610.12-1990] A diagram of a system in which the principle parts are represented by suitably annotated geometrical figures to show both the functions of the parts and their functional relationships
Bottom-up	Pertaining to an activity that starts with the lowest level component of a hierarchy and proceeds through progressively higher levels to the top level
Common cause failure	[IEC 191-04-23] Failures of different items, resulting from a single event, where these failures are not consequences of each other
Common mode failure	[IEC 191-04-24] Failures of items characterised by the same fault mode. Note – Common mode failures should not be confused with common cause failures as the common mode failures may result from differing causes
Competence	[HSE/IMCA M190] Competence is 'the ability to undertake responsibilities and perform activities to a recognised standard on a regular basis. It combines practical and thinking skills, knowledge and experience'
Component	One of the parts that make up a system
Configuration	[IEEE 610.12-1990] The arrangement of a system or component as defined by the number nature and interconnections of its constituent parts
Critical activity mode of operation (CAMO)	The CAMO sets out the most fault tolerant configuration for the DP system and associated plant and equipment. The CAMO should be implemented for all critical activities undertaken by the vessel. For DP class 2/3 vessels the CAMO usually defines the most robust fault tolerant configuration of the DP system ensuring that a single point failure does not exceed the vessel's identified worst case failure
Criticality	The degree of impact that a component necessary to a system has on the operation of the system when it malfunctions or fails
Criticality rating	The criticality rating is the mathematical product of the severity (or consequence) and occurrence (or frequency) ratings. Criticality = (S) x (O). This number is used to place priority on items that require additional quality planning
Degraded DP capability	[Based on USCG MODU definition] A failure of equipment in the DP or APM system (e.g. thruster, switchboard) that has either: A. Expanded the DP footprint and reduced the maximum environmental conditions under which the vessel can maintain position; or B. Reduced the redundancy of the DP system to the extent that it no longer meets equipment class 2 or 3 standards

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
Drift off	Drift off is a situation in which a vessel has suffered a loss of position owing to an unintentional reduction or loss of thrust rendering it unable to counter the prevailing environmental forces
Drive off	Drive off is a situation in which a vessel has suffered a loss of position owing to an unintentional increase in thrust which is in excess of the prevailing environmental forces
Effect	An effect is an adverse consequence that the item, subsystem or overall system might suffer
Fail safe	[IEEE 610.12-1990] Pertaining to a system or component that automatically places itself in a safe operating mode in the event of a failure
Failure	[IEEE610.12-1990] The inability of a system or component to perform its required functions within specified performance requirements
Failure mode	[IEEE 610.12-1990] The physical or functional manifestation of a failure. For example, a system in failure mode may be characterised by slow operation, incorrect outputs, or complete termination of execution
Failure testing	[IEEE 610.12-1990] To test the functions of a target system by inducing relevant failures in the system in order to verify compliance with the stated requirements
Fault tolerance	[IEEE 610.12-1990] The ability of a system or component to continue normal operation despite the presence of hardware or software faults, or the number of faults a system or component can withstand before normal operation is impaired
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
Functional testing	[IEEE 610.12-1990] Testing that ignores the internal mechanism of a system or component and focuses only on the outputs generated in response to selected inputs and execution conditions
Gap analysis	A gap analysis is "a methodical investigation throughout the whole area of a given technology to identify 'gaps', thus highlighting those areas in existing technology that are inadequate and open to speculation, with a view to improvement". The most useful time to carry out a gap analysis is on the draft revision of the FMEA when it is submitted to the vessel owner for review prior to class for approval
Hidden fault	[ISO 14224, 3.24] A hidden fault is a failure that is not immediately evident to operations and maintenance personnel
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
Interface	[IEEE 610.12-1990] A shared boundary across which information is passed or a component which connects two or more other components for the purpose of passing information from one to the other
Loss of position	A DP vessel has experienced a loss of position when the vessel is outside of its pre-determined positional limits whether it is stationary over a geographic point on the sea bed, in motion along a pre-determined track or following a remote operated vehicle (ROV). It also occurs when a vessel's heading angle varies from its desired heading beyond a pre-defined limit

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
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)
Mean time to repair (MTTR)	The statistical mean of the distribution of times-to-repair. The accumulation of active repair times during a given period divided by the number of malfunctions during the same interval of time
Median	That value such that 50% of the values in question are greater and 50% less than it
Mutually independent	System B is independent of system A when any single system failure occurring in system A has no effect on the maintained operation of system B. Two systems are mutually independent when a single system failure occurring in either of the systems has no consequences for the maintained operation of the other system
Occurrence	[Oxford English Dictionary] 1. Occurrence is the fact or frequency of something occurring. 2. An incident or event
Parameter	[IEEE 610.12-1990] A variable that is given a constant value for a specified application
Post failure DP capability	The remaining DP capability following any failure mode
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
Redundancy	The ability of a component or system to maintain or restore its function when a single failure has occurred. Redundancy can be achieved, for instance, by installation of multiple components, systems or alternative means of performing a function. In fault tolerance, redundancy is the presence of auxiliary components in a system to perform the same or similar functions as other elements for the purpose of preventing or recovering from failures
Redundancy concept	[DNV-RP-E307] The redundancy concept is the means by which the worst case failure design intent is assured
Redundant equipment group	One of a number of groups of components with each group performing the same function. One group will become unavailable when subjected to a single failure but the overall function will not be lost as one of the other groups will continue to perform the function. Redundancy groups will emerge as a consequence of the worst case single failure within each group. There are no limits (above 2) to the number of redundancy groups within an overall system, however, the groups will be identified in the FMEA and confirmed by FMEA testing
Reliability	[IEEE 610.12-1990] The ability of a system or component to perform its required function under stated conditions for a specified 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

Robustness	[IEEE 610.12-1990] The degree to which a system or component can function correctly in the presence of invalid inputs or stressful environmental conditions
Severity	Severity is an assessment of how serious the effect of the potential failure mode is on the overall system or process
Single point failure	A part of a system that, if it fails, will prevent the entire system from working as intended
Standby redundancy	The use of redundant elements that are left inoperative until a failure occurs in a primary element, i.e. not active but available to take over if the one functioning fails (see active redundancy)
Static component	A component which does not require an external source for operation and is characterised by inactivity, e.g. cables, pipes, manual valves, etc.
System	[IEEE 610.12-1990] A collection of components organized to accomplish a specific function or set of functions
Task appropriate mode (TAM)	TAM is a risk-based operating mode in which the DP vessel may be set up and operated, accepting that a single point failure could result in exceeding the vessel's identified worst case failure. TAM is usually applied to less critical activities where a risk assessment determines that the consequences of exceeding the vessel's identified worst case failure are acceptable
Top down	[IEEE 610.12-1990] Pertaining to an activity that starts with the highest level component of a hierarchy and proceeds through progressively lower levels
Validation	Validation is concerned with checking that the system will meet the customer's actual needs, i.e. is the right product being produced?
Verification	Verification is concerned with whether or not the system is well-engineered and error-free, i.e. is the product being produced right?
Verification and validation	[IEEE 610.12-1990] The process of determining whether or not the requirements for a system or component are complete and correct, the products of each development phase fulfil the requirements or conditions imposed by the previous plan and the final system or component complies with specified requirements
Worst case failure (WCF)	[DNV-RP-E307] The WCF is the identified single failure mode in the DP system resulting in maximum effect on DP capability as determined through FMEA study
Worst case failure design intent (WCFDI)	[DNV-RP-E307] The WCFDI is the single failure with the maximum consequences that has been the basis of the design and operational conditions. This usually relates to a number of thrusters and generators that can simultaneously fail

Abbreviations

ABS	American Bureau of Shipping
ASOG	Activity specific operating guidelines
AVR	Automatic voltage regulator
BSI	British Standards Institution
BV	Bureau Veritas
CAMO	Critical activity mode of operation
CAT	Customer acceptance test
CCR	Central control room
CFR	US Code of Federal Regulations
DEn	UK Department of Energy
DGPS	Differential Global Positioning System
DNV GL	Det Norske Veritas/Germanischer Lloyd
DP	Dynamic positioning
DPO	DP operator
DPVOA	DP Vessel Owners Association
DVTP	Design verification test procedure
ECR	Engine control room
EMC	Electromagnetic compatibility
ESD	Emergency shutdown
ET/ETO	Electrotechnical officer
F&G	Fire and gas system
FAT	Factory acceptance test
FMEA	Failure modes and effects analysis
FMECA	Failure modes, effects and criticality analysis
FO	Fuel oil
FSOG	Field specific operating guidelines
FTA	Fault tree analysis
GA	General arrangement
GLONASS	Global Navigation Satellite System (Russian)
GNSS	Global Navigation Satellite System
GPS	Global Positioning System (USA)
HAZID	Hazard identification study
HAZOP	Hazard and operability study
HIL	Hardware-in-the-loop (testing)
HPR	Hydroacoustic position reference system
HSC	High speed craft
HSE	UK Health & Safety Executive
HS&E	Health, safety and the environment
HV	High voltage (1kV and above in marine terms)
HVAC	Heating, ventilation and air conditioning
IACS	International Association of Classification Societies
INS	Inertial navigation system

IAS	Integrated automation system
IEC	International Electrotechnical Commission
IMCA	International Marine Contractors Association
I/O	Inputs/outputs (computer based system)
IMO	International Maritime Organization
IOGP	International Association of Oil & Gas Producers
ISO	International Organization for Standardization
ISDS	Integrated software dependent system
ISQM	Integrated software quality management guide
LNG	Liquefied natural gas
LO	Lubricating oil
LR	Lloyd's Register
LV	Low voltage (below 1kV in marine terms)
MEGI	Main engine gas injection
MMI	Man machine interface
MODU	Mobile offshore drilling unit
MOU	Mobile offshore unit
MRU	Motion reference unit
MSC	Maritime Safety Committee (IMO)
MSF	Marine Safety Forum
MTS	Marine Technology Society
NCR	Non conformance report
NI	Nautical Institute
NMD	Norwegian Maritime Directorate
OF	Over frequency
OIM	Offshore installation manager
OS	Operator station
OSV	Offshore support vessel
OV	Over voltage
P&ID	Process and instrumentation diagram
PLC	Programmable logic controller
PMS	Power management system
PRS	Position reference system
PSU	Power supply unit
QA	Quality assurance
QC	Quality control
QFA	Qualitative failure analysis
QMS	Quality management system
QRA	Qualitative and quantitative risk assessment
RAM	Reliability, availability and maintainability
RBD	Reliability block diagram
RBI	Risk based inspection
RCM	Reliability centred maintenance
RO	Recognised Organisation

SAE	US Society of Automotive Engineers
SMO	Safest mode of operation
SMS	Safety management system
STCW	Standards of Training, Certification and Watchkeeping for Seafarers
SV	Systems verification
SWIFT	Structured 'what if?' analysis
TAM	Task appropriate mode
TQ	Technical query
UF	Under frequency
USCG	United States Coast Guard
UV	Under voltage
VAr	Volt-ampere reactive
VFD	Variable frequency drive
VMS	Vessel management system
VRS	Vertical reference sensor
WCF	Worst case failure
WCFDI	Worst case failure design intent
WSOG	Well specific operating guidelines