



# **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**



# **Review of methods for demonstrating redundancy in dynamic positioning systems for the offshore industry**

**John Spouge**  
DNV Consulting  
Palace House  
3 Cathedral Street  
London  
SE1 9DE

This report reviews the current approach to demonstrating redundancy on offshore vessels with dynamic positioning (DP) systems, in order to establish whether it meets the requirements for suitable and sufficient risk assessment. The review covers the relevant formal requirements and guidelines, recent incident experience, failure modes and effects analyses (FMEAs) and trials reports, consultations with stakeholders in the industry, and a review of approaches used in other industries. It concludes that the current approach is appropriate in principle, although there are several areas of weakness in the way it is applied in practice. In order to make more effective use of FMEAs, the report recommends that management guidance should be developed, to provide an industry standard for how FMEAs of DP systems should be specified, managed, performed, verified and updated. Meanwhile, specific recommendations are made to each stakeholder on some of the key issues that would eventually be covered in the management guidance.

This report and the work it describes were funded by the Health and Safety Executive (HSE). Its contents, including any opinions and/or conclusions expressed, are those of the authors alone and do not necessarily reflect HSE policy.

© *Crown copyright 2004*

*First published 2004*

ISBN 0 7176 2814 0

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written permission of the copyright owner.

Applications for reproduction should be made in writing to:  
Licensing Division, Her Majesty's Stationery Office,  
St Clements House, 2-16 Colegate, Norwich NR3 1BQ  
or by e-mail to [hmsolicensing@cabinet-office.x.gsi.gov.uk](mailto:hmsolicensing@cabinet-office.x.gsi.gov.uk)

## ACKNOWLEDGEMENTS

As part of this work, the author gathered views from the key stakeholders listed in Table 1. Their contributions are gratefully acknowledged. The summary views expressed in the report are nevertheless the author's own.

**Table 1** Stakeholders consulted

<i>Group</i>	<i>Organisation</i>	<i>Contact</i>
Vessel operators	Subsea 7	Pete Sumner, Geoff Morris
	Technip-Coflexip	Steve Woodward, Brian Robertson
	Well-Ops	Graeme Alexander
Operators' association	IMCA	Jane Bugler
Consultants	Poseidon Maritime	Peter Napier
	Global Maritime	Chris Jenman
	DNV Consulting	Odd Fagerjord
	Independent	Holger Røkeberg
Classification societies	DNV	Knut-Helge Knutsen, Aleks Carlsen
	ABS	Cheung Wing Fo
	Lloyds Register	Peter Huntly-Hawkins
DP system suppliers	Kongsberg Maritime	Frank Maclean, Svein Solbakken
	Alstom	Bruce Kauffman
Field operators	Statoil	Geir Brandal
	Shell Expro	Frederic Fokkelman
Regulators	HSE-OSD	Max English, Peter Mills, Norman Turner
	NMD	Kjersti Høgestøl



# CONTENTS

## EXECUTIVE SUMMARY

<b>1. INTRODUCTION.....</b>	<b>1</b>
1.1 BACKGROUND.....	1
1.2 OBJECTIVES.....	1
1.3 REPORT STRUCTURE .....	1
1.4 INDEPENDENCE .....	2
<b>2. DP SYSTEMS.....</b>	<b>3</b>
2.1 DEFINITIONS.....	3
2.2 APPLICATION OF DP .....	3
2.3 DP VESSEL OPERATIONS .....	4
2.4 HAZARDS FROM DP .....	4
2.5 RISKS OF POSITION-KEEPING FAILURE .....	5
<b>3. FORMAL REQUIREMENTS AND GUIDELINES.....</b>	<b>6</b>
3.1 SAFETY PHILOSOPHY .....	6
3.1.1 <i>Historical Development.....</i>	<i>6</i>
3.1.2 <i>IMO Guidelines.....</i>	<i>6</i>
3.1.3 <i>HSE Requirements.....</i>	<i>6</i>
3.1.4 <i>Classification Society Requirements.....</i>	<i>7</i>
3.1.5 <i>IMCA Guidelines.....</i>	<i>8</i>
3.2 THE ROLE OF FMEA.....	8
3.2.1 <i>DNV Requirements.....</i>	<i>8</i>
3.2.2 <i>ABS Requirements.....</i>	<i>9</i>
3.2.3 <i>LR Requirements.....</i>	<i>9</i>
3.2.4 <i>IMCA Guidance.....</i>	<i>10</i>
3.3 GUIDANCE ON FMEA PRACTICE .....	11
3.3.1 <i>Sources of Guidance.....</i>	<i>11</i>
3.3.2 <i>Key Elements of FMEAs.....</i>	<i>11</i>
3.4 SITE-SPECIFIC RISK ANALYSIS .....	12
3.4.1 <i>IMO Guidelines.....</i>	<i>12</i>
3.4.2 <i>NMD Requirements.....</i>	<i>12</i>
3.4.3 <i>NORSOK Standard.....</i>	<i>12</i>
3.5 DP TRIALS.....	13
3.5.1 <i>IMO Guidelines.....</i>	<i>13</i>
3.5.2 <i>DNV Requirements.....</i>	<i>13</i>
3.6 TYPE APPROVAL OF DP SYSTEMS .....	14
3.7 QUALITY CONTROL OF SOFTWARE.....	14
<b>4. REDUNDANCY DEMONSTRATIONS IN PRACTICE .....</b>	<b>15</b>
4.1 DP FAILURE INCIDENTS .....	15
4.2 STAKEHOLDER INPUTS.....	15
4.3 FMEAS.....	17
4.4 SITE-SPECIFIC RISK ANALYSIS .....	18
4.5 DP TRIALS.....	18
<b>5. APPROACHES IN OTHER INDUSTRIES.....</b>	<b>20</b>
5.1 INTRODUCTION.....	20
5.2 SHIP PROPULSION.....	20

5.3	HIGH-SPEED MARINE CRAFT .....	20
5.4	CIVIL AIRCRAFT SYSTEMS.....	21
5.5	ELECTRICAL SAFETY-RELATED SYSTEMS .....	22
5.6	MILITARY PROGRAMMABLE SYSTEMS.....	23
<b>6.</b>	<b>EVALUATION OF CURRENT APPROACHES.....</b>	<b>25</b>
6.1	KEY QUESTIONS .....	25
6.2	WHAT IS A REDUNDANT DP SYSTEM? .....	25
6.2.1	<i>Redundancy</i> .....	25
6.2.2	<i>DP System Failures</i> .....	25
6.2.3	<i>Single Point Failures</i> .....	26
6.2.4	<i>Common Cause Failures</i> .....	26
6.3	WHY FOCUS ON REDUNDANCY? .....	27
6.3.1	<i>How Does Redundancy Affect Risks?</i> .....	27
6.3.2	<i>Is Redundancy Sufficient to Manage Risks?</i> .....	27
6.3.3	<i>Is There a Better Approach?</i> .....	28
6.3.4	<i>What Level of Redundancy is ALARP?</i> .....	28
6.4	IS FMEA THE RIGHT TECHNIQUE? .....	29
6.4.1	<i>How Can Redundancy be Demonstrated?</i> .....	29
6.4.2	<i>Is FMEA a Suitable Technique?</i> .....	29
6.4.3	<i>Would Other Techniques be Preferable?</i> .....	30
6.5	IS FMEA USED IN THE RIGHT WAY?.....	30
6.5.1	<i>Evaluation Criteria</i> .....	30
6.5.2	<i>Integration in Safety Management</i> .....	31
6.5.3	<i>Objectives</i> .....	31
6.5.4	<i>Classification Rules</i> .....	32
6.5.5	<i>FMEA Guidance</i> .....	32
6.5.6	<i>Competence of FMEA Practitioners</i> .....	32
6.5.7	<i>Integration of Component FMEAs</i> .....	33
6.5.8	<i>Integration with DP Trials</i> .....	34
6.5.9	<i>Integration with Ongoing Operations</i> .....	34
6.5.10	<i>Use of Incident Experience</i> .....	34
6.5.11	<i>Independent Review</i> .....	35
<b>7.</b>	<b>CONCLUSIONS.....</b>	<b>36</b>
7.1	OBSERVATIONS .....	36
7.2	RECOMMENDATIONS .....	37
7.2.1	<i>IMCA</i> .....	37
7.2.2	<i>Vessel Operators</i> .....	37
7.2.3	<i>Classification Societies</i> .....	38
7.2.4	<i>Consultants</i> .....	38
7.2.5	<i>DP System and Vessel Equipment Suppliers</i> .....	39
7.2.6	<i>HSE</i> .....	39
<b>8.</b>	<b>REFERENCES .....</b>	<b>40</b>
<b>APPENDIX I</b>	<b>INCIDENT DESCRIPTIONS .....</b>	<b>41</b>
I.1	INTRODUCTION .....	41
I.2	INCIDENT 1 .....	42
I.2.1	<i>Operational Status</i> .....	42
I.2.2	<i>The Incident</i> .....	42
I.2.3	<i>Conclusions as to Cause</i> .....	42
I.2.4	<i>Recommendations</i> .....	44

I.3 INCIDENT 2.....	46
<i>I.3.1 Operational Status</i> .....	46
<i>I.3.2 The Incident</i> .....	46
<i>I.3.3 Conclusions as to Cause</i> .....	46
<i>I.3.4 Recommendations</i> .....	47
I.4 INCIDENT 3.....	48
<i>I.4.1 Operational Status</i> .....	48
<i>I.4.2 The Incident</i> .....	48
<i>I.4.3 Conclusions as to Cause</i> .....	48
I.5 CONCLUSIONS.....	49



# **EXECUTIVE SUMMARY**

## **Objectives**

This study reviews the state of the art for demonstrating redundancy in dynamic positioning systems in the UK offshore industry, and recommends improvements in order to meet the requirements of the Health and Safety Executive for suitable and sufficient risk assessment.

## **Dynamic Positioning**

Dynamic positioning (DP) is a capability of a vessel to maintain its position automatically using thrusters. In the offshore industry it is used on diving support vessels, pipelay vessels, shuttle tankers, platform supply vessels etc. The DP system is the complete installation necessary for dynamically positioning a vessel, including the vessel's power system, thruster system and the DP control system.

## **Current Requirements**

The International Maritime Organization (IMO) "Guidelines for Vessels with DP Systems" specify three equipment classes:

- Class 1 – no redundancy.
- Class 2 – redundancy of all active components.
- Class 3 – redundancy and physical separation of all components.

For any given activity, the equipment class is usually chosen following industry common practice. For each equipment class, the IMO Guidelines and classification rules provide details on precisely what redundancy is required. They require a failure modes and effects analysis (FMEA) to demonstrate that the DP system design meets the required level of redundancy, together with a practical demonstration through trials.

## **General Approach**

DNV Consulting has reviewed the state of the art for demonstrating redundancy in DP systems in the UK offshore industry. The review covered the relevant formal requirements and guidelines, recent incident experience, actual FMEA studies and trials reports, consultations with stakeholders in the industry, and a review of approaches used in other industries.

## **Strengths and Weaknesses**

The main strengths in the current system are:

- A demonstration that a DP system is redundant is a suitable method of verifying its inherent safety, i.e. the measures adopted during design to reduce vulnerability to failures.
- The FMEA technique is suitable for demonstrating redundancy in principle, providing it is applied correctly.
- The trials are a suitable practical demonstration of the redundancy in the design.
- An additional benefit of FMEA is in training DP operators and technicians. It provides an integrated description of the DP system and its main failure modes, which is not available in any other document.

Several weaknesses have been identified:

- When FMEA is used to demonstrate that no critical single point failures can occur, there is a danger that failures may be overlooked.
- The definition of redundancy in the IMO Guidelines leaves unclear how common cause failures should be treated.
- Many FMEAs do not follow a systematic procedure for considering all relevant failure modes.
- Most FMEAs make little use of guidance documents on good practice.
- The quality of FMEAs and DP trials relies on the expertise of the personnel conducting them. Study team expertise is not usually documented.
- FMEAs of DP systems require a multi-disciplinary team to give adequate coverage of mechanical, electrical and electronic equipment.
- FMEAs mainly address technical failures. The human operator and the shore management are excluded from the definition of the DP system.
- There is sometimes a lack of information about the failure modes of bought-in systems such as DP control systems and power management systems.
- There is little use of site-specific risk analysis to select the equipment class.
- It is well known that some vessels are not operated in the way that is assumed in their FMEA.
- FMEAs of new-buildings are often commissioned too late to influence the design.
- Review of FMEAs by classification societies is sometimes not thorough. They often do not receive the reports early enough, and cannot justify delaying the trials.
- The 3 actual cases of loss of position through DP failure on the UKCS in 2002 revealed deficiencies in the designed redundancy, which more thorough FMEAs and trials programmes might have detected and highlighted for corrective action.

Despite these critical observations, most stakeholders believe that the FMEA approach is appropriate in principle, and needs improvements in practices rather than fundamental change.

## **Recommendations**

In order to make more effective use of FMEAs, it is recommended that management guidance should be developed, to provide an industry standard for how FMEAs of DP systems should be specified, managed, performed, verified and updated. This would not duplicate the existing IMCA guide on FMEAs, but would reference it. The new guide would be aimed at managers more than practitioners, providing specific, auditable standards rather than advice. It should be developed through IMCA, in association with manufacturers, classification societies and regulators, in order to ensure that all stakeholders see it as a common standard. Meanwhile, this report includes specific recommendations to each stakeholder on some of the key issues that would eventually be covered in the management guidance.

# 1. INTRODUCTION

## 1.1 BACKGROUND

Dynamic positioning (DP) systems are normally designed to meet classification rules, which are based on guidelines issued by the International Maritime Organization (IMO). The IMO Guidelines expect the appropriate level of DP system redundancy to be selected using a site-specific risk analysis of the consequences of loss of position. The classification societies require a failure modes and effects analysis (FMEA) to demonstrate that the DP system design meets the required level of redundancy. The FMEA is validated through trials.

For installations on the UK Continental Shelf (UKCS), the Health and Safety Executive (HSE) Offshore Safety Division requires operators to use suitable and sufficient risk assessment to demonstrate that risks have been made as low as reasonably practicable. For DP systems, this is normally satisfied by an FMEA and trials.

Three incidents of position keeping failure occurred on the UKCS within a 6-week period in 2002. Two of these involved DP systems meeting Class 3 in the IMO Guidelines, which is the highest level of redundancy. Although no lives were lost, the incidents could have been more severe. The incidents involved failure modes that the vessels' FMEAs had not identified.

In view of its concern that current approaches to demonstrating DP system redundancy may not meet the requirements of suitable and sufficient risk assessment, HSE commissioned DNV Consulting to review the state of the art and identify any necessary improvements.

## 1.2 OBJECTIVES

The objectives of the study are:

- To review the state of the art for demonstrating the level of redundancy in DP systems for the UK offshore industry.
- To evaluate whether current practices meet the requirements for suitable and sufficient risk assessment, taking account of recent incident experience, available risk assessment techniques, and practices in other industries.
- To recommend any necessary improvements to current approaches and any additional work required to achieve acceptable DP system reliability.

## 1.3 REPORT STRUCTURE

Section 2 of this report provides a definition of DP systems and a brief review of the factors that influence the risks of DP failure.

Section 3 reviews the relevant formal requirements and guidelines that are used by IMO and the offshore industry to define the role of FMEA and trials.

Section 4 summarises the inputs that have been made to the present study concerning the state of the art in practice. This includes a review of sample FMEAs that have been provided, discussions with stakeholders in the industry, and a review of actual incidents and the lessons that can be drawn from them. Further details on the incidents are given in Appendix I.

Section 5 reviews other approaches that might be used, based on what is done in other industries.

Section 6 gives a critical review of the state of the art, asking whether FMEA is appropriate in theory and in practice, and whether there are better techniques, in order to explore whether the current practices meet the requirements of suitable and sufficient risk assessment.

Section 7 summarises the observations about the strengths and weakness of the current practices, and recommends appropriate improvements.

#### **1.4 INDEPENDENCE**

DNV Consulting is an independent business area within Det Norske Veritas (DNV). As part of its marine and offshore classification activities, DNV also issues rules for DP systems and certifies vessels for compliance with these requirements. DNV recognises the need for continuous improvements to enhance safety, and believes that its classification activities place no constraint or bias on the ability of DNV Consulting to produce an independent and impartial evaluation of the state of the art. The report author has 16 years' experience in risk assessment, but has not been involved in writing or approving FMEAs prior to this study.

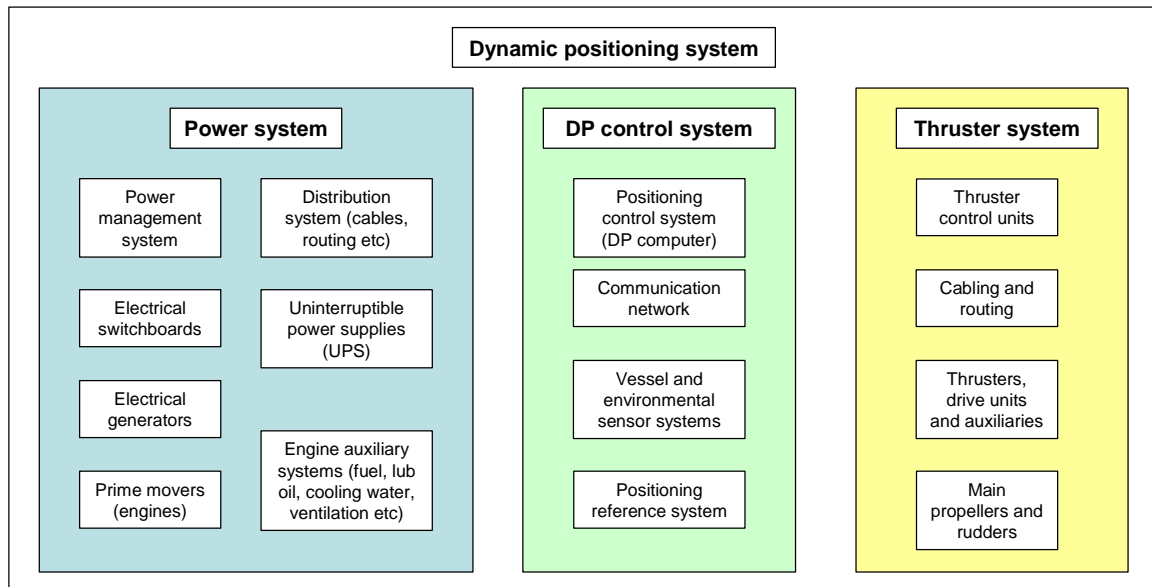
## 2. DP SYSTEMS

### 2.1 DEFINITIONS

**Dynamic positioning (DP)** is a capability of a vessel to automatically maintain its position using thrusters. This usually includes the vessel's heading as well as its location. It may maintain a fixed location or follow a pre-determined track.

In practice, a floating vessel cannot maintain a completely static position at sea. For practical purposes, position-keeping means maintaining a desired position and heading within limits that reflect the environmental forces and system capability.

The **DP system** is the complete installation necessary for dynamically positioning a vessel. Its main sub-systems are the power, thruster and DP control systems (Figure 1).



**Figure 1** DP System Components

These definitions are based IMO (1994), and are focussed on technical hardware, as is normal for an FMEA. However, a comprehensive evaluation of a DP system should include all elements with the potential to impair the vessel's position keeping. It should therefore consider the operators, as well as the vessel compartments in which the system elements are contained. This broader definition goes beyond that in the IMO Guidelines, and also beyond the normal scope of classification rules, although in practice the IMO Guidelines do consider single inadvertent acts. The definitions would be appropriate to consider in a future review of the IMO Guidelines, but this is outside the scope of the present study.

### 2.2 APPLICATION OF DP

DP vessels are used for a wide variety of purposes in the offshore industry. The main vessel types are:

- Diving support vessels (DSVs).

- Drilling vessels, including drill ships, semi-submersible drill rigs.
- Well stimulation and workover vessels etc.
- Floating production units
- Accommodation vessels (flotels)
- Crane vessels
- Shuttle tankers
- Pipelay, cable-lay and cable-repair vessels
- Dredging and rock-dumping vessels
- Remotely operated vehicle (ROV) support vessels
- Platform supply vessels and anchor-handling vessels

The present project aims to cover the application of FMEA to any of these vessel types.

### **2.3 DP VESSEL OPERATIONS**

Some features of DP vessel operations significantly influence the type of safety management that can be adopted:

- DP vessels mainly follow marine safety principles, which are intended to facilitate international competition while ensuring acceptable common safety standards. Overall safety principles are agreed internationally at the International Maritime Organization (IMO). Detailed structural, mechanical and electrical requirements are established by independent classification societies, who also survey vessels during construction and periodically in operation to ensure compliance. Formal regulatory oversight is provided by national administrations. In the UK, this is the Maritime and Coastguard Agency, which has a Memorandum of Understanding with HSE on offshore safety issues.
- DP vessels may be sold between owners, and hence the current operator may not have been involved in their design and construction, or in developing the safety documentation.
- DP vessels are mobile and so may operate in different countries under different regulatory regimes, and may be forced to change key DP personnel.
- There are relatively few DP vessels of each type, and even nominally similar vessels often differ in the specific DP system configuration.
- DP has been used for over 35 years, but in the last 10 years the technology has developed rapidly.

### **2.4 HAZARDS FROM DP**

The primary hazard from a DP system is of course “position-keeping failure”, i.e. failure to keep within critical limits for position and/or heading. In some operations, such as heavy lift, very stable and accurate position-keeping is needed, and so for these the hazard of “position instability” is also relevant.

In a full study of DP safety, various other hazards might also be considered, including occupational hazards to people working on or around the DP system, such as electrocution, fumes from electrical fires, danger to divers’ umbilicals from thrusters etc. However, these are not covered by the demonstration of redundancy, and are outside the scope of the present study.

Many cases of position-keeping failure are triggered by a technical failure in the DP system. Hence “DP system failure” is sometimes considered a hazard equivalent to “position-keeping failure”. However, it is also possible for loss of position to be triggered by operator error, while the system remains fully functional. If the DP system is defined broadly, including the operator, then such human errors can also be considered system failures.

## **2.5 RISKS OF POSITION-KEEPING FAILURE**

The “risk” from position-keeping failure means the combination of its likelihood and consequences. Comprehensive risk management necessarily requires consideration of both elements, as follows.

The consequences of position-keeping failure depend on:

- The type of operation that is in progress. In the case of diving support, position-keeping failure may result in death or injury of the divers underwater. In the case of operations close to a fixed structure, it may result in collision and possible loss of the vessel or structure. In other operations, it may result in damage to equipment, or simply delay in the operation. Hence, some DP operations are more safety-critical than others.
- The nature of the DP failure, i.e. whether quickly recoverable or not; whether involving uncontrolled drift or active propulsion in the wrong direction etc. Clearly, some failures are worse than others.
- The prevailing environmental conditions. In perfectly calm weather, a DP failure will not necessarily lead to a position-keeping failure. In severe weather, position-keeping failure can occur much more quickly, and the consequences are likely to be much greater than from an equivalent failure in more moderate conditions.

The likelihood of position-keeping failure may be the frequency per unit time in a continuous DP operation, or the probability given a specific discrete operation. It depends on:

- The inherent safety of the DP system design. “Inherent safety” means measures adopted during design to reduce vulnerability to failures (HSE 1999). In this context, it includes the way the DP system is installed on the vessel. The effectiveness of the design in preventing position-keeping failure may be measured in terms of reliability. In turn this is closely related to the redundancy of the design (defined in Section 6.2 below).
- The operational tasks and the standard of operator performance.
- The quality of safety management (training, procedures, maintenance etc).

When a DP vessel is designed, only the first of these can be specified. Hence, the DP system design naturally tends to focus on ensuring adequate redundancy. The adequacy of this is discussed in Section 6.3 below. The importance of operator performance and safety management are recognised but are outside the scope of this study.

## 3. FORMAL REQUIREMENTS AND GUIDELINES

### 3.1 SAFETY PHILOSOPHY

#### 3.1.1 Historical Development

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 in 1991 (see Section 3.1.5 below). It was developed into an international standard by IMO in 1994 (see Section 3.1.2). Classification society requirements have since been adjusted for consistency with this (Section 3.1.4), as have the NMD requirements (Section 3.4.2).

#### 3.1.2 IMO Guidelines

The International Maritime Organization's "Guidelines for Vessels with Dynamic Positioning Systems" (IMO 1994) provide an international standard approach to achieving acceptable reliability of position keeping. They define three "equipment classes", which are in practice different levels of redundancy, and allow the vessel owner to select the appropriate class based on the consequences of loss of position, as determined by a risk analysis. The three equipment classes are:

- Equipment class 1 – loss of position may occur in the event of a single fault.
- Equipment class 2 – loss of position should not occur from a single fault of an active component or system (e.g. generators, thrusters, switchboards, remote controlled valves etc). This includes a single inadvertent act by a person on board, if it is reasonably probable. However, loss of position may occur from the failure of a static component such as cables, pipes, manual valves etc, provided it has adequately documented protection and reliability.
- Equipment class 3 – loss of position should not occur from any single fault of an active component or system, any single failure of a static component, any single inadvertent act, fire or flooding in any one fire sub-division or watertight compartment.

In effect, these classes require the following levels of redundancy:

- Equipment class 1 – no redundancy.
- Equipment class 2 – redundancy of all active components.
- Equipment class 3 – redundancy and physical separation of all components.

The IMO Guidelines provide clarification on precisely what redundancy is expected in each case for each sub-system. They require a practical demonstration through testing (see section 3.5), but they do not require an FMEA.

#### 3.1.3 HSE Requirements

The Health & Safety at Work etc Act 1974 (HSWA) provides the foundation of offshore safety regulations on the UKCS. It imposes on an employer a duty "to ensure, so far as is reasonably practicable, the health, safety and welfare at work of all his employees" and "to conduct his

*undertaking in such a way as to ensure, so far as is reasonably practicable, that persons not in his employment who may be affected thereby are not exposed to risks to their health and safety”* (Sections 2 and 3).

The HSWA also imposes similar duties on manufacturers. In the case of a DP vessel, this duty may be transferred to the operator once they bring a foreign-built vessel into UK waters. In particular, it requires “*any person who undertakes the design or manufacture of any article for use at work to carry out or arrange for the carrying out of any necessary research with a view to the discovery and, so far as is reasonably practicable, the elimination or minimisation of any risks to health or safety to which the design or article may give rise*” (Section 6).

The Management of Health and Safety at Work Regulations 1992 (MHSWR) support the general duties under HSWA by requiring employers to undertake risk assessment for the purpose of identifying the measures that need to be put in place to prevent accidents and protect people against accidents.

The Offshore Installations (Safety Case) Regulations 1992 (SCR) require the duty holder (i.e. the owner or operator) for each fixed and mobile installation to prepare a safety case, which must be accepted by the HSE before the installation can be operated on the UKCS. Safety cases are required for some DP vessels (e.g. flotels, drill rigs, floating production units) but not others (e.g. DSVs, crane vessels, shuttle tankers). SCR does not include “loss of position” among the major hazards that it addresses explicitly.

HSE’s oversight focuses on vessels that are required to produce safety cases, and does not prioritise DP vessels such as DSVs and crane vessels, where the risks may be higher. This focus is a result of the boundaries of the SCR, and ultimately of the concerns expressed in the Cullen Inquiry into the *Piper Alpha* accident.

### **3.1.4 Classification Society Requirements**

The classification societies Det Norske Veritas (DNV), Lloyd’s Register of Shipping (LR), American Bureau of Shipping (ABS) and Bureau Veritas (BV) issue requirements in the form of class notations for DP vessels. These implement the IMO Guidelines, with more specific requirements, and specify the documentation that must be provided for approval, and specify the scope of testing.

Each classification society’s requirements differ slightly, and each awards different notations, but they correspond roughly to the IMO equipment classes as shown in Table 2. The differences are not significant for the present study.

**Table 2** Classification Society DP Notations

<i>IMO Equipment Class</i>	<i>DNV</i>	<i>LR</i>	<i>ABS</i>
Class 1	DYNPOS-AUT	DP(AM)	DPS-1
Class 2	DYNPOS-AUTR	DP(AA)	DPS-2
Class 3	DYNPOS-AUTRO	DP(AAA)	DPS-3

Among the required documentation for class notations equivalent to IMO equipment classes 2 and 3 is an FMEA. This is discussed in Section 3.2 below.

### 3.1.5 IMCA Guidelines

The International Marine Contractors Association’s “Guidelines for the Design and Operation of Dynamically Positioned Vessels” (IMCA 1999) define industry good practice for different types of vessels, including guidance on how to achieve acceptable redundancy. The guidelines were first published in 1991, but have since been updated to reflect industry practice.

They specify a philosophy that the DP system should reliably keep the vessel within half of a defined critical excursion. Reliable is defined as having hardware or software faults causing an interruption in position control less than once in 4000 DP operating hours. Critical excursion is defined as a movement that could injure personnel or cause substantial damage to equipment.

Safe working limits should be defined for each operational task and geographical location. These should take account of all possible failure modes, and the associated time to restore the DP system or cease work to prevent serious consequences. The safe working limits are defined as environmental limits within which a critical excursion from a single fault is very unlikely.

Most of the IMCA guidelines consist of more practical advice on how to achieve acceptable redundancy, communications, alerts and personnel responsibilities on different types of DP vessels.

This type of numerically defined philosophy is much more explicit than the equipment classes in the IMO Guideline, but the IMCA guideline does not indicate how to meet it, and does not attempt to link the more specific requirements to the reliability target. Stakeholder responses indicate that in practice this approach is not normally used. Nevertheless, it is a target that is met by many well operated vessels.

## 3.2 THE ROLE OF FMEA

### 3.2.1 DNV Requirements

The requirements for FMEA of DP systems in the DNV rules are stated in full in Table 3. The requirement for FMEA was introduced in 2001, when the rules were changed for consistency with the IMO Guidelines.

**Table 3** DNV requirements for FMEA of DP systems

<p>Rules for Classification of Ships <b>Part 6, Chapter 7: Dynamic Positioning Systems</b> <b>Section 1: D 600 Failure mode and effect analysis (FMEA)</b> 601 For vessels with the notations <b>AUTR</b> and <b>AUTRO</b>, documentation of the reliability of the dynamic positioning system is required in the form of a failure mode and effect analysis (FMEA). 602 The purpose of the FMEA is to give a description of the different failure modes of the equipment when referred to its functional task. Special attention is to be paid to the analysis of systems that may enter a number of failure modes and thus induce a number of different effects on the dynamic positioning system performance. The FMEA is to include at least the information specified in 603 to 605. 603 A breakdown of the dynamic positioning system, into functional blocks is to be made. The functions of each block are to be described. The breakdown is to be performed to such a level of detail that the functional interfaces between the functional blocks are shown. 604 A description of each physically and functionally independent item</p>
---

and the associated failure modes with their failure causes related to normal operational modes of the item is to be furnished.

605 A description of the effects of each failure mode alone on other items within the system and on the overall dynamic positioning system is to be made.

**Guidance note:**  
 Description of FMEA systematic may be found in IEC Publication 60812 and IMO HSC Code, Annex 4.  
 ---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

Although the rules state that the purpose of the FMEA is simply descriptive, in practice it is necessary to demonstrate that the vessel has acceptable redundancy according to the IMO Guidelines.

### 3.2.2 ABS Requirements

The requirements for FMEA of DP systems in the ABS rules are stated in full in Table 4.

**Table 4** ABS requirements for FMEA of DP systems

Rules for Building and Classing Steel Vessels  
**Part 4, Chapter 3, Section 5: Dynamic Positioning Systems**  
**15.1.4 Failure Modes and Effects Analysis**  
 A failure modes and effect analysis (FMEA) is to be carried out for the entire DP system. The FMEA is to be sufficiently detailed to cover all the systems' major components and is to include but not be limited to the following information:

- A description of all the systems' major components and a functional block diagram showing their interaction with each other
- All significant failure modes
- The most predictable cause associated with each failure mode
- The transient effect of each failure on the vessels position
- The method of detecting that the failure has occurred
- The effect of the failure upon the rest of the system's ability to maintain station
- An analysis of possible common failure mode

Where parts of the system are identified as non-redundant and where redundancy is not possible, these parts are to be further studied with consideration given to their reliability and mechanical protection. The results of this further study are to be submitted for review.

Although this does not directly state the purpose of the FMEA, it is evidently the same as in the DNV requirements.

### 3.2.3 LR Requirements

The requirements for FMEA of DP systems in the LR rules are stated in full in Table 5.

**Table 5** LR requirements for FMEA of DP systems

Rules and Regulations for the Classification of a Floating Offshore Installation  
**Part 3, Chapter 9: Dynamic Positioning Systems**  
**1.3 Information and plans required to be submitted**  
 (e) For assignment of **DP(AA)** or **DP(AAA)** notation, a Failure Modes

and Effects Analysis (FMEA) is to be submitted, verifying that the requirements of Sections 4 and 5, as applicable, have been met.

**Section 4: Class notation DP(AA)**

4.1.2 Power, control and thruster systems and other systems necessary for the correct functioning of the DP system are to be provided and configured such that a fault in any active component or system will not result in a loss of position. This is to be verified by means of a FMEA, *see* 1.1.1(e).

**Section 5: Class notation DP(AAA)**

5.1.2 The DP system is to be arranged such that failure of any one component or system necessary for the continuing function of the DP system, or the loss of any one compartment as a result of fire or flooding, will not result in a loss of position. This is to be verified by means of a FMEA, *see* 1.1.1(e).

These rules state the purpose of the FMEA as demonstrating redundancy rather than describing the failure modes. However, in practice, the requirements are little different to those of DNV and ABS.

### 3.2.4 IMCA Guidance

The IMCA “Guidance on Failure Modes & Effects Analyses” (IMCA 2002) includes the statement of objectives shown in Table 6.

**Table 6** IMCA guidance on objectives of FMEA of DP systems

**FAQ: What are the objectives of an FMEA?**

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

**Section 2.3: The FMEA Objectives**

The FMEA should give a description of the different failure modes for all the items of equipment in respect of their functional objectives. In this way, all catastrophic or critical single point failure possibilities can be identified, and either eliminated or minimised at an early stage in the project through design correction or the introduction of clear operational procedures....

Essentially the FMEA is to:

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

This approaches a synthesis of the good points from the different class rules, although the two sections that cover this subject give slightly different perspectives. Its purpose is to inform rather than to specify minimum requirements.

### **3.3 GUIDANCE ON FMEA PRACTICE**

#### **3.3.1 Sources of Guidance**

Guidance on good practice in performing FMEA is available from:

- IMCA “Guidance on Failure Modes & Effects Analyses” (IMCA 2002). This gives detailed guidance (64 pages) specifically for applying FMEA to offshore vessels.
- British Standard BS 5760:Part 5 (BSI 1991). This gives detailed guidance (43 pages) on FMEA/FMECA in general.
- IMO High-Speed Craft Code (IMO 2000) Annex 4. This gives brief guidance (11 pages) on FMEA, focussed on high speed craft but generally relevant.
- MoD Defence Standard 00-41. This gives brief guidance (6 pages) on FMEA/FMECA, focussed on military applications.
- IEC Standard 812 “Analysis Techniques for System Reliability – Procedure for Failure Mode and Effects Analysis”. This was an earlier version of BS 5760:Part 5.
- US Military Standard MIL-STD-1629A “Procedures for Performing a Failure Mode and Effect Analysis”, US Navy 1977. This was the original standard for FMEA.

#### **3.3.2 Key Elements of FMEAs**

Although most of these standards have some elements in common, there are also many differences. Only the IMCA guidance specifically addresses DP systems.

Based on a combination of the guidance material above, a thorough FMEA would be expected to include the following components.

- A statement of the objectives of the study (BS 5760).
- A description of the major functional blocks in the system, sufficient to show their interaction with each other (IMCA, BS 5760, IMO, DNV, ABS).
- A breakdown of the functional blocks into physically and functionally independent elements (IMCA, BS 5760, IMO, DNV).
- Identification of all significant failure modes for each element (IMCA, BS 5760, IMO, DNV, ABS).
- Indication of typical causes of each failure mode (IMCA, BS 5760, IMO, DNV, ABS).
- Description and categorisation of the effects of each failure on other items, on the DP system overall, and on the positioning of the vessel (IMCA, BS 5760, IMO, DNV, ABS).

- Definition of the method of detecting that the failure has occurred (IMCA, BS 5760, IMO, ABS).
- Compensating provisions intended to prevent or correct the failure (IMCA, BS 5760, IMO).
- Consideration of possible common failure modes (IMCA, BS 5760, ABS).
- Study-specific FMEA worksheets (IMCA, BS 5760, IMO).
- Documents and drawings on which the analysis was based (IMCA, BS 5760).
- Relationships of the FMEA with test programme and site-specific risk analysis (IMCA, BS 5760, IMO).
- Conclusions and recommendations, meeting the study objectives (IMCA, BS 5760).

This type of list of critical elements in an FMEA would appear essential for quality checking. However, it is notable that the IMCA guidance has no such list, and that some of the necessary elements are mentioned only in the appendices. This is in contrast to the clear and prominent lists in Section 2.2.3 of BS 5760, Section 6 of the IMO HSC Code and the ABS rules.

### **3.4 SITE-SPECIFIC RISK ANALYSIS**

#### **3.4.1 IMO Guidelines**

The IMO DP Guidelines states a requirement for a site-specific risk analysis as follows. *“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.”* There is no further guidance on what is meant by this risk analysis.

#### **3.4.2 NMD Requirements**

The Norwegian Maritime Directorate (NMD) Regulations of 4 September 1987 No.857 concerning anchoring/positioning systems on mobile offshore units, as amended on 11 April 2003, requires a DP system to satisfy the IMO Guidelines or an equivalent standard. It also states that *“the choice of equipment class shall be based on the consequences that any loss of position may have with regard to the operations which the unit is intended to carry out”*. This implies a relatively simple choice rather than a risk analysis.

#### **3.4.3 NORSOK Standard**

The Norwegian petroleum industry standard on “Marine Operations” (NORSOK 1997) includes guidelines on which of the IMO equipment classes should be selected for different DP operations (see Table 7). Most operations require class 2 or 3.

**Table 7** NORSOK guidelines for DP Equipment Classes

<i>Operation</i>	<i>Equipment Class</i>	<i>Notes</i>
Drilling	3	Applies to all drilling in hot zones
Production of hydrocarbons	3	
Subsea well workover	3	Workover operations entailing hydrocarbons on deck
Wireline operations on subsea wells	2	With subsea lubricator
Well stimulation	2	
Manned subsea operations	3	For diving inside structures etc
Manned subsea operations	2	For diving in open water
Support of diving from light craft	2	When the light craft is attached to the support vessel
Unmanned subsea intervention with ROT	2	Inside hot template
Accommodation vessel with gangway connection to installation	3	
Accommodation vessel outside 500m safety zone	2	
Well stimulation, platform wells	2	
Construction activities in general, inside 500m safety zone	2	
Construction activities in general, outside 500m safety zone	1	

### 3.5 DP TRIALS

#### 3.5.1 IMO Guidelines

The IMO DP Guidelines 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. commissioning trial).
- 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 5 years.
- Tests after a defect is discovered or an accident occurs, to demonstrate full compliance.

The tests should be witnessed by officers of the Flag State Administration, or delegated to recognised organisations such as classification societies.

#### 3.5.2 DNV Requirements

Extracts from the requirements for failure testing in the DNV rules are given in Table 8. In earlier rules, testing was an alternative to FMEA. Now it is required in addition.

**Table 8** DNV requirements for failure testing of DP systems

<p>Rules for Classification of Ships <b>Part 6, Chapter 7: Dynamic Positioning Systems</b> <b>Section 1: E Survey and Test upon Completion</b> <b>E100 General</b> 101 Upon completion, the dynamic positioning system is to be subjected to final tests. The program is to contain test procedures and acceptance criteria.</p> <p><b>E600 Complete DP-system test</b> 101 The complete DP-system is to be tested in all operational modes, with simulation of different failure conditions to try out switching modes, back-up systems and alarm systems.</p> <p><b>E700 Redundancy tests for AUTR and AUTRO</b> 701 A selection of tests within each system analysed in the FMEA is to be carried out. Specific conclusions of the FMEA for the different systems are to be verified by tests when redundancy or independence is required.</p> <p>702 The test procedure is to be based on the simulation of failures and shall be performed under as realistic conditions as possible.</p>
--

### **3.6 TYPE APPROVAL OF DP SYSTEMS**

Type approval is a voluntary qualification offered by classification societies. The certificate of type approval attests that a manufacturer can consistently produce a product conforming to a specific standard.

DP control systems may be type approved or individually approved case by case. Both approaches involve the same requirements, which cover both the hardware and the functionality of the software. The electronic components integrated for DP control functions are also type approved. This concentrates on environmental aspects such as emissions, electromagnetic interface susceptibility etc.

Type approval is primarily a quality standard, which is useful for both owners and vendors. However, it does not give complete assurance that the system will work reliably when integrated. This needs to be reviewed separately. However, the fact the system has been type approved may make it difficult to obtain further information about specific failure modes.

### **3.7 QUALITY CONTROL OF SOFTWARE**

The International Marine Contractors Association's "Guidelines for the Quality Assurance and Quality Control of Software" (IMCA 2001) provide guidance for the quality management of software for use in DP systems. This is based on general guidelines in ISO 9000-3. Classification societies also have requirements related to quality control of software manufacturing.

## 4. REDUNDANCY DEMONSTRATIONS IN PRACTICE

### 4.1 DP FAILURE INCIDENTS

Three actual incidents of DP failure have been reviewed (see Appendix I). In each case, faults in single equipment items led to loss of position on DP Class 2 or 3 vessels. All 3 events occurred within a 6-week period on the UKCS. Two involved failures in the power management system and one in the DP communications network. Two occurred while divers were in the water, and hence formed a significant safety hazard.

In each case an FMEA had been conducted of the DP system, but had failed to identify faults of this type, or any other faults involving loss of position.

All three events involved rather complex faults – erroneous signals, a partial failure, a failure to relinquish control. Hence the failure of the FMEAs to anticipate them may be regarded as understandable. Nevertheless, more specific guidance or checklists would be desirable to prompt consideration of such events in the future.

In all three incidents, the investigation revealed deficiencies in the level of redundancy in the DP systems, which a thorough FMEA and trials programme should have detected and highlighted for corrective action. Thus the incident experience suggests that FMEAs or trials of DP systems have not been sufficiently thorough to ensure adequate redundancy. However, at the time the vessels were built, FMEA was not required by the applicable class rules, and the fact that FMEAs were produced at all indicates a positive attitude to safety.

### 4.2 STAKEHOLDER INPUTS

The stakeholders listed in Table 1 have been consulted regarding their views on the adequacy of current methods for demonstrating DP redundancy.

It is apparent that this is a field that is understood by relatively few people. The majority of stakeholders were not involved in sufficient FMEAs to develop strong opinions about them.

The following points were made about the state of the art:

- The main benefit of FMEAs to vessel owners/managers was in training DP operators and technicians. They provided an integrated description of the DP system and its main failure modes, which was not available in any other document.
- FMEAs of new systems are often commissioned too late to influence the design. They are used to convince the classification society that the design complies with the rules. This discourages a comprehensive and open treatment of failure modes, particularly unlikely common cause failures.
- The FMEA technique is generally considered effective in demonstrating the redundancy level, providing it is applied correctly. Some FMEAs were not sufficiently thorough, due mainly to budgetary constraints.
- FMEAs require detailed understanding of the system design and operation. FMEAs of existing systems are impractical without as-built documentation (design philosophy, drawings, manuals etc), which is sometimes not available and must be recreated.

- Most FMEAs make little use of guidance documents on good practice. They rely on the experience of the author, and tend to follow previous template FMEAs. Tabular worksheets are sometimes omitted.
- A standard approach to FMEA requires a very detailed review of all possible component failure modes. This is not necessary or cost-effective for DP systems. There is no guidance on what is sufficient detail for an FMEA.
- Some authors use available DP incident data as a primary input to the FMEA, but many FMEAs show little evidence of systematic use of incident experience.
- FMEAs of DP systems require a multi-disciplinary team to give adequate coverage of mechanical, electrical and electronic equipment. It is difficult to verify whether sufficient competence has been provided.
- FMEAs address total failures of main equipment, but they are less successful at identifying system faults, common-cause failures and partial failures. Hazard checklists or creative hazard identification techniques are rarely used.
- Available information on bought-in systems (notably vessel management systems) is often inadequate for a full FMEA. The standard of information provided under type approval is very variable.
- Review of FMEAs by classification societies is sometimes not thorough. They often do not receive the reports early enough, and cannot justify delaying the trials.
- Supervision of construction and commissioning is sometimes inadequate, leading to defective components or systems not being as designed. Trials could not detect all these faults.
- The trials are effective in providing a practical demonstration of the redundancy in the design, and assisting with operator training.
- Some vessels whose 6kVA switchboard bus-ties were assumed open in the FMEA are routinely operated with bus-ties closed for reasons of economy and fuel efficiency. This is well-known in the industry.
- There is little use of site-specific risk analysis to select the equipment class. It was originally expected that there would be a marked difference in reliability between class 2 and 3 vessels, but in practice it tends to mean operations with closed or open bus-ties.
- Where safety cases are required for DP vessels, they typically quantify loss of position based on historical experience, and refer to the FMEA and trials reports, but do not normally carry out any extra work to integrate these studies.

Despite these criticisms, few stakeholders thought that the FMEA approach was inappropriate or needed fundamental change. Apart from the stakeholders directly affected, there was only a low level of awareness or concern about the 3 incidents that had occurred, and few other major concerns. Most stakeholders warned against fundamental changes on the grounds that:

- Industry was not ready for more demanding practices.

- The number of DP vessels would not be sufficient to sustain the necessary expertise.
- Imposing new assessment practices on existing vessels can introduce as well as eliminate hazards.
- The historical risk from DP failures has not been high, and does not appear to be getting significantly worse.
- The cost of a more demanding approach would not be justified.

### **4.3 FMEAS**

Six example FMEAs of DP systems have been reviewed against the criteria in Section 3.3.2. No account has been taken of the client's scope of work, except where this was stated in the study objectives. The key results were as follows:

- A clear statement of the objectives. This was present in 5 out of 6 studies.
- A description of the major functional blocks. In 5 out of 6 studies, there was a comprehensive textual description. However, diagrams showing their interaction were present in only 1 out of 6 studies.
- A breakdown of the functional blocks into independent elements. This was present in all 6 studies, but only 1 out of 6 showed evidence of a systematic and verifiable approach.
- FMEA worksheets. These were included in only 2 out of 6 study reports. It is possible that the other studies had used them but left them out of the report for brevity.
- Identification of all significant failure modes for each element. Only 2 out of 6 studies showed evidence of a systematic search for failure modes. The other studies mentioned obvious failure modes in the text.
- Consideration of possible common failure modes. Only 2 out of 6 studies explicitly considered common failure modes. These were not the same 2 studies that used worksheets.
- Indication of typical causes of each failure mode. This was only present in the 2 studies using worksheets.
- Description and categorisation of the effects of each failure on other items, on the DP system overall, and on the positioning of the vessel. This was only present in the 2 studies using worksheets.
- Definition of the method of detecting that the failure has occurred. This was only present in the 2 studies using worksheets.
- Compensating provisions intended to prevent or correct the failure. Compensating provisions are inherent to the search for critical failures, but these were only clearly presented in the 2 studies using worksheets.
- Documents and drawings on which the analysis was based. This was only present in 2 out of 6 studies.

- Relationships of the FMEA with test programme and site-specific risk analysis. One of the studies predated trials and clearly showed assumptions to be checked. The other 5 studies showed evidence of being updated following trials. None of the studies were linked to site-specific risk analyses.
- Conclusions and recommendations, meeting the study objectives. In each case the absence of critical single point failures was noted. Only 3 out of 6 studies included management recommendations, or showed evidence of having had such recommendations in previous versions. The lack of recommendations is not considered critical, since these normally appear in a preliminary version and once addressed are removed in the final issued version.

Overall, there was a poor level of compliance with standard procedures for FMEAs. All 6 studies could be criticised in this respect, although the 2 studies that used FMEA worksheets came closest to meeting the criteria. There was no apparent trend with time or difference in practice between consultants or operators that would explain the deficiencies. In summary, there is little consistency between different FMEA studies when measured against published guidance on FMEA practice.

Nevertheless, most of the studies appeared comprehensive, although this was very difficult to verify. Their quality depended mainly on the expertise of the authors. This was not stated in any of the cases, and in one case the authors' names were not stated. If inexperienced analysts attempt to emulate such studies, they can be expected to produce a poor quality report. If the independent reviewers are also inexperienced, a sub-standard FMEA can be expected.

It is recognised that the objective of the FMEA is to help demonstrate the DP system's inherent safety, and that this does not necessarily require a state-of-the-art FMEA. In fact, given the rather limited needs for the FMEA of DP systems (see Section 6.4 below), it is likely that a greatly simplified FMEA would be sufficient. This reinforces the need for a list of critical elements suitable for a DP system FMEA (Section 3.3.2).

#### **4.4 SITE-SPECIFIC RISK ANALYSIS**

No examples have been obtained of site-specific risk analyses justifying the equipment class for a particular operation, as indicated in the IMO Guidelines. Operators have indicated that this is a simple evaluation, based on standard practice (see Section 3.4).

One consultant indicated that site-specific risk analysis is usually performed to investigate the risks of using a Class 2 vessel when Class 3 has been specified but no suitable vessel is available, or a Class 3 vessel that is not fully compliant with the requirements. This type of analysis combines the vessel's FMEA with other risk and reliability studies. A DP collision risk study has previously been performed to assist such work (DPVOA 1994).

#### **4.5 DP TRIALS**

Two reports on annual DP trials have been reviewed. Both were primarily collections of test logsheets, defining the equipment, method, expected results, actual results and comments for each test. The reports documented the names of the personnel involved, the trials procedures, together with conclusions and recommendations for management action.

The reports appeared clear and comprehensive. However, the link to the associated FMEAs was less clear. Although there was evidence that the FMEAs had been modified following the trials (or previous annual trials), there was no clear link between the failure modes in the FMEA and

the tests in the annual trials. Hence it was extremely difficult to verify whether the trials programme and FMEA were comprehensive and coordinated.

Based on discussions with stakeholders, it would appear that these reports were not unusual in these respects.

## 5. APPROACHES IN OTHER INDUSTRIES

### 5.1 INTRODUCTION

The following sections review the approaches used in a selection of other industries, where there is a need to demonstrate reliability or redundancy in equipment design.

### 5.2 SHIP PROPULSION

All ships have a main propulsion system that requires high reliability, while depending on a complex set of auxiliary systems including power generation. Most ships use a single main engine and propeller, but some larger or more specialised vessels have multiple engines, and some recent oil tanker designs have adopted dual redundant engine room designs. Modern vessels are now controlled through automated vessel management systems. Hence, increasing numbers of conventional ships have a level of complexity equivalent to that in DP vessels.

The reliability of a ship's propulsion system is ensured through the use of classification rules, certification of components, inspection and testing, as for DP vessels. The rules include requirements intended to prevent key failures that have occurred in the past. Their aim is to ensure reliability, but this is not verified through any formal methods other than ensuring that each individual ship complies with the rules.

Redundant propulsion is a voluntary class notation, which owners can use to ensure an above-average standard of reliability. For example, in the DNV "*Rules for Classification of Ships*", the notation **RP** requires the ability to restore at least 50% of propulsive power after any single failure, while the notation **RPS** also requires this ability following fire or flooding in any compartment. An FMEA is required for the complete propulsion and steering systems and their auxiliaries, to show that these requirements are met. This is similar to the IMO DP Class 2 and 3 requirements, except that there is less guidance about what the FMEA should contain.

### 5.3 HIGH-SPEED MARINE CRAFT

Compared to conventional ships, high-speed marine craft such as catamaran and hydrofoil ferries tend to operate relatively close to the coast and are of lighter construction, often dynamically supported. Their high speed requires sophisticated control systems for directional and motion stability. The potentially severe consequence of failure for a high-speed light ferry requires a high level of reliability.

Their safety is governed through the "*International Code of Safety for High-Speed Craft*" (the HSC Code), issued by IMO (2000). Due to the rapid development of high-speed craft designs, this has fewer prescriptive requirements than conventional ship rules. For example, the machinery section requires reliability to be "adequate to its intended purpose". The HSC Code requires an FMEA of the craft as a whole, covering machinery systems and their associated controls, electrical systems, directional control systems and motion stabilisation system.

The HSC Code includes guidance on procedures for FMEA, covering several points that are relevant for DP systems. These include:

- The objectives are soundly specified, making clear that the FMEA is to provide information on failure characteristics (as opposed to proving that critical failures cannot occur).

- The objectives also make clear that the information is to be used by operators in their training, operational and maintenance procedures, thus promoting a link to the craft in operation.
- Before carrying out a detailed FMEA, the guidelines specify that a functional failure analysis of the main systems should be performed, in order to identify the most important systems for study. This should use diagrams to help understand their failure effects.
- A full FMEA is required of the critical systems, and reported on worksheets.
- Where redundancy is not available, probability of occurrence may be used to determine acceptance, with numerical values specified for different effect severities.
- Explicit criteria are given for linking the FMEA to the test programme.

The guidance is succinct (11 pages) and specific, making clear the essential features that are required in an FMEA. It would form a good model for revision of the FMEA guidance for DP systems, or for inclusion in a higher-level management guide.

The FMEA requirement was introduced in 1994, although its origin lay in a severe accident involving the catamaran ferry *Apollo Jet*, which went out of control in Hong Kong harbour in 1989. While moving to an overnight berth, the crew shut down one of the generators, and inadvertently switched off the electrical power to the main engines and steering controls on the bridge. As a result, the vessel lost control and steering and collided with 2 other vessels and a sea wall, causing 4 fatalities. Hong Kong Marine Department wrote the FMEA guidance, which was adopted by IMO. There has been no comparable loss of control accident since then. FMEA has been accepted by the industry, and when the Code was reviewed during 1997-2000, FMEA was not considered to need changing.

#### **5.4 CIVIL AIRCRAFT SYSTEMS**

Aircraft systems require a high level of reliability, due to the potentially catastrophic consequences of a failure. There are relatively few aircraft types, often built in large numbers by a very small group of manufacturers. This makes it efficient to devote substantial effort to ensuring the reliability of each design before it receives its airworthiness certificate.

Airworthiness standards for commercial transport aircraft are specified by Part 25 of the US Federal Air Regulations and the European Joint Airworthiness Requirements (FAR/JAR 25). These set reliability targets in the form of failure frequencies, which depend on the magnitude of the failure consequences. Compliance with these targets is to be demonstrated through safety assessment for each design.

Recommended practice for conducting the safety assessment is defined in a detailed (330 page) document “*Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*”, ARP4761 (SAE 1996). The safety assessment process for an aircraft or system consists of three main steps:

- Functional hazard assessment (FHA). This is conducted at the beginning of the aircraft/system development. It identifies failure conditions associated with aircraft functions, and classifies their severity in order to relate to the FAR/JAR reliability targets.
- Preliminary system safety assessment (PSSA). This is a systematic examination of each system, in order to determine how its failure can cause the hazards identified in the FHA.

From this, it establishes safety requirements for the system, and shows whether the proposed system design can be expected to have sufficient reliability. The PSSA typically uses fault tree analysis (FTA). In addition, the sensitivity of the design to common cause events is also analysed through a technique known as common cause analysis (CCA).

- System safety assessment (SSA). This is a systematic and comprehensive examination of each system, carried out at the detailed design stage, in order to demonstrate that the derived safety requirements from the PSSA are met. The SSA typically uses FMEA, FTA and CCA.

FMEA has a relatively minor role in the overall safety assessment, which is primarily based on quantitative reliability analysis. FMEA is performed at item level, and failure modes with the same effects are grouped in a failure modes and effects summary (FMES). This is used as an input to the system FTA. Brief (11 page) guidance is included in ARP4761, including a checklist to ensure that the correct steps are taken in order to perform a cost-effective and accurate FMEA.

Given the difference in populations between DP vessels and commercial aircraft, few of the features of aircraft system safety assessments appear suitable for DP vessels. However, DP vessel FMEAs might also benefit from a checklist to help balance completeness and cost-efficiency.

## 5.5 ELECTRICAL SAFETY-RELATED SYSTEMS

Many industries make use of electrical, electronic or programmable safety-related systems, whose failure may result in accidents. They include process control systems, process shut-down systems, rail signalling equipment, automotive controls, medical treatment equipment etc.

The International Electrotechnical Commission standard IEC 61508 “*Functional Safety: of Electrical/Electronic/Programmable Electronic Safety-Related Systems*” defines a generic approach to setting appropriate safety standards for any safety-related equipment (Smith & Simpson 2001). It can be used on its own, or as a template for developing industry-specific standards. Examples of these include IEC 61511 for safety instrumented systems in the process industry, IEC 61513 for instrumentation and control systems in nuclear power plants, and the UKOOA guidelines on process control and safety systems for offshore installations (UKOOA 1999).

IEC 61508 defines four safety integrity levels (SILs):

- SIL 1 – the minimum level for safety-related equipment, implying good design practice.
- SIL 2 – requiring good design and operating practice similar to ISO 9001.
- SIL 3 – requiring the use of sophisticated design techniques.
- SIL 4 – the highest target, requiring the use of state of the art techniques.

The approach requires a risk analysis early in the design process, determining which SIL target is appropriate, given the risks of accidents. The risk analysis typically uses a formal hazard identification technique such as HAZOP, combined with an outline quantitative risk assessment (QRA). It then requires a demonstration that the design meets the assigned target, together with in-service validation. It divides failures into two types:

- Random hardware failures. These are assigned quantitative targets for each SIL, and compliance is demonstrated through reliability modelling techniques such as FTA, including analysis of common cause failures.
- Systematic failures (e.g. software errors). These are minimised through procedural defences and design disciplines appropriate to each SIL. For system design, IEC 61508 specifies project management activities, system specification and design approaches, monitoring and testing requirements, operating and maintenance procedures, audits, protection against unauthorised modifications, and documentation requirements. For software design, it covers design and testing methods.

FMEA has a minor role in the functional safety assessment. IEC 61508 includes a requirement for minimum levels of redundancy, regardless of the calculated hardware reliability. These are expressed as a safe failure fraction, representing the proportion of failures that are either non-hazardous or revealed by self-test. FMEA can be used to demonstrate that this requirement is met.

The IEC 61508 approach is very comprehensive, but it is more readily applicable to shut-down systems than continuously operating control systems. Applying it to DP systems would be a major undertaking, involving the development of a new industry-specific standard, application of reliability analysis techniques and data collection for DP systems, and adoption of much more rigorous design approaches among the manufacturers. In the absence of clear evidence of high risk from the current approach, it does not appear that such an effort would be justified.

Nevertheless, some of the ideas from IEC 61508 could readily be adopted in demonstrating DP redundancy:

- Management attention should be balanced between hardware failures, which can be managed through an FMEA, and system/software failures, which require more procedural safeguards.
- Reliability management should be applied throughout the life cycle of the DP system, changing focus as appropriate as it moves from design to operation.

In addition, some elements from IEC 61508 could be tested through research to show whether they were effective for DP systems, such as:

- A DP reliability target, sufficient to ensure that operations were not placed at unacceptable risk, could be calculated in the same way as the quantitative SIL targets.
- A reliability analysis of random hardware failures could be tested for generic systems.

At present, it would be unwise to expect operators to undertake this work, as it might cause excessive concentration on hardware failures, at the expense of system/software failures.

## **5.6 MILITARY PROGRAMMABLE SYSTEMS**

Programmable electronic systems are increasingly used in modern technology, due to their functional flexibility. To manage their reliability it is necessary to anticipate and prevent failures, which may occur in obscure ways, not necessarily following historical patterns. Redundancy is not a practical management option.

The Ministry of Defence Standard 00-58 “*HAZOP Studies on Systems Containing Programmable Electronics*” proposes the use of hazard and operability (HAZOP) studies for such equipment. HAZOP is a group-based hazard identification technique, in which hazards are uncovered by systematically applying a set of guidewords to identify deviations from the system’s design intent. It was originally used for process hardware, based on systematic review of the process and instrumentation diagrams, but is also applicable to any system whose design intent can be defined in full and reviewed systematically. However, it is not clear that this is the case for programmable equipment. It appears that the HAZOP recommended in Def. Stan. 00-58 is intended to be a creative, group-based hazard identification process, rather than a strictly guideword-based HAZOP.

Compared to an FMEA, there are few advantages from the HAZOP approach that would be useful for DP systems. An FMEA is much more efficient for demonstrating redundancy, and is also much more likely to produce documentation readily comprehensible by operators. However, there are some advantages of HAZOP that it would be desirable to include:

- The use of a multi-disciplinary team is an important aid to effective hazard identification. It is an effective solution to the difficulty of any one person understanding complex system design. It is already adopted by some FMEA practitioners.
- The creative element of a group discussion is actively promoted in a HAZOP, while a traditional FMEA may overlook interaction between system elements. It would be desirable to add an element of creative hazard identification to the FMEA process. However, it would not be wise to replace an FMEA with a purely intuitive approach.

## 6. EVALUATION OF CURRENT APPROACHES

### 6.1 KEY QUESTIONS

In order to evaluate whether the current practices described in Section 4 meet the requirements for suitable and sufficient risk assessment, the following key questions are addressed in turn:

1. What does redundancy mean in the context of DP systems?
2. Why focus on redundancy to manage the risks of position-keeping failures? In other words, what is the underlying motivation for the approach?
3. Is FMEA the right technique? In other words, is FMEA suitable in principle to demonstrate redundancy?
4. Is FMEA being used in the right way? In other words, are FMEAs and DP trials sufficient in practice to demonstrate redundancy?

These are each broken down into more detailed questions below, leading into consideration of whether changes are needed in current practices, and whether better alternatives are available.

### 6.2 WHAT IS A REDUNDANT DP SYSTEM?

#### 6.2.1 Redundancy

Redundancy involves designing a system with independent components in parallel, so that the system can still function if one component fails. The simplest version, dual redundancy, involves two components in parallel.

The IMO Guidelines define redundancy as “ability of a component or system to maintain or restore its function, when a single failure has occurred”. This appears to equate redundancy to ability to withstand any single failure. However, this is impractical because of common cause failures (see below) and hence is confusing.

Elsewhere, redundancy is usually defined without reference to failure. For example, IEC 61511 defines redundancy as “use of multiple elements or systems to perform the same function”. This is slightly more relevant to DP systems than the definition in IEC 61508.

Are changes needed? It would be preferable if the IMO Guidelines could be made consistent with the IEC definition. Meanwhile, this can readily be clarified through improved guidance.

#### 6.2.2 DP System Failures

The underlying purpose of the redundancy demonstration is to help manage the risks of position-keeping failures, i.e. failures to keep within critical limits for position or heading while under DP control.

In practice, the redundancy demonstration focuses on *technical* failures of the DP system, as opposed to errors by the human operator or the company management. Thus the operator and the safety management system are excluded from the definition of the DP system, although the IMO Guidelines do require consideration of an “inadvertent act by a person on board”.

This technical focus is appropriate while technical failures dominate the risks, but may be considered obsolete once a high-reliability system has been obtained. It is desirable for operators to manage the totality of risks of position-keeping failures, not simply those due to technical failure. Although, this is not traditionally part of an FMEA approach, it would be possible to adopt such an increased scope, perhaps through improved guidance. At present it is covered separately through operational management practices such as IMCA's competency scheme and the IMO guidance on training requirements for DP operators.

### **6.2.3 Single Point Failures**

The IMO Guidelines and class rules require a demonstration that no single fault will cause a position-keeping failure. It gives examples of single failures for Classes 2 and 3, such as active and static components.

As a result, most FMEAs and DP trials in practice consider possible "single point failures", i.e. failures in single items of equipment. Unfortunately, this is not a standard term that is recognised in BS5760:Part5 or IEC 61508. Single point failures are not the same as common cause failures (see below), but the failure to make this distinction clear might be one reason for the deficiency of FMEAs in this respect.

Are changes needed? This term could readily be defined in guidance.

### **6.2.4 Common Cause Failures**

Common cause failures are events that cause failures in two or more separate components, leading to system failure (similar definitions are used in BS5760:Part5 and IEC 61508). They include:

- Utility failures in common auxiliary systems, control systems, fuel supplies etc. In principle these can be prevented by sufficient duplication.
- Switching failures at points within a duplex system where control is transferred in the event of a failure. The need for switching or arbitration prevents a system ever becoming fully redundant.
- Cascade failures, where the failure of one component results in overload and consequent failure of other components. One of the DP failures in Appendix I involved a similar cascade of corrupt electronic data.
- Partial failures, where a component operates incorrectly, causing a system failure without triggering a switch to the redundant component. Two of the DP failures in Appendix I involved this type of event.
- Environmental events such as high temperature, water ingress or voltage transients, which may cause the simultaneous failure of independent components.
- Operator error and sabotage. Even the most sophisticated technical design cannot prevent an incautious or malicious operator disabling the protective mechanisms and causing a failure.

Common cause failures are mentioned in the IMCA guidance on FMEA (IMCA 2002) and their guidelines for DP vessels (IMCA 1999). However, common cause failures are not mentioned in the IMO Guidelines. Since they may be single events this leads to confusion about whether they are prohibited. In reality, this would be impractical, since it is impossible to design a system

with no common mode failures. In fact, common cause failures may be the dominant failure mode in redundant systems. Hence, to overlook them would also be inappropriate. In practice, redundancy is normally interpreted as meaning reasonably practical protection against common cause failures. This is illustrated by the use of 3 independent position references in class 2 and 3.

Are changes needed? Clarity in the treatment of common cause failures would be promoted by wording that was more consistent with IEC terminology. For example, the IMO Guidelines could require redundancy in DP system design (e.g. through prescriptive requirements and validation trials) combined with a systematic attempt to minimise the risks of common cause failures (e.g. through use of FMEA). Although changes to the IMO Guidelines are outside the scope of this study, it is reasonable to expect a suitable and sufficient risk assessment to do this, since it is consistent with their intent, while also being consistent with IEC standard terminology.

### **6.3 WHY FOCUS ON REDUNDANCY?**

#### **6.3.1 How Does Redundancy Affect Risks?**

The risk from a DP system is the combination of likelihood and consequences of loss of position. Comprehensive risk management necessarily requires consideration of both elements. This should take account of the operations that are in progress, the environmental conditions, the standard of operator performance and the safety management quality. However, during vessel design, the only factor that can be controlled is the inherent safety of the DP system design given the anticipated vessel operations.

Inherent safety is desirable but difficult to measure. Reliability is one possible measure of it. In turn, this is closely related to its redundancy. For example, the risk from position-keeping failures is directly related to their frequency and severity. At a given degree of severity, the frequency is critical, i.e. the DP system reliability. Although high reliability can be achieved through the use of carefully designed, manufactured and maintained simplex components, the most common approach is to use redundancy. Hence, in general, adding redundancy can be expected to reduce the risk of failure.

#### **6.3.2 Is Redundancy Sufficient to Manage Risks?**

As a risk management measure, redundancy has several advantages:

- It is readily verified. Alternatives such as manufacture of components with intrinsic high-reliability, or use of safety management systems, may also reduce risk but are much harder to verify.
- It is inherent in the vessel, unlike safety management systems which may fall into disuse if not regularly monitored.

However, while redundancy can be greatly increased (e.g. by moving from dual to triple redundancy), the corresponding reduction in risk may be relatively small. For example:

- Once a system is redundant, adding further levels of redundancy tends to have diminishing benefits in terms of reliability. If common cause failures are not eliminated, moving from dual to triple redundancy will only slightly increase reliability.

- High levels of redundancy may induce complacency among the operators. A belief that the system is fault-tolerant is likely to reduce urgency in restoring failed components, counteracting the increase in reliability.
- Extra redundancy requires extra complexity in the design. Redundant control systems may require complex arbitration logic. This may introduce failure mechanisms that are hard to recognise, both in the design and during operation.

Hence, redundancy is considered *necessary* to manage DP risks, but it may not be *sufficient* to demonstrate that risks are ALARP. Other measures may still be cost-effective, once adequate redundancy has been established. These may include prevention of common cause failures, and operational safety measures. These should be considered as part of the operator's on-going safety management.

### 6.3.3 Is There a Better Approach?

A possible improvement to the redundancy demonstration would be to require a demonstration of adequate *reliability*. This would be consistent with the reliability target in the IMCA guidelines for DP vessels (see Section 3.1.4 above), and could be achieved through a combination of FMEA and fault tree analysis. It may be an appropriate step if further levels of redundancy are to be specified. However, it is quite difficult to predict and verify reliability for systems whose in-service population is relatively small, such as DP systems. Furthermore, it would require revision of the IMO Guidelines, which is beyond the scope of the present study. As a first step, it may be appropriate to conduct generic reliability analyses of DP systems, in order to evaluate the quality of available data. This approach has been used by the DP drilling industry.

A more comprehensive improvement would be to require a demonstration of adequate *safety management*. This would be equivalent to requiring a safety case approach for DP systems. At present, it is not clear whether it would be justified by the level of risk. However, a simple approach to this would be to develop an industry standard for safety management of DP systems.

Meanwhile, it is considered appropriate to continue to use redundancy as a verification standard for DP systems, provided that common cause failures are also managed.

### 6.3.4 What Level of Redundancy is ALARP?

In principle, the level of redundancy should be appropriate to counter the hazards that will be experienced during the vessel's operation. This should be evaluated by the operator when selecting the equipment class for a vessel, or by the customer when selecting a DP vessel for a particular operation. In practice these decisions are rarely based on site-specific risk analysis, but are based on client requirements and the cost differential between class 2 and class 3 vessels. This type of industry judgement is consistent with the principles of ALARP.

A thorough FMEA, which identifies failure modes and either mitigates them or demonstrates that their risk is negligible, will also assist in making risks ALARP. However, this is not sufficient to meet the intention of the IMO Guidelines, as it makes the redundancy demonstration the only element of the risk assessment of position-keeping failures, whereas risk is a much wider concept than this.

It would be desirable to promote further consideration of consequences of position-keeping failures and the appropriate level of redundancy. However, with only 3 equipment classes

available in the IMO Guidelines, this will be difficult to justify. In the future, it is possible that an improved set of equipment classes, perhaps selected using generic reliability analysis, would enable more site-specific risk analysis as envisaged in the IMO Guidelines.

## **6.4 IS FMEA THE RIGHT TECHNIQUE?**

### **6.4.1 How Can Redundancy be Demonstrated?**

The IMO Guidelines and class rules require a demonstration that no single fault will cause a position-keeping failure. If this simply means that the system should be redundant, i.e. have independent sub-systems in parallel (and, in the case of Class 3, physically separated), it is a very simple task. A simple description of the systems (and, if necessary, their location) is all that is needed. This is in fact the main component of most current FMEAs of DP systems. It also leads very simply into a set of DP trials in which each sub-system in turn is switched off, while verifying that position-keeping is maintained.

Some stakeholders have expressed the view that this is all that is required to satisfy the intent of the IMO Guidelines. If correct, this would not require an FMEA at all, and would involve much less work than is devoted to most current DP vessels.

However, this simple view is inadequate, because of the need to manage common cause failures. Such failures are always possible, even in multiply redundant systems. It may be argued that these are not “single point failures”, and hence not prohibited by the IMO Guidelines, but this would be to take advantage of the lack of clarity in the definitions. The main point is that system failures due to single faults are always possible. The main defence of a system designer is to make them very *unlikely*.

Hence it is appropriate to demonstrate a basic level of redundancy, and in addition to identify the most likely common cause failures and to demonstrate that they are very unlikely.

### **6.4.2 Is FMEA a Suitable Technique?**

FMEA is a flexible technique that can be used for various purposes in developing reliable designs (BSI 1991). It is appropriate for identifying safety-critical failures, categorising their effects and highlighting areas for management action.

If FMEA is simply used to show redundancy, i.e. that there are independent sub-systems in parallel (and if necessary separated), it should be possible to apply FMEA in a simple way, systematically considering the failure of each sub-system in turn, and stating which elements provide redundancy. It is not then necessary to consider each failure mode or comply with formal FMEA guidance.

However, if FMEA is used to show that no single failure can occur, this is a subtly different task. In fact, it can be accomplished only by overlooking common cause failures, which undermines the validity and purpose of the exercise. Thus it is important for the effectiveness of the FMEA that its objective is to find failure modes, not to prove their absence. Design and operational safety measures should then aim to minimise their risk.

Hence, FMEA is in principle suitable to demonstrate redundancy and identify common cause failures, provided it has an appropriate objective and careful guidance and checking to ensure that the demonstration is adequate.

### **6.4.3 Would Other Techniques be Preferable?**

There are many other techniques of risk assessment that might also be used to meet the same requirement (DNV 2001).

Techniques of quantitative risk assessment (QRA), including fault tree analysis (FTA), could be used to make the analysis more formal. They make the assumption that failures can occur, and then try to estimate and manage their likelihood. This is appropriate for common cause failures. However, they are much more difficult to conduct than FMEA, and would be less useful in operator training. It is concluded that they would be useful generic demonstrations of DP safety, but would not meet the practical needs of DP operators.

Semi-quantitative methods such as bow-tie analysis, risk matrices and failure modes, effects and criticality analysis (FMECA) could be used to extend an FMEA towards a more systematic quantitative approach. They would be useful for prioritising consideration of individual failure modes, and linking to the development of safeguards in design and their management in operation. However, because these methods require a more systematic approach they would inevitably increase cost. It would be more desirable to increase efficiency through a technique focussed directly on meeting the study objectives.

Hazard identification techniques such as hazard checklists, HAZOP and SWIFT could be used to promote greater creativity in considering common cause failures. However, they are less efficient than FMEA at reviewing component-based systems, and it is concluded that they could usefully supplement a DP FMEA, but should not replace it.

Thus, none of the other techniques have overwhelming advantages. For continuity, it is considered preferable to improve FMEAs rather than replace them.

## **6.5 IS FMEA USED IN THE RIGHT WAY?**

### **6.5.1 Evaluation Criteria**

The review of FMEAs in practice indicates that, while they appeared comprehensive, they did not follow a systematic procedure, and hence it was very difficult to verify their conclusions (Section 4.3). In the case of the 3 actual incidents of DP failure (Section 4.1), the investigations revealed deficiencies in the designed redundancy, which more thorough FMEAs might have detected. When evaluated against the criteria for FMEA adequacy (Section 3.3.2), these 3 FMEAs were not significantly different to ones on vessels that have not experienced failures. Hence, it is concluded that current FMEAs are in general insufficient to demonstrate redundancy.

In order to consider why this might be, they are evaluated against the following criteria in turn below:

- Integration in safety management
- Objectives
- Classification rules
- FMEA guidance
- Competence of FMEA practitioners
- Integration of component FMEAs
- Integration with DP trials
- Integration with on-going operations
- Use of incident experience

- Independent review

### 6.5.2 Integration in Safety Management

For FMEA to be effective as a safety management tool, it must be integrated within the safety management system. Discussions with the stakeholders have indicated that this is true for DP vessel operators, at least in the UK at present. However, there are some key problems in the way the redundancy demonstration is managed:

- The main link between the FMEAs and other safety management is in training DP operators and technicians. This is evident in the way that the FMEAs are written. However, it is not acknowledged in any FMEA objectives. Since it may conflict with the need for systematic FMEA worksheets, it would be desirable for this objective to be made explicit.
- FMEAs of new-buildings are often commissioned too late to influence the design. Although the IMCA (2002) guidance stresses that FMEA should be initiated early in the design process, this good advice is easy to overlook.
- The classification society is sometimes involved too late to perform an adequate review. It would be desirable for owners to involve class at an early stage, and for class to provide more guidance on how to design vessels to meet the requirements.

Are changes needed? In order to promote suitable and sufficient risk assessment in this area, it seems that some high-level guidance is required on the safety management of DP systems throughout the life cycle. It would be desirable if this were agreed as a common basis between all the stakeholders, rather than simply directed at vessel operators. Specific contents are considered further below.

### 6.5.3 Objectives

The objectives of FMEAs are often inadequately specified. Key problems are:

- Lack of acknowledgement of the need for a clear, readable system description, in order to support the role of the FMEA in training.
- Inappropriate focus on the “worst possible” single point failure, which discourages systematic treatment of all possible failures.
- Omission of the role of FMEA in identifying and minimising the risk of common mode failures.

The following generic objectives are suggested for FMEA studies of DP systems:

- Describe the DP system in a way that supports training of operators and technicians.
- Demonstrate redundancy by listing the independent components performing each system function (and, for Class 3, their locations).
- Identify possible failures that can occur, including common cause failures.
- Describe the design safeguards that minimise the risks of common cause failures.
- Record the operational measures needed to maintain the designed safeguards.

#### **6.5.4 Classification Rules**

The objectives and key requirements for FMEA are stated in the classification society rules, not in the IMO Guidelines.

There are some differences between the different classification society rules. While the DNV and ABS rules state that the FMEA is to identify failure modes, the LR rules makes clear that it is intended to demonstrate the required degree of redundancy. However, this difference does not have any practical effect. It merely shows the lack of clarity of purpose in DP FMEAs is reflected in the classification rules.

It would be desirable if the classification societies could agree a common set of rules for FMEA. However, guidance in good practice for FMEAs could be established as a first step, with a view to adoption by classification societies if suitable for their purposes.

#### **6.5.5 FMEA Guidance**

Although guidance on good practice in FMEA is available from several formal sources (IEC 812, BS 5760:Part 5 etc), these are not specific to DP systems, and are not really suited to routine support and review of DP system FMEAs.

Specific guidance is available for DP system FMEAs (IMCA 2002). This is a user-friendly document containing much sound advice. In particular, it covers virtually all of the key elements identified in this report as representing good practice in FMEAs (see Section 3.3.2). Unfortunately, this may be too demanding for FMEAs in practice. The need for all these elements is not established through the study objectives, and the problems raised in the present study concerning conflicts of objectives are not recognised.

DNV's main concern with this document is that at present it does not appear to be in use within the industry. Some of the stakeholders questioned in this study were unaware of its existence or contents, even though it would be expected to support their work of conducting and reviewing FMEAs. In part, this is because the production and review of FMEAs is based excessively on individual experience rather than transparent procedures. However, it is also because the IMCA guide is informative for training purposes, but too detailed to guide routine procedures or reviews.

Are changes needed? Although some improvements to the IMCA guide would be desirable, it is much more important to promote a management process in which guidance is actively sought and followed.

#### **6.5.6 Competence of FMEA Practitioners**

Lack of competence among FMEA practitioners might be an explanation for their shortcomings. FMEAs often appear to be the product of a single author, but DP systems require a multi-disciplinary team to give adequate coverage of electrical and mechanical equipment. The FMEA reports rarely document the expertise of the practitioners.

Nevertheless, DNV has seen no evidence that lack of competence is a major problem. Within any field, a range of competence is to be expected. To ensure that this does not result in poor quality studies, it is desirable to have adequate training material, procedural guidance, management oversight, definition of scope and verification of acceptable quality in the result. The problem, therefore, is not lack of competence in the practitioners, but weakness in the procedures for specifying, conducting and verifying the FMEA.

Surprisingly, it might be the case that a high level of competence among FMEA practitioners has allowed the industry to survive without guidance and with little verification. DP system FMEA experts do not need guidance and review. Provided they remain in charge of the FMEA activity, a good quality result can be expected. However, reliance on individual expertise is unsatisfactory once the experts retire or change responsibilities. Then, in the absence of procedures and verification, FMEA novices cannot produce studies of adequate quality. There is no suggestion that this has occurred in the 3 recent accidents, but it could occur in the future if the field is not made more transparent.

A desirable change would be to document the names and experience of the FMEA team in the FMEA report. This would enable verification that adequate competence continues to be employed.

### **6.5.7 Integration of Component FMEAs**

Some stakeholders have indicated a lack of information about the failure modes of bought-in systems such as DP control systems and power management systems, as opposed to the main DP hardware. All 3 DP failure incidents occurred in systems of this type. These systems are purchased as redundant units, and type approved by classification societies. However, the standard of information about failure modes provided by the manufacturers is very variable. In its absence, it is impossible to integrate the systems adequately into the overall DP FMEA.

Underlying the variable standard of information on failure modes is a variety of approaches taken by the manufacturers to the design process. For manufacturers specialising in safety-related equipment, failure modes are systematically identified at an early stage and minimised throughout the design, with documentation being produced at the end. Other manufacturers base their design on experience and in-service feedback, and when classification societies require an FMEA, this is produced at the end of the design process. It is likely that this accounts for some of the difficulty obtaining adequate information about failure modes of bought-in equipment.

System manufacturers also make use of components that they themselves buy from suppliers, such as computer hardware, network software etc. There may be minimal information about failure modes of these components for the same reasons as above.

A more integrated process would be desirable, especially for UK manufacturers and operators, who must satisfy the requirements of the HSWA (Section 3.1.2). Several options might be considered:

- Manufacturers could be obliged to provide a full FMEA of their system, perhaps through more stringent type approval requirements. However, if this is not necessary as part of the system design, it is unlikely that very high quality information would be generated.
- Operators could use their power as customers to ensure that manufacturers provided the necessary information for the overall FMEA. However, this power is limited given the small number of DP vessels in the UK.
- Classification societies could issue type approval for systems as being fully appropriate for Class 2 or Class 3 operations. However, this type of assurance is difficult to issue to systems in isolation, as their redundancy depends on how they are installed on the vessel.

Rather than expecting any one stakeholder to take responsibility for the necessary changes, it seems preferable to create an opportunity for all stakeholders to work together in pursuit of a common standard, which could be defined as part of the FMEA management guidance proposed

above. Such a standard would define what information the operators required, and how it would be used in the FMEA. This would enable the manufacturers to design their systems to prevent failures, providing appropriate self-checking facilities. It would enable classification societies to verify that adequate information was available before granting type approval. It could be used as part of the equipment specification.

The common standard should also promote interaction between all stakeholders while preparing the FMEA. At present, all attend the proving trials, but this is too late to influence the vessel design. If the system manufacturers are expected to share responsibility for ensuring adequate redundancy, it is appropriate to involve them at an early stage as part of the FMEA process.

#### **6.5.8 Integration with DP Trials**

Although DP trials are considered to be a successful demonstration of redundancy, they are not well integrated into the FMEA process. The selection of trials to perform is based on the expertise of the consultant preparing the trials programme. The manufacturer and classification society surveyor similarly use their individual expertise. The incentive for timely completion to avoid unnecessary delay to the vessel appears to produce an efficient result. However, the absence of any systematic procedure or documented link between FMEA and trials leaves the process critically dependent on the expertise of the people involved. If this is ever lost, an unsatisfactory result could be expected.

It would be desirable to have a clear link between redundant equipment identified in the FMEA and tested in the trials. This would assist with independent verification that the trials have achieved their objective.

#### **6.5.9 Integration with Ongoing Operations**

Verification that vessels are operated in the way assumed in the FMEAs is in principle delivered through audits of the vessel's safety management system under the International Safety Management Code. In practice, many stakeholders expressed concern about vessels whose 6kVA switchboard bus-ties were assumed open in the FMEA being routinely operated with bus-ties closed for reasons of economy and fuel efficiency. Several FMEAs included statements to the effect that redundancy and fault-tolerance could be assured through crew actions, without any evidence that this would be done in practice.

This indicates that greater linkage would be desirable between the FMEA process and the on-going safety management of DP operations. Some operators have included DP operating requirements in on-board checklists, and this illustrates the type of linkage that could be established. One stakeholder suggested that DP operators should be consulted early in the process, before selecting the vendor of the DP system, as a way of securing operational feedback. In the operational phase, it would be desirable for the FMEA to be a living document, being modified through appropriate change procedures when relevant changes are made to DP systems.

#### **6.5.10 Use of Incident Experience**

Any risk management technique should make use of previous incident and near-miss experience. This is particularly useful when identifying failure modes. In the case of DP systems, IMCA has published a systematic series of analyses of DP failure incidents. Consultants have indicated that they make extensive use of incident experience in staff training.

Surprisingly, there is no indication in the FMEA reports that have been reviewed in this study that this experience has been used. There is also no encouragement to do this in the IMCA FMEA guide. In part, this may be because FMEA is in general founded on systematic examination of each component in turn, rather than a creative response to incident experience. However, given that FMEAs appear insufficiently thorough, more transparent use of incident experience would be an efficient way of improving them.

It is possible that the available incident experience does not conveniently link to an FMEA study. If so, the gap could be bridged by developing a check-list of previous failure experience, which could be used to prompt for failure modes, and also check that the FMEA was comprehensive. There is a danger that such a checklist could be regarded as a complete list of failure modes, thus discouraging further hazard identification. However, this can best be prevented by good guidance and verification criteria.

#### **6.5.11 Independent Review**

Classification societies provide an independent review of FMEAs. This is appropriate given their concentration of expertise, and the fact that the requirement for FMEAs is stated in their rules. However, each classification society relies on the experience of individual surveyors, rather than any systematic standard. While they quote established guidance on FMEAs, they make little use of it in practice.

It would be desirable for all classification societies to follow an agreed common standard when reviewing FMEAs. This should reflect the experience of individual surveyors, but should also document it in case of disputes or unavailability of experienced personnel. For clarity, it would be desirable for the main elements of the standard to be included in the FMEA management guidance proposed above. This is consistent with the aim of a current working group of the International Association of Classification Societies, which is to develop unified requirements for FMEA.

## 7. CONCLUSIONS

### 7.1 OBSERVATIONS

The state of the art for demonstrating redundancy in DP systems in the UK offshore industry has been reviewed. The main strengths in the current system are:

- A demonstration that a DP system is redundant is a suitable method of verifying its inherent safety, i.e. the measures adopted during design to reduce vulnerability to failures.
- The FMEA technique is suitable for demonstrating redundancy in principle, providing it is applied correctly.
- The trials are a suitable practical demonstration of the redundancy in the design.
- An additional benefit of FMEA is in training DP operators and technicians. It provides an integrated description of the DP system and its main failure modes, which is not available in any other document.

Several weaknesses have been identified:

- When FMEA is used to demonstrate that no critical single point failures can occur, there is a danger that failures may be overlooked.
- The definition of redundancy in the IMO Guidelines leaves unclear how common cause failures should be treated.
- Many FMEAs do not follow a systematic procedure for considering all relevant failure modes.
- Most FMEAs make little use of guidance documents on good practice.
- The quality of FMEAs and DP trials relies on the expertise of the personnel conducting them. Study team expertise is not usually documented.
- FMEAs of DP systems require a multi-disciplinary team to give adequate coverage of mechanical, electrical and electronic equipment.
- FMEAs mainly address technical failures. The human operator and the shore management are excluded from the definition of the DP system.
- There is sometimes a lack of information about the failure modes of bought-in systems such as DP control systems and power management systems.
- There is little use of site-specific risk analysis to select the equipment class.
- It is well known that some vessels are not operated in the way that is assumed in their FMEA.
- FMEAs of new-buildings are often commissioned too late to influence the design.

- Review of FMEAs by classification societies is sometimes not thorough. They often do not receive the reports early enough, and cannot justify delaying the trials.
- The 3 actual cases of loss of position through DP failure on the UKCS in 2002 revealed deficiencies in the designed redundancy, which more thorough FMEAs and trials programmes might have detected and highlighted for corrective action.

Despite these critical observations, most stakeholders believe that the FMEA approach is appropriate in principle, and needs improvements in practices rather than fundamental change.

## **7.2 RECOMMENDATIONS**

### **7.2.1 IMCA**

IMCA is recommended to:

- Develop an FMEA management guide, to provide an industry standard for how FMEAs of DP systems should be specified, managed, performed, verified and updated. This would be aimed at managers more than practitioners, providing specific, auditable standards rather than advice. It should be developed in association with manufacturers, classification societies and regulators, in order to ensure that all stakeholders see it as a common standard.
- Plan to update the existing FMEA guide, as a document to be referenced by the management guide above. The update should establish whether the FMEA guide is being used and, if not, what would be needed to make it more useful to practitioners. It should aim to document and encourage existing good practice, rather than provide idealistic advice.

### **7.2.2 Vessel Operators**

Operators responsible for managing vessels with redundant DP systems are recommended to:

- In new systems, start the FMEA process early in the design to take advantage of its potential to enhance inherent safety.
- For existing systems, ensure that as-built design documentation is available or recreated before commencing the FMEA.
- Prepare an FMEA project plan defining how the FMEA process will be conducted. This should set the objectives and scope, identify the required inputs, specify milestones for completion etc.
- Provide sufficient budget to perform a thorough FMEA. For cost-effectiveness, focus on redundancy principles and major common cause failures rather than detailed consideration of each component.
- Involve all stakeholders (classification society, DP equipment manufacturers, DP operators etc) at intervals throughout the FMEA process, not simply at the commissioning trials.
- Ensure that consultants follow documented good practice for conducting FMEAs.
- Ensure that FMEAs make realistic assumptions about vessel operation, and that vessels are operated in the way that is assumed in the FMEAs.

More detailed recommendations on good practice would be obtained through involvement in the development of the FMEA management guide, as recommended above.

### 7.2.3 Classification Societies

Classification societies approving DP systems and sub-systems are recommended to:

- Develop consistent and comprehensive objectives for FMEAs of DP systems, specifying the need to:
  - Describe the DP system in a way that supports training of operators and technicians.
  - Demonstrate redundancy by listing the independent components performing each system function (and, for Class 3, their locations).
  - Identify possible failures that can occur, including common cause failures.
  - Describe the design safeguards that minimise the risks of common cause failures.
  - Record the operational measures needed to maintain the designed safeguards.
- Ensure that DP trials programme demonstrates that the claimed redundancy is provided in practice.
- Develop common standards for reviewing FMEAs of DP systems that enable consistent identification and correction of inadequate studies, without requiring excessive complexity.
- Continue development of the class rules as common standards for DP vessel design that enable consistent identification and correction of inadequate designs.
- Provide incentives for owners to involve class at an early stage and provide sufficient time for review. Review of the owner's FMEA project plan (see above) would be one possible approach.
- Encourage DP system suppliers to provide a uniform high standard of documentation of system failure modes as part of type approval.

These recommendations can be pursued through involvement in the development of the FMEA management guide, as recommended above.

### 7.2.4 Consultants

Consultants performing FMEAs and developing trials programmes are recommended to:

- Define and follow good practice in conducting FMEAs, complying with the IMCA guidance for FMEA of DP systems. If this guidance is inappropriate, this should be reported to IMCA.
- Ensure that the FMEA considers all relevant failure modes, through the use of:
  - Systematic procedures for reviewing each system in turn.
  - Checklists based on incident experience.
  - Creative group discussion following HAZOP or similar approach.
- Provide a study team with competence in relevant disciplines, such as electrical systems, electronics, mechanical equipment, human error and DP operations; and document the names and expertise of study team members in the report.

- Ensure that the study team has adequate knowledge of the DP system and the integration of system components (through documentation, interviews with the design team and/or operators, group discussion and team expertise) to conduct a thorough study.
- Include in the study report sufficient descriptive text and diagrams to give the reader adequate understanding of the DP system, its redundancy concept and possible failure modes.
- Follow a systematic approach in developing trials programmes, and document the link to the FMEA.

### **7.2.5 DP System and Vessel Equipment Suppliers**

Suppliers of DP control systems, power management systems, engine governors, vessel management systems and other equipment used in DP systems are recommended to:

- Follow established quality assurance procedures for system and software design (e.g. IMCA 2001).
- Provide a design philosophy or functional design description, to ensure that vessel operators and FMEA consultants have an adequate understanding of the system.
- Consider possible failures early in the design process, so that inherent safety can be maximised and documented cost-effectively.
- Identify what information on failure modes is needed by an FMEA, and provide this as part of the system documentation.

These recommendations can be pursued through involvement in the development of the FMEA management guide, as recommended above.

### **7.2.6 HSE**

HSE is recommended to:

- Encourage stakeholders to develop and document good practice for FMEAs and trials; preferably by means of the FMEA management guide, as recommended above.
- Encourage stakeholders to comply with the documented good practice.

The following additional research would explore the potential benefits and practicality of more fundamental developments in the regulatory approach:

- Generic analysis of the risk to people and property on the UKCS resulting from DP failures. This will show whether the assumption in this report, that risks are not sufficient to justify a major change in the approach, is justified. From this, a reliability target for DP systems could be developed, as required in IEC 61508.
- Analysis of the reliability of representative DP systems. This will show whether a more quantitative approach to hardware failures would be feasible in the future to demonstrate compliance with the target derived above.

## 8. REFERENCES

BSI (1991), “Guide to Failure Modes, Effects and Criticality Analysis (FMEA and FMECA)”, British Standard BS 5760 Part 5, British Standards Institution.

DNV (2001), “Marine Risk Assessment”, HSE Offshore Technology Report 2001/063.

DPVOA (1994), “Risk Analysis of Collision of Dynamically Positioned Support Vessels with Offshore Installations”, Dynamically Positioned Vessel Owners Association.

HSE (1999), “Hazard Management in Structural Integrity – Vol 4: Inherent Safety”, Offshore Technology Report OTO 98 151, Health & Safety Executive.

IMCA (2002), “Guidance on Failure Modes & Effects Analyses”, M166, International Marine Contractors Association, London.

IMCA (2001), “Guidelines for the Quality Assurance and Quality Control of Software”, M163, International Marine Contractors Association, London.

IMCA (1999), “Guidelines for the Design and Operation of Dynamically Positioned Vessels”, M103, International Marine Contractors Association, London.

IMO (2000), “International Code of Safety for High-Speed Craft”, Resolution MSC.97(73), International Maritime Organization, London.

IMO (1994), “Guidelines for Vessels with Dynamic Positioning Systems”, MSC Circ.645, International Maritime Organization, London.

SAE (1996), “Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment”, Aerospace Recommended Practice ARP4761, Society of Automotive Engineers, Warrendale PA, USA.

Smith, D.J. & Simpson, K.G.L. (2001), “Functional Safety; A Straightforward Guide to IEC 61508 and Related Standards”, Butterworth-Heinemann, Oxford.

UKOOA (1999), “Guidelines on Process Control and Safety Systems on Offshore Installations, UK Offshore Operators Association, London.

# APPENDIX I INCIDENT DESCRIPTIONS

## I.1 INTRODUCTION

This appendix describes three actual incidents of DP failure that have occurred on the UKCS. Two are taken from International Marine Contractors Association Safety Flashes (06/02 and 07/02), and the third description has been supplied by the vessel operator, whose assistance is gratefully acknowledged.

The following acronyms are used:

DGPS	differential global positioning system
DP	dynamic positioning
DPO	dynamic positioning officer
FMEA	failure modes and effects analysis
IMO	International Maritime Organization
PCB	printed circuit board
PLC	programmable logic controller
PMS	power management system
ROV	remote operated vehicle
UKCS	United Kingdom Continental Shelf
UPS	uninterruptible power supply
VMS	vessel management system

## **I.2 INCIDENT 1**

### **I.2.1 Operational Status**

At the time of the incident, the vessel was engaged in routine saturation diving operations and all the systems were operating normally. The weather was good, well within the limits for safe diving operations. There was a 21 knot wind from the south east and a 0.5m swell running. The dive teams had just completed an on-bottom hand over. An ROV was also at depth with a minor entanglement in some soft line.

### **I.2.2 The Incident**

At 02:55 hrs power from Board A to the Starboard bell was lost. Board B was selected. Numerous Starboard bell alarms activated. Some seconds later at 02:56 hrs, the vessel suffered a brief but complete loss of electrical power to all ship's systems, an event known in the industry as a "*black ship*" condition.

All vessel systems that were powered from the vessel's power management system (PMS) were lost due to the power failure. Some systems that should have been protected by uninterruptable power supplies (UPSs) also failed.

Some 2 minutes later as power and power management was returning, an azimuth thruster was restarted by the DPO. A further 2 minutes elapsed before a tunnel thruster started. With propulsion now available fore and aft, station keeping capability returned. At 03:07 hrs, control of the vessel was regained and by 03:11 hrs, all services had been restored, all generators were on line, all thrusters running and selected to DP. The divers were successfully returned to the bells and recovered to the surface.

By a combination of the efforts of the ship's crew and the automatic functions of the PMS, power was quickly and progressively restored to the vessel's systems.

Initial alarms on the Bridge included loss of power management and loss of propulsion followed quickly by loss of power. The loss of power in turn caused loss of communications, lighting, clocks, positioning systems and steering. Alarms for "*dive warning*" and "*abort dive*" were activated in sequence by the DPO.

During the period between the blackout and regaining control of the vessel, the vessel had moved some 190m from its original position at the work site.

### **I.2.3 Conclusions as to Cause**

The immediate causes of the incident have been identified as technical in nature. Management system failures were also found to have contributed to the incident.

#### ***Technical***

The technical failures that triggered the events that blacked out the vessel have been identified as:

Erroneous signals were issued from the PLC that manages the power distribution onboard the vessel. The erroneous signals were the result of physical degradation of the PLC's backplane through which all signals to and from the unit pass. This physical degradation definitely included loose contacts, dry joints and possibly also cracked and broken tracks in the circuit

board itself. All of these physical substandard conditions can be attributed to ageing of the backplane.

Terminal resistors on the printed circuit boards within the PLC had been snipped but not fully removed. It is likely that the attempted isolation of these resistors was done at the time the vessel was commissioned. With the natural vibration of the ship, these resistors were intermittently contacting the remainder of the circuit boards of which they were originally a part. The effect of this was to corrupt the data stored in the system that tells the system the status of the machinery on the vessel.

Wiring within the PLC unit was incorrect resulting in reverse polarity in the series of communications cables. The effect of this would have been to stress the electronic components within the system though no evidence was found that this stressing had caused failure in any components. The reversed polarity could also have caused corruption of the telegram signals between boards contributing to the corruption of data.

It was found that US1 detected a self-fault and initiated a change over. US2 took over from US1 as the master PLC. US1 shut down as it was receiving inconsistent data and interpreted this as a fault within itself. This occurred as a result of the corrupted signals issued from the faulty backplane. US2 took over as it was designed to do.

Once US2 took over from US1, the combination of erroneous signals and corrupt data caused the software to open the Port 230V secondary breaker and then to take both generators off the 6kV board and open the 6kV bus tie more or less simultaneously. This action left the vessel without power resulting in the blackout.

## ***Management Systems***

### **Prior History**

The investigation found that there was a significant history of unexplained starting and stopping of machinery onboard the vessel going back over many years though the significance of this history was not recognised either by offshore or onshore management.

In hindsight, it is clear that the previous events were significant in that they were indicating a fault condition that could, and ultimately did result in unsafe conditions. However, prior to the blackout and subsequent investigation, personnel operating the vessel believed that the FMEAs of the vessel's systems and the classification of the vessel confirmed that no single point failure could introduce unsafe conditions.

### **FMEA, Trials & Audits**

The DP FMEA for the vessel has been reviewed as part of the investigation and was found to be inadequate. This had not been identified either internally or in the process of the many trials programmes and audits which the vessel has undergone since the FMEA was written in 1991.

### **Planned Maintenance**

The investigation found that the UPSs onboard the vessel are not included in the planned maintenance system.

## Training and Procedures

Until the incident, it had been universally considered that a blackout condition was not possible onboard the vessel due to the configuration of the PMS. Consequently, the crew had not trained to deal with such an event, no procedures were in place and no back-up power available. Given the very sudden and comprehensive nature of the blackout, the crew responded in a professional manner to the event, normalising the situation without injury or significant damage.

### **1.2.4 Recommendations**

As a result of the incident and the findings of the investigation, the company involved has identified a number of recommendations which are set out below:

The existing PMS, which was installed some years ago and is becoming obsolete should be replaced with a more modern system. The learning from this incident should be incorporated in the specification for the new system.

Planned maintenance routines should be revised to include the UPSs onboard. Pre-operational checks should include testing of relevant UPSs. The UPSs should be reconfigured so that power is supplied to the consumer through the UPS at all times. Primary and secondary monitoring should also be installed on all UPSs

The scope of Dynamic Positioning FMEAs for other vessels in the fleet should be reviewed to ensure that all features affecting the redundancy capabilities of each vessel, including power management, are included in the analysis.

The scope of Diving System FMEAs for other vessels in the fleet should be reviewed to ensure that all features affecting the redundancy capabilities of the diving system, including power management are included in the analysis.

The impact of ageing on critical components on other vessels in the fleet should be considered as part of FMEA (or FMECA) and maintenance / upgrade system requirements adjusted accordingly. The age profile of existing safety critical electronic systems should be mapped.

The adequacy of the annual DP trials protocol should be reviewed to ensure that they verify the effectiveness of the redundancy provisions associated with power management and its criticality in respect of station keeping in accordance with revised FMEAs.

A review should be undertaken to determine if the timing mechanisms of the various systems onboard can be synchronised. If this is practical, it should be implemented.

Diving emergency and contingency procedures to be reviewed as a result of this incident and familiarisation of personnel with emergency power options emphasised.

The PMS/DP failure/maintenance records on the other vessels in the fleet should be reviewed to identify if any have similar history that could now indicate common failure modes.

Existing records of non-conformity (NCRs) should be reviewed to identify any trends that may suggest common fault modes in safety critical equipment. Consideration should be given to establishing a technical review panel to evaluate equipment related non-conformity reports.

Black box recording of fault detection and logging should be established for all key safety parameters. This would assist in identifying intermittent faults prior to incidents and the analysis of causal factors after incidents.

Policy in respect of supervision of work on safety critical systems should be reviewed with a view to improving control and addressing the potential for poor workmanship. This should include third party activities and should apply to new systems and change or modification of existing systems.

## **I.3 INCIDENT 2**

### **I.3.1 Operational Status**

At the time of the incident, the vessel was engaged in routine saturation diving operations and two divers were deployed working inside a subsea jacket within the 500 m zone. The weather conditions were moderate with a wind speed of 30 knots.

The vessel was operating in DP Class 2 with two 2 stern azimuth thrusters and two bow thrusters running with all enabled in the DP system. Three diesel generators were running with the bus tie closed and the other generator was on standby.

The reference systems in use at the time were a DGPS, the port and starboard tautwires and a hydroacoustic reference system.

### **I.3.2 The Incident**

At 1000 hours, due to the increasing weather conditions, a decision was made to start another bow thruster and at 1007 hours the Engineers operated the breaker to start the thruster. However it failed to start and within 10 seconds the two stern azimuth thrusters indicated 'not ready' and stopped. The power management system was checked which confirmed that the two stern azimuth thrusters were not in operation. The vessel started to move ahead under the influence of the wind and seas that were from astern.

The Red Abandon Dive Alarm was activated and the divers commenced returning to the bell. The vessel Master, upon hearing the alarm, went to the bridge. The Dynamic Positioning Operator (DPO) changed to DP manual control of the vessel. By this time, the vessel was down wind from her intended position some 15 metres off the platform.

One of the stern azimuth thrusters started and the DPO was able to gain some control by using full thrust astern and selecting yaw to control heading. The other stern azimuth thruster attempted to start causing both stern azimuth thrusters to stop. One stern azimuth thruster again started and the Engineers were instructed to leave the situation as it was but the power management again tried to start the other stern azimuth thruster leading to both units again stopping.

The port and starboard tautwires and bow beacon were deployed ahead of the vessel so that the above movements did not make them out of limits at any time therefore they were always available as references.

This sequence of events covered approximately 6 minutes and resulted in the vessel being a maximum of 40 metres from her intended location before being driven back some 10 metres towards the divers. At approximately 1016 hours the situation was stabilised. The divers were recovered to the bell and the bell was recovered to surface.

### **I.3.3 Conclusions as to Cause**

The incident is considered to have been caused by a failure of the timer in the bow thruster when starting it which lead to an overcurrent on the bus bar, which, due to the proximity of the control cables of the control system board to the bus bar, caused a partial failure in one of three cards on the control system board.

Two of these control system cards initiated the start/stop sequence for the vessel's thrusters. It was expected that if a failure occurred on a card the system would fail safe and maintain the status quo, i.e. if thrusters were operating they would continue to operate and the fault in the card would be indicated to the operator.

The situation was further exacerbated by the fact that the control system cards were not sufficiently segregated and that the damaged card contained the control functions for both stern azimuth thrusters which were shut down as a result of this incident.

The DP FMEA for the vessel was reviewed as part of the investigation and it was found that it did not identify the above single point failure. Neither had this fact been identified internally or during annual DP trials and audits which the vessel had undergone since the FMEA was first written. The FMEA has been regularly reviewed since first being produced and the document was on its fifth revision.

Until the incident, it had been considered that a failure of this type was not possible on board the vessel.

### **I.3.4 Recommendations**

As a result of the incident and the findings of the investigation, the company involved has identified a number of recommendations which are set out below:

The control system cards should be reconfigured to bring about a suitable segregation of critical consumers (thrusters and transformers) to remove the single card failure mode affecting systems on both sides of the switchboard.

An independent review of the reconfiguration should be undertaken to ensure that the modification is valid and will not bring about other failures that lead to undesired events.

Protection systems should be installed on the control boards such that the supply to the input channels (from field devices) is galvanically isolated from that used within the boards' processing package. The protection system should be demonstrated prior to acceptance.

The segregation of the data input cables from diesel generator protection units to the control systems cards should be increased to protect the cards from the possibility of an induced current or voltage.

An FMEA should be carried out on the reconfigured vessel management system (power management/integrated control systems) and a trials protocol developed to test and validate the FMEA findings.

A review of other vessels in the fleet vessel management systems should be undertaken to ensure that similar failure mechanisms are not present.

## **I.4 INCIDENT 3**

### **I.4.1 Operational Status**

At the time of the incident, the pipelay vessel was installing a 12" pipeline in the North Sea. The vessel was stopped in the water to fit a pipeline anode.

### **I.4.2 The Incident**

A fault occurred on a printed circuit board (PCB) within the processor selected to be DP system network arbiter. The PCB, by design, should have then relinquished arbiter function to the next processor in sequence however it did not and resultant network communication failure caused malfunction of both DP computers and the bridge thruster control station.

### **I.4.3 Conclusions as to Cause**

#### ***Technical***

The technical cause of the incident was a failure in the DP communications network. Two faults were identified on the failed processor

A PCB component failure occurred in the processor while it was acting as arbiter.

The processor had a hidden problem which prevented it from relinquishing control in the event of a failure. This was caused by an undetected design change in the card's architecture which was specific to cards produced after a certain batch number.

As a result, this processor continued to be arbiter while in a failed condition. This caused the failure of the entire network. Once the processor was isolated, the network restarted.

#### ***Design***

The DP system design complied with the applicable IMO guidelines and class rules. The changes recommended following the incident involved monitoring of the processors to detect faults. This suggests that the lack of a monitoring capability was a design fault. However, the reported difficulty of introducing this capability may suggest that it is not a reasonably practicable requirement.

#### ***Trials***

The dormant changeover fault on the processor could have been detected by manually stopping it while it was arbiter. It appears that a similar test was performed, presumably while another processor was acting as arbiter, and the assumption made that all processors would act the same. This assumption is understandable, given that the FMEA did not identify this as a potential failure. If the assumption had been clearly documented, it is possible that it might have been questioned.

Subsequently trials programs have been amended to ensure that this switching function is tested prior to conducting any pipelay operations and the ability of all five processors to relinquish control thoroughly demonstrated to auditors at the Annual FMEA Proving Trials.

## **I.5 CONCLUSIONS**

Three incidents have been reviewed in which faults in single equipment items led to loss of position on DP Class 2 or 3 vessels. All 3 events occurred within a 6-week period on the UKCS. Two involved failures in the PMS and one in the DP communications network. Two occurred while divers were in the water, and hence formed a significant safety hazard.

In each case an FMEA had been conducted of the DP system, but had failed to identify faults of this type, or any other faults involving loss of position.

All three events involved rather complex faults – erroneous signals, a partial failure, a failure to relinquish control. Hence the failure of the FMEAs to anticipate them may be regarded as understandable. Nevertheless, more specific guidance or checklists would be desirable to prompt consideration of such events in the future.

The subsequent investigations revealed actual deficiencies in the level of redundancy in the DP systems, which a thorough FMEA and trials programme should have detected. Thus the incident experience suggests that FMEAs or trials of DP systems have not been sufficiently thorough to ensure adequate redundancy. Possible reasons for this are considered elsewhere in this report.





**MAIL ORDER**

HSE priced and free  
publications are  
available from:

HSE Books  
PO Box 1999  
Sudbury  
Suffolk CO10 2WA  
Tel: 01787 881165  
Fax: 01787 313995  
Website: [www.hsebooks.co.uk](http://www.hsebooks.co.uk)

**RETAIL**

HSE priced publications  
are available from booksellers

**HEALTH AND SAFETY INFORMATION**

HSE Infoline  
Tel: 08701 545500  
Fax: 02920 859260  
e-mail: [hseinformationservices@natbrit.com](mailto:hseinformationservices@natbrit.com)  
or write to:  
HSE Information Services  
Caerphilly Business Park  
Caerphilly CF83 3GG

HSE website: [www.hse.gov.uk](http://www.hse.gov.uk)

**RR 195**

**£10.00**

ISBN 0-7176-2814-0



9 780717 628148