**GUIDANCE NOTES ON**

# FAILURE MODE AND EFFECTS ANALYSIS (FMEA) FOR CLASSIFICATION

**MAY 2015 (Updated March 2018 – see next page)**

**American Bureau of Shipping**
**Incorporated by Act of Legislature of**
**the State of New York 1862**


**ABS Plaza**
**16855 Northchase Drive**
**Houston, TX 77060 USA**

## Updates

### March 2018 consolidation includes:

- September 2017 version plus Corrigenda/Editorials

### September 2017 consolidation includes:

- July 2015 version plus Corrigenda/Editorials

### July 2015 consolidation includes:

- May 2015 version plus Corrigenda/Editorials

## Foreword

ABS requires clients to develop and submit FMEAs as part of Classification requirements for select systems. For instance, FMEAs are required for achieving many of the special or optional Classification notations such as **CDS**, **ACC**, **ACCU**, **R1**, **RQ**, **DPS-2**, **DPS-3**, **ISQM**. This document provides guidance and insight into the development process for FMEAs to comply with ABS Classification rule requirements. The utilization of this guidance will provide tangible benefits as the marine and offshore industry is able to realize the positive results of FMEAs that are developed correctly and managed appropriately throughout the lifecycle of a system. Some of these benefits include

- FMEAs that meet the intended objectives and are a support to the classification process
- Consistency in scope, depth and quality among comparable FMEAs
- Expedited FMEA review process
- Reduced failures, downtimes and incidents

These Guidance Notes become effective on the first day of the month of publication.

Users are advised to check periodically on the ABS website www.eagle.org to verify that this version of these Guidance Notes is the most current.

*We welcome your feedback. Comments or suggestions can be sent electronically by email to rsd@eagle.org.*

## Terms of Use

**GUIDANCE NOTES ON**

# FAILURE MODE AND EFFECTS ANALYSIS (FMEA) FOR CLASSIFICATION

## CONTENTS

This Page Intentionally Left Blank

# SECTION 1 Introduction

## 1 Background

In the marine and offshore industry, design and equipment configurations vary from one system to the next, and systems are in many cases increasingly complex. There are gaps in codes and standards which may lag technological innovations and there are issues related to interfaces between systems. Risk analyses such as Failure Modes and Effects Analysis (FMEAs) provide a formalized approach to identify hazardous situations, address the gaps and interconnection variances, and improve safety, environmental performance and operational downtime.

ABS requires clients to develop and submit FMEAs as part of Classification requirements for certain systems and to obtain certain special notations. This document provides guidance and insight into the development process for FMEAs to comply with ABS Classification Rule requirements for various special notations. The utilization of this guidance will provide tangible benefits as the marine and offshore industry is able to realize the positive results of FMEAs that are developed correctly and managed appropriately throughout the lifecycle of a system. Some of these benefits include:

- FMEAs that meet the intended objectives and are a support to the classification process
- Consistency in scope, depth and quality among comparable FMEAs
- Expedite the FMEA review process
- Reduce failures, downtimes, and incidents

## 2 Purpose of FMEAs

Whenever a system failure could result in undesirable consequences such as loss of propulsion, loss of propulsion control, etc., best practices advise carrying out a risk analysis, such as an FMEA, as an integral part of the design and operational development process. This analysis can be a powerful aid in identifying possible failures which could potentially leave a vessel, an offshore installation or its crew in peril.

The ultimate goal of an FMEA from the point of view of Classification is to use it as supporting documentation to demonstrate compliance with the ABS design philosophy and related Classification notation requirements and design intent for the particular system.

There are instances where the goal of the vessel or asset owner is to have a comprehensive and systematic risk-based approach to the design. When such approach is taken, design choices are prioritized based on the assessment of risks, thus the much broader FMEA goal is to identify and reduce a wider range of risks that could arise from failures. The ISQM (Integrated Software Quality Management) for software development is an example of such risk-based design framework.

## 3 FMEA Overview

An FMEA is a design and engineering tool which analyzes potential failure modes within a system to determine the impact of those failures. It was first developed by the US Department of Defense for use in systems design. The FMEA technique has since been adopted by commercial industries in an attempt to minimize failures and reduce safety, and environmental and economic impacts that could result from these failures.

FMEAs have more recently become a preferred risk analysis tool in the marine industry. It is required for certain systems by the International Maritime Organization, by Classification Societies, select regulatory bodies, and industry groups to improve the safety of a design or operation, to increase its reliability and to minimize undesired events. As a risk management practice, FMEAs are also an integral part of the design process of many proactive companies.

## 3.1 FMEA Process in a Nutshell

The FMEA is generated through a tabletop analytical process intended to identify system design and configuration weaknesses in all expected operational modes of the particular system. Once it has been determined that an FMEA will be performed and the scope of the study is agreed upon, an appropriate FMEA team of subject matter experts is assembled to carry out the analysis. A team is recommended for FMEAs, in particular for larger systems requiring different specialties. In some instances, a study carried out by an FMEA practitioner knowledgeable in the system(s) being analyzed and the development of FMEAs is an adequate alternative.

System boundaries are defined, and agreed upon, to clearly delineate what parts of the subject will be analyzed. The team will include or interface with the owners/stakeholders to exchange data, including collection of system schematics, operational procedures and manuals and system configurations. The team brainstorms on the potential failure modes, their effects, detection methods and corrective actions. Recommendations are provided for corrective action throughout the development process and these recommendations may be ranked according to the severity of the potential effect. This information is identified and recorded, usually in a tabulated format, and a preliminary report is issued to the owner/stakeholders and team for review and verification of accuracy.

An option is to recommend practical tests and trials to conclusively verify the analysis. For certain special notations and for certain organizations such as regulatory bodies, a further FMEA validation and trial program must be developed and executed on the vessel in order to validate that the system responds to failures and failures are detected and alarmed as described within the FMEA.

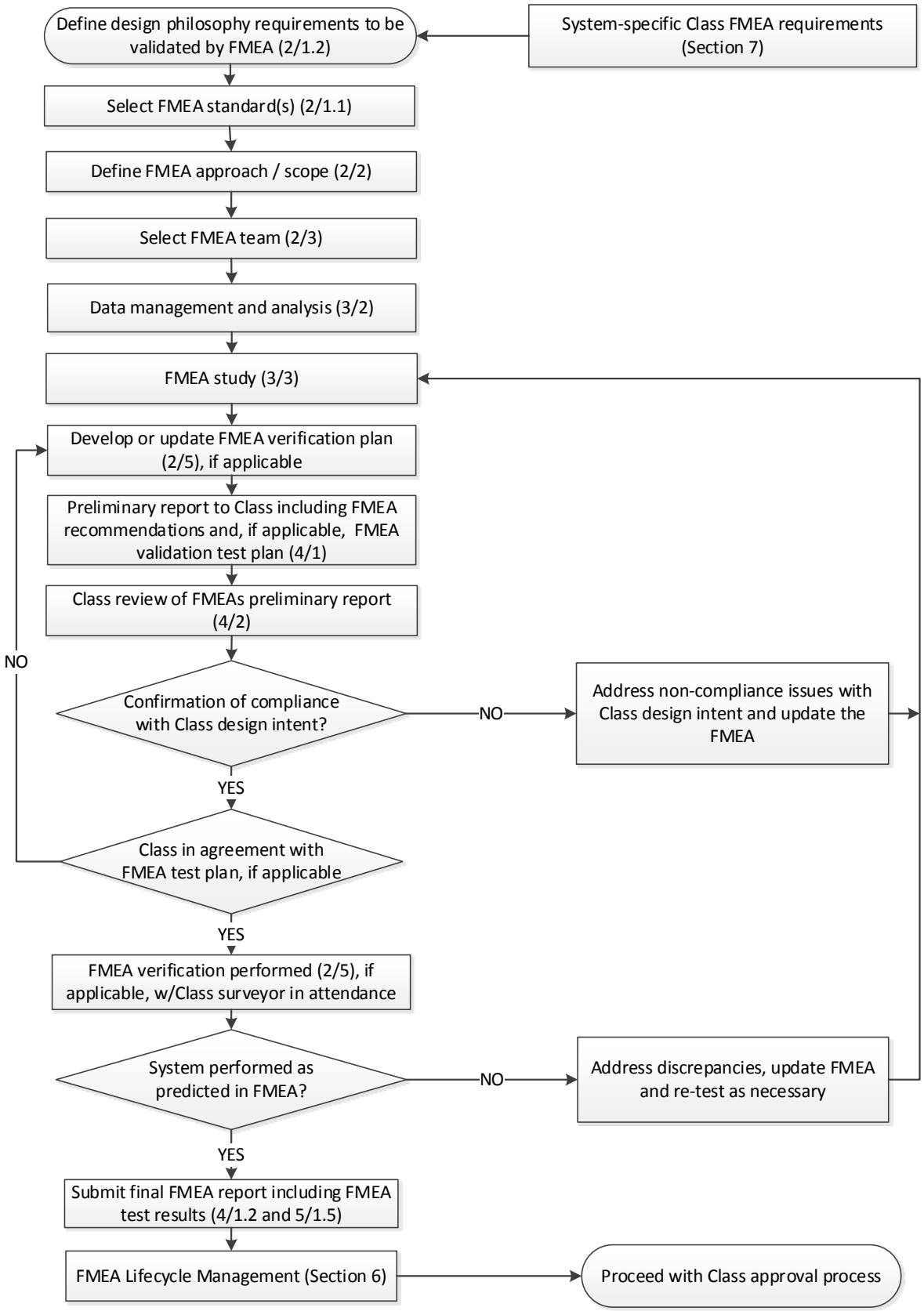
Once the comments from the team, owner and stakeholders on the preliminary document review have been received by the practitioner or FMEA team leader, the document will be updated and should be ready to be submitted to ABS for review. The entity that has the contract with ABS (e.g., shipyard, vessel owner) will have the ultimate responsibility for making sure the FMEA reports are submitted to Classification.

The general elements of the FMEA process are discussed in detail in Sections 1-6 and illustrated in Section 1, Figure 1. Section 7 provides the specific guidance for select ABS Classification FMEA requirements, as listed in Section 1, Table 1 below. Faced with a particular FMEA requirement, the user may choose to go directly to the respective requirement in Section 7 for guidance and clarification.

## TABLE 1
## Index of System-Specific Guidance for ABS FMEA Requirements

| *ABS Rule or Guide and Specific System* |
|---|
| **Steel Vessel Rules (SVR) • Offshore Support Vessels (OSV) • Under 90 meters [(1)] • Mobile Offshore Drilling Units (MODU) • Mobile Offshore Units (MOU) • Offshore Facilities • High Speed Craft (HSC) • High Speed Naval Craft (HSNC) • Gas Fueled Ships (GF) • Propulsion Systems for LNG Carriers • Lifting Appliances** |
| 7/1.1 Automation<br>General Automation,<br>Computer-Based Systems,<br>Wireless Data Communications for Vessel Services<br>Integrated Controls |
| 7/1.2 Electronically-controlled Diesel Engine |
| 7/1.3 Remote Control Propulsion<br>Automated Centralized Control (ACC)<br>Automated Centralized Control Unmanned (ACCU)<br>Automated Bridge Centralized Control Unmanned (ABCU) |
| 7/1.4 Gas Turbine Safety Systems |
| 7/1.5 Redundant Propulsion and Steering |
| 7/1.6 Single Pod Propulsion |
| **Dynamic Positioning Systems (DP)** |
| 7/1.7 Dynamic Positioning (DP) Systems |
| **Integrated Software Quality Management (ISQM)** |
| 7/1.8 Software |
| **Mobile Offshore Drilling Units (MODU)** |
| 7/1.9 Jacking and associated Systems |
| **Offshore Support Vessels** |
| 7/1.10 Subsea Heavy Lifting |
| **Certification of Drilling Systems** |
| 7/1.11 Drilling Systems/Subsystem/Equipment |
| 7/1.12 Integrated Drilling Plant (HAZID) |
| **Propulsion Systems for LNG Carriers** |
| 7/1.13 Dual Fuel Diesel Engine |
| **Gas Fueled Ships** |
| 7/1.14 Re-liquefaction, Dual Fuel Engine and Fuel Gas Supply |
| **Lifting Appliances** |
| 7/1.15 Motion Compensation and Rope Tensioning Systems for Cranes |

**FIGURE 1**
**Process Flow for Classification Required FMEAs**



# SECTION 2 Before the FMEA

## 1 Preparing for the FMEA

Conducting an FMEA or any risk analysis takes time, human resources and funds. However, the best way to save on resources is to do a proper FMEA the first time. Poorly done FMEAs take extra time and resources for revisions, corrections and clarifications, and in many cases, repeated analyses.

The following section provides an overview of the FMEA method, ground rules, assumptions and constraints to take into consideration when performing an FMEA for Classification.

### 1.1 FMEA Standards

By providing a clearly defined methodology and standards to be followed, the owner/stakeholder will be aware in advance how the FMEA will be generated and can have increased confidence in the results. Specifying standards does not guarantee an acceptable FMEA but it does guarantee an acceptable methodology and format. How well an analysis is performed, and to what level of detail, can only be achieved by selecting an FMEA team of subject matter experts or expert FMEA practitioner(s) experienced with the design, characteristics and performance of the systems being analyzed, as well as someone knowledgeable in the technique to lead the analysis.

Common FMEA standards used for reference include the following:

- IEC 60812, Analysis Techniques for System Reliability.
- US Military Standard MIL-STD-1629A, Procedures for Performing a Failure Mode, Effects and Criticality Analysis (cancelled in 1998 but it is still widely used as a reference)
- US Army Technical Manual TM 5-698-4, Failure Modes, Effects and Criticality Analysis (FMECA) For Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities, 2006

There are several guidance documents that although developed for specific systems or types of vessels such as DP, High Speed Craft, or automation, provide a wealth of useful information that is applicable to other systems in the marine and offshore environment:

- IMCA M166, Guidelines for Failure Modes and Effects Analyses (FMEA)
- IMCA M178, FMEA Management
- IMO MSC Circular 645, Guidelines for Vessels with DP Systems
- IMO HSC Code, Annex 4, Procedures for failure mode and effects analysis
- USCG MSC Guidelines for Qualitative Failure Analysis Procedure Number: E2-18 Revision Date: 11/10/2011
- USCG Marine Technical Notice 02-11, Review of Vital System Automation and Dynamic Positioning System Plans, refers to 46 CFR 62.20-3

For FMEAs for computer-based controls and software, the following general reference documents exist:

- National Aeronautics and Space Administration (NASA), “Software Safety Standard, NASA, Technical Standard, NASA-STD-8719.13B w/Change 1”, July 8. 2004,
- Nancy G. Leveson. “System Safety and Embedded Computing Systems” Aeronautics and Astronautics Engineering Systems, Massachusetts Institute of Technology (MIT), August, 2006

- Drs. Alex Deas, Sergei Malyutin, Vladimir Komarov, Sergei Pyko, Vladimir Davidov, "O.R. Rebreather Safety Case, FMECA Volume 5: Firmware and software", Revision A4, Deep Life Ltd., Glasgow, UK, August 12, 2008,
- Haapanen Pentti, Helminen Atte, "Failure Mode And Effects Analysis of Software-Based Automation Systems", STUK, Radiation and Nuclear Safety Authority, Helsinki, Finland, STUK-YTO-TR 190, August 2002.

## 1.2 Design Philosophy and FMEAs

It was noted earlier in this document that when ABS requires FMEAs, it is as a supporting document to verify that the system under review meets the specific Classification notation requirements and design philosophy. A general design philosophy for Classification is that a single failure shall not lead to an undesirable event or hazardous situation with immediate potential for injury to persons, damage to vessels, or pollution of the environment.

Examples of these undesirable events can include loss of functionality of system (or degradation beyond an acceptable level) or loss of control of system

Only certain design solutions achieve the end result of avoiding the undesirable event. Corrective actions include

- Redundancy in design
- Safe and controlled shutdown and restart
- Risk controls to diminish likelihood of occurrence of undesired events

Section 2, Table 1 below shows the standard solutions for identified failures based on failure design philosophy and the undesired event.

**TABLE 1**
**Typical Corrective Actions to Control Failure Scenarios**

| *Undesired Events* | *Solutions to comply with design philosophy that "No single failure shall lead to specified undesired event"* | *Example of Applicable Systems* |
|---|---|---|
| Any hazardous situation with immediate potential for injury, damage, or pollution | Safe and controlled shutdown | • Most drilling systems (except those used for well control and active heave compensation) (Certification of Drilling Systems, **CDS** Notation) |
| Loss of Functionality of System (1) | Complete redundancy of system (2)<br>Independent systems<br>No common-cause failures (3) | • Dynamic Positioning Systems (**DPS-2** or **DPS-3** Notation)<br>• Redundant Propulsion (**R1** or **R2** Notation)<br>• Redundant Steering (**R1** or **R2** Notation)<br>• Blowout Preventer (BOP) |
| Loss of System Control | Complete redundancy of controls and/or systems (2)<br>No common systems or common-cause failures | • Computer-based systems<br>• Drilling Systems Controls (Certification of Drilling Systems, **CDS** Notation)<br>• **ACC** and **ACCU** systems |

*Notes*

1 Loss of functionality or degradation beyond acceptable level.

2 Where complete duplication is not possible, robust and reliable design that offers a proven low likelihood of failure may be accepted on a case-by-case basis. These non-redundant parts are to be further studied with consideration given to their reliability and mechanical protection. The details and results of these further studies are to be submitted to ABS for review.

3 Definitions and examples of what can constitute common cause failure can be found in 3/3.3.4.

# 2 FMEA Scope and Ground Rules

Although the basics of the FMEA technique are standard regardless of the system being analyzed and the intent of the analysis, there is a certain level of customization that depends on

- Intent and scope based on Classification notation requirements being fulfilled
- Type of system being analyzed
- Other goals of the owners/stakeholders.

The scope of a particular FMEA shall be defined at the outset of development and shall be agreed upon by the parties involved. Before the FMEA gets underway, the following scope items must be defined:

1. Physical and operational boundaries
2. Failure criteria and types of failure
3. Depth of analysis/level of indenture
4. Design or operational philosophies (e.g., operating closed-bus vs. open-bus for a DP power distribution system
5. What are the consequences of interest (undesirable events)?
6. Criticality ranking (FMECA) if desired

Each of the items 1 through 6 above will be discussed in more detail in 2/2.1 through 2/2.7.

## 2.1 Equipment Scope and Physical Boundaries

The equipment to be analyzed will be defined at the outset of the analysis based on the goal of the FMEA for Classification requirements and the type of equipment. For defining the physical boundary of the FMEA, it can help to answer the following questions:

- What are the main systems/subsystems/equipment of interest in this FMEA?
- Systems/equipment interfacing with the main system under study?
- Supporting utilities? Control systems?
- What is excluded from the FMEA?

Section 2, Table 2 provides an example of the physical boundaries and the equipment that will be subjected to analysis for a Dynamic Positioning FMEA to comply with rule requirements.

All systems that have functional or physical interfaces with the system under study should be identified and should be subject to consideration in the FMEA. Examples of interfaces are data/signal communication between systems, input and outputs between systems, and even layout issues may provide interdependencies that need to be considered. As a minimum, the failures at the interfaces should be postulated and analyzed in the FMEA.

***Example: FMEA Scope for DP system and its Functional Interfaces***

*There is a requirement to do an FMEA for DP systems. The types of vessels employing DP systems is widely diverse and include but is not limited to semi-submersible mobile offshore drilling units (MODU), offshore support vessels and cruise ships.*

*A typical scope for equipment to be analyzed in a DP FMEA is provided in Section 2, Table 1. In addition, the FMEA should analyze failures at interfaces with equipment whose functions lie outside the system being analyzed.*

*For example, the scope of the FMEA for the DP system in an offshore support vessel designed for laying pipe will include functional interfaces that are unique for that type of vessel. In addition to the standard DP equipment, the FMEA scope of the pipe-lay vessel should include the tensioner system, for a MODU it should include functional interfaces with the riser, cranes, etc. The depth of the analysis with the functional interfaces shall be enough to ensure the FMEA objectives are met, and is up to the judgment of the FMEA team. For example, to meet the study objectives, it may be necessary to analyze components required for product lay such as deployment equipment (tensioner tracks, aligners, etc.), HPUs, electrical supplies, and control systems.*

For more detail, see IEC60812, Section 5.2.2.2 – Defining system boundary for the analysis.

## TABLE 2
## Examples of System/Subsystem's Physical Boundaries (for a DP System)

| | System | | Subsystem | Components |
|---|---|---|---|---|
| 1 | Marine Auxiliary Systems | 1.1 | Fuel | . |
| | | 1.2 | Remote control valve | . |
| | | 1.3 | Engine and generator lubricating oil | . |
| | | 1.4 | Seawater cooling | *Each subsystem has components whose failures should be evaluated. Representative component lists for select subsystems are included herein.* |
| | | 1.5 | Freshwater cooling | |
| | | 1.6 | Charge air | |
| | | 1.7 | Compressed air | . |
| | | 1.8 | Emergency generator | . |
| | | 1.9 | Engine management & safety system | . |
| | | 1.10 | HVAC and chilled water system | . |
| 2 | Power System | 2.1 | Generators | Generator switchgear, governors, AVR, etc., high voltage, medium voltage and low voltage AC distribution systems, emergency systems configuration and distribution, power management system (including load sharing, load shedding, load reduction, and black out recovery), UPS, transducers, interlocks and protection, safety systems, low voltage DC distribution systems and control power supplies, interfaces. |
| | | 2.2 | Power Distribution | |
| 3 | Propellers and Steering Gear | 3.1 | Main propellers | . |
| | | 3.2 | Steering gear | Power supply, main, auxiliary and backup pumps, hydraulics, cooling, controls (main, alternative, emergency), control power supply, protections, angle indications, alarms, ready signals, etc. |
| | | 3.3 | Tunnel Thrusters | . |
| | | 3.4 | Azimuth Thrusters | . |
| 4 | Vessel Management System | 4.1 | Switchboard PLC Communications | *Each subsystem has components whose failures should be evaluated. Representative component lists for select subsystems are included herein.* |
| | | 4.2 | Air Conditioning | |
| | | 4.3 | Network topology | |
| 5 | DP Control Systems | 5.1 | Independent Joystick (IJS) | . |
| | | 5.2 | Power Management System (PMS) | . |
| | | 5.3 | Networks | . |
| | | 5.4 | Reference and Sensors | DP control system and interfaces (including position reference systems, gyros, vertical reference sensors and wind sensors). Interfaces can include data interface with tensioner system, interface with survey package, etc. |
| | | 5.5 | DP Alert and communications | . |
| | | 5.6 | Cable routes | . |
| | | 5.7 | Backup DP Systems | . |
| 6 | Emergency Shutdowns | 6.1 | Emergency shutdown system (ESD) | . |
| | | 6.2 | Fire and Gas | . |
| | | 6.3 | Thruster Emergency Stops | *Each subsystem has components whose failures should be evaluated. Representative component lists for select subsystems are included herein.* |
| | | 6.4 | Group Emergency Stops | |
| | | 6.5 | Fans | |
| | | 6.6 | Dampers | |
| | | 6.7 | Fire Fighting Systems | |
| | | 6.8 | Quick closing valves | |
| 7 | Interfacing Systems | 7.1 | Riser (MODU) | |
| | | 7.2 | Tensioner (Pipe/product lay vessel) | |
| | | 7.3 | Crane | |

*Source: Modified from the Marine Technology Society DP Committee, Technical and Operational Guidance TECHOP ODOP O4 (D) FMEA Gap Analysis, October 2013*

## 2.2 Operational Boundaries (Global and Local)

Global operations are the overall operations of the facility or vessel. Local operations are the operations of the system that is within the boundaries of the FMEA.

Each operation and operational combinations can present distinct failure scenarios, (failure modes, hazards and consequences). The FMEA must define the global operations at the installation or vessel level as well as the local operations of the system that is within the boundaries of the FMEA. All operational combinations should be considered in the FMEA, as well as the switching between modes.

Examples of global operations for a DP vessel may include

- Station keeping
- Weather vanning
- ROV following
- Maneuvering
- Pipe-laying (if a product-laying offshore support vessel)
- Drilling (if a MODU)
- Underway fully laden for a tanker

Examples of local operational modes for the DP system would include

- Power management systems (PMS) configurations
- Blackout recovery
- Power load shed
- Manual
- Joystick
- Independent joystick system (IJS)
- Switching between modes.

## 2.3 Failure Criteria and Types of Failure

The proper and comprehensive identification of failures is a fundamental step in the FMEA exercise. Several considerations and basic assumptions regarding the failures to be considered should be understood by all team members before starting the FMEA:

- Single failure criteria
- Hidden failures
- Common-cause failures
- Treatment of unavailable systems
- Failure of passive and active components
- Consideration of external events

More detail on each of these is in 3/3.3.

## 2.4 Depth of Analysis

The equipment level to which an analysis is performed is very much dependent upon the system being evaluated, the intent of the FMEA and the goals of the owner/stakeholder. In general, FMEAs for the marine industry do not attempt to identify every possible fault of every component in the system, but will proceed to a level where additional analysis of failure modes from lower level components will not reveal additional effects on the system. Finding the appropriate level at which to stop on a given system is somewhat of an art and is developed with experience. An experienced FMEA team/practitioner should be able to determine the optimal depth of analysis that is sufficient to satisfy the intent of the FMEA.

The System-Specific FMEA Requirements tables presented in the body of this document give a more definite guideline of the depth of the analysis sought for most FMEAs requirements for Classification.

***Example: Defining Depth of Analysis***

*Let us consider a failure analysis on an automation system. The analysis typically would be performed assessing the failure for the acquisition unit modules, failure of inputs and outputs. A typical FMEA will stop at the module card level. Performing an analysis of individual circuit boards, resistors or failed data paths within the computer would not necessarily contribute to an assessment of the system as a whole. The end effect of those lower level failures on the system would be the same as failures already assessed at the higher level, therefore the recommendations to recover from those failures would already be addressed.*

*Above example refers to a standard automation FMEA which assumes the code is being programmed correctly. Note that the assumption may be different for ISQM software-focused FMEAs.*

For more detail, see IEC60812, Section 5.2.2.3 – Levels of analysis.

## 2.5 Criticality Ranking (FMECA)

A Failure Modes, Effects, and Criticality Analysis (FMECA) is an extension of the FMEA process which includes an additional criticality assessment. The criticality ranking explicitly and transparently brings to prominence the most critical issues and is extremely helpful for deciding the corrective actions. In the development, follow-up and implementation process of corrective actions, the criticality ranking helps to evaluate that the effort, time and resources are commensurate with the criticality of the item.

Criticality rankings based on risk use a combination of the consequence (severity) of the failure and the anticipated likelihood of the consequence occurring. The analysis will highlight failure modes with high probability of occurrence and severity of consequences, allowing corrective actions to be implemented where they will produce the greatest impact. Ideally, frequency estimates will be based on historically quantifiable data from the field, but in many cases data of this type is unavailable or poorly documented. The methods to determine criticality must be clearly defined prior to embarking on an analysis since the veracity of failure data (or lack thereof) can greatly influence the results.

It is worth noting that some standards make a difference between a qualitative and quantitative criticality assessment. The quantitative assessment as described by the MIL STD 1629 is quite involved and will not be discussed here as it not a requirement of Classification. The qualitative assessment of criticality uses expert judgment to place the event in criticality or risk matrix or a criticality benchmark. When a criticality analysis is asked for by the Classification requirement, the qualitative criticality assessment is not only sufficient, but also the recommended method.

The most common method for qualitative evaluating the criticality is the use of ranking systems which scale severity of consequence vs. likelihood, as shown in Section 2, Figure 1. The matrix in Section 2, Figure 2 example has four levels of consequence and four levels of likelihood. More levels can be defined as needed, but anything less than four levels may not provide enough granularity to make appropriate risk-based decisions.

Given the overall lack of reliability data for many marine systems and components, performing an assessment on a qualitative level based on experience and knowledge of the system under study is sometimes the only means by which to achieve a meaningful criticality assessment. A high severity and high likelihood event is not acceptable, and risk control measures to reduce either the likelihood of occurrence or severity may need to be developed.

*Very few Classification requirements specifically request an FMECA. As detailed in Section 7, ISQM and System Verification do explicitly require an FMECA. However, Classification will accept any voluntary submission of an FMECA instead of an FMEA.*

## 2.6 FMEA Naming Convention within this Document

An FMECA is an FMEA with an additional analysis of the criticality of each failure scenario. Thus, the term "FMEA" is used generically in this document to include both FMEAs and FMECAs. For example, the next section discusses the "FMEA Team" and it could be entitled "FMEA/FMECA Team" since its content is equally applicable to FMECAs. However, it would be tiring to the reader to see the convention "FMEA/FMECA" throughout this document. The reader can assume that anytime the term FMEA is used in this document, it can be substituted by the term FMECA. This inverse however, does not hold true. When the term FMECA is used, it can only mean an FMEA with the criticality extension.

**FIGURE 1**
**Typical Risk Matrix for FMECA**

| LIKELIHOOD | | | | | |
|---|---|---|---|---|---|
| **Frequent** Incident is likely to occur at this facility within the next 5 years. | 4 | | | High Risk | High Risk |
| **Occasional** Incident is likely to occur at this facility within the next 15 years. | 3 | | | | |
| **Seldom** Incident has occurred at a similar facility and may reasonably occur at this facility within the next 30 years. | 2 | | Medium Risk | | |
| **Unlikely** Given current practices and procedures, incident is not likely to occur at this facility. | 1 | Low Risk | | | |
| | | CONSEQUENCE | | | |
| | | 1 | 2 | 3 | 4 |
| | | **Incidental** | **Minor** | **Serious** | **Major** |
| ***Personnel*** | | Minor or no injury, no lost time. | Single injury, not severe, possible lost time. | One or more severe injuries. | Fatality or permanently disabling injury. |
| ***Community*** | | No injury, hazard or annoyance to the public. | Odor or noise complaint from the public. | One or more minor injuries. | One or more severe injuries. |
| ***Environmental*** | | Environmentally recordable event with no Agency notification or permit violation. | Release which results in Agency notification or permit violation. | Significant release with serious offsite impact | Significant release with serious offsite impact and likely to cause immediate or long term health effects. |
| ***Facility*** | | Minimal equipment damage at an estimated cost less than US$100K, negligible downtime. | Some equipment or structural damage at an estimated cost greater than US$100K, 1 to 10 days of downtime | Major damage to installation at an estimated cost than US$1 MM but less than US$10 MM, 10 to 90 days of downtime | Major or total destruction to installation estimated at a cost greater than US$10 MM; downtime in excess of 90 days. |

## 2.7 US Coast Guard Supplemental Requirements for Qualitative Failure Analyses (QFA)

Vessels under U.S. flag require an FMEA or "qualitative failure analysis" for many of the same systems for which Classification requires FMEAs.

As per 46 Code of Federal Regulations "one copy of a qualitative failure analysis must be submitted for propulsion controls, microprocessor-based system hardware, safety controls, automated electric power management, automation required to be independent that is not physically separate and any other automation that in the judgment of the reviewing authority potentially constitutes a safety hazard to the vessel or personnel in case of failure. The QFA should enable the designer to eliminate single points of failure"

The qualitative failure analysis is intended to assist in evaluating the safety and reliability of the design. It should be conducted to a level of detail necessary to demonstrate compliance with applicable requirements and should follow standard qualitative analysis procedures. The QFA must explicitly list.

- Assumptions
- operating conditions considered
- failures considered
- cause and effect relationships
- how failures are detected by the crew
- alternatives available to the crew, and
- necessary design verification tests should be included.

Questions regarding failure analysis should be referred to the reviewing authority at an early stage of design.

## 3 FMEA Team

There are two typical styles of conducting an FMEA. One is using a workshop setting with in-house subject matter experts with first-hand knowledge on the system being analyzed. The other style is to hire a third-party FMEA practitioner to develop the FMEA. The FMEA practitioner assembles a multi-disciplinary team to perform the analysis, which is developed nearly independently from the stakeholders, other than for initial inputs and review of the FMEA.

The appropriate multi-disciplinary FMEA team is selected based on specialized knowledge needed for the analysis. The disciplines that form the FMEA team should include subject matter experts in machinery, control, electrical and naval architecture, as applicable. The team should also have knowledge of design, manufacturing, assembly, service, quality, reliability and operation. A workshop-type FMEA must have an FMEA facilitator, who is first and foremost: 1) knowledgeable of the FMEA technique, 2) has good communication and administration skills and is 3) familiar with the type of system to be analyzed and its intended operation.

### 3.1 Stakeholder's Workshop Setting

Stakeholder's multi-discipline workshop FMEAs are developed using a meeting setting where several parties are directly and simultaneously involved in the process. Participants might include the builder/shipyard, third-party FMEA practitioners, Classification, operators, owners, etc. Workshops are very useful when applied early in the design stage of a system since the analysis will involve several parties with a vested interest in the outcome of the design, and takes place at a time when the design can be modified if required. A potential downside to forming a workshop of this nature is that some of the parties involved may have conflicting interests, which can slow the process down or impede free sharing of information needed to develop the FMEA.

The workshops are simple brainstorming sessions conducted in enough detail to identify and discuss specific failure modes. Part-time participants may be commissioned to provide input according to their area of expertise, usually via part-time participation in the FMEAs workshop.

### 3.2 Third-Party FMEA Practitioner(s)

A third-party FMEA practitioner working solo or a team of FMEA practitioners may be contracted to perform the FMEA. The level of interaction between the team and the stakeholders, and within the team itself will depend largely on the scope of the analysis, specific team member expertise and experience and size of the project.

The practitioner team may perform the analysis in a workshop style where the team meets to examine the system under study. They may also perform the analysis in a more independent fashion where the team initially meets for a collaborative brainstorming session to pool data and concepts for the analysis, each member then independently performing an analysis in their respective area of expertise and then reconvening for a group review of the overall analysis. The analysis may also be performed without workshops or brainstorming

sessions. Team members may already be familiar with the type of system being analyzed and may be able to proceed into individual analyses without requiring a workshop or brainstorming session. Each piece of the analysis would then be integrated by a project lead with oversight of the entire project.

Where the scope of analysis is limited or for simpler systems, an individual with the appropriate level of knowledge and experience may be sufficient to perform the FMEA. Though only a single person is performing the analysis, the overall development process remains the same.

| ***Typical Team Selection - Example*** |
| --- |
| *In the case of an FMEA for a Dynamic Positioning (DP) vessel, a typical third-party practitioner team consists of individuals with expertise in mechanical, electrical, DP operations as well as an individual familiar with all systems involved to take leadership of the FMEA and provide an integration function between the various system experts. For a stakeholders multi-discipline team conducting the FMEA in a workshop format, the disciplines will be the same as in the third-party practitioner team, but will also need an FMEA workshop leader/facilitator with experience in the FMEA technique and a technical recorder to capture all the information generated during the workshop.* |

### 3.3 ABS Participation in the FMEA Workshop

As indicated in 2/3.1 and 2/3.2, the FMEAs can be carried out as a stakeholder's workshop setting or commissioned to a third-party. The stakeholder's workshop style is the preferred method to take into account the opinions and experience of all the stakeholders.

There is no requirement that ABS personnel be part of the FMEA workshop. However, benefits can be derived by the participation of an ABS Engineering representative that will be directly involved in reviewing the FMEA and the system in order to grant Classification approval. Some of the benefits include:

*i)* As a participant in the FMEA workshop, the ABS Engineering representative will be able to point out the issues that ABS considers relevant for the classification of the proposed design, and thus should be discussed during the FMEA

*ii)* Participation in the FMEA workshop of the ABS representative that will be reviewing the FMEA will minimize the amount of questions and clarifications at the time of the ABS review of the FMEA because he/she will be familiar with the study and design.

### 3.4 Team Preparation

Team preparation should include project introduction and discussion on the scope of the analysis. Any training needs should be identified. For example, with many FMEA facilitation tools readily available, is the technical recorder adequately trained to use the selected tool? If specific fault identifying techniques are going to be used in the process of identifying failure modes particular to the analysis, is the team capable of applying them? Such analysis techniques may include root cause analysis, fault tree analysis, etc. The team should also be clear on the approach, ground rules, assumptions and constraints placed on the analysis and be able to appropriately address those limitations.

## 4 Ideal Timing to Conduct FMEAs

Though an FMEA can be carried out at any point in the lifetime of a system, it is most advantageous to be performed early on in the design process. FMEAs performed early in the design stage have the advantage of catching design or system configuration issues in time to allow for modifications before construction. The FMEA can be used as an input in the design review process and will be updated to reflect any design changes. Although fully integrating an analysis of this type into the design process can slow development and increase costs due design changes, the benefits outweigh the initial expenditure. The benefits include 1) safer design as the most optimum risk control options are typically those incorporated early in the design process and 2) the savings realized by eliminating costly retrofits or system upgrades post-build may outweigh the initial expenditure.

The usefulness of an FMEA will largely depend on the level to which its findings and corrective actions were incorporated in the design process.

The timing and delivery for an FMEA performed to comply with Classification requirements will depend largely on the type of FMEA being performed and the requirements that need to be satisfied. Small self-contained systems can have their FMEAs performed at the vendor stage. Larger systems that are heavily integrated with other systems should have an FMEA performed by the system integrator prior to installation/commissioning. In some cases, it may be necessary to have an FMEA of the small self-contained system early on, and then the larger-scope integration FMEA (or similar type of risk study) later on in the design.

Regardless of when the FMEA study takes place, Classification society reviewers would look for evidence (e.g., updated drawings, documentation, etc.) that the FMEA findings were made part of the design and integration process.

*For a new vessel or installation, the building contract should specify that input from the FMEA or risk study requested by Classification be taken into consideration, and the FMEA should be commissioned as early as possible in the project. This needs to be negotiated accordingly in the contract.*

For an existing vessel or installation, company management needs to be aware that changes to the system may be required as a result of the recommendations arising from the FMEA and that sufficient funds must be made available to meet the changes.

FMEAs should be updated or re-performed in whole when modifications are made to an existing system covered by the FMEA or when retrofits or replacement controls systems are installed. The extent to which the FMEA is modified will depend upon the nature of the changes to the system(s) being analyzed.

On the other hand, if a vessel is converted for new purpose and it is required to have an FMEA, the output of the FMEA may be limited to the systems affected by the changes. Although extremely useful in discovering potential issues related to failure modes and their effects, FMEAs performed on existing systems have the disadvantage of not being integral to the system design process and FMEA recommendations may drive costly system modifications to meet the established criteria. If the FMEA is to be performed on an existing system, the solutions to FMEA findings can be managed through system upgrades or mitigated by operational procedures.

# SECTION 3 Developing the FMEA

## 1 Developing the FMEA

The following sections describe the development steps typically followed when performing an FMEA,

*i)* Data Management

*ii)* FMEA Study

*iii)* FMEA Report

## 2 Data Management

### 2.1 Data Collection to Support the Analysis

After concluding the initial tasks of establishing a scope and intent of study, selecting a team, etc., the owner/stakeholder will be engaged to deliver as much information on the subject of the FMEA as possible. This information might include general configuration and layout data, hardware listings, system schematics (such as electrical, HVAC, piping diagrams, etc.), previously performed system/subsystem FMEAs, prior trials documentation and operational philosophy documentation. Vendor-specific FMEAs may also be referenced for each piece of equipment, but are typically generalized documents that do not include installation specifications required for an accurate system analysis.

Data may also be collected by interviewing design personnel, operations, testing, and maintenance personnel, component suppliers and outside experts to gather as much information as possible.

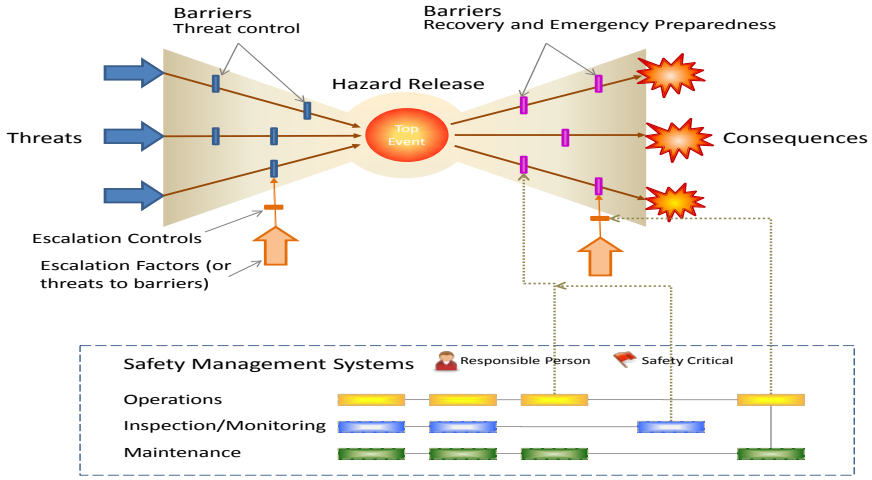
### 2.2 Other Risk Analysis as Input to the FMEA

Other types of risk analysis such as HAZIDs and HAZOPs are sometimes used for input to the preparation of an FMEA. They can play an important role in gathering data for failure analysis, particularly for systems without historical data to review or previous analyses. Other tools that might be used or fed into the process include fault tree, root cause and event tree analyses. They are described in detail in Section 3, Table 1. Note that none of these items are a standard input to FMEA development, but, if available, they can provide invaluable input, in particular to an FMEA that is being developed by third-party FMEA practitioners who more than likely were not involved in previous design or analysis activities for that particular vessel/system.

### 2.3 Data Analysis

The data analysis process used by the FMEA team is iterative and incorporates the above data sources, as available, to develop an overall analytical approach to the FMEA. The FMEA team facilitator will perform an assessment as data is received to determine if additional information is needed on system design, operational concepts, procedures, etc., and engage the necessary parties (including hardware vendors) to obtain the desired information and subsequent distribution to relevant FMEA team members. By approaching data collection and analysis in this manner, the team can establish a complete picture of the subject and concurrently focus on areas of interest to more readily identify potential issues.

## TABLE 1
## Risk Analyses that could Provide Input Information to an FMEA

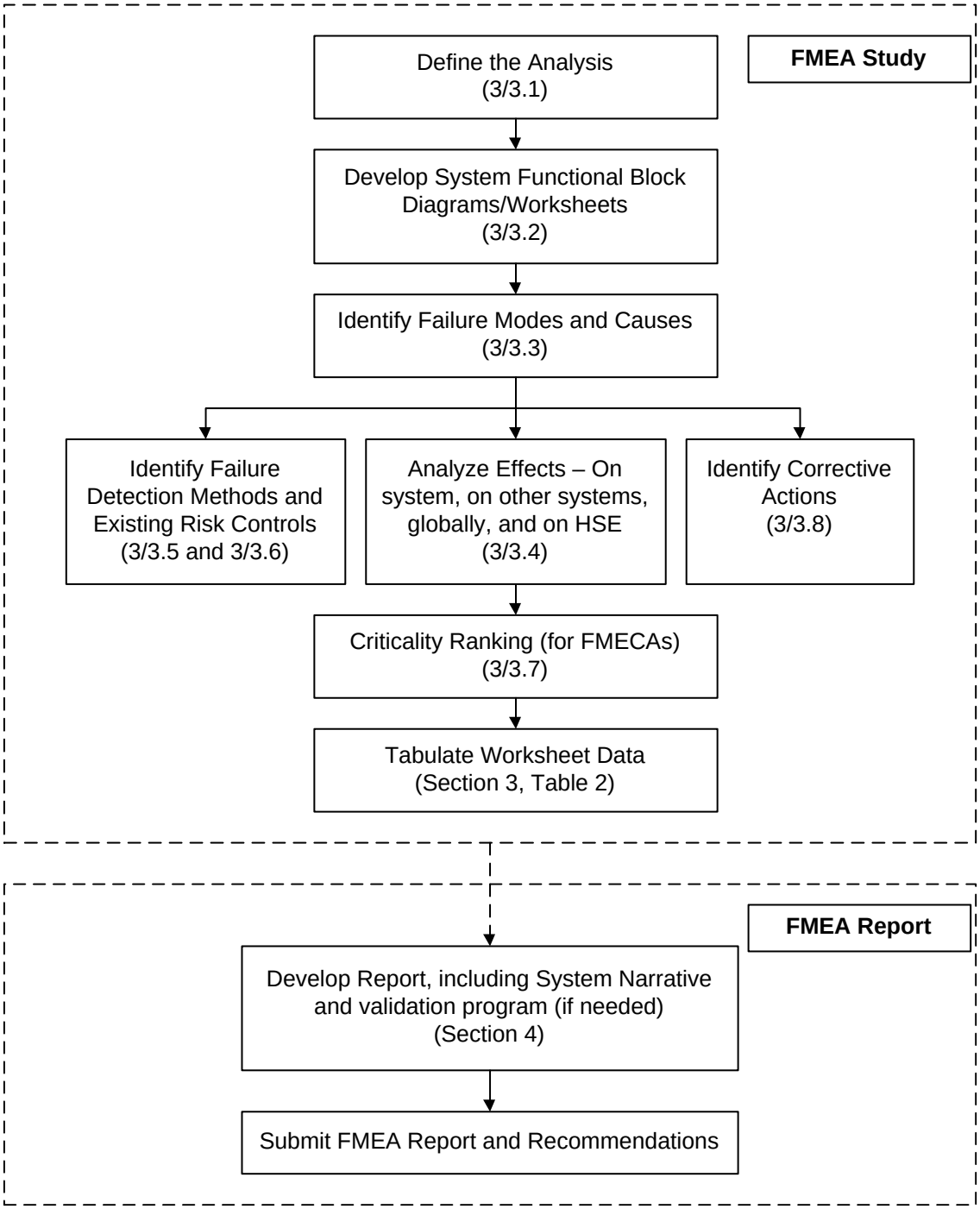
| *Type of Analysis* | *Description* |
|---|---|
| HAZID | Hazard Identification (HAZID) is a process used to examine potential causes of hazardous events (accidents), how likely it is the stated event might occur, what the potential consequences are if it did, and what options there are for preventing/mitigating the event. Hazard identification is an integral part of the risk assessment and management process. A HAZID study is performed via brainstorming workshops consisting of individuals with expert knowledge of the systems under study. The team identifies and classifies hazards using checklists, "what-if" lists, accident and failure statistics, by experience from previous projects, etc. |
| HAZOP | A Hazard and Operability study (HAZOP) is a qualitative, structured and systematic examination of processes and operations to identify and evaluate issues that may represent risks to personnel or equipment, or prevent efficient operation. The HAZOP technique was initially developed to analyze chemical process systems, but has been extended to other types of systems and complex operations. Much like a HAZID study, a HAZOP study is performed via workshops where experts meet to examine the system under study. The method can be applied to any process where design information is available. This commonly includes a process flow diagram which is examined in small sections, such as individual components and common equipment. A design intention is specified for each of these. The HAZOP team then determines what the possible significant deviations are from each intention, along with feasible causes and likely consequences. It can then be decided if existing safeguards are sufficient or if additional actions are necessary to reduce risk to an acceptable level. |
| Root Cause Analysis | Root cause analysis is a process designed for use in investigating and categorizing the fundamental cause of an initiating event with safety, health, environmental, quality, reliability and production impacts. The analysis helps identify what, how and why something happened with the intent of developing recommendations for corrective measures to prevent future occurrences of similar events. |
| Event Tree Analysis* | Event tree analysis is a technique to identify and evaluate the sequence of events that results from an initiating event. The analysis is performed by creating "event trees" that follow a logical sequence. An event tree analysis can result in different possible outcomes from a single initiating event. The objective of the analysis is to determine whether an initiating event will result in a mishap or if the event is sufficiently controlled by safety systems or procedures. |
| Fault Tree Analysis* | Fault tree analysis is a top-down, deductive failure analysis in which an undesired state of a system is analyzed using Boolean logic to combine a series of lower-level events. This analysis method is mainly used to determine the probability of an accident or a particular functional failure. |
| BowTie Analysis* | BowTie analysis is a risk approach that graphically displays the relationships between hazardous events, its causes and consequences and the risk control barriers in place to stop the accident sequence.<br>  <br><br>BowTies can be used as a simplified single diagram joining for an undesired event, its fault and event trees into one visualization. The left side of the BowTie is a pseudo fault tree that seeks all the potential precursors (or failures) and underlying causes of the accident and preventive control measures to avoid it.<br>The right side of the BowTie is a pseudo-event tree that describes the potential outcomes of a top event, and what controls are in place to prevent or mitigate the outcomes. |

* *Analyses marked with * are carried out for a select number of scenarios, where more detailed analysis is needed regarding the types of failures, combinations of failures, causes, potential outcomes etc. They are likely to be conducted after the FMEA to shed light into scenarios that had uncertainties.*

## 3 FMEA Study

The overall flow of the FMEA process is outlined in Section 3, Figure 1 below. Each of the blocks is discussed in detail in subsequent pages.

**FIGURE 1**
**FMEA Study Flowchart**



## 3.1 Define the Analysis

The system to be analyzed is defined by the system physical and operational boundaries, the equipment scope and depth of the analysis, system functions, interface functions, expected system performance and constraints, and failure definitions. High-level functional narratives of the system including descriptions of tasks to be performed for different operational phases and modes should also be developed at this stage.

## 3.2 Develop the Analysis Approach

The most common method for an analysis to identify failure modes is the use of failure mode worksheets supported by functional/reliability block diagrams.

### 3.2.1 Functional Block Diagrams and Reliability Block Diagrams

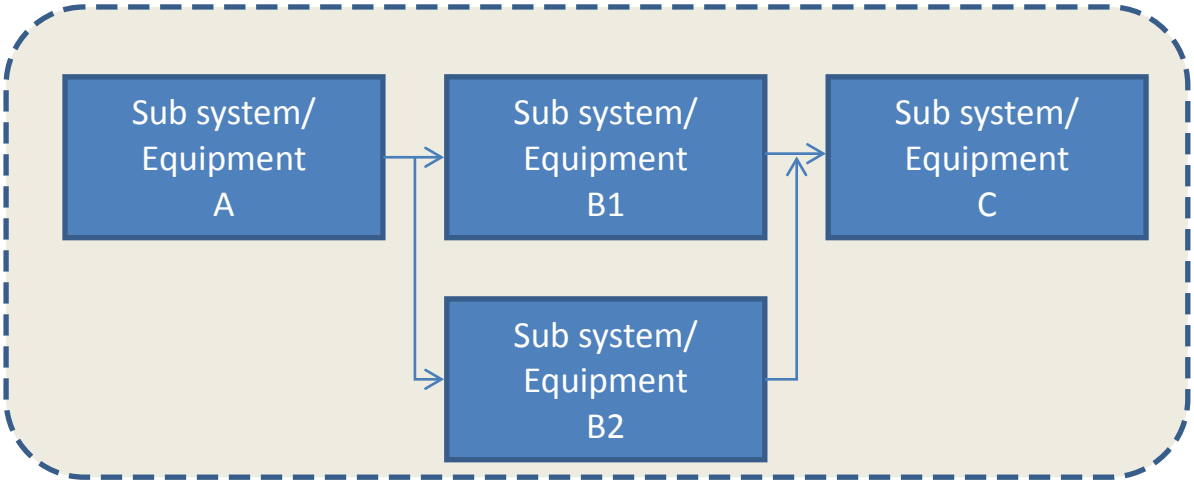
A functional block diagram is used to show how the different parts of the system interact with one another. They are powerful illustrative tools which aid in visualizing the interfaces and interdependencies between elements involved in system functionality. Block diagrams provide:

*i)* A high-level basis by identifying the chain of required systems/subsystems needed for successful operation, and

*ii)* For easier identification of possible failure modes and effects, failure causes and possible locations of hidden failures.

A special type of block diagram, the reliability block diagram (or dependence diagram), is well-suited for aiding in defining the scope and physical boundaries of an FMEA, in particular, FMEAs to prove the redundancy of a system. A reliability block diagram represents a system with its major parts drawn as blocks connected to each other, either in series or in parallel (See Section 3, Figure 2). A path in series indicates that if any of those blocks fail, the whole system fails. The parallel paths indicates there is a redundancy for that particular block and the system as a whole can still continue to operate through the other parallel path.

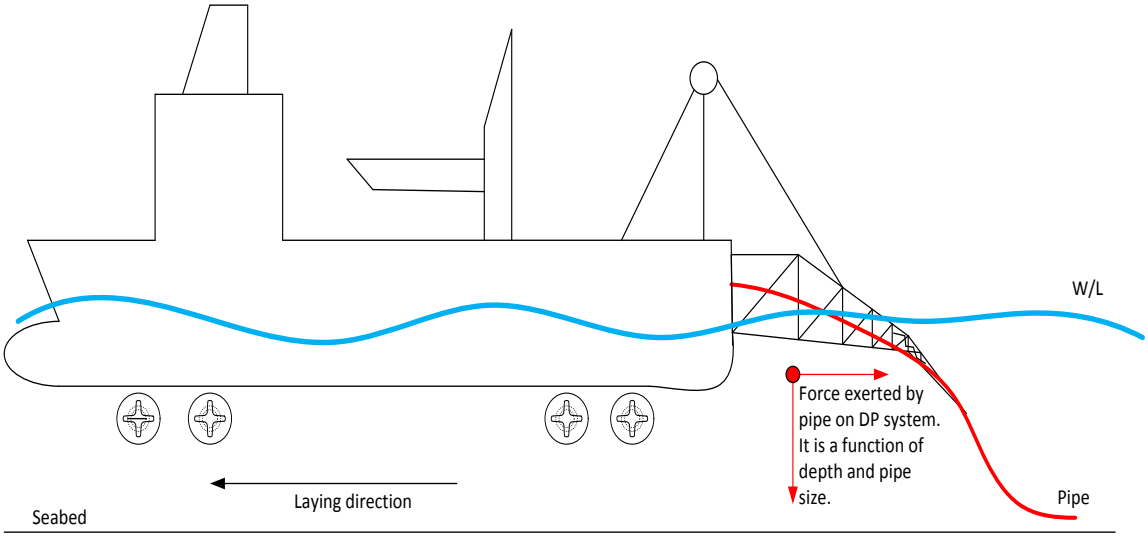
**FIGURE 2**
**Reliability Block Diagram (or Dependency Diagrams)**




One method for analyzing the system being studied is to break it down into different levels (i.e., system, subsystem, equipment, and field replaceable components). Schematics and other engineering drawings are reviewed to show how different subsystems, equipment or components interface with one another by their critical support systems such as power, hydraulics, actuation signals, data flow, etc., to understand the normal functional flow requirements. A list of all functions of the equipment can be prepared before examining the potential failure modes of each of those functions. Operating conditions such as temperature, loads, and pressure, as well as environmental conditions may be included.

The general vessel/installation operations should be understood and the likely impact of a failure within the operating environment should be related in the analysis process. This impact can be illustrated with a pipe-laying activity. Section 3, Figure 3 shows how the pipe-laying operation has an effect on the positioning of the vessel by applying a force to the DP system by virtue of the weight and size of the pipe being laid. This force is a function of the depth of water and size of pipe being laid and is thus project-specific. The FMEA study of the pipe-laying tensioner should include the potential wider impact on the vessel. If the pipe tensioner stops operating, the vessel is effectively anchored to the seabed by the pipe. This could be very relevant in a worsening weather condition.

**FIGURE 3**
**Example of External/Operational Forces That May Impact FMEA Study**




### 3.2.2 Failure Mode Worksheets

FMEA worksheets are tabulated data related to the identified failure modes and are a necessary organizational tool for performing the analysis that allows a condensed reference to all pertinent aspects of the analysis. A typical worksheet is populated with numerous pieces of information including the item or function being analyzed, associated failure modes and causes, local and global effects on the system, detection methods, safeguards, recommended corrective actions and risk/criticality classification. There is no set standard or style required for a worksheet, so content and organization may vary. However, it is important that content is sufficient to capture the analysis and convey relevant information regarding the system and the intent of the analysis. An example of a blank FMEA worksheet is provided in Section 3, Table 2. Note the highlighted columns for severity and likelihood assessments. This is risk-based ranking or criticality for the particular scenario that is captured during the analysis, thus turning the FMEA into a Failure Modes, Effects, and Criticality Analysis (FMECA). This is an optional but very useful step to help prioritize the corrective actions.

**TABLE 2**
**Sample FMEA/FMECA Worksheet**

| Operational Mode: | | Describe the operational mode | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Description of Unit | | Description of failure | | | Effects of Failure | | Safeguards | | Severity[1] | Likelihood[1] | Corrective Actions |
| ID | Function | Failure Mode | Failure Causes | Detection of Failure | Local | Global | Prevention of Failure | Mitigation of Effect | Low / Med / High | Low / Med / High | |
| | | | | How do you know that the failure is occurring? | Effects on the same system<br><br>Loss of function ? | Effects on other systems, on the overall system and effects on HSE | | | | | |

1 The severity and likelihood assessments in the highlighted columns are the risk-based ranking or criticality that is captured during the FMECAs. If the severity and likelihood are in the unacceptable range based on previously agreed criteria, corrective actions are needed, and the risk "after" corrective actions should also be evaluated.

## 3.3 Identify Failure Modes

Potential failure modes are determined by studying the relevant data compiled, in particular the functional element outputs. Failure modes within the physical and operational limits of the study scope are identified and described. The following typical failures are to be considered when determining failure modes and causes, but are by no means a complete list:

- Premature or spurious operation
- Failure to operate when required
- Intermittent operation
- Failure to stop operating when required
- Loss of output or failure during operation
- Degraded output or degraded operational capability

Section 3, Table 3 offers an example of failure modes used for FMEA of equipment, including the equipment control system. Note that these lists of failure modes are examples only. Different lists would be required for different types of systems.

**TABLE 3**
**Sample Failure Modes of Mechanical and Electrical Components**

| *Mechanical Components* | *Electrical Components* |
|---|---|
| External Leak or Rupture | Loss of/Degraded Power |
| Internal Leak | Fails with No Output Signal or Communication |
| Plugged | Fails with Low or High Output Signal |
| Mechanical Failure (e.g., fracture, galling, fatigue) | Erratic Output |
| Mechanical Damage (e.g., broken by external forces) | Fails to respond to Input |
| Wear | Processing Error |
| Corrosion or erosion | Electrical short |
| Loss of function [define the specific function(s)] | Loss of function [define the specific function(s)] |
| Loss of pressure | |

In addition, there are certain ground rules and considerations regarding failures that need to be in the mind of the FMEA participants, such as:

- What types of failure shall be discussed – functional failures vs. component-level failures
- If multiple failures shall occur simultaneously in order to result in the undesirable event, shall such a scenario be analyzed?
- What if the failures do not occur simultaneously but one failure could have occurred and was not detected, such as in safety equipment, and only when there was a demand for the safety equipment as a result of another failure, the safety equipment failure was discovered?
- How might a common initiating cause result in simultaneous failures of equipment? For example, the loss of power supply can result in the loss of function of multiple equipment.

These considerations are discussed in the following sections. Also, refer to IEC 60812, Section 5.2.3 for further guidance on Failure Mode Determination.

### 3.3.1 Functional Failures/Functional FMEA

A common approach for FMEA is to analyze failures related to a particular function of the equipment not being performed or being performed incorrectly.

Let us assume a system needs to pump *x gpm* from *point A* to *point B*. Typical functional failures for such a system would include: failure of pumping capability, pumping at a rate below requirements, pumping at a rate exceeding requirements and pumping backwards. The causes or failure mechanisms for these functional failures would include motor failure; loss of power; degraded pump or motor, under voltage to motor; over voltage to motor; leaky non-return valve on discharge of pump.

In order to perform a functional failure FMEA, the functions of the item under review must be defined. Note that the system/equipment under review may have more than one function.

### 3.3.2 Single Failure Criteria

FMEAs for Classification are typically performed to assess single failures and their effects (i.e., two simultaneous independent failures are not considered). It is customary to also consider a single act of mal-operation as a single failure. Assessments of this type are usually limited to errors that would result in unwanted consequences. A "single act" is generally taken to mean the operation of a single button, switch, lever, etc. There are two distinct instances when more than one failure should be considered in the FMEA:

*i)* When one of the failures can be latent, undetected or hidden

*ii)* When two or more systems or components can fail due to a single specific event or cause (common cause failures)

Both of these exceptions to the "single failure" criteria are discussed in the next section.

### 3.3.3 Hidden Failures

An exception to the single failure criteria is for the case of latent, or hidden, failures where their presence is undetectable. In such cases, single failures in combination with an initial hidden failure and their combined consequences will be analyzed. Since the initial hidden failure is unknown until the second failure occurs, the two failures would be considered together as a single event. Equipment that performs a back-up function and is in a non-operational or standby state may fall into this category if the functionality of the stand-by equipment cannot be verified until it is activated. Likewise, most safeguards and barriers are prone to hidden failures. They are not needed for operation and without proper monitoring to detect their failure. It is only discovered when there is a demand for the safeguard due to another failure. Refer to 3/3.6 for special considerations on hidden failures of safeguards and barriers.

It is important to note that not every hidden failure will necessarily be assessed. The level to which hidden failures are assessed depends on the goals and intent of the analysis. Typically, the analysis will be limited to hidden failure/additional failure combinations that lead to an undesired event, but loss of either component on its own will not.

***Hidden Failures – Example***

*Take a dual pump system where the loss of both pumps is considered unacceptable. Switchover from the primary to the back-up pump is performed automatically by a separate controller (which does not have fault detection). A failure of the switchover controller (undetected) followed by a failure of the primary pump would cause a total loss of the system since switchover to the secondary pump would not occur. In this case, the two failures would be considered a single event since the first failure (controller) was unknown until the second failure (primary pump) was realized.*

### 3.3.4 Common Cause Failures

A common cause failure is the loss of two or more systems or components due to a single specific event or cause: a design deficiency, a manufacturing defect, operation and maintenance errors, an environmental issue, an operator-induced event, or an unintended cascading effect from any other operation, failure within the system, or a change in environmental conditions. For the purposes of FMEA development, it is critical to identify aspects of the system design where a single event could cause the loss of more than one component leading to the system failing to perform its intended function.

In conducting the FMEA, consideration should be given to external factors such as temperature, humidity and vibration which can lead to common cause failures in redundant systems. An example of common cause failure might be a common power supply provided for redundant displays.

Common connections between systems create paths by which a fault in one system may affect another independent system. This is particularly true for redundant systems. Certain connection points are not only unavoidable but advantageous. The FMEA should consider the impacts of failure propagation and ensure adequate mitigation exists or is proposed.

***Common Cause Failures – Examples***

- *Simultaneous failure of two cooling water pumps due to power failure caused by damage to an electrical cableway, which contained power supply cables for the pumps, resulting in blackout conditions.*
- *Simultaneous failure of two computer networks due to software-related failure, resulting in the total loss of computer functionality.*
- *Loss of communications causes both master and slave drive to fail simultaneously because slave drive does not receive status of master drive and fails to automatically take over upon loss of master drive*

See IEC 60812, Section 6.1 for further guidance on Common Cause Failures.

### 3.3.5 Unavailability of Redundancy (due to maintenance or other cause)

In redundant systems, the second system provides an extra level of safety. For redundant Classification notations such as redundant propulsion or **DPS-2** or **DPS-3**, the operational philosophy expected by Classification is that during normal operations both systems are available. If one of the redundant systems is down for maintenance, the normal operations should cease until both systems are functional. Therefore, analyzing an FMEA scenario of failure of one system while the redundant counterpart is down for maintenance is not a requirement of Classification because such operational philosophy is not contemplated by Classification.

However, the owner/stakeholder may wish to perform an FMEA to include a reliability focus. A typical example may be where a particular system has a history of unreliability with certain components, requiring some part of the system to be down for maintenance on a regular basis. In this case, it might be desirable for the owner/stakeholder to ask that the analysis be performed not merely including a single failure of the unreliable component, but with the assumption that one of the unreliable components will already be unavailable at any given time during operations due to known maintenance issues. Such analysis, combined with criticality, may point the more likely failures, the most critical and would allow for corrective actions to increase the system reliability.

### 3.3.6 Failure of Active and Passive Components

Certain Classification FMEAs, such as those required for DP Systems, make use of a concept of passive and active components when deciding what types of failures will be included in the FMEA. The concept of passive and active equipment can be explained as follows:

- Active or rotating components in mechanical systems refer to machinery that moves and rotates during operation (e.g., pumps, compressors, generators, thrusters, remote controlled valves, etc.). For electrical/electronic systems, active equipment refers to those that require being powered in some way to make them work (e.g., integrated circuits, PLCs, switchboards, etc.).
- Passive or static components in mechanical systems refer to those having parts that normally do not move (e.g., pipes, tanks, vessels, shell-and-tube heat exchanger, manual valves, etc.). For electrical/electronic systems, passive components are those that do not require energy to make them work (e.g., electrical cables, resistors, capacitors, etc.).

Passive static components are, in general, considered to be of high reliability, whereas active components have a lower reliability. However, unless otherwise indicated (e.g., DPS-2 FMEAs), Classification position is that even passive components can have a significant probability of failure in mechanical systems (i.e., small diameter pipes, gaskets, flanged connections in the pipe, etc.) and its failure should be considered in the FMEA and demonstrated to be mitigated to an acceptable level.

### 3.3.7 External Events as Failure Modes

FMEA purists will contest that external events leading to equipment failure shall not be discussed in FMEAs. Traditional FMEAs are about assessing the impact of the failures that originate within the equipment. However, the coverage of credible external events is needed to fulfill the intent of many Classification-required FMEAs.

The system response to such external events such as fire and explosion in the vicinity, flooding scenarios, or adverse environmental conditions such as hurricanes and typhoons should be analyzed. One way to include these items in the analysis is to include them as the “failure mode”, and then proceed to complete the FMEA.

A clear example of this is the FMEA for a DPS-3 system. The intent of a DPS-3 FMEA is to prove that the system is not only redundant, but that there exists physical separation between redundant systems such that an event external to the DP system (e.g., fire or flooding) will not compromise both systems and result in the loss of the DP functionality. In these cases, it makes sense to list the external event as a “failure mode”, and analyze its impacts and existing control measures.

The analysis of these external influences shall analyze if the

- Equipment in question is designed to safely react to the external event
- External event can produce equipment failure of interest, including damaging the existing risk control measures
- External event can cause multiple failures (common-cause)

As an example of common-cause failures caused by external events, let us assume a fire near the diesel fire-fighting pump. Due to its location, the fire can damage nearby equipment which includes fire-fighting equipment, thus making the extinguishing of the fire difficult.

#### 3.3.8 FMEAs of Controls, Instrumentation and Safety Systems

There are multiple instances of in the ABS Rules and Guides of requirements to carry out FMEAs for instrumentation and safety systems.

These FMEAs are to consider the failure of the components within the instrumentation and safety systems, and its effects to verify that no hazardous consequences arise from their failure.

However, it is important to note that analyzing the failure of a safety system (safety ESD, alarm, etc.) will not result in a consequence unless coupled with a demand for its functionality. This demand upon the safety system is caused by a problem in the system it is protecting or controlling. Therefore, failures of the equipment under control should also be considered as to ascertain the adequacy of the safety system to protect the equipment.

## 3.4 Analyze Effects

Each failure mode is analyzed in terms of possible consequences on operation, function or system status. The failure mode under consideration may have a larger effect than just on the one element or function under study. So, in addition to the local effects, wider global effects are also considered. Particular attention should be paid to the impact a failure will have on the overall functionality of the system and how the system will react/behave after the failure is realized. The consequences of each identified failure affecting the item are captured in the analysis to provide a basis to evaluate any existing safeguards or to allow recommendation for corrective actions. Note that operational modes and interfaces become important factors to analyze the properly analyze global effects of failures. Paragraph 2/2.1 discusses functional and physical interfaces in FMEAs. When analyzing effects of a failure in one system, the effects on their interrelated systems must also be analyzed to give an accurate picture of the effects beyond the local system. Equally important for adequate analysis of local and global effects is to analyze failures within the context of each relevant operational mode as discussed in 2/2.2.

Section 3, Figure 2 and its explanation illustrate the relationship between operations and the FMEA. The FMEA should identify the end effect of any failure in terms of the impact on the safety and the operation, as in many cases, unsafe situations derive from negative impacts of failure on the operations.

#### 3.4.1 Effects of Interest (Undesirable Events)

The end goal of an FMEA is to evaluate whether enough measures are in place to prevent the occurrence of a hazardous or otherwise undesired event due to a single failure. Examples of such events could be:

- Injury
- Pollution
- Loss of integrity
- Inability to perform a function (such as maintaining position in a DP system, or propulsion in a Redundant Propulsion system, or well control capability in a BOP system)

A failure can result in consequences with limited local impact to the system where the failure occurred or in wider impacts to the vessel or installation. A leak of a flammable fluid from a pump can result in a loss of the pump, loss of the system and a fire that can spread and have effects beyond the immediate system of interest. All the potential consequences should be discussed,

It is important to determine as part of the FMEA scoping what are the undesirable events or effects of interest. Before the FMEA, these effects of interest should be communicated to all participants to help focus the analysis. During the FMEA, the possible realization of these effects should be considered in every failure and clearly documented if the possibility exists. This approach minimizes the possibility of FMEAs that do not satisfy their intent because they do not clearly discuss or document if the effect of interest could be realized upon a particular failure.

*It is a best practice for FMEAs to consider the worst credible potential effects that could result from the failure. This includes considering what could happen if the risk controls that are supposed to detect, prevent or mitigate the failure do not work because they are themselves in an undetected failed state (hidden failures) or due to common-cause failures (common precursor led to both failures).*

See IEC 60812, Section 5.2.5 for further guidance on Failure Effects.

## 3.5 Identify Failure Detection Methods

A given failure mode will manifest itself in a way which can be observed through system behavior and through any number of indications. A necessary component of an FMEA is the identification of failure detection methods for each failure mode.

Detection can occur by various means including visual or audible alarms, sensor limit warnings, sensor health and status checks, data comparison algorithms, operator observation, etc. By identifying detection methods, an assessment can also be made concurrently to determine if detection methodology is sufficient to accurately identify the failure, either by the system or the operator. If insufficient detection exists (see 3/3.3.3) or if the failure can be easily misdiagnosed leading to a larger issue, corrective actions should be made to add additional detection methods (e.g., additional sensors, operator checklists).

Adequate time must be available to react in case operation action is required to reach safe state or prevent escalation. If this is a concern, failure detection is no sufficient and prevention of the specific failure mode is necessary.

## 3.6 Identify Existing Risk Control Methods

This is the part of the analysis where we take note of all the existing protection mechanisms to prevent the failure or to mitigate its consequences. In a new-built situation, only the risk control methods shown in the drawings should be assumed to be in-place in the design. If a particular risk control method is not shown in the drawings, and the FMEA team deems it is needed, then a corrective action should be stated so that it will be implemented.

When analyzing risk controls, it is important to consider their potential for hidden or latent failures. Risk controls tend to be safety equipment or equipment that performs a back-up function and is in a non-operational or standby mode. Without proper monitoring to detect a failure of the risk controls, such failure is only discovered when there is a demand for the risk control due to another failure. Since the initial hidden failure is unknown until the second failure occurs, the two failures can be considered together as a single event, and thus analyzed together in the FMEA.

It is important to note that not every hidden failure will necessarily be assessed. The level to which hidden failures are assessed depends on the goals and intent of the analysis. Typically, the analysis will be limited to hidden failure/additional failure combinations that lead to an undesired event, but loss of either component on its own will not.

See IEC 60812, Section 5.2.7 for further guidance on “Failure Compensating Provisions”.

## 3.7 Criticality Ranking (for FMECA)

See 2/2.5 as well as IEC 60812, Section 5.2.8 and 5.2.9 for further guidance

## 3.8 Identify Corrective Actions

If the analysis indicates that the undesirable consequences can result from a single failure, corrective actions should be suggested to demonstrate compliance with the class design philosophy.

Typical solutions suggested during FMEAs to correct identified failures in a manner compliant with the design philosophy set forth in the Classification requirements are:

- Redundancy in design (this may be the only corrective action acceptable if the system functionality must continue after a single failure)
- Safe and controlled shutdown
- Actions to reduce likelihood of the failure

Any repercussions or changes deriving from implementation of the FMEA corrective actions should also be noted and submitted to Classification such as modifications to maintenance procedures or schedules, updates to drawings, documentation, etc.

Recommendations can be categorized into priority groups, for example, “Classification Requirement”, “For Immediate Attention”, “For Serious Consideration”, and “For Future Improvement. Decisions.” It is the responsibility of the entity engaged on the contract with Classification (i.e., shipyard, owner, etc.) to follow through on the corrective actions needed to comply with Classification requirements.

# SECTION 4 FMEA Report and Classification Review of FMEA

## 1 FMEA Report

The FMEA report should contain sufficient system information for the reader to understand the stated failure modes, effects, existing risk control measures and related recommendations. In addition to a detailed narrative description of a system, failure modes and effects narratives should also be included to describe each of the relevant failure modes and effects for a given system.

### 1.1 Report Structure

An FMEA report is structured according to the scope of the study. At a high level, the parts of the FMEA report should include:

- Executive Summary
- Introduction and Background
- Description of Systems
- Conclusions and Corrective Actions
- FMEA Worksheets
- Reference Data

The executive summary should present the conclusions and corrective actions of the FMEA, pending as well as those corrective actions already implemented.

The introduction should give all the background information needed so the report can later be understood and used by someone that did not participate in the study. It should include a statement of the purpose of the FMEA, when it was developed, who the participants were, assumptions, approach, etc.

The description of the system(s) should include a narrative as well as a block diagram graphically identifying the scope of study. The block diagram is helpful to the team in preparation for the analysis as well as a valuable resource during the analysis and to anybody reviewing or consulting the final FMEA report.

Each major system within the scope of the study is given its own section of the document which should contain enough descriptive information for the reader to understand overall layout, design and functionality, along with sufficient data (including functional schematics, drawings, etc.) to allow comprehension of the failure modes and effects.

The report should contain descriptions of identified failure modes, causes and effects as they pertain to the subject of the study, a summary of any conclusions or recommendations, and any outstanding or unresolved action items.

The FMEA worksheets are typically used to record, in a tabulated format, failure modes, causes, effects, detection methods, safeguards and recommendations throughout the FMEA process. These can be included at the end of each system section or compiled in their entirety as an appendix.

When FMEA proving trials are planned or required, there should be a trials program report that is either a stand-alone report or incorporated as part of the FMEA report. The trials program report is to provide test sheets for failure modes identified through the analysis. The test sheets will contain methods for testing, procedures to perform the tests, results from the tests, and any comments or recommendations. Results from trials may influence the content of the FMEA report and the FMEA should be updated accordingly.

A typical FMEA report contains the information depicted in Section 4, Table 1.

## TABLE 1
## Sample FMEA Report Structure

| Sections | Subsections | Description |
|---|---|---|
| *Executive Summary* | Intent of FMEA | This summary provides a global assessment of priority issues and recommendations, if any. It can be presented in a tabulated format showing the overall number of failure modes, causes, criticality ranking of the failures, if carried out. If the FMEA identified any issues that need attention to reduce risk and comply with Classification requirements, a list of the plan actions should be provided in order to make the system comply with the Classification requirements. |
| | Summary of FMEA Conclusions | Additionally, for large and complex systems, it helps to provide a summary of conclusions for each major subsystem or equipment. |
| *Introduction and Background* | General | General description of the scope and purpose of the document in an introduction of the FMECA. This is a concise, aggregated description of the purpose of the FMECA, and should include the date it was conducted, the intended audience of the FMECA, as well as its contents. |
| | Applicable ABS Rules | Refer to the applicable Rules, desired Classification notation and specific requirement for which the FMEA is developed. |
| | Scope and Intent of FMEA | This is a description of the scope and intent of the FMEA. Should include the intended audience, as well as its contents. |
| | FMEA Version/Date | Identify if prior FMEAs have been conducted, what are the changes and the version for the current document, as well as dates when prior and current FMEAs were conducted. |
| | Design Changes | If the system in question has experienced design modifications since the previous version of FMEAs or there have been modifications to supporting systems or other systems which may impact system under analysis, describe those changes. |
| | Participants and Reviewers | List the names and roles of the FMEA participants, facilitators, reviewers and editors. This provides a source of informed personnel and/or accountability. For multiple revisions of an FMEA, provide a log listing the names and roles as well as which version they reviewed or edited. |
| | Key Design Concepts | Describe the key design features for the system redundancy, including the redundant features of the supporting utilities. This is only applicable for systems required to have redundancy and for which the FMEA is performed in order to determine the existence and adequacy of the redundancy. |
| | Main Equipment (Physical Boundaries) | Identify the pieces of equipment and machinery that were analyzed in the FMEA. List the higher level system/subsystems and individual equipment, as applicable. |
| | Modes of Operations (Operational Boundaries) | Description of all modes of operations considered. This should include both the high level operations of the vessel/installation, critical activity modes or missions, as well as the modes of operation of particular systems analyzed. |
| | Vessel Overview and Specs | Provided for quick definition reference. |
| | FMEA Approach | An introduction and explanation of the process as a way to inform the reader how to interpret the results of the FMEA. If risk assessment and risk matrix were utilized, provide the risk matrix and describe how it was used. |
| | Ground Rules and Assumptions | Ground rules could be type of failures, ultimate consequences of concern, excluded items, etc. Needed for transparency of the analysis so that all users and reviewers of the FMEA understand the basic ground rules and assumptions. |
| | Glossary | Abbreviations and definitions provided for quick reference |
| *Description of Systems* | Subsystem 1<br>Subsystem 2<br>Subsystem 3<br>Subsystem 4 | Failure modes and related recommendations, per system. For example, for a DP FMEA, these sections would include:<br>• Power Generation<br>• Power Management<br>• Propulsion and Thrusters<br>• DP Control |
| *Conclusions/ Corrective Actions* | | An overall assessment of the findings of the FMEA. List of corrective actions that originated from the FMEA. If none, are all the failure modes analyzed in compliance with the Classification design philosophy? |
| *Reference* | | List of drawings with revision numbers, manuals, etc., used to develop the FMEA. |
| *Appendices* | FMEA Worksheets | Completed FMEA worksheets. |
| | Tables of Abbreviations | Table of abbreviations used in FMECA is provided for quick definition reference. |
| *Verification plan* | Selected tests, procedures, and expected results. | A verification plan to validate the conclusions of the FMEA is not required for every FMEA. This may be a separate stand-alone document. See Section 5 for details. |

### 1.2 FMEA Internal Review Process

The review process during FMEA development is somewhat iterative in nature. A provisional report with preliminary recommendations will be supplied to the owner/stakeholder for review. Any modifications, technical issues or areas of interest will be discussed among the FMEA team and stakeholders so that the analysis and recommendations are clearly defined and understood. If any modifications are necessary, the FMEA team will appropriately amend the document and deliver a final version for acceptance.

## 2 Classification Review of the FMEA

The entity that has signed the contract with Classification is ultimately responsible to see that an FMEA report that satisfies the intent of the FMEA requirement is submitted to Classification. In the majority of cases the FMEA will be submitted directly by the vendors contracted and Classification will use the FMEA conclusions as evidence that the design is in compliance with the Classification philosophy requirements (i.e., redundant systems, no single failure leading to unsafe situation, etc.).

The FMEA should refer to the version of the design submitted for Classification approval. Any revisions to drawings or documents referenced in the FMEA report may affect the findings of the FMEA, and require updating of the FMEA as necessary and submitted for review.

If the FMEA was conducted with additional goals over and beyond meeting Classification requirements, such as optimizing the design, identifying situations critical to operations, or developing a reliability-centered maintenance plan, it would facilitate the review if the Classification items are somehow highlighted.

### 2.1 Pitfalls and Common Problems in Classification Submitted FMEA

This section highlights typical problems encountered on FMEAs submitted to Classification. There are issues that may be specific or more prevalent among certain systems, but the reader can use this list as a checksheet to avoid making these common pitfalls. Guidance on how to avoid these pitfalls is given elsewhere in this report and the specific section also referred to in the information in parenthesis.

**Scope**

- Parts of the system omitted in the analysis (see 2/2.1, 3/3.2.1 and specific requirement in Section 7)
- Critical operations omitted the analysis (see 2/2.2, 3/3.2.1 specific requirement in Section 7)

**Failures**

- Incomplete failure list (see 3/3.3 and specific requirement in Section 7)
- No consideration of common-cause failures (see 3/3.3.4)
- No consideration of hidden failures (see 3/3.3.3)

**Effects**

- Global end effects not addressed (see 3/3.4)

**Controls**

- No consideration of hidden failures on existing controls (see 3/3.5 and 3/3.6)

**Corrective Actions**

- Failure of or delayed follow through of corrective actions (see 3/3.8)

**Overall**

- Insufficient descriptions in the worksheets to understand the failure scenarios (see 3/3.2.2)
- Insufficient information in FMEA Report (see Section 4 and specific requirement in Section 7)
- FMEAs not matching the latest design or off-the shelf FMEAs (see Subsection 4/2)
- Submittals too late (see specific requirements in Subsection 2/4)

## 2.2 FMEA and Supporting Documentation Submittal

Items required to be submitted to ABS to support the FMEA are listed in the individual Classification Rule requirements. However, as a general rule, the following documentation enhances understanding of the system and the FMEA, and it should be submitted to Classification as applicable:

- FMEA Worksheets (Mandatory), indicating revision number, date
- FMEA system Boundary Description
- System Design Specifications
- Functional or Reliability Block Diagram(s) showing interactions of all systems
- Detailed narrative of system functional description
- Piping and instrumentation diagram (P&ID)
- Basic schematics or equipment drawings
- General arrangement
- Process flow diagrams (PFD)
- Control system details
- Cause and effect matrix (useful in particular for items such as control, PLC and safety systems)
- One-line diagrams
- Bill of materials
- Operating procedures manual
- Emergency procedures
- Maintenance, Inspection, Testing (MIT) procedures
- FMEA validation plan and procedure, if required by Classification

As most of the items in the list above have been discussed elsewhere or are self-explanatory, they will not be expanded upon here. The cause and effect matrix and the operations manual have not been discussed before and are clarified in the next section.

*It must be emphasized that the FMEA should refer to the version of the design submitted for Classification approval. Any revisions to drawings, documents, functions or operations referenced in the FMEA report may affect the findings of the FMEA, and require updating of the FMEA as necessary and submitted for review.*

### 2.2.1 Cause and Effects Matrix

The cause-and-effects matrix was originally derived from Safety Analysis Function Evaluation (SAFE) Charts in API RP 14C for offshore facilities for documenting safety requirements. It is an easy way for those familiar with the equipment and operations to understand the logic being implemented in the safety system.

A cause and effects matrix identifies the possible causes (or deviations), listed in rows down the left side of the matrix. The system responses and their resulting effects are listed in columns across the top. The intersection cell in the matrix defines the relationship between the cause and the effect and aids in understanding the system safety control logic.

**FIGURE 1**
**Sample Cause and Effect Matrix**

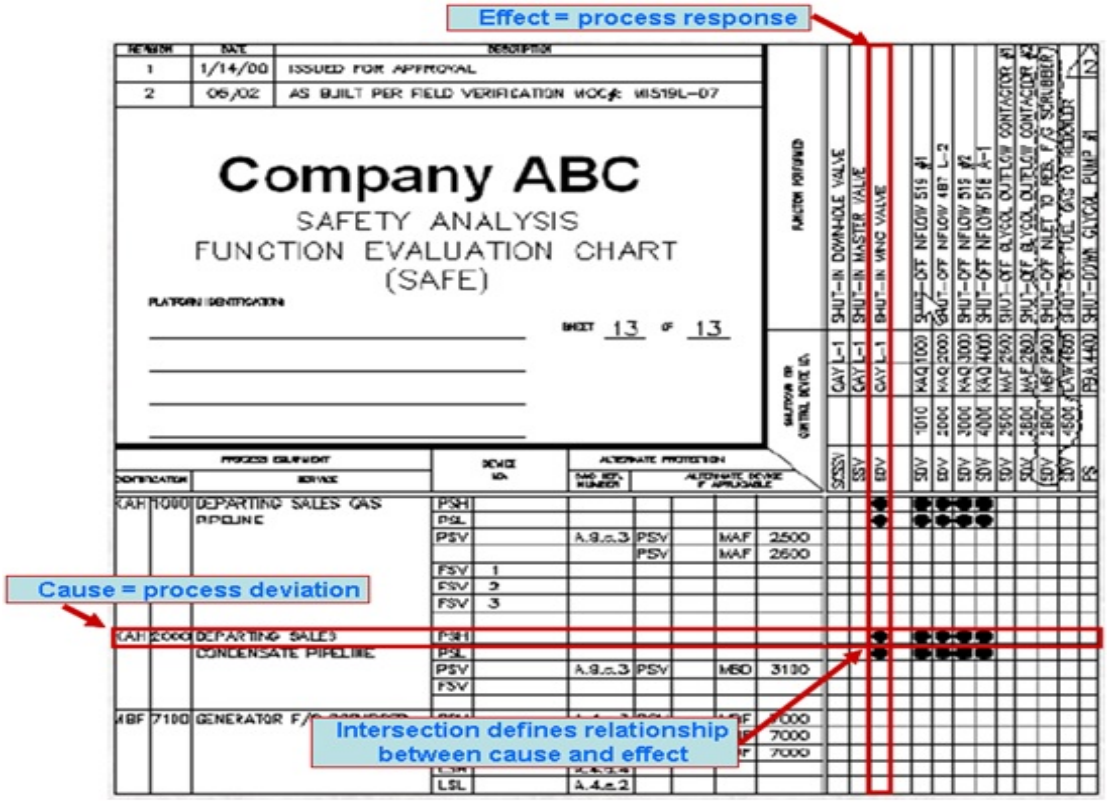



*Diagram courtesy of CFSE, Certified Functional Safety Expert*

### 2.2.2 Operational Manuals (Operations, Inspection and Maintenance, Emergency)

The requirement to submit operational and maintenance procedures to ABS serves several purposes during the classification process:

*i)* To demonstrate compliance with design and manufacturer's requirements

*ii)* As an aid to understand how the system will be operated, and what constraints, if any, are put in the operation of the system (e.g., for redundant systems, are there any operational limitations defined for the case when one system is unavailable?)

*iii)* To confirm that FMEA findings have been incorporated into the equipment operating phases, as needed

Recommendations from an FMEA performed early in the design process can usually be implemented to eliminate or reduce the adverse effects of a failure. However, when it is not possible to do so, operational and maintenance procedures and plans can be developed and/or updated to mitigate failures and their effects, in addition to providing a means to communicate actions to be taken when a failure does occur.

# SECTION 5 FMEA Verification Program

## 1 Purpose

The FMEA is a tabletop study and it alone may be insufficient to provide a satisfactory level of assurance. Thus, the FMEA process may also incorporate a trials program to verify that the systems will perform as predicted in the analysis.

Trials prove the FMEA in a structured manner. The specific tests included in a trials plan are designed to verify conclusions reached in the FMEA study.

For the purposes of this document, the terms FMEA testing, FMEA proving trials, FMEA validation and FMEA verification program are equivalent. They refer to trials and testing necessary to prove the conclusions of the FMEA or to establish conclusively the effects of failure modes that the FMEA desktop exercise had a high degree of uncertainty about. The standard term used is this document is FMEA verification program.

A verification program are not always required as part of an FMEA study. The inclusion of a verification program will be determined by Classification requirements for the particular system or by the owner/stakeholder's goals. FMEA verification programs for Classification have traditionally been limited to DP systems, certain drilling equipment for the CDS notation, and to a lesser extent for electronically controlled diesel engines. However, many stakeholders choose to perform an FMEA verification program for other types of systems simply to validate the conclusions of the FMEA, even though such program may not be required by Classification.

### 1.1 Scope of FMEA Verification Program

A question to be resolved early in the planning of the FMEA verification program is what failures are to be verified. The scope of the testing will be established by the FMEA team to comply with the Classification requirements, as well as other goals specified by the owner/stakeholder. In general terms, FMEA results that should be included in the verification program are as follows:

*i)* Those areas of a mechanical or control system which has mitigating barrier(s) to prevent the occurrence of a hazardous situation. The verification program is to validate that upon the specified failure, a minimum of one mitigating barrier performs as intended in order to prevent occurrence of a hazardous situation. Examples of such mitigating barriers are hydraulic load holding valves, alarms, sensors, etc.

*ii)* Those results for which there is reasonable uncertainty or disagreement of the FMEA assumptions. During the FMEA, uncertain assessments results are to be identified and discussed with the designer at time of Design Review for resolution. If a resolution is not achieved, these items should be included in the verification program. Examples of areas where inadequate data may be available to perform definitive analysis, thus should be part of the verification program include the behavior of interlocks that may inhibit operation of essential systems.

It is a best practice to identify, as part of the FMEA scoping and during the FMEA, the verification necessary to prove the FMEA conclusions.

Other items traditionally tested during FMEA verifications include

- System wiring checks
- Control software functionality and response to failures
- Confirmation of system's ability to operate with failures, in accordance with design intent
- Confirmation of system response to common system failures
- For redundant systems, confirmation of continued functionality after failure of a redundant system

When the Classification requirement necessitates that FMEA trials be carried out, the trial plans shall be submitted to ABS with enough lead time to allow for ABS review and input both by ABS Engineering and Survey.

Test procedures are to be submitted for approval and retained aboard the vessel. Test techniques must not simulate monitored system conditions by maladjustment, artificial signals, improper wiring, tampering, or revision of the system unless the test would damage equipment or endanger personnel.

As the Classification Surveyor prepares for witnessing the verification program, he or she will review and compare the FMEA, the verification plan and the current vessel drawings. The Classification Surveyor has the discretion to modify the verification plan to change or increase testing if he or she realizes that the FMEA does not accurately reflect the vessel or the vessel systems under trial (e.g., changes made to the vessel after the FMEA was developed, inaccuracies or gaps in existing FMEA).

The verification plan will be submitted to the owner/stakeholder for review and input prior to testing. It may be a conflict of interest when the entity developing the system is also in charge of finding its faults and testing for them, for example, a new-built situation where verification plans are typically developed by the shipyard. It is advantageous that other stakeholders, the owner in particular, have an input in the development of these plans.

The verification program can be carried out in a number of ways depending on the tests to be performed or functions to be verified. Tests that can be performed dockside or at the vendor facility will be identified so they can be verified independent of sea trials, if desired. If equipment FMEA tests are performed at the vendor facility, there may be a particular items regarding integration with the complete vessel or facility that can only be tested after integration.

#### 1.1.1 Alternate Testing Methods

Certain verification tests may not be feasibly carried out, such as when a system cannot be tested without causing damage to hardware or creating a situation that would be imminently hazardous to personnel. For this case, an alternative test method should be proposed together with an explanation of why it is an equivalent test.

If failure cannot be reproduced, at the very least, the safeguards to protect in case of such failure shall be tested to verify their existence, specifications, functionality, maintainability and methods by which a safeguard failure will be made evident.

Nontraditional tests, such as hardware-in-the loop (HIL) testing and self-diagnosis test, may be accepted on a case-by-case basis.

## 1.2 Verification Program Test Sheets

The verification plan, test sheets and associated procedures are created by the FMEA team and reviewed by the owner and Classification prior to being performed.

Test sheets are developed based on the established scope and identified failure modes from the FMEA report. Each test sheet usually represents a single set of tests for a given component or function. Each test sheet must be in a step-by-step or check off list format and should include:

- Description of the hardware/function being tested
- Purpose of the test, linking it to the FMEA and specific failure of concern
- Test methodology, including apparatus necessary to perform the test
- Procedures to perform the test (including equipment status, safety precautions, safety controls and alarms set points)
- Expected results (these are subject to change for first-time tested equipment based on results of initial testing and agreement from all parties involved).
- Test point and success/acceptance criteria
- Space to describe actual results and any comments

An example test sheet is provided in Section 5, Figure 1.

**FIGURE 1**
**FMEA Trial Test Sheet Example**

| EQUIPMENT: | REFERENCE SYSTEM | |
|---|---|---|
| Test # | HiPAP Test | FMEA Reference #: |

**Method :**

- On DP.
- All thrusters on line.
- HiPAP and DGPS online .

1. Interrogate transponder and select as reference on DP.
2. Lift transponder used for DP without deselecting.
   a) Select transponder to DP when suspended to test voting.
   b) Make small move.
   c) Stabilize .
3. Fail power to HiPAP transceiver unit. DPUPS5 Vacon Room.

**Results expected:**

1. DP uses HiPAP and it agrees other references.
2. Transponder rejected when moved. Transponder rejected when suspended.
3. Alarm . HiPAP rejected on power failure .

**Results found:**

**Comments:**

**Witnessed by:** **Date:**

## 1.3 Performing FMEA Verification Program

The verification tests are performed by the stakeholders, usually with oversight of representatives from the FMEA team and attended by a Classification surveyor, if it is a Classification requirement. Test sheets are provided to the owners/stakeholders in advance of the verification tests to allow time for review and comment. This also provides the stakeholders an opportunity to understand the tests that will be performed and that proper coordination has occurred on board to allow testing to go smoothly.

## 1.4 Results and Recommendations

Overall results of the FMEA verification program are discussed on board and any potential issues presented so that the owner/stakeholder will have an early opportunity to address items of importance prior to a preliminary report being delivered. A short one or two-page summary of issues and recommendations is provided by the FMEA trial team prior to their departure from the site.

Recommendations may include required system changes or mitigation strategies to meet Classification, or may be simple items that would improve system operability but are not required to satisfy any requirements.

If the system does not work as expected during a trial even though the FMEA and the trial plan seem to accurately reflect the as-built condition, a need for repair is normally identified to correct the situation.

If the system does not behave as expected in the FMEA because the analysis does not accurately reflect the as-built condition or because of an overlooked engineering issue, the Classification Surveyor writes an outstanding requirement in his or her report and requires the modification to be tested once in compliance with the Rules.

## 1.5 FMEA Verification Program Report

The complete FMEA verification program report with test results and recommendations should be developed. If being developed by a third-party, this complete document should be reviewed and accepted by owner/ stakeholders and submitted to Classification. There will be a dialogue between parties throughout the process so that recommendations are appropriate, corrective actions are properly implemented and requirements are met to the satisfaction of Classification and, if involved, the FMEA team. Close-out items are tracked within the document so that there is a single source of information and tracking for all parties involved to reference. Responsibility for closing-out items as well as additional revalidation tests shall be indicated.

A typical verification program report consists of a set of tests organized by system and comprised of numerous individual test sheets. Once the verification tests are performed, the complete FMEA report should capture the test data verifying the conclusions of the FMEA.

It is recommended that the List of Alarms (i.e. signal list, inputs/outputs list) be provided as an appendix to the FMEA verification program report so that alarm titles, set-points, and time delays can be verified during testing. In many cases, during a test, unforeseen alarms may occur and it is important for the Surveyor to be able to verify if the anticipated alarms specified in the test procedure actually occur. In some cases, a failure may have unintended consequences that were not expected.

A sample FMEA verification program report structure (using a DP example) is shown in Section 5, Table 1.

**TABLE 1**
**Sample FMEA Verification Program Report Structure (for a DP FMEA)**

| *Main Section* | *Subsections* |
|---|---|
| **Executive Summary** | |
| **General Background** | • Introduction<br>• Scope of Work<br>• Conduct of Trials<br>• Personnel<br>• System Limitations<br>• Reference Documentation<br>• Vessel Overview and Specs |
| **Trials Findings and Conclusions** | |
| **Recommendations** | |
| **Equipment Status and Records Verification** | |
| **Closeout Tabulations** | |
| **Trials Program** | • Test Sheets for Each System<br>• Power Generation<br>• Power Management<br>• Propulsion and Thrusters<br>• DP Control |
| **Appendices** | • Supplemental/Supporting Data from Trials<br>• Action Item Close-out Communication/Status<br>• Alarm List, Signal List, Input/Output List with alarm titles, set-points, and time delays. |
| **Trials Report Addendum** | |

## 1.6 United States Coast Guard Design Verification Test Procedure

For vessels under the United States flag which must undergo the U.S. Coast Guard (USCG) regulatory body review of a vital automation system, this phase of the approval process is known as the Design Verification Test Procedure (DVTP).

A Design Verification test is to be performed once, immediately after the installation of the automated equipment or before issuance of the initial Certificate of Inspection (and thereafter whenever major changes are made to the system or its software), to verify that automated systems are designed, constructed and operate in accordance with the applicable ABS rules and requirements of this supplement. The purpose of design verification testing is to verify the conclusions of the qualitative failure analysis (QFA). The DVTP is therefore an extension of the QFA and the two may be combined into one document. The DVTP should demonstrate that all system failures are alarmed and that all switchovers from a primary system component to a back-up component are also alarmed.

Design Verification and Periodic Safety test procedures are to be submitted for approval and retained aboard the vessel. Test procedure documents must be in a step-by-step or check off list format. Each test instruction must specify equipment status, apparatus necessary to perform the tests, safety precautions, safety control and alarm set points, the procedure to the followed, and the expected test result. Test techniques must not simulate monitored system conditions by maladjustment, artificial signals, improper wiring, tampering, or revision of the system unless the test would damage equipment or endanger personnel. Where a test meeting the restrictions on test techniques will damage equipment or endanger personnel, an alternative test method shall be proposed together with an explanation of why it is an equivalent test

The DVTP is a detailed test procedure to verify each failure mode identified in the QFA. Each test should include:

*i)* Safety precautions

*ii)* Equipment status prior to testing

*iii)* Equipment required to perform the test

*iv)* Control or alarm set-points

*v)* Test procedure to be followed

*vi)* Expected results

*vii)* Space for the cognizant Officer in Charge, Marine Inspection (OCMI) or Authorized Classification Society (ACS) Surveyor to record results during testing.

# SECTION 6 FMEA Lifecycle Management

## 1 Best Practices for FMEA as a Living Document

As general rule, ABS does not address the management of the FMEAs after granting of the Classification or special notation. However, ABS should be notified of any changes such as design, function, operations that impact the basis of the Classification requirements and it will be up to the discretion of the ABS reviewer whether to require a revised FMEA.

*In certain notations, such as CDS and DP, it is not discretionary, but a requisite that any changes to the design, function or operations of the systems that may affect the findings of the FMEA requires that the FMEA be updated as necessary and submitted for review. Such requirements are listed in Section 7 as applicable.*

The information contained in this Section 6 describes best industry practices.

Even though Classification may not address FMEA management specifically, the following questions should be posed by the asset owner to decide what is desirable and feasible for their particular situation:

- Is the FMEA to be kept on board as reference? This may not be possible for vendor-performed FMEAs, as the information within the FMEA may be vendor-proprietary. However, if the FMEAs are developed with this additional goal in mind, the information that makes them proprietary may in some cases be omitted without compromising the quality of the FMEA.
- Shall the FMEA be updated regularly or after a change? If so what, kind of change should trigger an FMEA revision?
- If the FMEA was originally performed by the vendor, who would perform any updates required as result of a change? Ideally, the vendor would be involved in the updating FMEA.

As per industry standard practice, certain FMEAs, in particular the FMEA and verification program (trials) reports for DP systems, are living documents that are intended to be maintained through the life of the system to which they pertain. They should be kept up-to-date on board for use by staff as required. The reports should be updated to reflect the latest information on a given subject including any system upgrades, modifications in configuration or changes to operational setup.

### 1.1 Best Practices for FMEA as an Operations Resource Document

An important use for the FMEA developed during the design phase of a system is to be a resource for operations and training for the crew. The FMEA can be a reference document to improve operator understanding of the risks and corrective actions in place shall a particular failure occur. For example, the FMEA can be used to find out, upon detecting a particular failure, information such as:

- The predicted consequences and impact on other systems
- What corrective action shall be taken
- The impact on the redundant features of a system if an item of equipment is taken out of service

The findings of the FMEA are incorporated into the operations, maintenance, emergency and training manuals. In the case of DP FMEAs, it is a best practice to incorporate the FMEA findings within the Well/Activity Specific Operating Guidelines (WSOG/ASOG) for mobile offshore drilling units (MODUs) and offshore support vessels, respectively.

## 1.2 Best Practices for FMEA Lifecycle Management

Ideally, proprietary issues can be worked out with the vendor and the owner of the vessel or installation, so the FMEAs conducted for the systems can be shared with the operating company that is responsible for the safe operation of the vessel or offshore installation.

In certain cases, such as FMEAs for DP, the full responsibility and ownership of the FMEA should be with the operating company. The DP FMEA is kept onboard and used as a reference, but the ownership of the FMEA typically resides within the management team ashore who is the responsible point for changes. It is not an individual's responsibility as such, though it is common that the vessel superintendent or the asset manager in the shore-side management office be designated the focal point and should have a thorough understanding of the FMEA management process. Key personnel onboard have the responsibility to make the shore management team aware of any deficiencies or inaccuracies in the FMEA as they themselves become aware of them. The management team is responsible for ensuring that any such deficiencies or inaccuracies are corrected in a timely manner.

The FMEA should be identified as a controlled document embedded within the quality management system of the owner. Any changes to the FMEA contents will be identified through the audit trail.

It is essential that an FMEA change control management procedure is in place as part of the company quality or safety management system under the ISM Code. Adopting this procedure provides a formal process to track every change in the vessel or installation systems and to capture, record and feedback decisions to the vessel for implementation of corrective actions.

*The change control management procedure must include a facility to feed back into the FMEA any failures in operation, including those not resulting in an incident.*

## 1.3 Changes to the Classed System and FMEA Revisions and Submittals

Any upgrades, modifications or changes that affect the FMEA must be evaluated to determine what action will be taken so that the documentation is in sync with the latest system configuration. This may entail simply modifying an existing FMEA study and issuing a revised report or producing a completely new FMEA and report along with a new or modified verification program. Modifications that pertain to a Classification requirement should trigger the resubmission of a revised FMEA report to Classification.

It is a best practice that the FMEA report be periodically reviewed for accuracy as changes may creep in that are not obvious. It is a Classification requirement for certain systems, such as for DP systems, that a review of the FMEA occurs every five years, even if no apparent changes to the subject have occurred over that time frame. The idea is to catch hidden or unreported modifications or changes that had slowly and almost imperceptibly crept into the system and operations.

## 1.4 FMEA and Management of Change

The FMEA is a tool to aid in the verification of vessel safety and compliance with certain Classification design requirements. Significant changes to the classed system may require updating of the FMEA to assist in verification that the changes did not compromise vessel safety or hinder compliance with Classification requirements.

The FMEA should be governed by the company's management of change program. If no such program exists, it is suggested that the updating of the FMEAs be governed by the company's safety management system and a management of change form specific to the FMEA process be developed. An FMEA Management of Change form will include, as a minimum, the entries listed in Section 6, Table 1 below.

Section 7 gives guidance on when the FMEA should be updated. As a general rule, ABS needs to be notified of any changes made that impact the basis of the Classification requirements. It will be up to the discretion of the ABS reviewer whether to require a revised FMEA.

**FIGURE 1**
**FMEA Lifecycle Management**

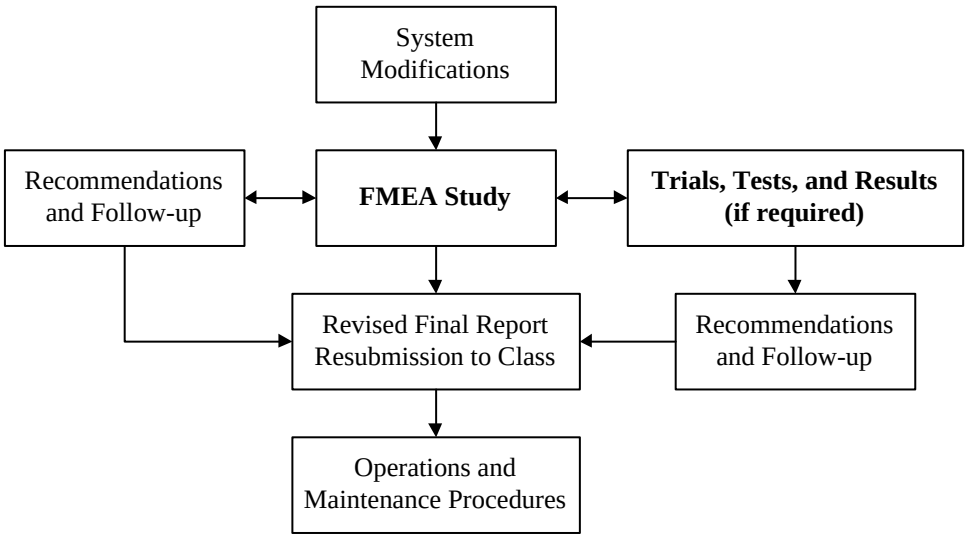



**TABLE 1**
**Suggested Entries in Management of Change Form for FMEAs**

| | |
|---|---|
| **General descriptors** | Date, Name of Vessel or facility, FMEA Reference No, Systems Affected, |
| **Background** | Reason for change (i.e., incident, accident, unavailability of in-kind replacement, etc.)<br>Description of the change, |
| **Effects of change on FMEA** | Does it affect the FMEA?<br>Has the FMEA been updated accordingly?<br>How was the FMEA modified? |
| **Recommendations** | What recommendations came out of the FMEA update?<br>How were they implemented?<br>Which relevant personnel need to know about actions arising from the FMEA?<br>How are they communicated to relevant personnel? |
| **Classification** | Do the change and the FMEA recommendations affect a Classification requirement?<br>If so, resubmit the revised FMEA and appropriate documents to Classification? |
| **FMEA Verification/Trial** | Test required? If so, what kind of tests? Have they been carried out?<br>Will test need to be witnessed by Classification? |
| **Other documents** | Do the change and/or FMEA recommendations affect the Operations Manual? Emergency operations manual? Maintenance manual? Drawings? Training?<br>If the change does affect any of these documents, have they been changed accordingly? |
| **Training and Communication** | Has the change and implemented FMEA recommendations been communicated?<br>Is training required?<br>Has personnel been trained? |
| **Fleet applicability** | Does this change and/or FMEA recommendation also apply to other vessels or facilities within the organization?<br>If so, what action has been taken? |
| **Circulation list** | Typical positions to be notified include Master or Offshore Installation Manager for an offshore installation, officers, Chief Engineer, maintenance, electrical, drilling crew, shore-based personnel, etc. |
| **Signatures** | Appropriate signatures from vessel or installation management and/or supervisors |

# SECTION 7 System-Specific FMEA Requirements

## 1 Guidance for System-Specific FMEA Requirements

The use of risk studies in the industries served by Classification is becoming increasingly prevalent. The general elements of the FMEA process were discussed in detail in Sections 1 through 6. Section 7 provides the detail and clarification of select FMEA requirements that appear in the ABS Rules.

Section 7, Table 1 lists the different systems in Classification for which a risk study (i.e., FMEA or alike) is required and the subsection index to facilitate finding specific guidance. Faced with a particular Classification FMEA requirement, the user may choose to go directly to the relevant subsection as indexed in Section 7, Table 1. The tables in Section 7 can be used to clarify a certain requirement, much in the manner as one would use the dictionary to clarify a word.

The guidance addresses the following aspects for each individual FMEA Classification requirement:

- Purpose
- Undesired events (e.g.; consequences of interest)
- Systems or subsystems (physical scope)
- Modes of operation (operational scope)
- Typical failures
- Timeline and team
- Verification program
- Supporting documents
- Lifecycle management

The explanation for what is covered in each of these bullet entries can be found in Section 7, Table 2.

## TABLE 1
## Index of FMEA Requirements in ABS Rules and Guides

| **Steel Vessel Rules (SVR) • Offshore Support Vessels (OSV) • Under 90 meters [(1)] • Mobile Offshore Drilling Units (MODU) • Mobile Offshore Units (MOU) • Offshore Facilities • High Speed Craft (HSC) • High Speed Naval Craft (HSNC) • Gas Fueled Ships (GF) • Propulsion Systems for LNG Carriers • Lifting Appliances (LA)** |
|---|
| 1.1 Automation<br>General Automation,<br>Computer-Based Systems,<br>Wireless Data Communications for Vessel Services<br>Integrated Controls |
| 1.2 Electronically-controlled Diesel Engine |
| 1.3 Remote Control Propulsion<br>Automated Centralized Control (ACC)<br>Automated Centralized Control Unmanned (ACCU)<br>Automated Bridge Centralized Control Unmanned (ABCU) |
| 1.4 Gas Turbine Safety Systems |
| 1.5 Redundant Propulsion and Steering |
| 1.6 Single Pod Propulsion |
| **Dynamic Positioning Systems (DP)** |
| 1.7 Dynamic Positioning (DP) Systems |
| **Integrated Software Quality Management (ISQM)** |
| 1.8 Software |
| **Mobile Offshore Drilling Units (MODU)** |
| 1.9 Jacking and associated Systems |
| **Offshore Support Vessels** |
| 1.10 Subsea Heavy Lifting |
| **Certification of Drilling Systems** |
| 1.11 Drilling Systems/Subsystem/Equipment |
| 1.12 Integrated Drilling Plant (HAZID) |
| **Propulsion Systems for LNG Carriers** |
| 1.13 Dual Fuel Diesel Engine |
| **Gas Fueled Ships** |
| 1.14 Re-liquefaction, Dual Fuel Engine and Fuel Gas Supply |
| **Lifting Appliances** |
| 1.15 Motion Compensation and Rope Tensioning Systems for Cranes |

*Notes:*

1 For vessels constructed to the *Under 90m Rules*, certain FMEAs may not be required depending on the vessel tonnage and length or when a requirement is not cited to the *Steel Vessel Rules*.

## TABLE 2
## Structure of the Guidance for Each FMEA Requirement

| | |
|---|---|
| **System:** | **Name of system for which the FMEA is required** |
| Rule/Guide: | Rule or Guide stating the FMEA requirement for the system above, |
| **Requirement** | *This block is a textual copy of the Rule or Guide indicating the FMEA.* |
| **Purpose of FMEA** | The purpose of an FMEA is to demonstrate compliance with the design philosophy for failure situations. The failure design philosophy will be stated as "a *single* failure shall not lead to a specified *undesired event"*.<br><br>The specified undesired event is typically one of the three listed in the section below.<br><br>As part of the FMEA process, corrective action measures should be proposed to correct situations of noncompliance with the failure design philosophy. Identified non-compliances with the design philosophy should have been resolved or otherwise addressed by the time of submittal of the FMEA. |
| **Undesired Events** | This section specifies the system and/or global consequences that could occur after a failure and that the design must address and avoid. These undesired consequences of interest or events fall within these following broad categories:<br><br>1. Loss of system or equipment function or degraded beyond an acceptable level<br><br>2. Loss of equipment control<br><br>3. Any unsafe situation with potential to harm individual, environment or equipment.<br><br>Generally, Classification requirements cover systems whose functionality and control is critical to the safety of the vessel and personnel (i.e., propulsion in a ship, well control equipment on a MODU). For many of these Classification systems the loss of equipment or system function and loss of equipment control can ultimately result in an unsafe situation. Therefore, Classification design philosophy requirements for those systems are their continued functionality. |
| **Systems or Subsystems** | This section lists systems and subsystems whose failures are required to be addressed in the FMEA to determine their compliance with Classification' design philosophy. The list is not exhaustive and is the responsibility of the entity contracting Classification to determine and analyze all the classed systems whose failure can result in the undesired event specified above. |
| **Modes of Operation** | A system normally has multiple modes of operation and each mode can present distinct failure scenarios. In particular, failure modes can be operation-specific and the resultant consequences of the failure can vary greatly depending on the mode of operation.<br><br>The FMEA is to define the global operations at installation or vessel level (i.e., drilling operation, or pipe-laying), and local operations of the system/equipment which is part of the scope of the FMEA. |

| | |
|---|---|
| | The FMEA must analyze all the modes of operations (global and local) to identify failures, hazards and consequences of concern.<br><br>This section will present a list of modes of operations that are to be explicitly considered on the FMEA. The list is not exhaustive and it is the responsibility of the entity contracting Classification to determine and analyze all the modes of operations during which a failure can result in the undesired event specified above. |
| **Typical Failures** | This section illustrates the types of failures that are expected to be analyzed in the FMEA. The list is not comprehensive; does not address all possible failures and may include some that are not relevant for the design. All foreseeable failures are to be considered in the FMEA, even if not listed in this section. |
| **Timeline/ Team** | This section suggests the optimal time in the system life to conduct the FMEA. It also suggests who, of all the parties involved in the Classification process, should have the main responsibility for the FMEA and which type of subject matter experts should participate in the analysis. |
| **Verification Program** | If the system requires testing of FMEA results, this section gives a description of the expectations and responsibilities associated with testing the equipment, as well as the anticipated response to identified failures. |
| **Supporting Documents** | This section provides a list of the documents that aid in the review and understanding of the FMEA. |
| **Lifecycle Management** | This section indicates how the FMEA is to be used and updated during the operational life of the asset, as well as any requirement for resubmittal to ABS in case of changes that may impact the original basis upon which Classification was granted. |
| **Additional Notes** | Comments and notes not fitting in the other categories. |

## 1.1 Automation (General Control, Safety-Related Functions of Computer-Based Systems, Wireless Data Communication, Integrated Automation Systems)

RULE/GUIDE Steel Vessel Rules (SVR) • Offshore Support Vessels (OSV) • Under 90 meters Mobile Offshore Drilling Units (MODU) • Mobile Offshore Units (MOU) • Offshore Facilities • High Speed Craft (HSC) • High Speed Naval Craft (HSNC) • Gas Fueled Ships • Propulsion Systems for LNG Carriers • Lifting Appliances

---

**SVR Rule Reference**

[identical requirements for OSV, <90m, MODU, MOU, Facilities, HSC, HSNC, Gas Fueled Ships, Propulsion Systems for LNG Carriers, Lifting Appliances]

**Part 4** Vessel Systems and Machinery

**Chapter 9** Automation

**Section 2** Essential Features Requirements

**Subsection 3** Control Systems

**3.1** Conceptual Requirements **3.1.5** Failure Mode and Effect Analysis

***

**Section 3** Computer-Based Systems

**Subsection 5** Systems Requirements **5.5** Failure Mode and Effect Analysis

**Subsection 13** Data Communication

**13.3** Wireless Data Communications **13.3.3(a**) Risk Analysis.

***

**Section 4** Integrated Automation System

**Subsection 5** FMEA

---

**SVR Rule Requirements**

[identical requirements for OSV, <90m, MODU, MOU, Facilities, HSC, HSNC, Gas Fueled Ships, Propulsion Systems for LNG Carriers, Lifting Appliances]

**General Automation (4-9-2/3.1.5)**

*Failure modes and effects analysis (FMEA) may be carried out during system design to investigate if any single failure in control systems would lead to undesirable consequences such as loss of propulsion, loss of propulsion control, etc. The analysis may be qualitative or quantitative.*[(1)]

***

**Computer-Based Systems (4-9-3/5.5.1)**

*FMEA is to be used to determine that any component failure will not result in the complete loss of control, the unsafe shutdown of the process or equipment, or other undesirable consequences.*

***

**Wireless Data Communications (4-9-3/13.3.3(a))**

*A suitable risk analysis (such as a Failure Modes and Effects Analysis (FMEA)) is to be performed which demonstrates that an interruption or failure in the wireless data `communication will not lead to a hazardous situation.*

*Note: Consideration is to be given to the possibility of corrupted data and intermittent failures with comparatively long recovery times between interruptions.*

***

**Integrated Automation Systems (4-9-4/5)**

*Where the integration involves control functions for essential services or safety functions, including fire, passenger, crew, and ship safety, an FMEA is to be carried out. The FMEA is to demonstrate that the integrated system will 'fail-safe', and that essential services in operation will not be lost or degraded.*

1 Note: not in the Rule text: USCG requires a qualitative failure analysis such as FMEA.

---

**Purpose of FMEA**

Automation requirements, including the requirements to conduct an FMEA, apply to electrical, hydraulic, electronic, computer-based systems and equipment for control, monitoring, alarm and safety on board vessels.

Automation systems have Classification requirements to develop FMEAs for:

- General automation for essential services
- Safety-related functions of computer-based systems
- Systems utilizing wireless data communications
- Integrated automation systems involving control functions for safety and/or essential services

The purpose is to demonstrate that any single failure will not lead to an undesirable event such as:

- Lost or degraded function beyond acceptable performance criteria
- Hazardous situation (such as a state that is not fail-safe, complete loss of control, unsafe shutdown of equipment, loss of propulsion, blackout, etc.)

Corrective action measures should be proposed to correct situations of noncompliance with the single-failure design philosophy.

---

**Undesired Events**

The FMEA is to systematically analyze all foreseeable failures and investigate and document if there is a potential for

- Lost or degraded function beyond acceptable performance criteria of the system under control (i.e., loss of propulsion)
- Hazardous situation (such as a state that is not fail-safe, complete loss of control, unsafe shutdown of equipment)

*Note on Fail-safe concept:* A fail-safe concept is to be applied to the design of all control systems, manual emergency control systems and safety systems. In consideration of its application, due regard is to be given to the safety of individual machinery, the system of which the machinery forms a part and the vessel as a whole.

Below are examples of typical fail-safe states:

| *System or Component* | > | *Typical Fail-safe States* |
|---|---|---|
| • Propulsion speed control | > | Maintain state |
| • Controllable pitch propeller | > | Maintain state |
| • Propulsion safety shutdown | > | Maintain state and alarm |
| • Alarm system | > | Annunciated |
| • Cooling water valve | > | In most cases, open |

---

**Systems or Subsystems**

Computer-based systems subject to Classification requirements are to be assigned into the appropriate system category (I, II or III) according to the possible extent of the damage that may be caused by a single failure within the computer-based system.

| *System Category* | *Effects of Failure* |
|---|---|
| I | Failure will not lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment (e.g., nonessential systems, information and diagnosis) |
| II | Failure could eventually lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment. (e.g., Cargo tank gauging system, control systems for auxiliary machinery, main propulsion remote control systems (e.g., the control system from navigation bridge, etc.)) |
| III | Failure could immediately lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment. |

Category I systems by definition will not cause unsafe operation upon failure, thus there is not a Classification requirement to develop an FMEA.

Category II systems may include safety-related functions but there is no specific requirement for the FMEA to be submitted to Classification for review.

Note that where independent effective backup or other means of averting danger for the control functions is provided, the system Category III may be decreased to Category II.

Also note that in some cases a main propulsion remote control system, automation system or DPS system may be Cat II and because an additional special notation such as **ACCU** or **DPS-2** is selected. In these cases, the FMEA is required to be done as per the requirements of the special notations.

Category III systems have the most severe and immediate safety and environmental consequences in case of failure, and do require development on an FMEA and submission to ABS to support the Classification process. Examples of Category III systems include, but are not limited to:

- Safety system/equipment for main propulsion and electric power generating system associated with propulsion
- Burner control and safety systems
- Control system for propulsion machinery or steering gear (e.g., the control system from centralized control station, control system for common rail main diesel engine, etc.)
- Synchronizing units for switchboards

Failures of components within the computer-based control system are to be addressed in the FMEA, including the interfaces with other systems such as I/O signals.

Functional failures of equipment under control shall also be considered as to ascertain the adequacy of the actions of the safety-related functions in case of these failures. In other words, if the control system controls a pumping system, functional failures of the pump and its effects should be analyzed to determine what actions the control system takes to mitigate either the likelihood or the effects of the failure.

Certain systems with special notations have explicit automation FMEA requirements in the *Steel Vessel Rules* which are based on this FMEA concept for safety-related function of computer-based control:

- Control system from centralized control station (**ACC** and **ACCU** notation)
- Gas turbine safety systems
- Electronically controlled diesel engine
- Gas fueled engines

The intent of these requirements is very similar to the automation requirement discussed here, but for sake of clarity, they are described in detail in their respective System-Specific FMEA Requirements in Section 7.

### Modes of Operation

The failure analysis should consider failure scenarios under all potential modes of operations, as the failure mode, the likelihood and the consequences of the failure scenario vary depending on the operational modes.

The modes of operation are specific to the equipment under control. For example, typical modes of operation for a propulsion system will include:

- Start and stop

- *Underway.* Consider full range of speeds up to maximum speed and any special issues such as low NOx, fuel optimization.
- *Emergency actions.* Consider crash stop from full ahead to full stern, acceleration to maximum rpm (i.e., propellers emerged in heavy seas), etc.

Integrated automation systems can issue commands for the collective benefit and operation of the vessel. This ability to command multiple otherwise independent devices could theoretically direct two or more different devices to act in ways that, in combination, could be detrimental. The risk assessment (FMEA or alike) for integrated automation systems is to address possible risks associated with commands given to multiple devices in a way which could lead to a combined undesirable outcome.

The risk assessment for integrated automation systems should

- Consider all possible dangerous outcomes
- Identify situations that can result in these dangerous outcomes (they could arise from a malfunction of IAS or even from an IAS that works as intended, but their collective operation can create dangerous outcomes).
- Assess and/or suggest risk controls for situations that could lead to dangerous outcomes, either by software (Cat II/III requirements) or be addressed by means outside of the IAS.

---

**Typical Failures**

The lowest level of physical component failure required to be included in the FMEA for control systems is typically at the data acquisition unit level which includes the CPU, its I/O modules, the powering of the device, and any communication between multiple devices.

Physical components whose failures should be analyzed in the FMEA include

- CPU microprocessor/PLC
- Input/output modules
- Power supplies
- Electrical power cables
- Network hubs
- Buses
- Communication/data link cables
- Interfaces/displays
- Electrical power cables
- Others, as applicable

For functions permitting wireless data communications, consideration is to be given to the possibility of corrupted data and intermittent faults with comparatively long recovery times between interruptions.

Software may reside in several different areas of a given system and at multiple levels (i.e., operating system, PLC embedded logic). Software failures are to be considered at a higher level, almost like a system failure; to address how the system can prevent and recover from, for example, malware.

With the exception of the ISQM FMEAs, a detailed software failure analysis is not usually something considered in FMEAs. Classification Rules require the system developer to follow a recognized software quality assurance program, so it is generally assumed that by the time software is delivered and installed, it is error free.

Relays, terminal boards, indicator lights, switches, meters and instruments do not have to be included in the FMEA unless their failure would lead to a hazardous situation not discussed with a higher level component.

The risk assessment (FMEA or alike) is also to consider the interfaces in the system, analyzing failures related to the i/o such as faults in

- Signals arriving at IAS (for incorrect data and its effect on system operation)
- Signals leaving IAS (for combinations that could lead to dangerous outcomes

**Timeline/ Team**

The sponsor of the FMEA is either the designer of the equipment under control or the system integrator.

The optimal time for performing the FMEA is during detailed design when the design is mature enough to have sufficient detail about the system and equipment available, but still enough time is left in the process to include FMEA recommendations in final design and integration process.

The FMEA should include participation from subject matter experts in the control systems, operations, design and relevant vendors.

**Verification Program**

The specific goals of the FMEA trial tests include testing the:

- Effectiveness of system to identify failures
- Effect of identified failures on system/equipment
- Response of safety controls
- Verification of redundancy as needed
- Verification of fault tolerance, as needed
- Other measures to protect against failure

Even though there is no general FMEA validation trial for the computer-based systems in this particular requirement, it is to the discretion of the ABS Surveyor or ABS Plan reviewer to recommend specific testing of FMEA failures for which there is a higher degree of uncertainty. Self-tests such as Hardware-in-the-Loop (HIL) can be substituted, if adequate to prove intent and goals of verification program. If system failures cannot be replicated (destructive test, safety concerns, etc.), a partial test may be carried out to test functionally and verify existing safeguards, as indicated in the FMEA to detect/prevent/mitigate the failure.

Certain systems such as dynamic position systems have computer-based control, and are required under special notation requirements to submit an FMEA and FMEA trial plan. These requirements are specified in the DP FMEA requirements (7/1.7).

**Supporting Documents**

The FMEA must be submitted to ABS for review. In order to carry out a proper review of the FMEA, the ABS Plan reviewer needs the following information included with the FMEA report:

- General description of the scope and purpose of the FMEA
- Dates when the FMEA was conducted
- FMEA participants

- Summary of any corrective actions performed or pending as a result of recommendations of the FMEA.
- Detailed description, narrative and drawings of the system under control, and its control system.
- Layout and general arrangement drawings
- Single line diagrams
- System design specifications
- Description of the physical and operational scope and boundaries for the FMEA, including:
  - Functional blocks arranged in a reliability block diagram, showing interactions among the blocks (parallel paths for redundant functional blocks, in series for single blocks)
  - Modes of operation for the system
- FMEA worksheets, including:
  - Modes of operation
  - All significant failure modes associated with each mode of operation
  - Cause associated with each failure mode
  - Method for detecting that the failure has occurred
  - Effect of the failure on system functionality
  - Global effect of the failure on other systems, the asset, and HSE
  - Existing controls to prevent and/or mitigate the failure
  - Corrective actions needed to comply with ABS Classification requirements

Block diagram showing the system configuration including the user interface, description of hardware specifications, hardware FMEA, fail-safe features, security arrangements, power supply, and independence of systems (control, monitoring and safety shutdown).

For systems where loss of function upon a single failure is not an acceptable option, but redundancy is not possible, further study of non-redundant parts with consideration to their reliability and mechanical protection must be provided.

The operations, maintenance, inspection, testing, and emergency manuals are needed for ABS to confirm compliance with design and manufacturer's requirements and that the findings of the FMEA have been incorporated into the equipment operating phases. These manuals can all show operational configurations in which the systems redundancy can be bypassed.

**Lifecycle Management**

ABS needs to be notified of any changes made that impact the basis of the Classification requirements. It will be up to the discretion of the ABS reviewer whether to require a revised FMEA.

**Additional Notes**

## 1.2 Electronically Controlled Diesel Engines

RULE/GUIDE Steel Vessel Rules (SVR), Offshore Support Vessels (OSV), High-Speed Craft (HSC), High-Speed Naval Craft, Vessels Under 90 m

---

**SVR Rule Reference**
[identical requirement for OSV, HSC, HSNC, <90m]

**Part 4** Vessel Systems and Machinery
**Chapter 2** Prime Movers
**Section 1** Diesel Engines
**Appendix 1** Plans and Data for Diesel Engines
**Subsection 13** Testing, Inspection and Certification of Diesel Engines

---

**SVR Rule Requirements**
[identical requirement for OSV, HSC, HSNC, <90m]

**4-2-1A1 – Footnote 6**
… *Where engines incorporate electronic control systems, a failure mode and effects analysis (FMEA) is to be submitted to demonstrate that failure of an electronic control system will not result in the loss of essential services for the operation of the engine and that operation of the engine will not be lost or degraded beyond an acceptable performance criteria of the engine.*

***

**4-2-1/13.7.4(b) Stage B: type tests to be witnessed by the Surveyor.**
*iii)(e) Integration Test (2009): For electronically controlled diesel engines, integration tests are to verify that the response of the complete mechanical, hydraulic and electronic system is as predicted for all intended operational modes. The scope of these tests is to be determined based on the FMEA as required in Appendix 4-2-1A1 of the Rules.*

---

**Purpose of FMEA**

The FMEA requirement applies to any electronically controlled diesel engines (e.g., main propulsion engines as well as engines for auxiliary systems such as generators, or other mission-critical functions).

The purpose of the FMEA is to demonstrate that a single failure of any component within the electronic control system of the diesel engine will not result in the loss of function for the whole system below Classification performance requirements:

- For main propulsion, it is not to result in a loss of propulsion performance beyond that allowed per applicable notation requirement
- For auxiliary systems, it is not to result in the loss of the essential service the system is provided.

---

**Undesired Events**

The FMEA is to evaluate the potential for a failure to result in the following consequences:

- For propulsion system, loss of propulsion performance beyond that allowed per applicable notation requirements
- For auxiliary systems, loss of the essential service provided by system

---

**Systems or Subsystems**

Failures within the following systems are to be addressed in the FMEA:

- Electronic control systems (for any electronically controlled diesel engine), including but not limited to:
  - Electronic governor
  - Remote telegraph control
  - Fuel control (e.g., timing control, electronic over speed, etc.)
  - Engine valve control (e.g., exhaust valve, intake valve, etc.)

The FMEA requirement extends to all services which are considered essential to the operation of the engine, therefore, the FMEA of electronically controlled diesel engine shall include the following:

- For main propulsion engine, include failure analysis of the power management for diesel electric/multiple engine arrangements
- For auxiliary systems, include failure analysis of the generators (e.g. control for generator speed, isosynchronous, etc.)

---

**Modes of Operation**

The FMEA should consider failures of the engine in each of the following modes of operations, in addition to other operations that may be relevant:

- Start and stop
- *Underway.* Consider full range of speeds up to maximum speed, and any special issues such as low NOx, fuel optimization, etc.
- *Emergency actions.* Consider crash stop, from full ahead to full stern, acceleration to maximum rpm (e.g., propellers emerged in heavy seas), etc.
- Bunkering
- Maneuvering in port/coastal passage/ocean passage
- Mooring

---

**Typical Failures**

The lowest level of physical component failure required to be included in the FMEA for control systems is typically at the data acquisition unit level which includes the CPU, its I/O modules, the powering of the device, and any communication between multiple devices.

Physical components whose failures should be analyzed in the FMEA include:

- CPU microprocessor/PLC
- Input/output modules
- Power supplies
- Electrical power cables
- Network hubs
- Buses
- Communication/data link cables
- Interfaces/displays

- Electrical power cables
- Others, as applicable

For functions permitting wireless data communications, consideration is to be given to the possibility of corrupted data and intermittent faults with comparatively long recovery times between interruptions.

Software may reside in several different areas of a given system and at multiple levels (i.e. operating system, PLC embedded logic). Software failures are to be considered at a higher level, almost like a system failure; to address how the system can prevent and recover from, for example, malware.

Classification Rules require the system developer to follow a recognized software quality assurance program, so it is generally assumed that by the time software is delivered and installed, it is error free.

Relays, terminal boards, indicator lights, switches, meters and instruments do not have to be included in the FMEA unless their failure would lead to a hazardous situation not discussed with a higher level component.

**Timeline/ Team**

The sponsor of the FMEA is the equipment vendor. The FMEA should be performed early in the design stage to allow for modifications that may be needed, as well as adequate testing of any of the FMEA assumptions and conclusions. The FMEA should include participation from subject matter experts in the control systems, design and operations.

**Verification Program**

For electronically controlled diesel engines, integration tests are to verify that the response of the complete mechanical, hydraulic and electronic system is as predicted for all intended operational modes.

An FMEA verification program shall be developed and performed to verify the results of the FMEA. The specific goals of the tests include validating the:

- Effectiveness of system to identify failures
- Effect of identified failures on system/equipment
- Response of safety controls
- Other measures to protect against failure

As a minimum, the FMEA verification plan should include testing all failures with potential to result in loss of system function. Self-tests such as Hardware-in-the-Loop (HIL) can be substituted, if adequate to prove intent and goals of the verification program. If system failures cannot be replicated (destructive test, safety concerns, etc.), then existing safeguards must be functionally tested and verified, as indicated in FMEA to detect/prevent/mitigate the failure.

**Supporting Documents**

The FMEA must be submitted to ABS for review. In order to carry out a proper review of the FMEA, the ABS Plan reviewer needs the following information included with the FMEA report:

- General description of the scope and purpose of the FMEA
- Dates when the FMEA was conducted
- FMEA participants

- Summary of any corrective actions performed or pending as a result of recommendations of the FMEA.
- Detailed description, narrative and drawings of the system and the electronic control system for the diesel engine
- Layout and general arrangement drawings
- Single line diagrams
- System design specifications
- Description of the physical and operational scope and boundaries for the FMEA, including:
  - Functional blocks arranged in a reliability block diagram, showing interactions among the blocks (parallel paths for redundant functional blocks, in series for single blocks)
  - Modes of operation for the system
- FMEA worksheets, including:
  - Modes of operation
  - All significant failure modes (associated with each mode of operation)
  - Cause associated with each failure mode
  - Method for detecting that the failure has occurred
  - Effect of the failure on system functionality
  - Global effect of the failure on other systems, the asset, and HSE
  - Existing controls to prevent and/or mitigate the failure
  - Corrective actions needed to comply with ABS Classification requirements

For systems where loss of function upon a single failure is not an acceptable option, but redundancy is not possible, further study of non-redundant parts with consideration to their reliability and mechanical protection must be provided.

The operations, maintenance, inspection, testing, and emergency manuals are needed for ABS to confirm compliance with design and manufacturer's requirements and that the findings of the FMEA have been incorporated into the equipment operating phases. These manuals can all show operational configurations in which the systems redundancy can be bypassed.

**Lifecycle Management**

ABS needs to be notified of any changes made that impact the basis of the Classification requirements. It will be up to the discretion of the ABS reviewer whether to require a revised FMEA.

**Additional Notes**

## 1.3 Remote Control Propulsion [Automatic Centralized Control (ACC), Automatic Centralized Control Unmanned (ACCU), Automatic Bridge Centralized Control Unmanned (ABCU)]

RULE/GUIDE Steel Vessel Rules (SVR), Offshore Support Vessels (OSV), High-Speed Craft (HSC), High-Speed Naval Craft, Vessels Under 90 m

---

**SVR Rule Reference**
[identical requirement for OSV, HSC, HSNC, <90m]

**Part 4** Vessel Systems and Machinery
**Chapter 9** Automation
**Section 5** ACC + **Section 6** ACCU

---

**Rule Requirements**

4-9-5/3.3 and 4-9-6/3.5

*FMEA to be conducted to demonstrate that control, monitoring and safety systems are so designed that any single failure will not result in the loss of propulsion control, the loss of propulsion or other undesirable consequences. The FMEA report is to be submitted for review.*

---

**Purpose of FMEA**

The purpose is to demonstrate that any single failure in the control system will not lead to lost or degraded propulsion beyond acceptable performance criteria.

---

**Undesired events**

The FMEA is to analyze all potential failures, one at a time, and investigate and document if there is a potential for lost or degraded propulsion beyond acceptable performance criteria.

---

**Systems or Subsystems**

- Failures of components within the computer-based control system are to be addressed in the FMEA.
- Failures of the interfaces i/o are to be considered
- Functional failures of equipment under control shall also be considered as to ascertain the adequacy of the actions of the safety-related functions upon the controlled equipment failure.

---

**Modes of Operation**

The failure analysis should consider failure scenarios under all potential modes of operations, as the failure mode as well as the likelihood and the consequences of the failure scenario vary depending on the operational modes.

Typical modes of operation for a propulsion system will include:

- Start and stop
- *Underway.* Consider full range of speeds up to maximum speed, and any special issues such as low NOx, fuel optimization, etc.
- *Emergency actions.* Consider crash stop, from full ahead to full stern, accelerating to maximum rpm (e.g., propellers emerged in heavy seas), etc.

---

**Typical Failures**

The lowest level of physical component failure required to be included in the FMEA for control systems is typically at the data acquisition unit level which includes the CPU, its I/O modules, the powering of the device, and any communication between multiple devices.

Physical components whose failures should be analyzed in the FMEA include:

- CPU microprocessor/PLC
- Input/output modules
- Power supplies
- Electrical power cables
- Network hubs
- Buses
- Communication/data link cables
- Interfaces/displays
- Electrical power cables
- Others, as applicable

For functions permitting wireless data communications, consideration is to be given to the possibility of corrupted data and intermittent faults with comparatively long recovery times between interruptions.

Software may reside in several different areas of a given system and at multiple levels (i.e. operating system, PLC embedded logic). Software failures are to be considered at a higher level, almost like a system failure; to address how the system can prevent and recover from, for example, malware.

Classification Rules require the system developer to follow a recognized software quality assurance program, so it is generally assumed that by the time software is delivered and installed, it is error free.

Relays, terminal boards, indicator lights, switches, meters and instruments do not have to be included in the FMEA unless their failure would lead to a hazardous situation not discussed with a higher level component.

---

**Timeline/ Team**

The sponsor of the FMEA is either the designer of the equipment under control or the system integrator.

The optimal time for performing the FMEA is during detailed design when the design is mature enough to have sufficient detail about the system and equipment available, but still enough time is left in the process to include FMEA recommendations in the final design and integration process.

The FMEA should include participation from subject matter experts in the control systems, operations, design and relevant vendors.

---

**Verification Program**

The specific goals of the FMEA trial tests include testing the:

- Effectiveness of system to identify failures
- Effect of identified failures on system/equipment
- Response of safety controls
- Other measures to protect against failure

Even though there is no general FMEA validation trial for FMEAs for **ACC** or **ACCU** notation, it is up to the discretion of ABS Surveyor or ABS Plan reviewer to recommend specific testing of FMEA failures for which there is a higher degree of uncertainty. Self-tests such as Hardware-in-the-Loop (HIL) can be substituted if adequate to prove intent and goals of the verification program. If system failures cannot be replicated (destructive test, safety concerns, etc.), a partial test may be carried out to test functionally and verify existing safeguards indicated in FMEA to detect/prevent/mitigate the failure.

### Supporting Documents

The FMEA must be submitted to ABS for review. In order to carry out a proper review of the FMEA, the ABS Plan reviewer needs the following information included with the FMEA report:

- General description of the scope and purpose of the FMEA
- Dates when the FMEA was conducted
- FMEA participants
- Summary of any corrective actions performed or pending as a result of recommendations of the FMEA.
- Detailed description, narrative and drawings of the system and its control system.
- Layout and general arrangement drawings
- Single line diagrams
- System design specifications
- Description of the physical and operational scope and boundaries for the FMEA, including:
  - Functional blocks arranged in a reliability block diagram, showing interactions among the blocks (parallel paths for redundant functional blocks, in series for single blocks)
  - Modes of operation for the system
- FMEA worksheets, including:
  - Modes of operation
  - All significant failure modes (associated with each mode of operation)
  - Cause associated with each failure mode
  - Method for detecting that the failure has occurred
  - Effect of the failure on system functionality
  - Global effect of the failure on health, safety and the environment
  - Existing controls to prevent and/or mitigate the failure
  - Corrective actions needed to comply with ABS Classification requirements

For systems where loss of function upon a single failure is not an acceptable option, but redundancy is not possible, further study of non-redundant parts with consideration to their reliability and mechanical protection must be provided.

The operations, maintenance, inspection, testing and emergency manuals are needed for ABS to confirm compliance with design and manufacturer's requirements and that the findings of the FMEA have been incorporated into the equipment operating phases. These manuals can all show operational configurations in which the systems redundancy can be bypassed.

**Lifecycle Management**

ABS needs to be notified of any changes made that impact the basis of the Classification requirements. It will be up to the discretion of the ABS reviewer whether to require a revised FMEA.

**Additional Notes**

## 1.4 Gas Turbine

RULE/GUIDE Steel Vessel Rules (SVR), Offshore Support Vessels (OSV), High-Speed Craft (HSC), High-Speed Naval Craft, Vessels Under 90 m

---

**SVR Rule Reference**
[identical requirement for OSV, HSC, HSNC, <90m]

**Part 4** Vessel Systems and Machinery
**Chapter 2** Prime Movers
**Section 3** Gas Turbines
**Subsection 7** Gas Turbine Appurtenances
**7.7** Safety Systems and Devices

---

**Rule Requirement**

**4-2-3/7.7.1 General**
*Gas turbines are to be fitted with automatic safety systems and devices for safeguards against hazardous conditions arising from malfunctions in their operations. The design of such systems and devices is to be evaluated with failure mode and effect analysis, which is to be submitted for review.*

---

**Purpose of FMEA**

Demonstrate that a single failure in the gas turbine and the gas turbine safety system will not cause a hazardous situation

---

**Undesired Events**

The hazardous situations (or consequence) of concern are:

- Uncontrolled gas ignition
- Loss of propulsion

---

**Systems or Subsystems**

- Gas turbines safety system
  - Shutdowns, temperature controls, alarms, starting system, etc.
- Gas turbines (mechanical system)
  - Combustion air system
  - Fuel system (gas)
  - Compressor
  - Power turbine
  - Lube oil
  - Exhaust gas
  - Enclosure

---

**Modes of Operation**

- Normal operations
- Normal startup/shutdown
- Emergency shutdown

**Typical Failures**

This analysis of the safety systems shall include both:

*i)* Failures of the components in the safety system (e.g., electronic circuit boards, power supplies, microprocessors/PLCs, memory boards, input/output modules, cables, sensors, etc.)

*ii)* Failures of the mechanical system in order to identify the adequate response of the safety control following the failure

Typical failures of components and logic within the safety system that need to be analyzed in the FMEA include, but are not limited to:

- Controls and sensors on safety systems related to automatic shutdown, including over speed; high vacuum at compressor inlet, low lubricating oil pressure, low lubricating oil pressure in reduction gear, loss of flame during operation, excessive vibration, excessive axial displacement of rotor, high exhaust gas temperature. (SVR 4-2-3/7.7.2)
- Controls and sensors related to automatic temperature controls for lube oil/fuel oil/exhaust gas (SVR 4-2-3/7.7.3)
- Controls and sensors related to the starting system safety including automatic purging, ignition detection devices, shut off of main fuel valve, and commencing of the purge phase (SVR 4-2-3/7.7.4)
- Controls and sensors related to SVR 4-2-3/Table 1, including loss of control system power
- Hand trip gear
- Air-intake filters and anti-icing

Typical failures within the mechanical system (gas turbines) that need to be analyzed include:

- Machinery or mechanical components (e.g., failure of rotors, bearing discs, drums, blades, couplings, gears, motor, shaft brake)
- System response to functional failures of supporting utilities
- Failures at interfaces or interconnections between systems
- Failures caused by credible external events, especially those that may result in a hazardous situation (e.g., nearby fire, explosion, excessive sea spray, low temperature ambient air, flooding)
- Others, as applicable

Particular attention should be paid in the analysis to identify all relevant:

- Common-mode failures and functional dependencies
- Hidden failures and their analyses in combination with the initial failure that makes the hidden failure evident (for example, a backup pump does not start upon the failure of the duty pump

**Timeline/ Team**

- The gas turbine vendor is to coordinate and develop the FMEA, and involve relevant operations and subject matter experts.
- Any corrective actions arising from single failures that lead to the hazardous situation of concern shall be implemented.

**Verification Program**

Test the controls and sensors of the safety system by simulating excessive parameter inputs from the sensors and verifying that desired outcome occurs.

**Supporting Documents**

The FMEA must be submitted to ABS for review. In order to carry out a proper review of the FMEA, the ABS Plan reviewer needs the following information included in the FMEA report:

- General description of the scope and purpose of the FMEA
- Dates when the FMEA was conducted
- FMEA participants
- Detail narrative of relevant systems, including a detail description and narrative of safety system and devices
- Functional block diagram showing the interactions between systems
- System design specifications
- FMEA worksheets, including:
  - All significant failure modes
  - Cause associated with each failure mode
  - Common cause failures
  - Method for detecting that the failure has occurred
  - Effect of the failure on propulsion functionality
  - Effect of the failure on gas fire and explosion
  - Existing controls to prevent and/or mitigate the failure
  - Corrective actions, as needed, to comply with Classification requirements

For systems where loss of function upon a single failure is not an acceptable option, but redundancy is not possible, further study of non-redundant parts with consideration to their reliability and mechanical protection must be provided.

The operations, maintenance, inspection, testing and emergency manuals are needed for ABS to confirm compliance with design and manufacturer's requirements and that the findings of the FMEA have been incorporated into the equipment operating phases.

**Lifecycle Management**

Any changes in the operating criteria should involve a review of the safety shutdown system FMEA. ABS needs to be notified of any changes made that impact the basis of the Classification requirements. It will be up to the discretion of the ABS reviewer whether to require a revised FMEA.

**Additional Notes**

## 1.5 Redundant Propulsion and Steering

RULE/GUIDE Steel Vessel Rules (SVR), Offshore Support Vessels (OSV), High-Speed Craft (HSC), High-Speed Naval Craft, Vessels Under 90 m

---

**SVR Rule Reference**
[identical requirement for OSV, HSC, HSNC, <90m]

**Part 4** Vessel Systems and Machinery
**Chapter 3** Propulsion and Maneuvering Machinery
**Section 6** Propulsion Redundancy
**Subsection 1** General

---

**Rule Requirement**

**4-3-6/1.7 Plans and Data to be Submitted**

*ii) The integrity of the propulsion systems, steering systems and auxiliary service systems is to be verified by means of a Failure Mode and Effect Analysis (FMEA) or equivalent method and is to show that a single failure will not compromise the criteria as specified in 4-3-6/7.*

---

**Purpose of FMEA**

Demonstrate that a single failure in any propulsion machine or auxiliary service system will not result in propulsion performance inferior to that required by SVR 4-3-6/7.1 or 4-3-6/7.3, as applicable

---

**Undesired Events**

The hazardous situations of concern are:

- Loss of propulsion performance inferior to that required by SVR 4-3-6/7.1, or SVR 4-3-6/7.3, as applicable

---

**Systems or Subsystems**

- Propulsion machinery
- Steering machinery
- Vessel auxiliary services
- Propulsion control system
- Electrical generation
- Power management system

---

**Modes of Operation**

- Underway
- Normal startup/shutdown
- Emergency shutdown

---

**Typical Failures**

Typical failures that need to be analyzed in the FMEA include, but are not limited to:

- Machinery or mechanical components (e.g., failure of gears, motor, brake)
- Propulsion and steering response upon functional failures of supporting utilities
  - Fuel oil system
  - Lube oil system
  - Cooling water
  - Compressed air
  - Fire protection system
  - Ventilation
  - Emergency shutdowns
  - Hydraulic system
- Control system (e.g., electronic circuit boards, power supplies, microprocessors/PLCs, memory boards, input/output modules, cables, etc.)
- Failures at interfaces or interconnections between systems
- Failures caused by credible external events, especially those that may result in eliminating both redundant systems (e.g., fire, explosion, flooding)
- Others, as applicable

Particular attention should be paid in the analysis to identify all relevant:

- Common-mode failures and functional dependencies that can nullify both redundant systems
- Hidden failures and their analyses in combination with the initial failure that makes the hidden failure evident (for example, a backup pump does not start upon the failure of the duty pump).

---

**Timeline/ Team**

Two important aspects in this FMEA are common-mode failures and functional dependencies that can defeat both redundant systems. Thus, the optimal time to perform the FMEA is at the system integration phase (shipyard). The propulsion system interfaces with services, controls, etc. will be detailed and the potential common-cause failures will be more evident.

If the FMEA for propulsion and steering equipment is performed before the integration with auxiliary systems is finalized, a functional failure analysis of these systems/interfaces should be performed once the design is final in order to evaluate potential common-cause failures.

---

**Verification Program**

There is no specific requirement for testing the conclusions of the FMEA. It is at the discretion of the ABS Surveyor to test select FMEA failures to validate the system response. Tests of the controls, safety systems, shutdown devices, starting system and emergency power supply, and alarms are to be conducted as per 4-3-4/21.7 of the *Steel Vessel Rules*.

---

**Supporting Documents**

The FMEA must be submitted to ABS for review. In order to carry out a proper review of the FMEA, the ABS Plan reviewer needs the following information included with the FMEA report:

- General description of the scope and purpose of the FMEA
- Dates when the FMEA was conducted
- FMEA participants
- Summary of any risk reducing actions performed or pending as a result of recommendations of the FMEA.
- Detailed description, narrative and drawings of relevant systems:
  - Redundant propulsion and steering systems
  - Propulsion control system
  - Power management system
  - Services/utilities relevant to the redundant propulsion and steering
  - Vessel automation system
  - Vessel particulars (notations, type of vessel, etc.)
- Layout and general arrangement drawings
- Single-line diagram
- System design specifications
- Functional block diagram showing interactions among the systems, parallel paths for redundant systems, in series for single systems.
- FMEA worksheets, including:
  - Modes of operations
  - All significant failure modes associated with each mode of operation
  - Causes associated with each failure mode
  - Method for detecting that the failure has occurred
  - Effect of the failure on propulsion functionality
  - Effect of the failure on gas release, fire and explosion
  - Global effect of the failure on other systems, the asset and HSE
  - Existing controls to prevent and/or mitigate the failure
  - Corrective actions needed to comply with ABS Classification requirements

For systems where loss of function upon a single failure is not an acceptable option, but redundancy is not possible, further study of non-redundant parts with consideration to their reliability and mechanical protection must be provided.

The operations, maintenance, inspection, testing, and emergency manuals are needed for ABS to confirm compliance with design and manufacturer's requirements and that the findings of the FMEA have been incorporated into the equipment operating phases. These manuals can all show operational configurations in which the systems redundancy can be bypassed.

**Lifecycle Management**

ABS needs to be notified of any changes made that impact the basis of the Classification requirements. It will be up to the discretion of the ABS reviewer whether to require a revised FMEA.

**Additional Notes**

## 1.6 Single Pod Propulsion

RULE/GUIDE Steel Vessel Rules (SVR), Offshore Support Vessels (OSV), High-Speed Craft (HSC), High-Speed Naval Craft, Vessels Under 90 m

---

**SVR Rule Reference**
[identical requirement for OSV, HSC, HSNC, <90m]

**Part 4** Vessel Systems and Machinery
**Chapter 3** Propulsion and Maneuvering Machinery
**Section 7** Podded Propulsion Units
**Subsection 1** General
**1.7** Design Requirements +
**Subsection 11** Machinery and System

---

**Rule Requirement**

**4-3-7/1.7.1 Redundancy**
*Where the propulsion system comprises a single pod propulsor, a detail risk analysis is to be carried out in the form of an FMEA (Failure Modes and Effects Analysis) or other effective methodology in order to ascertain that the system is fault-tolerant. The analysis is to be conducted by the pod manufacturer and is to be submitted for review.*

---

**Purpose of FMEA**

For single pod propulsor design, demonstrate that a single failure will not cause a loss of propulsion and/or steering capability

---

**Undesired Events**

The hazardous situation of concern is the:

- Loss of propulsion and/or loss of steering capability beyond that allowed per applicable notation requirements

---

**Systems or Subsystems**

Machinery and systems associated with podded propulsion:

- Propulsion system (i.e., motor, shafting, brake, propeller)
- Steering system
- Pod enclosure and shaft seals (to be designed with a double failure criteria)
- Bilge pumping system
- Pod thrust bearing
- Lubricating system
- Cooling and ventilation system
- Control system for podded propulsor (i.e., hydraulic, pneumatic, electrical, power management)
- Monitoring and alarm systems, etc. and their subcomponents

---

**Modes of Operation**

- Underway
- Normal startup/shutdown
- Emergency shutdown

**Typical Failures**

Typical failures to be considered in the podded propulsion systems:

- Machinery or mechanical components (e.g., failure of gears, motor, brake)
- System response to functional failures of supporting utilities (e.g., lubrication, cooling, hydraulic, pneumatic, electrical, etc.)
- Failures in podded propulsor and steering control system
- Failures at interfaces or interconnections between systems
- Failures caused by credible external events, especially those that may result in a hazardous situation (e.g., flooding, fire and explosion, etc.)
- Others, as applicable

Particular attention should be paid in the analysis to identify all relevant:

- Common-mode failures and functional dependencies
- Hidden failures and their analyses in combination with the other failure that makes the hidden failure evident (for example, a backup pump does not start upon the failure of the duty pump

**Timeline/ Team**

- The optimal time for performing the FMEA is at the detailed design when there is enough information about the system and equipment, but still time to include FMEA recommendations in the final design and integration process.
- The sponsor of the FMEA should be the propulsion system vendors. Needed subject matter experts in design, controls and operations should participate in the FMEA.

**Verification Program**

No specific requirement for testing the conclusions of this FMEA. Tests of the starting system, controls, safety systems, alarms, shutdown devices and emergency power supply are to be conducted. See 4-3-7/17 of the *Steel Vessel Rules*. However, it is at the discretion of the ABS Surveyor to test select FMEA failures to validate the system response

**Supporting Documents**

The FMEA must be submitted to ABS for review. In order to carry out a proper review of the FMEA, the ABS Plan reviewer needs the following information included in the FMEA report:

- General description of the scope and purpose of the FMEA
- Dates when the FMEA was conducted
- FMEA participants
- Summary of any corrective actions performed or pending as a result of recommendations of the FMEA.

- Detail narrative of relevant systems
- System design specifications
- Layout and general arrangement drawings
- Description of the physical and operational scope and boundaries for the FMEA, including:
  - Functional blocks arranged in a reliability block diagram, showing interactions among the blocks (parallel paths for redundant functional blocks, in series for single blocks)
  - Modes of operation for the system
- FMEA worksheets, including:
  - Modes of operations
  - All significant failure modes associated with each mode of operation
  - Cause associated with each failure mode
  - Common cause failures
  - Method for detecting that the failure has occurred
  - Effect of the failure on propulsion functionality
  - Existing controls to prevent and/or mitigate the failure
  - Corrective actions, as needed for compliance with Classification requirements

For systems where loss of function upon a single failure is not an acceptable option, but redundancy is not possible, further study of non-redundant parts with consideration to their reliability and mechanical protection must be provided.

The operations, maintenance, inspection, testing, and emergency manuals are needed for ABS to confirm compliance with design and manufacturer's requirements and that the findings of the FMEA have been incorporated into the equipment operating phases.

**Lifecycle Management**

ABS needs to be notified of any changes made that impact the basis of the Classification requirements. It will be up to the discretion of the ABS reviewer whether to require a revised FMEA.

**Additional Notes**

## 1.7 Dynamic Positioning Systems (DPS)

RULE/GUIDE Guide for Dynamic Positioning Systems

**Rule Reference**

**Section 2** Dynamic Positioning System Design
**Subsection 11** Failure Mode and Effects Analysis

**Rule Requirements**

*The purpose of the FMEA is to indicate whether or not the DP system meets the requirements of the relevant DP notation and complies with the vessel's WCFDI.*

*The DP FMEA is to be performed based on this Guide, IMCA M 166, IMCA M 178, IEC 60812, "DP Vessel Design Philosophy Guideline" by MTS, Annex 4 of IMO High Speed Craft Code or equivalent.*

*The objective of the DP FMEA is to, at least, include the following:*

*i) Identify and provide recommendations to eliminate or mitigate the effects of all single faults and common mode failures in the vessel DP equipment which, if any occurs, would cause total or partial loss of station keeping capability.*

*ii) Demonstrate effective redundancy.*

*iii) Identify potential "hidden" failures and determine the effects of a second failure.*

*Note:*
*Worst Case Failure (WCF):* The identified single fault in the DP system resulting in maximum effect on DP capability as determined through the FMEA study. This worst case failure is to be used in the consequence analysis.

*Worst Case Failure Design Intent (WCFDI):* The worst case failure design intent describes the minimum amount of propulsion and control equipment remaining operational following the worst case failure. The worst case failure design intent is used as the basis of design. This usually relates to the number of thrusters and generators that can simultaneously fail.

**Purpose of FMEA**

The purpose of the DP FMEA is to verify that system/subsystem and equipment complies with the following failure design philosophy:

- No single failure will lead to a total or partial loss of station keeping capability
- Effective redundancy exists
- Hidden failures are identified and controlled

**Undesired Events**

Partial or total of station keeping capability. Redundancy usually needed if a single failure shall not result in a loss of function.

**Systems or Subsystems**

The systems to be subject to failure analysis include 1) the main DP systems, 2) DP auxiliary systems and 3) mission-specific systems that interface or have an impact on the DPS and station keeping capability.

**Main DP Systems**

| *System* | *Subsystems/Equipment (non-exhaustive list)* | *Components* |
|---|---|---|
| Power system | i) Prime movers with necessary auxiliary systems including piping<br>ii) Generators<br>iii) Switchboards<br>iv) Electrical distribution system (cabling and cable routing)<br>v) Power management if applicable | Each subsystem has components whose failures should be evaluated A typical list of representative components is shown below for computer system. |
| Thruster system | i) Thrusters with drive units and necessary auxiliary systems including piping<br>ii) Main propellers and rudders if under the control of the DPS<br>iii) Thruster control electronics<br>iv) Manual thruster controls<br>v) Associated cabling/cable routing | Each subsystem has components whose failures should be evaluated A typical list of representative components is shown below for computer system. |
| DP Control System | i) Computer system/joystick system<br>ii) Position reference systems<br>iii) DP sensor system<br>iv) Display system (operator panels)<br>v) Associated cabling and cable routing | **Computer System**: Includes programmable electronic devices, associated software, peripherals, interface, etc. |

**Auxiliary Systems**

For **DPS-2** and **DPS-3** notations, failures within the auxiliary systems are to be included in the FMEAs. These systems include, but are not limited to, the following:

*i)* Fuel oil

*ii)* Lubricating oil

*iii)* Cooling water

*iv)* Compressed air

*v)* Hydraulic

*vi)* Pneumatic

*vii)* Ventilation/HVAC

*viii)* Piping system equipment (e.g., purifier, heat exchanger, transfer pump)

**Mission Specific Equipment**

The types of vessels employing DP systems is widely diverse and include, but are not limited to, semi-submersible mobile offshore drilling units (MODU), offshore support vessels and cruise ships. The FMEA is to include failures of mission-specific equipment that interfaces or has an impact on the DP. It is not feasible to show examples of all the potential mission-specific systems, but as an example, typical system-specific operational modes for a pipe-laying vessel may include pipe tensioner and for a MODU, the emergency disconnect and jack-up system may be included, among others.

The depth of the analysis with the functional interfaces shall be sufficient to meet the FMEA objectives in the judgment of the FMEA team. For example, to meet the study objectives it may be necessary to analyze components required for product lay such as deployment equipment (tensioner tracks, aligners, etc.), HPUs, electrical supplies and control systems.

**DPS-2 and DPS-3**

One difference between the DPS-2 and the DPS-3 FMEAs lies in how the static components are addressed. Static components in mechanical systems refer to those having parts that normally do not move (e.g., pipes, tanks, vessels, shell-and-tube heat exchanger, manual valves). For electrical/electronic systems, passive components are those that do not require energy to make them work (e.g., electrical cables, resistors, capacitors). For FMEAs conducted for **DPS-2** vessels, the failure of the static components is not considered unless it is deemed that these components are not adequately protected from damage and their reliability is unproven.

For the FMEAs conducted for **DPS-3** vessels, the failures of the static components must be analyzed, as well as two consequences of two other events, fire and flooding.

## Modes of Operation

The FMEA shall consider both global operations at vessel level (e.g., drilling operation for a MODU) and local operations of the DPS (e.g., closed-bus operations). The technical configuration of the DPS system varies for each vessel operation. The FMEA should document the DPS configuration for each vessel operation and analyze failures in all possible modes of operations (global and local systems configurations) in order to identify failures, hazards and consequences of concern.

**Vessel/Mission-Specific Operations**

The FMEA is to include failures of mission-specific equipment that interface or have an impact on the DP and station keeping. The DPS FMEA shall analyze failures during all the overall vessel operations as the failure modes and the consequences will vary from one operation to the next. For example, operations to be considered during the DP FMEA of a MODU include:

*i)* Drilling

*ii)* Emergency shutdown

*iii)* Safe disconnection of risers

Other operations to consider on DP vessels include, but are not limited to, station-keeping, maneuvering, weathervaning, product-laying and dredging.

**DPS Power Management System Configurations**

When there are more configurations for the diesel electric plant design to cope with equipment unavailability (e.g., failures or equipment taken down for maintenance), it is important that all configurations that are possible to be included in DP operations are analyzed in the vessel's DP system FMEA to prove that the DP system remains redundant.

*i)* Open-bus operations

*ii)* Closed-bus operations, etc.

**DPS Control System Modes**

The DPS control system has several modes of operation, which should be analyzed in all the possible combinations with the vessel operations and the power configurations. A non-exhaustive list of the DP control modes include:

*i)* DP control mode (automatic position and heading control)

*ii)* Manual position control mode (centralized manual position control with selectable automatic or manual heading control)

*iii)* Auto track mode (considered as a variant of DP position control, with programmed movement of reference point),

*iv)* Manual thruster control mode (individual control of thrust (pitch or speed), azimuth, start and stop of each thruster).

**Typical Failures**

For a **DPS-2** or a **DPS-3** notation, loss of position is not allowed to occur in the event of a single fault. Single fault includes, but is not limited to, the following:

*i)* All redundant components, systems or subsystems

*ii)* A single inadvertent act of operation (ventilation, fire suppression, ESD) where applicable and if such an act is reasonably probable

*iii)* Hidden failures (such as protective functions on which redundancy depends) where applicable

*iv)* Common failure modes

*v)* Governor and AVR failure modes where applicable

*vi)* Main switchboard control power failure modes

*vii)* Bus-tie protection where applicable

*viii)* Power management system

*ix)* DP control system input and output arrangement

*x)* Position reference processing

*xi)* Networks

*xii)* Communication failure

*xiii)* Automatic interventions caused by external events, when found relevant (e.g., automatic action upon detection of gas)

*xiv)* Fire and flooding events (for **DPS-3** notation, and for **DPS-2** with additional Fire and Flood Protection notation **EHS-F**)

For the **DPS-2** notation, static components will normally not be considered to fail.

For the **DPS-2** notation, a single fault includes:

*i)* Any active component or system (generators, thrusters, switchboards, DP control computers, sensors, remote-controlled valves, etc.)

For the **DPS-3** notation, a single fault includes:

*i)* Items listed above for **DPS-2**, and any normally static component is assumed to fail

*ii)* Any components in any one watertight compartment from flooding

*iii)* Any components in any one fire subdivision from fire

**DPS Control System Failures**

The lowest level of physical component failure required to be included in the FMEA for control systems is typically at the data acquisition unit level which includes the CPU, its I/O modules, the powering of the device, and any communication between multiple devices.

Physical components whose failures should be analyzed in the FMEA include:

- CPU microprocessor/PLC
- Input/output modules
- Power supplies
- Electrical power cables
- Network hubs
- Buses
- Communication/data link cables

- Interfaces/displays
- Electrical power cables
- Others, as applicable

For functions permitting wireless data communications, consideration is to be given to the possibility of corrupted data and intermittent faults with comparatively long recovery times between interruptions.

Software may reside in several different areas of a given system and at multiple levels (i.e. operating system, PLC embedded logic). Software failures are to be considered at a higher level, almost like a system failure; to address how the system can prevent and recover from, for example, malware.

Classification Rules require the system developer to follow a recognized software quality assurance program, so it is generally assumed that by the time software is delivered and installed, it is error free.

Relays, terminal boards, indicator lights, switches, meters and instruments do not have to be included in the FMEA unless their failure would lead to a hazardous situation not discussed with a higher level component.

**DPS-2 and DPS-3 Notation with EHS-series**

In addition to the failure modes provided in Subsection 2/11 of the *DP Guide*, for EHS-series notations, the following failure modes, where applicable, are also to be considered in the FMEA.

*i)* Operation of protection systems (breakers, bus-ties, etc.) related to short circuit

*ii)* Severe voltage dips associated with short circuit faults in power plant configured as a common power system

*iii)* Failure due to excess and insufficient fuel

*iv)* Over and under-excitation

*v)* Governor and AVR failure modes

*vi)* Failure modes related to standby start and changeover

*vii)* Power management failure on load sharing, malfunction, etc.

*viii)* Phase back thrust and large load

*ix)* Blackout recovery

---

**Timeline/ Team**

- The FMEA should be developed by a group of subject matter experts that includes the following disciplines: 1) controls 2) electrical 3) mechanical/marine 4) operations
- For a new built, the FMEA should be performed early enough to allow design modifications in case there is a finding of noncompliance with Classification failure design principles such as the no-single failure criteria.
- The FMEA is a tool relied on extensively during operations. The DP FMEA must reflect the vessel "as built" condition; therefore, a review and update of the FMEA may be necessary to reflect modifications in the vessel from the time the FMEA was originally developed to the time the vessel is delivered.
- The FMEA is to be updated after major modifications

---

**Verification Program**

As per the 2/11.5.2 of the *DP Guide*, the FMEA proving trial procedure is to be developed as part of the FMEA study. The objective of the FMEA proving trial is to confirm the FMEA analysis findings and also to confirm that essential functions and features upon which the fault tolerance of the DP system depends are functional in so far as it is practical to do so (protections, power management, etc.).

The proving trial report is to establish the FMEA test list and the corresponding test procedures including, but not limited to, the following:

*i)* Purpose of test or failure mode

*ii)* Vessel and equipment setup

*iii)* Test method

*iv)* Expected results

*v)* Observed results

*vi)* Failure detection

*vii)* Failure effects

*viii)* Outstanding or resolved action items

*ix)* Comments

*x)* Witness name, signature and date for each test

After completion of DP proving trials, the final version of DP FMEA and DP proving trial report, including final analysis/conclusions based on actual results from DP testing, are to be submitted.

The FMEA verification plan should include testing all failures that have a potential to affect functionality (if existing controls fails) as identified in the FMEA.

The FMEAs that include a criticality ranking are helpful to decide on which items to submit to the proving trial. In general, failures that have potential for major consequences, regardless of the likelihood, should be tested.

Self-tests such as Hardware-in-the-Loop (HIL) can be substituted if adequate to prove intent and goals of the verification program. If system failures cannot be replicated (destructive test, safety concerns, etc.), then existing safeguards must be functionally tested and verified , as indicated in FMEA to detect/prevent/mitigate the failure.

**Supporting Documents**

The FMEA must be submitted to ABS for review in support of the Classification process. 2/11.5.1 of the *DP Guide* provides a non-exhaustive list of the information that should be provided along with the DP FMEA report.

Below is an expanded list of information that, when provided, facilitates a comprehensive review of FMEA by the ABS Plan reviewer, thus having an overall positive impact in the Classification review process:

- FMEA report, including FMEA worksheets and FMEA verification plan.
- General description of the scope and purpose of the FMEA
- Dates when the FMEA was conducted
- FMEA participants
- Summary of corrective actions performed or pending as a result of recommendations of the FMEA.

- Detailed description, narrative and drawings of the system functional description and control
- A description of all the systems associated with the dynamic positioning of the vessel and a functional block diagram showing their interaction with each other. Such systems would include the DP electrical or computer control systems, electrical power distribution system, power generation, fuel systems, lubricating oil systems, cooling systems, backup control systems, etc. [*DP Guide* 2/11.5.1iv)]
- Layout and general arrangement drawings
- Brief description of the vessel, vessel's worst-case failure design intent and whether the analysis has confirmed or disproved it [*DP Guide* 2/11.5.1i)]
- Definitions of the terms, symbols and abbreviations [*DP Guide* 2/11.5.1ii)]
- Analysis method and assumptions [*DP Guide* 2/11.5.1iii)]
- Single line diagrams
- System design specifications
- Cause and effect chart showing the control logic
- Description of the physical and operational scope and boundaries for the FMEA, including:
  - Functional blocks arranged in a reliability block diagram, showing interactions among the blocks (parallel paths for redundant functional blocks, in series for single blocks) (expanded from [*DP Guide* 2/11.5.1v)]
  - Modes of operation for the vessel, including vessel industrial functions and the DPS configuration for each of the vessel industrial functions
- FMEA worksheets, including:
  - Modes of operation
  - Description of each physically and functionally independent item and the associated failure modes (*DP Guide* 2/11.5.1vi))
  - Cause associated with each failure mode
  - Method for detecting that the failure has occurred
  - Effects of each failure mode alone on other items within the system and on the overall DPS functionality [*DP Guide* 2/11.5.1vii)]
  - Existing controls to prevent and/or mitigate the failure
  - Conclusions including worst case failure and recommended changes [*DP Guide* 2/11.5.1ix)] needed to comply with ABS Classification requirements
  - FMEA verification plan [(*DP Guide* 2/11.5.1x)]
- Operations, maintenance, inspection and testing manuals

The FMEA report is to be updated after major modifications and is to be kept onboard the vessel.

For systems where loss of function upon a single failure is not an acceptable option, but redundancy is not possible, further study of non-redundant parts with consideration to their reliability and mechanical protection must be provided.

The operations, maintenance, inspection, testing and emergency manuals are needed for ABS to confirm compliance with design and manufacturer's requirements and that the findings of the FMEA have been incorporated into the equipment operating phases. These manuals can all show operational configurations in which the systems redundancy can be bypassed.

**Lifecycle Management**

The FMEA is to be updated after major modifications and resubmitted to ABS to demonstrate that the system is still in compliance with the ABS design philosophy.

Types of changes that would typically require submittal of revised FMEAs for ABS' review include:

- Operating criteria changes
- System configuration/boundary changes
- Equipment changes
- New application/mission

New FMEA proving trials may be required to validate the conclusions of the updated FMEA.

**Additional Notes**

Example of helpful columns on a DP FMEA worksheet is shown in the following page.

## TABLE 3
## Sample DP FMEA Worksheet Template

| Operational Mode: | | Station-keeping while drilling | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Unit | | PMS and IAS | | | | | | | | | | |
| Description of Unit | | Description of failure | | | Effects of Failure | | | Safeguards | | Testing | Corrective Action | Respon-sible |
| Function | ID# | Failure Mode | Failure Causes | Detection of Failure | Local | Redundancy affected? | Global | Prevention of Failure | Mitigation of Effect | | | |
| … | … | … | … | … | … | | … | … | … | | … | … |

## 1.8 Software Control System

RULE/GUIDE ABS Guide for Integrated Software Quality Management

**Rule Reference**

**Section 4** Software Development Life Cycle: Requirements and Design (RD) Phase
**Subsection 5** Requirements and Design (RD) Phase Documents
**5.5** Risk Management
***
**Section 5** Software Development Life Cycle: Construction Phase
**Subsection 5** Construction Phase Document
**5.3** Risk Management
***
**Section 9** Software Development Life Cycle: Design Group
**Subsection 5** Risk Management

**Rule Requirement**

**4/5.5.4 Software Control System FMECA**
*The purpose of the FMECA is to determine that a single Software Module failure will not lead to failures of other Software Modules or loss of the control system.*

*i)* *IL2 and IL3 assigned ISQM control systems are to have a software-focused functional FMECA performed.*

*ii)* *A Control System FMECA is to provide traceability of the Software Modules to the relevant functions in the Traceability Matrix.*

*iii)* *A Control System FMECA of IL2 and IL3 functions is to be performed including interfaces with integrated control systems that may have an effect upon the function.*

*iv)* *Update the Software Requirements Specifications (SRS) and Software Design Specifications (SDS) or Functional Description Documents (FDD) with FMECA recommendations.*

***

**5/5.3.4 Software Control System FMECA**
*i)* *A Control System FMECA is to provide traceability of the Software Modules to the relevant functions in the Traceability Matrix.*

*ii)* *A Control System FMECA is to be performed on the integrated system as a whole for functions changed during the Construction Phase.*

*iii)* *A Control System FMECA of IL2 and IL3 functions is to be performed for functions changed during the Construction Phase.*

***

**9/5.3 Safety Reviews and FMECA**
*i)* *A safety review is to be performed on ISQM control systems to which IL1, IL2 and IL3 designations are assigned.*

- *The safety review may be combined with other safety or operability reviews, hardware FMEA, or evaluations, or software FMECA.*
- *It is recommended that SI, Owner, DCO, IA, SBI and ABS be present during the safety reviews.*

*ii) A FMECA is to be performed on ISQM control systems to which IL2 and IL3 designations are assigned. See 4/5.5.4 and 4/5.5.5.*

**Purpose of FMECA**

For control functions with Integrity Levels (IL) 2 and 3, the FMECA is to demonstrate that a single failure within the control system (software/firmware/hardware) will not cause the failure or degradation of the other functions controlled by the ISQM control system.

Corrective actions shall be put in place to eliminate any identified potential for losing a control function upon a single failure.

System Verification requires a safety analysis report and does not require a FMECA

**System/Global Consequences of interest**

IL 2 and IL 3 correlate to the most severe safety and environmental consequences in case of failure or degradation of any of the functions controlled by the ISQM control system.

The consequence of failure of function is defined as follows:

- **IL2 – Critical** - Permanent injury or multiple lost time injuries, mission critical system damage, or significant financial or social loss.
- **IL3 – Catastrophic** - Loss of human life, loss of asset, loss of system safety or security, or extensive financial or social loss.

**Systems or Subsystems**

The FMECA shall analyze failures of the control system (software/firmware/hardware) and as well as failures in the system under control for system functions that have been defined as IL 2 or IL3. A partial listing of recommended ISQM equipment rated IL2 and IL3 follows, based on Section 3, Table 2 of the *ISQM Guide*. The equipment is selected by the owner based on the owner's risk tolerance.

- Acoustic BOP control
- Acoustic DP input
- Ballast Control
- Ballast Water Treatment
- Blowout Preventer (BOP)
- Cement Pump
- Chemical gas or oil processing separation
- Draw works
- Drilling control system
- Drilling heave control
- Drilling power system
- Drilling top drive
- Dual fuel engine fuel system
- Dynamic positioning
- Emergency Shutdown (ESD)
- Engine control system
- Fixed Rig Power management
- Fuel Treatment
- Governor
- Horizontal pipe handling
- Ice load monitoring
- Lifting appliances
- LNG refrigeration
- Mud monitoring control system
- Mud pumps
- Process Safety Instrumented System
- Production Subsea ESD
- Production subsea monitoring thruster
- Vertical pipe handling
- Vessel management
- Vessel Power management
- Vessel stability

- Emergency disconnect (EDS)
- Zone monitoring system
- Fire and gas

For each system, ISQM is interested in the analysis of:

*i)* Failures within the control system (software, firmware, and hardware) and

*ii)* Failures of the equipment under control (EUC)

Examples of components whose failures must be analyzed include, but is not limited to:

- Microprocessors/PLCs
- Computers
- Memory boards
- Adapter cards
- Communication boards
- Ethernet cables
- Input/output modules
- Power supplies
- Circuit drivers
- Input and output card, either remote or local
- Microcontrollers
- Circuit boards containing solid state devices
- Electronic circuit boards
- Software

As a rule of thumb, the lowest level of firmware and hardware component failure that should be included in the FMECA is each easily replaceable component. The subsequent section on "Typical Failures for Analysis" addresses the type of software failures to be considered in the analysis.

The EUC is the set of all equipment or machinery used for the industrial activities, process, drilling, transportation, etc. (i.e., pumps, compressors, propulsion equipment, power plant, thrusters, cranes, etc.). The EUC can give rise to hazardous events for which the control and safety-related system is required. Therefore, failures within the EUC must be analyzed to verify that the control responses and safety-related protection are adequate for all situations. Examples of failures within the machinery/EUC include:

- Functional failures
- Failures that have the potential to cause unsafe situations
- Interfaces of EUC and the control system
- Failures of sensors in the EUC

**Modes of Operation**

The FMECA is to analyze failures occurring under each of the software operating modes and equipment states:

1. Normal
2. Degraded
3. Failed (single point)
4. Fail-Safe
5. Startup
6. Shutdown

In addition, the FMECA is to analyze operational modes specific to the mechanical system under control. Each operational mode may entail different control logic, as well as mode-specific types of failures and consequences.

**Typical Failures**

Typical software failure modes during each of the operating modes include the following:

| | | |
|---|---|---|
| *1.* | *Lack of Functionality* | Software provides no output or control action not provided when expected |
| *2.* | *Improper functionality* | The programmed control system software performs an unexpected action as defined by the operator of the equipment. |
| *3.* | *Timing* | Software event happens too late or too early or control action mistimed |
| *4.* | *Sequence* | Software event occurs in wrong order or control action with incomplete sequence concept error |
| *5.* | *False alarm/action* | Software detects an error when there is no error or control action provided when not expected |
| *6.* | *Faulty logic and ranges* | Concept error where the software contains incomplete or overlapping logic or control action contains incomplete or overlapping logic |
| *7.* | *Incorrect algorithm* | Software computes incorrectly based on some or all inputs or control action is based on wrong computation |
| *8.* | *Memory Management* | Software runs out of memory or memory leakage or control action stops due to lack of memory |
| *9.* | *Interface failure* | Software failed due to failure of hardware interfaces such as power supply, watch dog timer, clocks, reset circuits, etc. |
| *10.* | *Software virus* | Software did not function on demand due to software virus |

Explicit analysis of the following failure modes for each function should be described in the FMECA:

- Any two opposing functions that canp81 be simultaneously initiated (e.g., valve open and valve close)
- Degraded and/or failed third party components in a Safety Instrumented System (SIS) (as defined by IES61508 and 61511) system.
- Sensor inputs and outputs are degraded or failed for any function (e.g., components receive a corrupted signal, or a fluctuating signal, a wireless component gets signal interference, etc.)
- Any two degraded or failed complimenting components, including common-cause failures. (e.g., the brake off solenoid/air circuit and ACS sensors both fail)
- For redundancy systems with multiple components, consider if one or more redundancy component is degraded or failed.

The failure analysis should include the causes and consequences of the failures, the controls to detect and indicate the failure, and the fail-safe action or logic that will prevent either the cause or the consequence.

**Example of a Failure**

Failure of Sensors

- *Control system function*: Monitor the enclosed air pressure in a section.
- *Failure:* Corrupted signal on pressure transmitter sensor indicating low pressure when in reality there is high pressure
- *Consequences:* Potential to build up pressure in section without it being noticed. Potential for rupture of section and release of hydrocarbons. Potential for fire.
- *Failure Indicating Safeguards*: Redundant transmitter with high pressure alarm.
- *Safeguards*: two out of three voting transmitters, maintenance of the transmitters, pressure relief valve on the section, hydrocarbon detection, area classification, fire protection and fire-fighting.
- *Detectability*: How does the failure get detected?

**Timeline/ Team**

- The sponsor of the FMECA is the system provider
- In addition to the system provider, it is recommended that the owner, operator (driller or crew organization), ship builder integrator, suppliers involved in integrated software system development, implementation, operation and maintenance, ABS ISQM representative and independent auditors are to be present during the FMECA reviews.
- The optimal time for performing the FMECA is at the detailed design when there is enough detail about the system and equipment, but still time to include FMECA recommendations in the final design and integration process. Note that an important focus of the ISQM FMECA is to identify concept errors early to minimize schedule impact.
- Needed subject matter experts in operations, design and relevant vendors should participate in the FMECA

**Verification Program**

No specific requirement for testing the conclusions of this FMECA, but it can utilized for verification plan and testing scenarios. However, it is to the discretion of ABS and the owner to test select FMEA failures to validate the system response.

**Supporting Documents**

The FMECA must be submitted to ABS for review. In order to carry out a proper review of the FMECA, the ABS reviewer needs the following information included in the FMECA report:

- General description of the scope and purpose of the FMECA
- Dates FMECA was conducted
- FMECA participants
- Summary of any risk-reducing actions performed or pending as a result of recommendations of the FMECA. For large systems, provide the summary for each component. This can also be a table that for each component shows the overall number of failure modes, causes, low-, medium- and high-risk failure modes, etc. and recommendations
- Detail narrative of relevant systems
- Design specifications
- Functional block diagram showing their interaction with each other
- Unique function identifier for each function for traceability purposes. These are the same identifiers used throughout the project (functional description documents, FMECA, etc.)
- Integrity Level assignments for each function to highlight the importance and criticality of the function to the system. They also represent the severities of the potential consequences. A table is recommended.
- Risk matrix used for criticality assessment
- FMECA worksheets, including:
  - Mode of operation
  - Description of functions and unique function identifier
  - All significant failure modes
  - Cause associated with each failure mode
  - Common cause failures

- Method for detecting that the failure has occurred and how the information is passed on to the operator. Should describe the degree of detectability of the function failure. Accompanying tables should be available to explain any value used.
- Effect of the failure upon the system's ability to perform its function – most likely and worst-case outcome
- Description of major or critical consequences, including potential impacts to personnel and/operational safety.
- Controls to prevent and/or mitigate the failure
- Risk ranking for each failure mode (severity and consequence)
- Corrective actions - Functions that have been determined to have an unacceptable risk level should describe actions that will be taken to remove or mitigate these risks. For other functions, status on recommendations and action items should be included in the report, if applicable.
- If system is to be fault-tolerant (i.e., continue working uninterruptedly after a single hardware failure) but redundancy is not possible, provide further study of non-redundant part with consideration to their reliability and protection mechanisms.

The operations, maintenance, inspection, testing and emergency manuals are needed for ABS to confirm compliance with design and manufacturer's requirements and that the findings of the FMEA have been incorporated into the equipment operating phases.

**Lifecycle Management**

If the function IL 2 or IL 3 was added after the initial Software Control System FMECA, a new FMECA is to be conducted to address any risks with the new functions and associated Software Modules.

The software FMECA report is a living document and it should be updated for any subsequent modifications to the system under control as well as to the control system to demonstrate that system is still in compliance with the ISQM requirements.

Types of changes requiring submittal of revised FMEA for ABS' review include:

- Operating criteria changes (this does not include parameterization changes with the operating limits of the equipment)
- Equipment changes
- Major software changes for IL2/IL3 system (any functionality updates to IL2 or IL3 functions or software functions that may affect IL2 or IL3 functions are to have updated FMECA.
- Previously unidentified failure modes are discovered
- Underlying assumptions are determined to be erroneous (e.g., historical data shows a different likelihood or consequences than the estimated in the analysis)

**Additional Notes**

Below is a summary of the characteristics expected in a software-focused, top down functional FMECA of IL2 and IL3 designated ISQM control systems for ISQM.

**a) Unique function identifier for each function**

Each system function in the system is to have a unique identifying number for traceability purposes, provided to give clarity and avoid confusion. These are the same identifiers used throughout the project (functional description documents, FMECA, etc.)

**b) Integrity Level assignments for each function**

The IL assignment gives information regarding the importance and criticality of the function to the system. They also represent the severities of the potential consequences. A table is recommended.

**c) Explicit statement for any control system failures that may have an effect upon other IL2 and IL3 functions or components**

This is to provide the designer a troubleshooting guide to cascading failures.

**d) Corrective actions**

Functions that have been determined to have an unacceptable risk level contain information on actions that will be taken to remove or mitigate these risks. For other functions, statuses on recommendations and action items should be included in the report, if applicable. This to provide risk-reducing actions performed or pending as a result of recommendations and negative conclusions in the summary section of the FMECA

**e) FMECA worksheets for ISQM control software modules assigned IL3 or IL2**

A Control System FMECA is to provide traceability of the Software Modules to the relevant functions. It should provide the failure/function, causes of failures, the effects, method on how and when is the failure detected, the criticality, and what do to reduce the risk of them occurring from a local and global perspective. It should provide the qualitative measure probabilities, the most likely and worst-case outcomes.

The criticality should be based on the severity of the outcome and the frequency of the occurrence of the outcome. A risk matrix is the recommended tool for assessment of criticality.

Worksheets should include a description of how the failure detection is passed on to the operator. It also may state the degree of detectability of the function.

Accompanying documentation should be available to explain any value used. This tells the designer which system, alarm or sensor will detect and react given the failure.

**f) Description for any two opposing functions which can be simultaneously initiated**

This is to provide the designer with the fail-safe action or logic that will occur when two conflicting inputs impact the functions simultaneously.

*Example:* Valve position switch indicates it is open and closed simultaneously.

**g) Description for the case that the sensor is degraded or failed for any function that controls hardware dependent upon sensors for various positioning or measuring actions**

This is to provide the designer the consequences of a degraded or defective sensor.

*Example:* If components receive a corrupted signal or fluctuating analog signal what would be the effect? Wireless components?

**h) Description of the cause and effect of any two degraded or failed complimenting components**

This is to provide the designer the consequences of any two complimenting components which can fail simultaneously.

*Example:* The brake off solenoid/air circuit and ACS sensor both fail

**i) Description for the case that the sensor/input is degraded or failed for any function controlling hardware that is dependent upon control valves, motors, wires, pipes, oil/lubrication, air supply, another component for various positioning or measuring actions**

This is to provide the designer the causes and consequences of degraded or failed auxiliary components have on various positioning or measuring actions.

**j) For redundancy systems with multiple components, if one or more redundancy component is degraded or failed, provide a description of the causes and effects.**

This is to provide the designer the causes and effects of systems that have lost their redundancy (fail-safe) components.

**Sample FMEA**

Appendix 2 shows a sample FMEAs for Software as per ABS ISQM requirements.

## 1.9 Jacking Systems

RULE/GUIDE ABS Rules for Building and Classing Mobile Offshore Drilling Units, 2014

**Rule Reference**

**Part 6** Rules for Equipment and Machinery Certification
**Chapter 1** Material, Marine Equipment and Machinery Certification
**Section 9** Jacking and Associated Systems
**Subsection 7** Failure Mode and Effect Analysis

**Rule Requirement**

*A failure modes and effects analysis (FMEA) is to be carried out on the jacking system and holding mechanism for the purpose of demonstrating that a single failure of any component will not cause an uncontrolled descent of the unit. The FMEA methodology has to ensure that any predictable failure mode relevant to the purpose of the FMEA has been considered and is to be sufficiently detailed to cover all systems associated with the jacking and holding operations. The FMEA is to be submitted for review and is to include, but not be limited to, the following information:*

- *A description of all the systems associated with the jacking and holding operations of the unit and a functional block diagram showing their interaction with each other. Such systems would include the jacking systems, the fixation systems, jackcase, electrical power distribution system, hydraulic power system, control systems (including programmable systems and their physical components such as programmable logic controllers, network hubs, cards, buses, cabling, encoders, and interfaces/displays), monitoring and alarm systems, etc. and their subcomponents.*
- *All significant failure modes relevant to the purpose of the FMEA*
- *Each predictable cause associated with each failure mode*
- *The method of detecting that the failure has occurred*
- *The effect of the failure upon the rest of the system's ability to jack the unit, including time effects (i.e., if necessary time is available for manual intervention)*
- *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.*

**Purpose of FMEA**

Demonstrate that a single failure of any component will not cause uncontrolled descent of the unit

**Undesired Events**

Loss of jacking function > Loss of holding function > Uncontrolled descent

**Systems or Subsystems**

The jacking system and holding mechanism comprise the physical scope of the FMEA including:

- Jacking systems
- Fixation systems
- Jack case
- Electrical power distribution system
- Hydraulic power system
- Control systems (including programmable systems and their physical components such as programmable logic controllers, network hubs, cards, buses, cabling, encoders, and interfaces/ displays)
- Monitoring and alarm systems, etc. and their subcomponents.

---

**Modes of Operation**

- *Jacking up* – raising of the hull, both normal and pre-load
- *Normal holding* – holding of the hull, both normal and pre-load
- *Lowering* – lowering of the hull, both normal and pre-load
- *Severe storm holding* – elevated and holding under impact load conditions
- *Emergency operations* – jacking up or lowering

---

**Typical Failures**

Typical failures that need to be analyzed in the FMEA include, but are not limited to:

- Machinery or mechanical components (e.g., failure of gears, motor, brake)
- Supporting utilities (e.g., loss of hydraulic, electrical systems)
- Control system (e.g., electronic circuit boards, power supplies, microprocessors/PLCs, memory boards, input/output modules, cables, etc.)
- Nonstructural static components (e.g., pipes, cables, block valves)
- Critical mechanical components in fixation system
- Mechanical components of structural members
- Failures at interfaces or interconnections between systems
- Failures caused by credible external events (e.g., fire, hurricane)
- Others, as applicable

Particular attention should be paid in the Jacking Systems FMEA to:

- The interfaces between the jacking system and other systems that have the potential to affect it.
- The effect of the failure upon the rest of the system's ability to jack the unit including time effects (i.e. if necessary time is available for manual intervention).
- Yoke and pin type jacking system – pin failure, lifting frame structure failure in the severe storm condition if applicable.
- VFD failure for torque control, speed control and in relationship to brake operation timing, etc.
- Power supply circuit breakers/relays, wiring and control interlocks.

- Punch-through and control panel location on open deck.
- Anti-collision between the hull and the spud-can.
- Critical monitoring failures such as RPD, speed, overload, overcurrent, over-torque and safety system actions based on the normal operation of these monitoring.
- Rack chock/fixation system failure.

**Timeline/ Team**

- The optimal time for performing the FMEA is at the detailed design stage when there is enough detail about the system and equipment, but still time to include FMEA recommendations in the final design and integration process
- Needed subject matter experts in operations, design and relevant vendors should participate in the FMEA

**Verification Program**

There are no specific Classification requirements for testing to validate FMEA conclusions for jacking systems. However, it is at the discretion of the ABS Surveyor or ABS Plan reviewer to recommend specific testing of FMEA failures for which there is a higher degree of uncertainty.

**Supporting Documents**

The FMEA must be submitted to ABS for review. In order to carry out a proper review of the FMEA, the ABS Plan reviewer needs the following information included in the FMEA report:

- General description of the scope and purpose of the FMEA
- Dates when the FMEA was conducted
- FMEA participants
- Summary of any risk-reducing actions performed or pending as a result of recommendations of the FMEA.
- Detail narrative of relevant systems
- System drawings, layout and general arrangement, Process Flow Diagrams, etc.
- Functional block diagram showing systems interactions, parallel paths for redundant systems, in series for single systems.
- Description of the system boundaries, both physical and operational
- System design specifications
- FMEA worksheets, including:
  - Modes of operations
  - All significant failure modes associated with each operational mode
  - Cause associated with each failure mode
  - Common cause failures
  - Method for detecting that the failure has occurred
  - Effect of the failure upon the system, including its ability to carry out its function
  - Global effect of the failure on other systems, the asset and HSE
  - Controls to prevent and/or mitigate the failure

Where redundancy is needed to prevent "uncontrolled descent" but is not possible, further study of the non-redundant parts must be carried out to provide evidence of their reliability and mechanical protection.

The operations, maintenance, inspection, testing and emergency manuals are needed for ABS to confirm compliance with design and manufacturer's requirements and that the FMEA findings have been incorporated into equipment operating phases.

**Lifecycle Management**

If any subsequent modifications to the jacking/holding system are carried out, risk studies are to be updated to demonstrate that the system is still in compliance with the ABS no-single failure criteria. Types of changes requiring submittal of revised FMEA for ABS' review include:

- Operating criteria changes
- System configuration/boundary changes
- Equipment changes
- New application
- Revalidation of previous FMEA from vendor

**Additional Notes**

## 1.10 Subsea Heavy Lifting

RULE/GUIDE ABS Rules for Building and Classing Offshore Supply Vessels, 2014

**Rule Reference**

**Part 5** Specialized Services
**Chapter 9** Heavy Lift
**Appendix 2** Subsea Lifting

**Rule Requirement**

**5-9-A2/5 Subsequent De-rating for Subsea Lifting (recommended)**

…..

*vi)* *A risk analysis according to the ABS Guide for Risk Assessment Applications for the Marine and Offshore Oil and Gas Industries should be conducted.*

*vii)* *A failure mode and effects analysis (FMEA) should be conducted and this should include vessel power failure.*

*viii)* *Each subsea lift operation is to have its own unique modeling and analyses scenarios.*

**Purpose of FMEA**

Demonstrate that a single failure during sub-sea heavy lifting will not cause loss of control of load, structural damage or other hazardous situations such as fire and explosion, pollution or injury.

**Undesired Events**

Loss of control of load, structural damage or other hazardous situations such as fire and explosion, pollution or injury.

**Systems or Subsystems**

The physical scope of the heavy lifting system for subsea includes crane, winches, cylinders, accumulators, active/passive heave compensation, electric circuits and control system.

**Modes of Operation**

The FMEA is to consider failure during all foreseeable subsea lifting modes of operations, including the use of active heave compensation, passive heave compensation, constant tension or any combination of these systems.

**Typical Failures**

Typical failures that need to be analyzed in the FMEA include, but are not limited to:

- Electric failures
- Hydraulic failures
- Active/passive heave compensation failure
- Mechanical failures
- Failure of crane power supply from vessel

- Failures of lifting active equipment components
- Failures of passive components such as pipes, cables, block valves, etc.
- Failure of mechanical components of structural members
- Failures of control systems at I/O level (e.g., sensors, power supply, PLC, cables, etc.)
- Failures at interfaces or interconnections between systems
- Failures caused by credible external events (e.g., fire, hurricane)
- Others, as applicable

Particular attention should be paid in the FMEA to the interfaces between the heavy lift system and other systems that have the potential to affect it.

**Timeline/ Team**

- The optimal time for performing the FMEA early design is at the vendor stage when there still time to include FMEA recommendations in the final design and integration process
- Ideally, subject matter experts in operations, design and relevant vendors should participate in the FMEA
- The FMEA report shall be submitted to ABS with approval drawings

**Verification Program**

There are no specific Classification requirements for testing to validate the FMEA conclusion. However, it is at the discretion of the ABS Surveyor or ABS Plan reviewer to recommend specific testing of FMEA failures for which there is a higher degree of uncertainty.

**Supporting Documents**

The FMEA must be submitted to ABS for review. In order to carry out a proper review of the FMEA, the ABS Plan reviewer needs the following information included in the FMEA report:

- General description of the scope and purpose of the FMEA
- Dates when the FMEA was conducted
- FMEA participants
- Summary of any risk-reducing actions performed or pending as a result of recommendations of the FMEA.
- Description of active or passive heave system functions, control and reliability
- Description of vessel power supply system
- System drawings, including layout/general arrangement, schematics.
- Functional block diagram showing systems interactions, parallel paths for redundant systems, in series for single systems.
- Description of the system boundaries, both physical and operational
- System design specifications

- FMEA worksheets, including:
  - Modes of operations
  - All significant failure modes associated with each operational mode
  - Cause associated with each failure mode
  - Common cause failures
  - Method for detecting that the failure has occurred
  - Effect of the failure upon the system
  - Global effect of the failure on other systems, the asset and HSE
  - Controls to prevent and/or mitigate the failure

The operations, maintenance, inspection, testing and emergency manuals are needed for ABS to confirm compliance with the design and the manufacturer's requirements and that the FMEA findings have been incorporated into the equipment operating phases.

**Lifecycle Management**

If any subsequent modifications to the vessel or the cranes are carried out, risk studies are to be updated to demonstrate that the system is still in compliance with the ABS design philosophy. Types of changes requiring submittal of the revised FMEA for ABS' review include:

- Operating criteria changes
- System configuration/boundary changes
- Equipment changes
- New application
- Revalidation of previous FMEA from vendor

**Additional Notes**

## 1.11 Drilling Systems/Subsystems/Individual Equipment

RULE/GUIDE Certification of Drilling Systems (CDS)

**Rule Reference**

**Section 2** Design of Drilling Systems

**Subsection 5** Design Considerations

**5.9** Risk Assessment for Drilling Systems

**Rule Requirements**

**2/5.9.4 Functional FMEA/FMECA**

*Functional FMEA/FMECA as specified in 2/5.9.1ii) above are to be performed covering individual systems, subsystems, equipment and components as defined in Subsection 3/1 of this Guide.*

*i)* *The functional FMEA/FMECA is to evaluate that the intended control functions, such as hydraulic, pneumatic, electrical, electro-hydraulic, acoustic, or computer-based system's components, as applicable, will not cause unsafe operation in compliance with the design principles in Subsection 3/3, 3/15.1, 3/15.3, 3/15.5.*

*ii)* *The functional FMEA/FMECA is to evaluate that the well control, drilling support, and general support systems will not cause unsafe operation in compliance with the design principles in Subsection 3/3, 3/15.1, 3/15.3, 3/15.5.*

*iii)* *The results of the functional FMEA/FMECA are to identify critical systems/functions to be further analyzed during component level FMEA/FMECA.*

***

**2/5.9.5 Component-Level Risk Assessments**

*i)* *The detailed component level FMEA/FMECA is to be performed for the critical components as identified during the functional FMEA/FMECA.*

*ii)* *The component level FMEA/FMECA is to correlate to the functional FMEA/FMECA to provide an overall understanding of the local effects of the equipment failure mode and 'global' effects of the failure of the control/safety function and other equipment/ interfaces in the system.*

**Purpose of FMEA**

To verify that the system/subsystem and equipment comply with the following failure design philosophy:

- No single failure will lead to a hazardous situation to people, environment or equipment, and
- That there are at least two protections in place to prevent the hazardous event

**Undesired Events**

1. Injury, pollution or equipment damage
2. Loss of functionality is also a consequence of concern for well control systems and drill string systems with active heave compensation (AHC).

Safe shutdown usually sufficient to prevent the hazardous situation, and redundancy usually needed if a single failure shall not result in a loss of function.

## Systems or Subsystems

A typical list of systems contained in a drilling unit is included in Section 3 of CDS Guide, and is reproduced below. All major well control, drilling support and general support systems need an FMEA in order to validate the failure design philosophy. Simple systems can be validated without an FMEA as indicated in section below.

| *Well Control* | *Drilling Support* | *Support* |
|---|---|---|
| Blow out preventers | Derrick/Mast | Storage |
| Lower Marine Riser Package | Mud Conditioning/Return | Nitrogen generation/charging |
| Marine drilling risers | Cementing | Hydraulic and Pneumatic Systems |
| Diverter systems | Conductor Tension System Unit | Utilities and Instrument Air |
| Choke and kill systems | Drill String Compensators | Chemical Injection Unit |
| Well circulation | Riser tensioning | Sea Water |
| Auxiliary Well Control Equipment | Hoisting equipment | |
| Secondary Well Control Systems | Lifting/cranes | |
| Emergency Well Control System | Pipe/Riser/BOP Handling | |
| | Rotary Equipment | |
| | Hydraulic Power Units | |
| | Well Test** | |
| | Hydrocarbon Disposal** | |

** For hydrocarbon systems, a HAZOP is a good alternative to FMEAs.

### Systems Exempt from FMEAs

Complex drilling systems need an FMEA in order to properly evaluate compliance with Classification failure design principles, but for simple systems, standard engineering methods suffice to demonstrate compliance with design principles. Simple systems are those for which the following statements hold true:

- Manual control only – could be hydraulic, pneumatic, electrical, etc. (e.g., on/off switches, manual lever)
- Do not have any PLC or computerized control system
- Control function cannot be altered by operator
- Go mechanically to safe state in all failure modes
- Failure of control will not impact other machine
- System will not be impacted by other machine failure

Examples of simple systems are air-powered winch (hoisting equipment) and joy stick-controlled equipment.

## Modes of Operation

A system normally has multiple modes of operation and each mode can present distinct failure scenarios.

The FMEA shall consider both global operations at installation or vessel level (i.e., drilling operation), and local operations of the system/equipment which is part of the scope of the FMEA as relevant. The FMEA must analyze all the modes of operations (global and local) to identify failures, hazards and consequences of concern.

The following list gives an example of modes of operations that should be explicitly considered on the FMEA, both for failure modes that are operation-specific, as well as resultant consequences that vary depending on the operations.

Global MODU operations in a MODU may include the following:

- Transit between wells (transit/operations/preparations in between drilling two wells)
- Pre-drilling
- Deployment
- Upon latching
- Normal drilling and well control
- Simultaneous operations
- Emergency operations
- Transient operations
- Subsystem-specific operational modes

It is not feasible to show examples of all the local operational modes for all systems, but as an example, typical system-specific operational modes for the Active Heave Compensated draw works may include the following:

- Tripping
- Weighting on cement (WOC)
- Active heave compensation (during drilling)
- Lock-to-bottom (while running BOP)
- Slip and cut

---

**Typical Failures**

**Mechanical Designs (Functional FMEA)**

Typical failures that need to be analyzed during failure analysis of a system/subsystem or equipment include, but are not limited to:

- Machinery or mechanical components (e.g. pump, compressor)
- Components within the control system
- Nonstructural static components (e.g., pipes, cables, block valves)
- Mechanical components of structural members
- Interconnections between systems
- Credible external events (e.g., fire, hurricane)

**Programmable Computer Controls (Component-Level FMEA)**

The systems with programmable computer controls should include a failure analysis of the components of the control system. The lowest level of physical component failure required to be included in the FMEA for control systems is typically at the data acquisition unit level which includes the CPU, its I/O modules, the powering of the device, and any communication between multiple devices.

Physical components whose failures should be analyzed in the FMEA include:

- CPU microprocessor/PLC
- Input/output modules
- Power supplies

- Electrical power cables
- Network hubs
- Buses
- Communication/data link cables
- Interfaces/displays
- Electrical power cables
- Others, as applicable

For functions permitting wireless data communications, consideration is to be given to the possibility of corrupted data and intermittent faults with comparatively long recovery times between interruptions.

Software may reside in several different areas of a given system and at multiple levels (i.e., operating system, PLC embedded logic). Software failures are to be considered at a higher level, almost like a system failure; to address how the system can prevent and recover from, for example, malware.

Classification Rules require the system developer to follow a recognized software quality assurance program, so it is generally assumed that by the time software is delivered and installed, it is error free.

Relays, terminal boards, indicator lights, switches, meters and instruments do not have to be included in the FMEA unless their failure would lead to a hazardous situation not discussed with a higher level component.

**Timeline/ Team**

- Individual systems and equipment FMEA are ideally performed by the vendor
- Timing early enough to allow design modifications in case there is a finding of noncompliance with Classification failure design principles such as the no-single failure criteria.

**Verification Program**

As per sections 2/5.9 and 2/5.11 of the *CDS Guide*, a Validation Program is to be developed and performed to verify selected/critical results of the FMEA/FMECA/Risk Assessment of the Equipment.

The specific goals of the tests are to validate the:

- Effectiveness of system to identify failures
- Effect of identified failures on system/equipment
- Response of safety controls
- Other measures to protect against failure

This testing program is subject to ABS Engineering Approval and Survey Witness.

The Equipment Possessing Controls Systems subject to ABS Engineering Approval and Unit Certification are required to undergo Validation Testing with Survey witness and acceptance.

*i)* FMEA/FMECA validation is to be carried out at the vendor's plant, in accordance with 4/3.3.1 and Subsection 8/3 of the *CDS Guide*.

*ii)* When final testing requires assembly and installation on-board facility, it may not be possible to perform all required testing at vendor's plant. In this case, FMEA/FMECA validation is be carried out as part of the system integration testing (SIT) during commissioning, in accordance with 4/3.3.2 and Subsections 8/5 and 8/7 of the *CDS Guide*.

*iii)* The test program results are to be documented to confirm that the FMEA/FMECA conclusions are valid. When equipment control systems possess mitigating design barriers which prevent single-point-failures (of controls systems) from cascading to unsafe events, the appropriate function response of an applicable barrier to perform as intended is the critical result subject to validation testing. Critical Results subject for validation testing should NOT be directly correlated to a client's chosen Criticality ranking of an FMECA. While a FMECA Criticality ranking can be aligned toward this criterion to help identify such mitigating barriers, a direct correlation of clients chosen criticality ranking method for identifying CDS Critical results should NOT be done until the designers' chosen methodology is verified to identify alignment.

Critical Results are defined as those areas of a mechanical or control system which has mitigating barrier(s) to prevent the occurrence of a hazardous situation. The verification program is to validate that upon the specified failure, a minimum of one mitigating barrier performs as intended in order to prevent occurrence of a hazardous situation. Examples of such mitigating barriers are hydraulic load holding valves, alarms, sensors, etc.

Selected Results are defined as those results for which there is reasonable uncertainty or disagreement of the FMEA assumptions. During the FMEA, uncertain assessments results are to be identified and discussed with the designer at time of Design Review for resolution. If a resolution is not achieved, these items should be included in the verification program.

Examples of areas where inadequate data may be available to perform definitive analysis, thus should be part of the verification program include the behavior of interlocks that may inhibit operation of essential systems.

**Technical Notes**

Successful FMEA/Risk Validation Testing will verify the appropriateness of design but one test cannot be extended for Unit Certification for additional equipment assemblies. The reason for this is that the construction, assembling, and component integrity can vary with each manufacturing which in turn may result with a needed barrier not performing as intended. Thus as required by 4/3.3.1, 4/3.3.2, 4/Table 1 and Subsections 8/5 and 8/7. Validation Testing is to be conducted for each manufactured unit for all equipment/control systems requiring Engineering Design approval and Unit Certification as applicable per the *CDS Guide*.

If a Barrier is identified to be tested for Validation that cannot be tested without damage to the unit, the requirement for repeating the testing on each subsequent manufactured unit may be waived on a case by case basis at the discretion of the reviewing ABS Engineering Office, subject to a successful outcome of the testing of the first unit.

Self-tests such as Hardware-in-the-Loop (HIL) can be substituted if adequate to prove intent and goals of verification program. When a full test of a system failure cannot be performed (destructive test, safety concerns, etc.), its functional testing must be carried out as far as mutually agreed. In addition, the barriers to detect/prevent/mitigate the failure, as indicated in the FMEA, must be functionally tested.

**Supporting Documents**

The FMEA must be submitted to ABS for review. In order to carry out a proper review of the FMEA, the ABS Plan reviewer needs the information listed in Subsection 2/7 of the *CDS Guide*. This essential documentation includes the following:

- FMEA report, including FMEA worksheets and FMEA verification plan.
- General description of the scope and purpose of the FMEA
- Dates when the FMEA was conducted
- FMEA participants
- Summary of any risk-reducing actions performed or pending as a result of recommendations of the FMEA.
- Detailed description of the system and its function(s)
- Drawings of the system and control,
- Layout and general arrangement drawings
- Single line diagrams
- System design specifications
- Cause and effect chart showing the control logic
- Description of the physical and operational scope and boundaries for the FMEA, including:
  - Functional blocks arranged in a reliability block diagram, showing interactions among the blocks (parallel paths for redundant functional blocks, in series for single blocks)
  - Modes of operation for the system
- FMEA worksheets, including:
  - Modes of operation
  - All significant failure modes (associated with each mode of operation)
  - Cause associated with each failure mode
  - Method for detecting that the failure has occurred
  - Effect of the failure on system functionality
  - Global effect of the failure on health, safety and the environment
  - Existing controls to prevent and/or mitigate the failure
  - Corrective actions needed to comply with ABS Classification requirements
- FMEA Verification plan
- Operations, maintenance, inspection and testing manuals

For systems where loss of function upon a single failure is not acceptable, but redundancy is not possible, provide a further study of non-redundant parts with consideration to their reliability and mechanical protection.

The operations, maintenance, inspection, testing and emergency manuals are needed for ABS to confirm compliance with design and manufacturer's requirements and that the findings of the FMEA have been incorporated into the equipment operating phases. These manuals may also highlight operational configurations in which the systems redundancy could be bypassed.

**Lifecycle Management**

Risk studies* results are to be maintained by the Owner of the drilling unit. If any subsequent modifications to the drilling system, subsystems, equipment or components are carried out, risk studies are to be updated to demonstrate that 1) any hazards derived from the modifications have been mitigated and 2) system is still in compliance with the ABS no-single failure criteria.

These risk studies shall be resubmitted to ABS after the modification.

* Risk Studies refers to the analysis of the integrated systems (e.g., HAZID) and systems/equipment analysis (e.g., FMEA)

**Additional Notes**

- Equivalent risk method can be used as long as it fulfills the intent of the FMEA.
- FMEA recommended because it is well suited for mechanical systems.
- The *CDS Guide* uses term FMEA/FMECA. The FMECA is an FMEA that includes a criticality assessment of the failure and its consequences. This criticality assessment is not needed for ABS review purposes of CDS equipment. For the purposes of the *CDS Guide*, an FMEA will always be sufficient. The FMEA is to prove compliance with key principles of the ABS design philosophy. These principles need to be complied with, regardless of the assessed criticality.

## 1.12 Integrated Drilling Plant

RULE/GUIDE Certification of Drilling Systems (CDS)

**Rule Reference**

**Section 2** Design of Drilling Systems
**Subsection 5** Design Considerations
**5.9** Risk Assessment for Drilling Systems

**Rule Requirements**

**2/5.9 Risk Assessments for Drilling System**
*For a drilling system as defined in Subsection 3/1 of this Guide, risk assessment for the drilling system and individual systems, subsystems, and equipment is to be performed.*

*Qualitative risk assessments are to be conducted with the following objectives:*

*i) Identifying and assessing major hazards, but not limited to, those defined in 1/7.9 of this Guide*

*ii) Potential risks associated with the drilling system, including its impact on other systems*

*iii) Demonstrate compliance with the design principles as stated in this Guide*

*iv) Identify prevention and mitigation measures, as appropriate*

*v) Areas or issues requiring further analysis, testing, or risk evaluations*

***

**2/5.9.1 Levels of Risk Assessment**
*Three (3) levels of risk assessments are to be performed, as applicable:*

*i) Qualitative hazard identification studies such as HAZID, HAZOP, "What-if", etc., or similar*

*ii) Functional FMEA/FMECA*

*iii) Component level FMEA/FMECA*

*These assessments are to be performed sequentially, starting with the identification of hazards for the overall design, and focusing to detailed risk studies driven by the findings of the previous studies, as necessary*

***

**2/5.9.3 Integrated Drilling System**
*The objective of drilling system risk assessment is to identify major hazards related to the system, subsystem, and equipment as defined in Subsection 3/1 as an integrated system on a drilling unit. Risk assessment is to consider, but not limited to, major hazards as defined in 1/7.9 of this Guide.*

*i) Qualitative risk assessments as defined in 2/5.9.1i) above are to performed covering the integrated drilling system.*

**Purpose of HAZID**

The purpose of the Hazard Identification (HAZID) study is to identify the major hazards to people, environment and equipment associated with the integrated drilling systems/drilling plant and verify the adequacy of the risk control measures.

The HAZID study shall focus on identifying hazardous situations* originating from:

*i)* Arrangement, location and general layout of drilling systems, subsystem, equipment

*ii)* Integration and interconnections between the different drilling systems, sub-systems and equipment

*iii)* Interfaces with drilling support systems, utilities and marine systems

*iv)* Various operating modes

**Undesired Events**

Harm to 1) human safety, 2) the environment or 3) equipment.

**Systems or Subsystems**

In the *CDS Guide*, integrated drilling systems refers to the collective of systems, subsystems and equipment related to well control, drilling support and support systems installed on the drilling unit.

The integrated drilling systems to be analyzed for major hazards include all the systems identified in Chapter 2, Section 7 and Chapter 3 of the *CDS Guide*, such as:

- Well control
- Marine drilling riser
- Drill string compensation
- Riser tensioning
- Drilling fluid system – Mud conditioning and circulation
- Bulk storage and transfer
- Drilling
- Hoisting, lifting, tubular handling
- Mechanical load-bearing equipment
- Well testing, completion, servicing system
- Control and monitoring system for above
- Drilling support
- Others, as appropriate

The detailed analysis of these systems will be accomplished via the FMEA of CDS systems/ subsystems and components.

The layout and physical location of systems is important to consider in the HAZID as it can be the cause of hazardous situations. The areas below should be looked into during the HAZID:

- Derrick and drill floor and surrounding area
- Moon pool area
- Driller's control cabin
- Central controls area
- Local electrical room
- Choke & kill manifold area

- BOP and x-mas tree storage area
- BOP central control unit (CCU)
- Hydraulic Power Unit (HPU) area (BOP/Diverter, Drilling system)
- Subsea engineer's room
- Well test area
- Drain, drain collection
- Mud pit area
- Mud pump room
- Cementing unit area
- Mud treatment
- Mud lab
- Cuttings/solid disposal and storage
- Bulk material transfer area and storage
- Storage areas (e.g., pneumatic bottles, tools, equipment)
- Drilling switchboard room
- Tubular handling areas
- Tubular storage (forward and aft of moon pool)
- Overhead cranes
- Pipe, cable, utility trunk
- Mud gas separator, choke and kill manifold area
- Flare boom
- Remote-operated vehicle (ROV) storage and launch area
- Utilities and drilling support system areas (e.g., nitrogen generation, chemical injection)
- Others, as appropriate

**Interfaces with Marine Systems**

Marine systems are not covered in the CDS Guide but their interfaces with the drilling plant must be addressed in the HAZID study, as they can result in hazardous situations to people, environment or equipment

The integrated system HAZID study must analyze the potential issues/hazards from interfaces with marine areas such as:

- DP system/mooring
- Supply vessels
- Laydown areas
- Air compressor room
- Electrical supply (e.g., high voltage and drilling switchboard rooms)
- Drain collection and cleaning
- Exhaust systems

- Heat tracing
- Firefighting systems
- HVAC
- Other utilities (e.g., potable water, control air, cooling media)
- Other emergency systems

### Modes of Operation

A system normally has multiple modes of operation and each mode can present distinct failure scenarios (failure modes, hazards, consequences).

HAZID must analyze all the modes of operations to identify hazards and consequences of concern.

The HAZID shall consider both global operations at installation or vessel level (i.e., drilling operation), and local operations of the systems in question.

The following list gives examples of modes operations that should be explicitly considered on the HAZID study for the hazards that are operation-specific. Other operations may need to be included, as applicable.

Typical **global** and **local** operations of a drilling unit that should be considered in the HAZID are listed below.

| *Operation* | *Typical Activities Occurring During Global Operations of Drilling Unit* |
|---|---|
| Before drilling | Preparations of tubulars, drilling fluids, etc. prior to drilling such as:<br>• Complete testing per API 53 requirements for all well control equipment<br>• Functional test other surface equipment as necessary<br>• Precharge BOP accumulator<br>• Conduct well control drill and emergency drill<br>• Make drill stand |
| Transit between wells | Operations and preparations in between drilling two wells such as:<br>• Inspect retrieved BOP/LMRP equipment, riser, C&K line diverter equipment etc.<br>• Perform necessary maintenance and inspection on all well control equipment |
| Deployment and retrieval | • Deployment of rig, BOP, LMRP, etc.<br>• Drill bare hole using drill string<br>• Install outer conductor casing, cementing<br>• Lower BOP stack assembly using riser<br>• Deploy C&K hoses, flow line, hot line, mud boost line etc.<br>• line up diverter for shallow drilling<br>• Retrieval of BOP, LMRP, riser, and moving to designated stored position |
| Upon latching | Latching of BOP, LMRP, riser, etc. Once latched perform all testing per API 53 requirement, function test all functions for BOP, C&K, diverter, etc. |
| Normal drilling and well control | • Drilling the surface hole and subsequent section of well per drilling plan, tripping out, casing, cementing, testing, completing, etc.<br>• Well-kicks, unexpected pressures, gas cut mud, etc. |
| Simultaneous operations | • Dual-derrick operations – such as drilling on derrick, making casing string on other<br>• Two or more operations being carried out concurrently such as production, construction, heavy lifts, barges, rig movement, emergency response, etc. |
| Emergency operations | Weather-related emergencies, loss of well control, collision, EDS, loss of DP, loss of power, riser string component breakage, tensioning system failure, marine event such as loss of ballast control, AHD draw work failure etc. |

| | |
|---|---|
| Special and transient operations | Startup, shutdown, riding storms, wireline, jarring, well test, well completion |
| Subsystem-specific operations | It is not feasible to show examples of all the operational modes for all systems, but as an example, typical system-specific operational modes for the Active Heave Compensated (ACH) drawworks may include, but are not limited to the following:<br>• Tripping-in and tripping-out<br>• Active heave compensation (during drilling)<br>• Lock-to-bottom (while running BOP or well testing)<br>• Riding a storm attached<br>• Others as applicable |

**Typical Failures**

HAZID workshop shall identify potential hazardous situations and verify that adequate risk control measures are provided to address:

- Loss of control of load/dropped objects
- Release of hydrocarbons
- Release of $H_2S$
- Release of toxic chemicals
- Fire and explosion
- Pollution to the sea
- Loss of well control/blowouts
- Release of pressurized fluids
- Loss of system function
- Loss of station-keeping
- Loss of stability/buoyancy
- Structural damage
- Damage of subsea equipment
- Equipment collisions
- Injury due to interface with machinery
- Blackout
- Environmental events
- Failure of mechanical components under stress
- Domino effects/impairment of emergency response equipment/activities (Not to be considered on its own, but in conjunction with each hazardous event)

The integrated drilling plant HAZID study shall look into the following items:

- Safety of personnel and operation
- Separation of nonhazardous areas from classified hazardous areas
- Separation of fuel and ignition source as far as practical
- Minimizing likelihood of uncontrollable releases of hydrocarbon
- Minimizing spread of flammable liquids and gases
- Minimizing probability of ignition

- Minimizing consequences of fire and explosions
- Preventing fire escalation and equipment damage
- Providing for adequate arrangements for escape and evacuation
- Facilitating effective emergency response
- Minimizing dropped object hazards to personnel, equipment (on installation and subsea) and structure
- Protection of critical systems, subsystems, equipment and/or components from damage during drilling operation, such as:
  - Electrical cables and cableways
  - Well control equipment
  - Exhaust ducting and air intake ducting
  - Control and shutdown systems
  - Fire/gas detection and fire-fighting equipment arrangement so that they are protected from damage during drilling operations
- Equipment arrangements provide access for inspection and servicing and safe means of egress from all machinery spaces

---

**Timeline/ Team**

The HAZID for the integrated drilling plant should be performed early enough in the design stage to facilitate implementation of recommendations that may involve a design change.

The HAZID sponsors are typically the:

- Overall Drilling Plant integrator (shipyard) and the
- Vessel owner

Subject-matter experts in appropriate disciplines are key to the successful identification of hazards and appropriate development of the HAZID scenarios.

Additional participants in the HAZID include subject matter experts from:

- Owner
- Operations (e.g., drilling, pipe handling, mud, process)
- Integrator or party responsible for integration (e.g., shipyard or major equipment supplier)
- Shipyard
- Major equipment vendors
- Control system integrator
- Classification subject-matter experts.
- Subsea
- Marine
- Mechanical/piping
- Electrical/Instrumentation and control
- Safety/HSE
- HAZID team facilitator and HAZID scribe with extensive experience facilitating/recording HAZID studies

---

**Verification Program**

Not applicable to Integrated Drilling Plant HAZID studies

**Supporting Documents**

The HAZID report must be submitted to ABS for review. In order to carry out a proper review, the ABS Plan reviewer needs the following information:

- Completed HAZID report including the following:
  - Description of objective and scope
  - Description of hazard identification technique used
  - List of team members who participated in workshop
  - Description of each action item and responsible party to close the item, as identified by the team during the workshop
  - Completed HAZID workshop record describing the potential accident scenarios discussed by the team as well as corrective actions.
- Detailed description, narrative and drawings of the system functional description and control
- Layout and general arrangement drawings
- System design specifications
- Cause and effect chart showing the control logic
- Description of the physical and operational scope and boundaries for the risk study
- Operations , maintenance, inspection and testing manuals

The operations, maintenance, inspection, testing and emergency manuals are needed for ABS to confirm compliance with the design and the manufacturer's requirements and that the findings of the risk study have been incorporated into the equipment operating phases.

**Lifecycle Management**

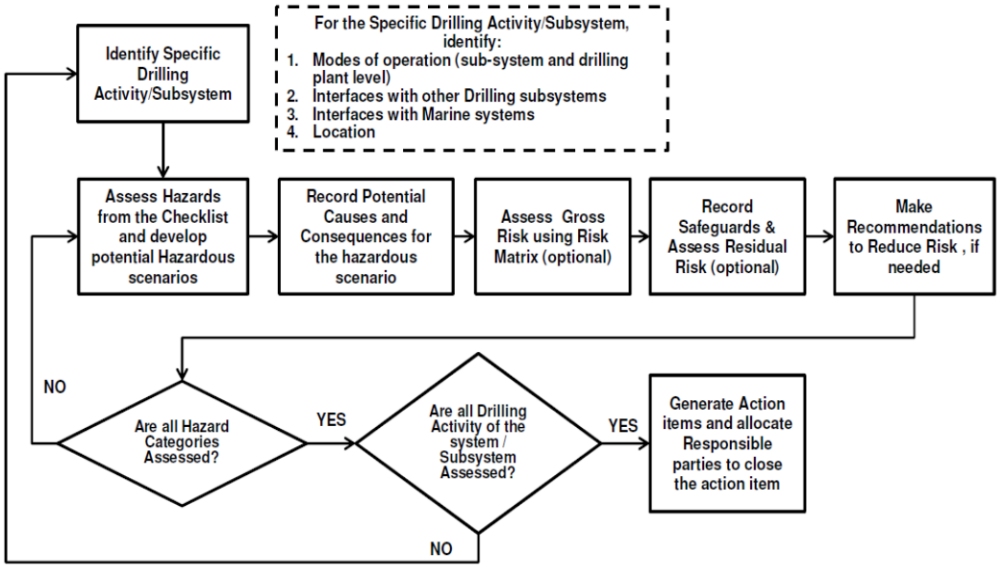
Risk studies* results are to be maintained by the Owner of the drilling unit. If any subsequent modifications to the drilling system, subsystems, equipment or components are carried out, risk studies are to be updated to demonstrate that any hazards derived from the modifications have been mitigated. These risk studies shall be resubmitted to ABS after a modification.

* Risk Studies refers to Integrated systems (e.g., HAZID) and Systems/Equipment (e.g., FMEA)

**Additional Notes**

- The requirements for FMEAs for the CDS individual systems are discussed in 7/1.11.
- Note that a drilling plant HAZID is always a requirement of the *CDS Guide*, even if the drilling plant is a standard design. For previously-approved designs for which a risk assessment exists, the HAZID should be updated. If no risk assessment exists, a complete HAZID must be carried out

**Summary of HAZID process for CDS**




**Sample HAZID Table**

**HAZID**

| | |
|---|---|
| **Area** | Mud process room and Shale Shaker Room |
| **Major Equipment in area** | Shale shaker, gumbo conveyor, APV, degasser, flow divider, mud process control room |
| **Modes of Operation** | Drilling operations |
| **Interfaces with other drilling subsystems** | Cyber base and control system |
| **Interfaces with marine systems** | Electrical system, utility system, sea water, etc. |
| **Reference Docs/Dwgs** | GA |

| Hazardous Situations | Causes | Consequences | Safeguards | Recommendation | Comments |
|---|---|---|---|---|---|
| **Release of H2S, CO2, hydrocarbons**, etc. into the mud process room and shale shaker room | Formation gases coming back | • Potential for injury or loss of life<br>• Fire and Explosion<br>• Equipment failure<br>• **Of special concern is the location of the operator's control room within the mud process area.** | • H2S gas detector<br>• Zone certified equipment<br>• Negative pressure in Shaker room<br>• Positive pressure in operator's control room<br>• Air change ratio 12x<br>• Crew operational training H2S<br>• Fire fighting / detection arrangement<br>• Breathing apparatus or cascade systems as applicable<br>• H2S operational procedures | Consider a fire and gas and an evacuation study to determine if there is need to relocate operator's control room or add additional safeguards. | The location of the manned operator's control room within the mud process area is of concern as there is a significant likelihood of toxic or flammable gases in area. |
| ... | ... | ... | ... | ... | ... |
| ... | ... | ... | ... | ... | ... |

An optional step is the risk ranking of the hazardous scenarios based on a risk matrix. This risk ranking typically would be based on the severity of the consequences and the likelihood of achieving the ultimate consequences, taking into account the reliability of existing safeguards. The resulting risk ranking (e.g.; high, medium or low risk) depends on the location of the hazardous scenario along the severity axis and the likelihood axis in the risk matrix and is very useful to focus efforts on the high risk items. If a risk ranking step is included, the HAZID table above will include three more columns – one for the consequence ranking, one for the consequence ranking, and one for the resulting risk ranking. Another best practice is to have a "before" and "after" risk ranking. The "before" risk ranking shows the risk of the hazardous event with existing controls. If this "before" risk is intolerable, recommendations are made and a new risk ranking, taking into account the recommendations, will show the "after" risk, which should now be within the tolerable range.

## 1.13 Dual Fuel Diesel Engines (DFDE)

RULE/GUIDE Rules for Building and Classing Steel Vessels Part 5C, Chapter 8 "Vessels Intended to Carry Liquefied Gases in Bulk"

---

**Rule Reference**

**Part 5C** Specific Vessel Types

**Chapter 8** Intended to Carry Liquefied Gases in Bulk

**Appendix 5** Reliquefaction System (ABS)

**Subsection 1** General

**Subsection 7** Instrumentation and Safety Systems

***

**Appendix 7** Dual Fuel Diesel and Single Gas Fuel Engines (ABS)

**Subsection 5** Gas Fuel Engines

***

**Appendix 8** Dual Fuel Gas Turbine Propulsion System (ABS)

**Subsection 5** Plans and Data to be Submitted

---

**Rule Requirements**

**5C-8-A5/1.5 Plans and Data to be Submitted**

- Failure Modes and Effects Analysis (FMEA) to determine possible failures and their effects in the safe operation of the reliquefaction system [see 5C-8-A5/7.1ii)]

**5C-8-A5/7.1 General**

*ii)* An analysis is to be carried out for the reliquefaction system identifying component criticality.

***

**5C-8-A7/5.7 Protection against Explosion**

In addition to the requirements in 4-2-1/7, a Failure Modes and Effects Analysis (FMEA) is to be carried out by the engine manufacturer in order to determine necessary additional means of safeguards to address the hazard associated with the use of gas as a fuel.

The analysis is to identify all plausible scenarios of gas leakage and the resulting possible explosion. Then the analysis is to identify necessary means to control the identified explosion hazards.

The FMEA is to be submitted to ABS for approval.

Unless the FMEA proves otherwise, the monitoring and safety system functions for the dual fuel diesel engine are to be provided in accordance with 5C-8-A7/Table 1.

The alarms required by 5C-8-A7/Table 1 are to be provided at the engine control station. In addition, a summary alarm is to be provided at the navigation bridge.

***

**5C-8-A8/5 Plans and Data to be Submitted**

- Failure Modes and Effects Analysis (FMEA) to determine possible failures and their effects in the safe operation of the dual fuel gas turbine

---

**Purpose of Risk Study**

Risk studies are required for gas fueled engines ships for the following two cases:

*i)* FMEA on instrumentation and safety systems of re-liquefaction unit

*ii)* Risk study (HAZID, FMEA, or alike) on the dual fuel diesel and single gas fuel engines, or in the dual fuel gas turbine propulsion systems.

***

**FMEA of Instrumentation and Safety Systems**

The purpose of carrying out an FMEA on the **instrumentation and safety systems** is to demonstrate that any single failure will not lead to an undesirable event such as:

- Lost or degraded function beyond acceptable performance criteria
- Hazardous situation (such as a state that is not fail-safe, complete loss of control, unsafe shutdown of equipment, loss of propulsion, blackout, etc.)

Corrective action measures should be proposed to address situations of noncompliance with the single-failure design philosophy and mitigate the risk of hazardous events.

***

**FMEA of Gas Fueled Engine/Turbine**

The purpose of the risk study of **the engine or turbine** is to identify the major hazards to people, environment, and equipment associated with the engine and verify the adequacy of the risk control measures.

The risk study shall focus on identifying hazardous situations originating from

- Gas leakage/loss of containment
- Explosion/fire
- Loss of propulsion

Appropriate corrective action measures should be proposed to mitigate the risk of hazardous events that do not have adequate risk controls.

The risk analysis of the engine/turbine can be accomplished via the HAZID technique, the HAZOP techniques, or the FMEA technique or a combination of techniques.

---

**Undesired Events**

Harm to 1) human safety, 2) the environment or 3) equipment.

---

**Systems or Subsystems**

**FMEA of Instrumentation and Safety Systems**

Failures of components within the computer-based control system for the re liquefaction unit are to be addressed in the FMEA, including the interfaces with other systems such as I/O signals.

Functional failures of the equipment under control shall also be considered as to ascertain the adequacy of the actions of the safety-related functions in case of these failures.

***

**FMEA of Gas Fueled Engine/Turbine**

The physical boundaries or the **engine/turbine** risk study should include the following systems:

- Dual Fuel Diesel and Single Gas Fuel Engines
- Control and monitoring system for above
- Interfaces with other systems and utilities and emergency systems (e.g., gas line, gas combustion unit, reliquefaction unit, etc.).

**Modes of Operation**

A system normally has multiple modes of operation and each mode can present distinct failure scenarios (failure modes, hazards, consequences). The risk studies must analyze all the modes of operations to identify hazards and consequences of concern. Modes of operations to be analyzed include, but are not limited to, the following:

- Fueling
- Underway (laden and ballasted)
- Stand-by
- Loading/Unloading
- Leaving berth/maneuvering in port/coastal passage/ocean passage
- Normal startup/shutdown
- Emergency shutdown

**Typical Failures**

**FMEA of Instrumentation and Safety Systems**

The lowest level of physical component failure required to be included in the FMEA for control systems is typically at the data acquisition unit level which includes the CPU, its I/O modules, the powering of the device, and any communication between multiple devices.

Physical components whose failures should be analyzed in the FMEA include:

- CPU microprocessor/PLC
- Input/output modules
- Power supplies
- Electrical power cables
- Network hubs
- Buses
- Communication/data link cables
- Interfaces/displays
- Electrical power cables
- Others, as applicable

For functions permitting wireless data communications, consideration is to be given to the possibility of corrupted data and intermittent faults with comparatively long recovery times between interruptions.

Software may reside in several different areas of a given system and at multiple levels (i.e., operating system, PLC embedded logic). Software failures are to be considered at a higher level, almost like a system failure; to address how the system can prevent and recover from, for example, malware.

Classification Rules require the system developer to follow a recognized software quality assurance program, so it is generally assumed that by the time software is delivered and installed, it is error free.

Relays, terminal boards, indicator lights, switches, meters and instruments do not have to be included in the FMEA unless their failure would lead to a hazardous situation not discussed with a higher level component.

***

**FMEA of Gas Fueled Engine/Turbine**

The risk assessment workshop shall identify potential hazardous situations and verify that adequate risk control measures are provided. The list of hazards will be the guide to assist the team in identifying potential loss scenarios. The suggested list of hazards to be considered in the analysis are as follows:

- Gas leakage/loss of containment
- Explosion/fire
- Loss of propulsion

In addition, the risk assessment is to analyze issues regarding integration and interconnections between the Dual Fuel Diesel Engine or Single Fuel Gas Engine, utilities, the re-liquefaction unit, GCU, etc.

---

**Timeline/ Team**

The risk assessment study should be performed early enough in the design stage to facilitate implementation of recommendations that may involve a design change.

**FMEA of Instrumentation and Safety Systems**

The sponsor of the FMEA will be the shipyard in conjunction with the vendor of the re-liquefaction unit and the vendor of the control system (if different).

Subject-matter experts in appropriate disciplines are key to the successful identification of hazards and appropriate development of the hazardous scenarios.

Participants in the risk assessment workshop include subject matter experts from:

- Vendor (fuel gas supply system, dual fuel diesel engine, re-liquefaction unit, gas combustion unit)
- Operations
- Shipyard
- Control system integrator
- Safety/HSE
- Team facilitator and scribe with extensive experience facilitating/recording risk assessment studies

***

**FMEA of Gas Fueled Engine/Turbine**

The sponsor of the engine FMEA is the engine manufacturer. Ideally, the FMEA team would include not only specialists in the engine, but in operations and in systems that the engine may interface with such as re-liquefaction unit and gas combustion unit.

---

**Verification Program**

Not applicable.

**Supporting Documents**

The intent and scope of these requirements are the same as those for Gas Fueled Engines. Refer to 7/1.14 of these Guidance Notes.

**Lifecycle Management**

Risk studies results are used as an aid to demonstrate the safety of the design. If any subsequent modifications are to be carried out, the risk studies are to be updated to demonstrate that any hazards derived from the modifications have been mitigated. These risk studies shall be resubmitted to ABS after a modification.

**Additional Notes**

It is a recommended practice to use a risk matrix to qualitatively assess the consequence and the likelihood of the hazardous situations identified in the risk assessment. This risk ranking will aid in the decision as to what type of corrective actions, if any, is needed. More information on this subject is in 2/2.5 of this document.

Both the FMEA for controls and safety systems and the risk study for the engine/turbine can benefit from explicitly addressing criticality via a risk matrix to allow a more clear and transparent focus on the most critical items.

## 1.14 Gas-Fueled Engines

RULE/GUIDE Rules for Building and Classing Steel Vessels Part 5C, Chapter 13 "Vessels Using Gases or other Low-Flashpoint Fuels"

---

**Rule Reference**

**Part 5C** Specific Vessel Types
**Chapter 13** Vessels Using Gases or other Low-Flashpoint Fuels
**Section 6**, **Appendix 2** Reliquefaction Systems (ABS)
**Subsection 7** Instrumentation and Safety Systems
***
**Section 6, Appendix 3** Gas Combustion Units (ABS)
**Subsection 5** Gas Burner Unit and Burner Management System
***
**Section 9** Fuel Supply to Consumers
**Subsection 4** Regulations on Safety Functions of Gas Supply System
**Subsection 10** Vaporizers, Heaters and Pressure Vessels (ABS)
***
**Section 10** Power Generation Including Propulsion and other Gas Consumers
**Subsection 3** Regulations for Internal Combustion Engines of Piston Type
***
**Section 10, Appendix 1** Dual Fuel Gas Turbine Propulsion System (ABS)
**Subsection 3** Electrical, Automation, Instrumentation and Control Systems
***
**Section 14** Electrical Installations
**Subsection 3** Regulations - General
***
**Section 15** Control, Monitoring and Safety Systems
**Subsection 3** Regulations for Gas Engine Monitoring

---

**Rule Requirements**

**5C-13-6A2/1.5 Plans and Data to be Submitted**

- Failure Modes and Effects Analysis (FMEA) to determine possible failures and their effects in the safe operation of the reliquefaction system [see 5C-13-6A2/7.1ii)]

**5C-13-6A2/7.1 General**

*ii)* An analysis is to be carried out for the reliquefaction system identifying component criticality.

***

**5C-13-6A3/1.3 Plans and Data to be Submitted**

- Failure Modes and Effects Analysis (FMEA) [see 5C-13-6A3/5i)]

**5C-13-6A3/5 Gas Burner Unit and Burner Management System**

*i)* The gas burner management control philosophy for all modes of operation is to be submitted. This should be accompanied by a safety analysis identifying the modes of failures and shutdown and startup sequences of the system.

***

**5C-13-9/4.14 (ABS)**
Where the auxiliary heat exchange circuits are likely to contain gas in abnormal conditions as a result of a component failure (refer to FMEA), they are to be arranged with gas detection in the header tank. Alarm is to be given when the presence of gas is detected. Vent pipes are to be independent and to be led to a non-hazardous area and are to be fitted with a flame screen or flame arrester.

**5C-13-9/10.4 (ABS)**
Where the auxiliary heat exchange circuits are likely to contain gas in abnormal conditions as a result of a component failure (refer to FMEA), they are to be arranged with gas detection in the header tank. Alarm is to be given when the presence of gas is detected. Vent pipes are to be independent and to be led to a non-hazardous area and are to be fitted with a flame screen or flame arrester.

***

**5C-13-10/3.1.4 Interpretation – Auxiliary System Venting (ABS)**
Auxiliary system circuits, such as cooling water or dry/wet sump lubricating oil systems, that are likely to contain gas in normal conditions or abnormal conditions as a result of a component failure (refer to FMEA) are to be arranged in accordance with the following requirements:

*i)* Auxiliary system circuits are to be arranged to avoid cross connection between engine systems and to avoid the migration of gas to non-hazardous areas;

*ii)* Vent pipes are to be independent and to be led to a safe location external to the machinery space and to be fitted with a flame screen or flame arrester.

**5C-13-10/3.1.14 Protection Against Explosion (ABS)**
A Failure Modes and Effects Analysis (FMEA) is to be carried out by the engine manufacturer in order to determine necessary additional safeguards to address the hazards associated with the use of gas as a fuel. This is in addition to the FMEA required by 4-2-1A1/Table 1.

The analysis is to identify all plausible scenarios of gas leakage and the resulting possible explosion. Then the analysis is to identify necessary means to control the identified explosion hazards.

The FMEA is to be submitted to ABS for review.

***

**5C-13-14/3.4**
*Failure modes and effects of single failure for electrical generation and distribution systems in 5C-13-14/2 shall be analysed and documented to be at least equivalent to those acceptable to the Organization.*[(30)]

*(Note 30 Refer to IEC 60812)*

***

**5C-13-15/7.1 Engine Control and Monitoring Systems (ABS)**
*ii)* Unless the FMEA proves otherwise, the monitoring and safety system functions for the engines are to be provided in accordance with 5C-13-15/Table 8 (ABS), as applicable.

---

**Purpose of Risk Study**

Risk studies are required for gas fueled engines ships for the following two cases:

- FMEA on instrumentation and safety systems for fuel gas (FG) supply system, re-liquefaction unit, and gas combustion units (GCU).
- Risk study (HAZID, FMEA, or alike) on the dual fuel diesel and single gas fuel engines, or in the dual fuel gas turbine propulsion systems.

***

**FMEA of Instrumentation and Safety Systems**

The purpose of carrying out an FMEA on the **instrumentation and safety systems** is to demonstrate that any single failure will not lead to an undesirable event such as:

- Lost or degraded function beyond acceptable performance criteria
- Hazardous situation (such as a state that is not fail-safe, complete loss of control, unsafe shutdown of equipment, loss of propulsion, blackout, etc.)

Corrective action measures should be proposed to correct situations of noncompliance with the single-failure design philosophy and mitigate the risk of hazardous events.

***

**FMEA of Gas Fueled Engine/Turbine**

The purpose of the risk study of **the engine or turbine** is to identify the major hazards to people, environment and equipment associated with the engine and verify the adequacy of the risk control measures.

The risk study shall focus on identifying hazardous situations originating from:

- Gas leakage/loss of containment
- Explosion/fire
- Loss of propulsion

Appropriate corrective action measures should be proposed to mitigate the risk of hazardous events that do not have adequate risk controls.

**The risk analysis of the engine/turbine can be accomplished via the HAZID technique, the HAZOP techniques, or the FMEA technique or a combination of techniques.**

---

**Consequences of Concern**

Harm to 1) human safety, 2) the environment or 3) equipment.

---

**Systems or Subsystems**

**FMEA of Instrumentation and Safety Systems**

Failures of components within the computer-based control system for:

1. Fuel gas supply system
2. Re liquefaction unit
3. Gas combustion units/thermal oxidizers

are to be addressed in the FMEA, including the interfaces with other systems such as I/O signals.

Functional failures of the equipment under control shall also be considered as to ascertain the adequacy of the actions of the safety-related functions in case of these failures.

***

**FMEA of Gas Fueled Engine/Turbine**

The physical boundaries or the **engine/turbine** risk study should include the following systems:

- Dual Fuel Diesel and Single Gas Fuel Engines
- Control and monitoring system for above
- Interfaces with other systems and utilities and emergency systems (e.g., gas line, gas combustion unit, reliquefaction unit, etc.).

**Modes of Operation**

A system normally has multiple modes of operation and each mode can present distinct failure scenarios (failure modes, hazards, consequences). The risk studies must analyze all the modes of operations to identify hazards and consequences of concern. Modes of operations to be analyzed include, but are not limited to, the following:

- Fueling
- Underway (laden and ballasted)
- Stand-by
- Loading/Unloading
- Leaving berth/maneuvering in port/coastal passage/ocean passage
- Normal startup/shutdown
- Emergency shutdown

**Typical Failures**

**FMEA of Instrumentation and Safety Systems**

The lowest level of physical component failure required to be included in the FMEA for control systems is typically at the data acquisition unit level which includes the CPU, its I/O modules, the powering of the device, and any communication between multiple devices.

Physical components whose failures should be analyzed in the FMEA include:

- CPU microprocessor/PLC
- Input/output modules
- Power supplies
- Electrical power cables
- Network hubs
- Buses
- Communication/data link cables
- Interfaces/displays
- Electrical power cables
- Others, as applicable

For functions permitting wireless data communications, consideration is to be given to the possibility of corrupted data and intermittent faults with comparatively long recovery times between interruptions.

Software may reside in several different areas of a given system and at multiple levels (i.e., operating system, PLC embedded logic). Software failures are to be considered at a higher level, almost like a system failure; to address how the system can prevent and recover from, for example, malware.

Classification Rules require the system developer to follow a recognized software quality assurance program, so it is generally assumed that by the time software is delivered and installed, it is error free.

Relays, terminal boards, indicator lights, switches, meters and instruments do not have to be included in the FMEA unless their failure would lead to a hazardous situation not discussed with a higher level component.

Functional failures of the equipment under control shall also be considered as to ascertain the adequacy of the actions of the safety-related functions in case of these failures.

***

**FMEA of Gas Fueled Engine/Turbine**

The risk assessment workshop shall identify potential hazardous situations and verify that adequate risk control measures are provided. The list of hazards will be the guide to assist the team in identifying potential loss scenarios. The suggested list of hazards to be considered in the analysis are as follows:

- Gas leakage/loss of containment
- Explosion/fire
- Loss of propulsion

In addition, the risk assessment is to analyze:

- Issues regarding integration and interconnections between the Dual Fuel Diesel Engine or Single Fuel Gas Engine, utilities, the re-liquefaction unit, GCU, etc.

---

**Timeline/ Team**

The risk assessment study should be performed early enough in the design stage to facilitate implementation of recommendations that may involve a design change.

***

**FMEA of Instrumentation and Safety Systems**

The sponsor of the FMEA will be the shipyard in conjunction with the vendor of the particular equipment (Fuel Gas Supply system, re-liquefaction unit, gas combustion units) and the vendor of the control system (if different).

Subject-matter experts in appropriate disciplines are key to the successful identification of hazards and appropriate development of the hazardous scenarios.

Participants in the risk assessment workshop include subject matter experts from:

- Vendor (fuel gas supply system, dual fuel diesel engine, re-liquefaction unit, gas combustion unit)
- Operations
- Shipyard
- Control system integrator
- Safety/HSE
- Team facilitator and scribe with extensive experience facilitating/recording risk assessment studies

***

**FMEA of Gas Fueled Engine/Turbine**

The sponsor of the engine FMEA is the engine manufacturer. Ideally, the FMEA team would include not only specialists in the engine, but in operations and in systems that the engine may interface with such as re-liquefaction unit and gas combustion unit.

---

**Verification Program**

Not applicable.

**Supporting Documents**

The risk assessment report must be submitted to ABS for review. In order to carry out a proper review, the ABS Plan reviewer needs the following information:

- Completed risk assessment report including the following:
  - Description of objective and scope
  - Description of hazard identification technique used
  - List of team members who participated in workshop
  - Description of each action item and responsible party to close the item, as identified by the team during the workshop
  - Completed risk assessment workshop record describing the potential accident scenarios discussed by the team as well as corrective actions.
- Detailed description, narrative and drawings of the system functional description and control
- Layout and general arrangement drawings
- System design specifications
- Cause and effect chart showing the control logic
- Description of the physical and operational scope and boundaries for the risk study
- Operations, maintenance, inspection and testing manuals

The operations, maintenance, inspection, testing and emergency manuals are needed for ABS to confirm compliance with the design and manufacturer's requirements and that the findings of the FMEA have been incorporated into the equipment operating phases.

**Lifecycle Management**

Risk studies results are used as an aid to demonstrate the safety of the design. If any subsequent modifications are to be carried out, the risk studies are to be updated to demonstrate that any hazards derived from the modifications have been mitigated. These risk studies shall be resubmitted to ABS after a modification.

**Additional Notes**

It is a recommended practice to use a risk matrix to qualitatively assess the consequence and the likelihood of the hazardous situations identified in the risk assessment. This risk ranking will aid in the decision as to what type of corrective actions, if any, is needed. More information on this subject is in 2/2.5 of this document.

Both the FMEA for controls and safety systems and the risk study for the engine/turbine can benefit from explicitly addressing criticality via a risk matrix to allow a more clear and transparent focus on the most critical items.

## 1.15 Motion Compensation and Rope Tensioning Systems for Cranes

RULE/GUIDE ABS Guide for Certification of Lifting Appliances, 2015

**Rule Reference**

**Chapter 2** Guide for Certification of Cranes
**Section 12** Motion Compensation Systems for Cranes
and
**Chapter 2** Guide for Certification of Cranes
**Section 13** Rope Tensioning Systems for Cranes

**Rule Requirement**

**2-12/3.1: Motion Compensation Systems for Cranes – General Requirements, Design**

…..

*ii) Motion compensation systems are to be designed so that a single failure in the system does not cause loss of control of the load. Compliance with this requirement is to be verified by means of a risk analysis (See 2-12/3.3 below) or equivalent means.*

**2-13/3.1: Rope Tensioning Systems for Cranes – General Requirements, Design**

…..

*iii) Rope tensioning systems are to be designed so that a single failure in the system does not cause loss of control of the load. Compliance with this requirement is to be verified by means of a risk analysis (See 2-13/3.3 below) or equivalent means.*

**Purpose of FMEA**

Demonstrate that a single failure of the motion compensation systems and rope tensioning systems for cranes will not cause loss of control of load.

**Undesired Events**

Loss of control of load, structural damage or other hazardous situations such as fire and explosion, pollution or injury.

**Systems or Subsystems**

Motion compensation systems and rope tensioning systems for cranes.

**Modes of Operation**

The FMEA is to consider failure during all foreseeable crane modes of operation.

**Typical Failures**

Typical failures that need to be analyzed in the FMEA include, but are not limited to:

- Electric failures
- Hydraulic failures

- Mechanical failures
- Failure of crane power supply from vessel
- Failures of lifting active equipment components
- Failures of passive components such as pipes, cables, block valves, etc.
- Failures of control systems at I/O level (e.g., sensors, power supply, PLC, cables, etc.)
- Failures at interfaces or interconnections between systems
- Failures caused by credible external events
- Others, as applicable

Particular attention should be paid in the FMEA to the interfaces between systems.

**Timeline/ Team**

- The optimal time for performing the FMEA early design is at the vendor stage when there still time to include FMEA recommendations in the final design and integration process
- Ideally, subject matter experts in operations, design and relevant vendors should participate in the FMEA
- The FMEA report shall be submitted to ABS with approval drawings

**Verification Program**

There are no specific Classification requirements for testing to validate the FMEA conclusion. However, it is at the discretion of the ABS Surveyor or ABS Plan reviewer to recommend specific testing of FMEA failures for which there is a higher degree of uncertainty.

**Supporting Documents**

The FMEA must be submitted to ABS for review. In order to carry out a proper review of the FMEA, the ABS Plan reviewer needs the following information included in the FMEA report:

- General description of the scope and purpose of the FMEA
- Dates when the FMEA was conducted
- FMEA participants
- Summary of any risk-reducing actions performed or pending as a result of recommendations of the FMEA.
- System drawings, including layout/general arrangement, schematics.
- Functional block diagram showing systems interactions, parallel paths for redundant systems, in series for single systems.
- Description of the system boundaries, both physical and operational
- System design specifications
- FMEA worksheets, including:
  - Modes of operations
  - All significant failure modes associated with each operational mode
  - Cause associated with each failure mode

- Common cause failures
- Method for detecting that the failure has occurred
- Effect of the failure upon the system
- Global effect of the failure on other systems, the asset and HSE
- Controls to prevent and/or mitigate the failure

The operations, maintenance, inspection, testing and emergency manuals are needed for ABS to confirm compliance with the design and the manufacturer's requirements and that the FMEA findings have been incorporated into the equipment operating phases.

**Lifecycle Management**

If any subsequent modifications to the cranes are carried out, risk studies are to be updated to demonstrate that the system is still in compliance with the ABS design philosophy. Types of changes requiring submittal of the revised FMEA for ABS' review include:

- Operating criteria changes
- System configuration/boundary changes
- Equipment changes
- New application
- Revalidation of previous FMEA from vendor

**Additional Notes**

# APPENDIX 1 Definitions, Acronyms and Abbreviations

## 1 Definitions

*Closed Bus.* Closed bus often describes an operational configuration for a Dynamic Positioning System (DPS) where all or most sections and all or most switchboards are connected together, that is, the bus-tie breakers between switchboards are closed. The alternative to closed bus is open bus, sometimes called split bus or split ring. Closed bus is also called joined bus, tied bus or closed-ring.

*Common Cause Failure.* Failure of multiple components in a system as a result of a single cause.

*Component Failure.* Failure of individual hardware or component items. For purposes of this document, a component is a part that is easily replaceable on location. An FMEA addressing component failures is much more detailed that an FMEA that addresses failures at a functional level.

*Computer-based System.* A system of one or more programmable electronic devices, associated software, peripherals and interfaces. Microprocessors, Programmable Logic Controller (PLC), Distributed Control Systems (DCS), PC or server-based computation systems are examples of computer-based systems.

*Detection Method.* Means by which a failure is detected.

*Enhanced System Notation (EHS).* Enhanced System (**EHS**) notation, as a supplement to the Dynamic Positioning Systems (**DPS**)-series notation, may be assigned to a **DPS-2** or **DPS-3** vessel. The main objective of the enhanced system notation is to improve reliability, operability and maintainability of the DP vessel. The enhanced system notations mainly emphasize the following properties of the DP system:

*i)* Robust design of power plant and thruster system;

*ii)* Enhanced protection systems for generators and thrusters:

*iii)* Failure detection and discrimination of failed components before a full or partial blackout situation occurs

*iv)* Quick automatic blackout recovery;

*v)* Enhanced position reference system and sensor system for increased availability and reliability;

*vi)* Fire and flood protection for higher risk areas.

The notation includes provisions for standby start, closed bus operation and transferable generators. These are beneficial to the overall environment, operational flexibility and system maintainability. Three separate enhanced notations are provided as follows:

- Enhanced Power and Thruster System (**EHS-P**): This notation covers the requirements for the power system and thrusters that are beyond those for the DPS-series notations.
- Enhanced Control System: (**EHS-C**): This notation covers the requirements on the DP control systems including control computers, position reference systems and sensors, which are beyond the minimum requirements for DPS-series notations.
- Fire and Flood Protection System (**EHS-F**): This notation covers the requirements for fire and flood protection considering the risk level of the areas. This is a supplement for a DPS-2 system. It is not necessary for a DPS-3 system since a DPS-3 system has higher requirement in this regard.

*Equipment Under Control.* Equipment that receives commands from the control system.

*Essential Service.* Essential Services are those considered necessary for: 1) Continuous operation to maintain propulsion and steering (primary essential services); 2) Noncontinuous operation to maintain propulsion and steering and a minimum level of safety for the vessel's navigation and systems including safety for dangerous cargoes to be carried (secondary essential services); and 3) Emergency services as described in 4-8-2/5.5 of the *Steel Vessel Rules*.

*Failure Cause.* Defects in design, process, quality or operation which have led to failure or which initiate a process which leads to failure. For example, a circuit breaker contact was manufactured out of specification or a pump was operated in a thermal environment beyond its design capability.

*Failure Mode.* Manner in which a component fails functionally. For example, a pump fails to provide pressure or a circuit breaker fails to open.

*Failure Modes and Effects Analysis (FMEA).* A systematic process to identify potential failures to fulfill the intended function, to identify possible failure causes so the causes can be eliminated, and to locate the failure impacts so the impacts can be reduced.

*Failure Modes, Effects and Criticality Analysis (FMECA).* A variation of the FMEA that includes an explicit estimation of the severity of the consequences of the failure or a combination of the likelihood of the failure and severity of the consequences.

*Fault Tolerance.* Ability of a system to keep functioning to a predetermined level of satisfaction in the presence of faults or failures. Single fault tolerance refers to the ability of system to keep functioning to a predetermined level of satisfaction in presence of a single fault or failure.

*Fault Tolerant System.* A system that is able to keep functioning to a predetermined level of satisfaction in the presence of faults or failures. A fault-tolerant system is designed from the ground up for reliability by building multiple and independent critical components. In the event one component fails, another seamlessly takes over.

*Firmware.* Firmware is the combination of persistent memory and program code and data stored in it. The lowest level of firmware component failure that should be included in the FMEA is each easily replaceable component.

*FMEA Testing.* See "Verification Program".

*FMEA Trials.* See "Verification Program".

*Functional Failure.* Failures pertain to a particular function of the equipment not being performed or performed incorrectly. For example, for a system that needs to pump *x* gpm from point A to point B, typical functional failures would include: failure of pumping capability, pumping at a rate below requirements, pumping at a rate exceeding requirements and pumping backwards. The causes or failure mechanisms for these functional failures would include motor failure; loss of power; degraded pump or motor; under voltage to motor; overvoltage to motor; leaky non-return valve on discharge of pump. In order to perform a functional failure FMEA, the functions of the item under review must be defined. Note that the system/equipment under review may have more than one function.

*Global Effects.* Total effect an identified failure has on the operation, function or status of the installation or vessel and end effects on safety and the environment.

*Global Operations.* Global operations are the overall operations of the facility or vessel.

*Hardware.* In ISQM terms, hardware refers to the control system physical electronic devices hardware or network such as:

*HIL Testing.* Hardware-in-the-loop (HIL) simulation tests control algorithms without using actual systems.

*Integrated Automation.* An Integrated Automation System (IAS) is a combination of computer-based systems with redundant architecture which are interconnected in order to allow communication between computer systems; between computer systems and monitoring, control, and vessel management systems; and to allow centralized access to information and/or command/control. For example, an integrated system may consist of systems capable of performing passage execution (e.g., steering, speed control, traffic surveillance, voyage planning); machinery management and control (e.g., power management, machinery monitoring, fuel oil/lubrication oil transfer); cargo operations (e.g., cargo monitoring, inert gas generation, loading/discharging); etc.

Functions are integrated to reduce the need for hardware and software functions and to reduce interface requirements.

For Integrated Automated Systems, the following design philosophies for Classification must be complied with to avoid hazardous situations:

*i)* All active devices have local/integrated control over detailed functions

*ii)* Control of the device/machine is limited to functions permitted by the local integrated control (limited instruction set). Machine looks after its own internal safeties.

*iii)* All data/indications/alarms are available to the Integrated Automation System

*iv)* Integrated automation system cannot give commands to devices that will override the safeties or produce dangerous outcomes.

If the philosophy is not complied with, the details of the means of controlling the individual devices and associated safeties are to be submitted for consideration.

*Integrated Software Quality Management (ISQM).* ISQM is a risk-based software development and maintenance process built on internationally recognized standards. The ISQM process verifies the software installation on the facility, places emphasis on the verification of the integration of multiple software packages, and monitors for consistency when there are software updates or a change in hardware.

*Local Effects.* Impacts that an identified failure mode has on the operation or function of the item under consideration or adjacent systems.

*Local Operations.* Local operations are the operations of the system that is within the boundaries of the FMEA.

*Operational Modes.* High-level system(s) configurations for a specific set of operations. See "Local Operations" and "Global Operations".

*Owner.* Entity that owns the vessel or offshore facility under study in the FMEA and is responsible for getting Classification approval on it

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

*System Boundary.* Imaginary perimeter encompassing all components within a specified system.

*Validation Program.* See "Verification Program".

*Verification Program.* For the purposes of this document, the terms FMEA tests, FMEA proving trials, FMEA validation and FMEA verification program are equivalent. They refer to trials and testing necessary to prove the conclusions of the FMEA or to establish conclusively the effects of failure modes that the FMEA desktop exercise had a high degree of uncertainty about.

*Worst Case Failure (WCF).* For dynamic positioning systems, the identified single fault in the DPS resulting in maximum effect on DP capability as determined through the FMEA study. This worst case failure is to be used in the consequence analysis.

*Worst Case Failure Design Intent.* Minimum acceptable remaining system functionality after the worst case (most significant system impact) single failure. This is typically only applicable to DP system analysis.

*Worst Case Failure Design Intent (WCFDI).* For dynamic positioning systems, the worst case failure design intent describes the minimum amount of propulsion and control equipment remaining operational following the worst case failure. The worst case failure design intent is used as the basis of design. This usually relates to the number of thrusters and generators that can simultaneously fail.

## 2 Acronyms and Abbreviations

| | |
|---|---|
| ABCU | Automatic Bridge Centralized Control Unmanned |
| ACC | Automatic Centralized Control |
| ACCU | Automatic Centralized Control Unmanned |
| ASOG | Activity Specific Operating Guidelines |
| BOP | Blowout Preventer |
| CDS | Certification of Drilling Systems |
| DFDE | Dual Fuel Diesel Engine |
| DG | Diesel Generator |
| DP | Dynamic Positioning |
| ER | Engine Room |
| ESD | Emergency Shutdown |
| EUC | Equipment under Control |
| FMEA | Failure Modes and Effects Analysis |
| FMECA | Failure Modes, Effects, and Criticality Analysis (normally pronounced “Fuh-Mee-Kah”) |
| FO | Fuel Oil |
| HSE | Health, Safety, and the Environment |
| HVAC | Heating, Ventilation, and Air Conditioning |
| IACS | International Association of Classification Societies |
| IAS | Integrated Automation System |
| IEC | International Electrotechnical Commission |
| IL | Integrity level |
| IMCA | International Marine Contractors Association |
| IMO | International Maritime Organization |
| ISQM | Integrated Software Quality Management Guide |
| MODU | Mobile Offshore Drilling Unit |
| OSV | Offshore Support Vessel |
| P&ID | Process and Instrumentation Diagram |
| PFD | Process Flow Diagram |
| PLC | Programmable Logic Controller |
| PMS | Power Management Systems |
| ROV | Remotely Operated Vehicle |
| SV | System Verification Guide |
| SVR | ABS Steel Vessel Rules |
| WSOG | Well Specific Operating Guidelines |

# APPENDIX 2 Sample FMEA/FMECA Worksheets

## 1 Sample FMEA/FMECA Worksheets

This Appendix provides sample worksheets to illustrate the characteristics of an FMEA or a FMECA requested to demonstrate compliance with Classification. Only one or two representative pages of an FMEA or a FMECA are provided for illustration. **The examples shall by no means be considered a full worksheet for the system nor shall they be construed to be the only suitable approach and format.**

There is not significant variation among the characteristics expected for each of the FMEAs or FMECA required for Classification. However, certain requirements are more defined than others, and this section intends to show those variations.

The sample worksheet shown is for FMEA for the BOP Control System which would satisfy ISQM as well as CDS FMEA/FMECA requirements.

### 1.1 FMECA Worksheet Example (for ISQM and for CDS)

The example shown in Appendix 2, Table 2 illustrates select sections of the FMECA worksheet for the BOP control system on a drilling unit. This FMECA would satisfy both the requirements of the *ISQM Guide* and the *CDS Guide*.

The ISQM FMECA requirements are well defined, as indicated in Appendix 2, Table 1, and include specific suggestions on how to document the FMECAs. Appendix 2, Table 1 below demonstrates the typical BOP control systems, their expected Integrity Levels, and selected typical functions for each. It is recommended that the functions be listed in a separate table and that each function be given a unique identifier. **Note that the determination of Integrity Levels or the criticality is not a requirement of the *CDS Guide*, only of ISQM.**

## TABLE 1
## Example of BOP Control Functional Items

| *BOP Control System* | *Integrity Level* | *Functions* |
|---|---|---|
| Power/Communication Distribution Cabinet Y | IL3 | F1. Well shut-in<br>F2. Subsea communication<br>F3. Closure of Riser Gas Handling Annular<br>F4. Casing emergency disconnect (EDS)<br>F5. Drill pipe emergency disconnect (EDS)<br>F6. Controlled release of riser tension via Riser Recoil system during emergency disconnect t |
| Power/Communication Distribution Cabinet Z | IL3 | Each subsystem has one or more functions that needs to be determined. In this example, functions are illustrated only for the Power/Communication Distribution Cabinet Y above |
| Driller's Control Panel | IL3 | … |
| Bridge Control Panel | IL3 | … |
| Diverter Control Unit | IL3 | … |
| Subsea Electronics Module | IL3 | … |
| Automatic Mode Function | IL3 | … |
| Emergency Disconnect | IL3 | … |
| Riser Message String Interface | IL2 | … |
| Network Interfaces | IL3 | … |
| Event Logger, Remote Logging server, BOP Test system, Acoustic Function | IL1 | N/A. Outside scope of FMEA |

## TABLE 2
## FMECA Worksheet Example (Select Sections of a FMECA for BOP Control System)

| Operational Mode: | | Normal drilling operation | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Unit | | Power / Communication Distribution Cabinet (PCDC) PLC – X | | | | | | | | | | | |
| Description of Unit | | Description of failure | | | Effects of Failure | | Safeguards | | Severity | Likeli-hood | Risk | Corrective Action | Respon-sible |
| Function | ID# | Failure Mode | Failure Causes | Detection of Failure | Local | Global | Prevention of Failure | Mitigation of Effect | L, M or H | L, M or H | L, M or H | | |
| … | … | … | … | … | … | … | … | … | … | … | … | … | … |
| F5: Drill pipe emergency disconnect (EDS) | PDCX5.1 | *Lack of functionality:* EDS does not occur on demand upon a well control event | Sensor failure, code error, communication failure | Visual | None | Potential escalation of well control event. Major safety, environmental and business impacts. | Software review, software test, functional test, preventive maintenance | Shear rams | High | Low | Med | Safeguards considered adequate | |
| F5: Drill pipe emergency disconnect (EDS) | PDCX5.2 | *False action:* EDS initiates spuriously | Sensor failure, code error, communication failure | Visual | Interruption of drilling | Potential for safety, environmental and business impacts. | Software review, software test, functional test, preventive maintenance | Manual override | High | Low | Med | Safeguards considered adequate | |
| F5: Drill pipe emergency disconnect (EDS) | PDCX5.3 | *Improper functionality*: Erroneous EDS sequence | Sensor failure, code error, communication failure | | None | Potential for safety, environmental and business impacts. | Software review, software test, functional test, preventive maintenance | | High | Low | Med | Safeguards considered adequate | |
| F5: Drill pipe emergency disconnect (EDS) | PDCX5.4 | *Timing:* Incorrect timing of valve commands upon ESD demand | Code error, communication failure | Visual indication at event logger | None | Potential safety, environmental and business impacts | Software review, software test, functional test | None | High | Low | Med | Safeguards considered adequate | |
| F5: Drill pipe emergency disconnect (EDS) | PDCX5.5 | *Sequence:* Wrong valving sequence (upon ESD demand) | Code error, communication failure | Visual indication at event logger | None | Potential safety, environmental and business impacts | Software review, software test, functional test | None | High | Low | Med | Safeguards considered adequate | |

## TABLE 2 (continued)
## FMECA Worksheet Example (Select Sections of a FMECA for BOP Control System)

| Operational Mode: | | Normal drilling operation | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Unit | | Power / Communication Distribution Cabinet (PCDC) PLC – X | | | | | | | | | | | |
| Description of Unit | | Description of failure | | | Effects of Failure | | Safeguards | | Severity | Likeli-hood | Risk | Corrective Action | Respon-sible |
| Function | ID# | Failure Mode | Failure Causes | Detection of Failure | Local | Global | Prevention of Failure | Mitigation of Effect | L, M or H | L, M or H | L, M or H | | |
| F5: Drill pipe emergency disconnect (EDS) | PDCX5.6 | *Memory Management:* EDS errors | Memory errors | Visual, audible alarm | Potential for crash of PLC-X | Loss of PLC redundancy | Software review, software test, functional test | Redundant PLC-Z | Low | Med | Low | Safeguards considered adequate | |
| F6: Controlled release of riser tension via Riser Recoil system during EDS | PDCX6.1 | *Lack of functionality:* Controlled release of riser tension did not occur during an emergency disconnect | Code error, interface error, communication error | Visual at event logger and HMI lack of output from PLC | None | Potential safety and business impacts | Software review, software test, functional test, signals | None | High | Low | Med | Safeguards considered adequate | |
| F6: Controlled release of riser tension via Riser Recoil system during EDS | PDCX6.2 | *False Action:* Spurious controlled release of riser tension | Code error, interface error, communication error | Visual at event logger and HMI | None | Potential safety and business impacts | Software review, software test, functional test, signals | None | High | Low | Med | Safeguards considered adequate | |
| … | … | … | … | … | … | … | … | … | … | … | … | … | … |