GUIDANCE NOTES
GD 16-2017

CHINA CLASSIFICATION SOCIETY

GUIDELINES FOR APPLICATION OF FAILURE MODE AND EFFECTS ANALYSIS

2017

Effective from 1 September 2017

Beijing

CONTENTS

CHAPTER 1 GENERAL

1.1 General requirements

1.1.1 The Guidelines contain provisions for the general method of Failure Mode and Effects Analysis (FMEA), specify technical requirements for FMEA in terms of high speed craft, dynamic positioning systems, dual fuel engines and electronically controlled systems of diesel engines and provide examples of FMEA application of dynamic positioning systems, for the purpose of providing guidance for the implementation of FMEA as required by CCS rules and IMO mandatory instruments.

1.1.2 FMEA is a systematic procedure for the analysis of a system to identify the potential failure modes, their causes and effects on system performance (performance of the immediate assembly and the entire system or a process).

1.1.3 FMEA is to be performed early in the development cycle insofar as practicable. FMEA report is to be submitted as part of plans and documents to CCS for approval or information and FMEA testing is to be included in the testing plan of shipyard.

1.2 Purpose and objectives of the analysis

1.2.1 The purpose of undertaking FMEA includes the following:

(1) to identify those failures which have unwanted effects on system operation, e.g. termination of system operation, significant degradation of system operation, affecting the navigational safety of ship or personnel safety etc.;

(2) to allow improvements of the system's reliability or safety (e.g. by design modifications or quality assurance actions);

(3) to allow improvement of the system's maintainability (by highlighting areas of risk or nonconformity for maintainability);

(4) to assist in the selection of alternative design plan with high reliability.

1.2.2 The objectives of an FMEA include the following:

(1) a comprehensive identification and evaluation of all the unwanted effects and the sequence of events brought about by each identified item failure mode, from whatever cause, at various levels of the system's function hierarchy;

(2) the determination of the criticality or priority for addressing/mitigation of each failure mode with respect to the system's correct function or performance and the impact on the process concerned;

(3) identification of measures for eliminating or reducing the risks associated with each failure mode, including design improvement plan and maintenance plan;

(4) identification of trials and testing necessary to prove the conclusions;

(5) information provided to operators and maintainers of the system in order that they understand the capabilities and limitations of the system to achieve best performance.

1.3 Terms and definitions

1.3.1 For the purpose of the Guidelines, the following definitions apply:

(1) *Item*: Any component, device, subsystem, functional unit, equipment or system that can achieve intended purpose and can be individually considered. The process that can achieve intended purpose is also defined as an item, for which a process FMEA can be conducted. In general, people as well as the interaction between people and hardware/software are not considered in the hardware FMEA and human behavior is generally included in the process FMEA.

(2) *Component*: A constituent basic element or item of a system, e.g. a sensor, a processor, an electromagnetic valve etc.

(3) *System*: Set of interrelated or interacting elements. In the FMEA context, a system will have:

.1 defined purposes expressed in terms of required functions;

.2 stated conditions of operation use;

.3 a defined boundary;

.4 a hierarchical system structure.

(4) *Failure*: Termination of the ability of an item or component to perform a required function under stated conditions.

(5) *Failure Cause*: Circumstances during design, manufacture or use which have led to a failure.

(6) *Failure Effect*: Immediate consequences of a failure on operation, function or functionality, or status of some item.

(7) *Failure Mode*: Observed manner of failure of an item.

(8) *Failure Rate*: The number of occurrences of failure per unit time.

(9) *Failure Probability*: The degree of confidence in the occurrence of a failure, measured on a scale from zero to one. An event with a probability of zero means that it is believed to be impossible; an event with the probability of 1 means that it is believed it will certainly occur.

(10) *Failure Severity*: Significance or grading of the failure mode's effect on item operation, on the item surrounding, or on the item operator; failure mode effect severity as related to the defined boundaries of the analysed system.

(11) *Failure Criticality*: Combination of the severity of an effect and the frequency of its occurrence or other attributes of a failure as a measure of the need for addressing and mitigation.

(12) *Hidden Failure*: A failure that cannot be immediately found by operating and maintenance personnel.

(13) *Function*: A Function is what the system or equipment item is designed to do. Each function should be documented as a function statement that contains a verb describing the function, an object on which the function acts, and performance standard(s).

(14) *Design Intent*: A detailed explanation of the ideas, concepts, and criteria that are defined by the designer to be important, which typically includes system requirements, design conditions and system limitations.

(15) *Essential Services*: Equipment and systems necessary for the design intent and safe operation of the engine (e.g. fuel oil supply, cylinder lubrication, waste gate control, etc.).

(16) *Redundancy*: Redundancy is the duplication of critical components or functions of a system with the intention of increasing reliability of the system.

(17) *Reliability*: Reliability is the ability of an item to perform a required function for a stated period of time under stated conditions. Reliability = 1- failure rate.

(18) *Common Cause Failure (CCF)*: Failures of different items, resulting from a single event, where these failures are not consequences of each other.

(19) *System Boundary*: The system boundary forms the physical and functional interface between the system and its environment, including other systems with which the analysed system interacts. The definition of the system boundary for the analysis should correspond to the boundary as defined for design and maintenance. This should apply to a system at any level. Systems and/or components outside the boundaries should explicitly be defined for exclusion.

(20) *Interface*: A point at which independent systems or components interact or communicate.

CHAPTER 2 GENERAL METHOD OF FMEA

2.1 General requirements

2.1.1 Traditionally there have been wide variations in the manner in which FMEA is conducted and presented. The analysis is usually done by identifying the failure modes, their respective causes and immediate and final effects. The analytical results can be presented on a worksheet that contains a core of essential information for entire system and details developed for that specific system. It shows the ways the system could potentially fail, the components and their failure modes that would be the cause of system failure, and the cause(s) of occurrence of each individual failure mode.

2.1.2 The FMEA procedure consists of the following four main stages as shown in Figure 2.1.2:

(1) preparation of FMEA: establishment of the basic ground rules for the FMEA, planning and scheduling and preparation of data and relevant information required for the analysis to ensure that the time and expertise is available to do the analysis;

(2) executing the FMEA using the appropriate worksheet or other means such as logic diagrams or fault trees;

(3) summarizing and reporting of the analysis to include any conclusions and recommendations made;

(4) updating FMEA further based on design change as necessary, in accordance with the development of design work and relevant testing conditions.

2.1.3 In case any change to the system design during the life cycle of ship, it is to be analysed in line with the original FMEA and recorded as annexes to the FMEA.

2.2 Development of analysis plan

2.2.1 FMEA activities, follow up activities, procedures, relationship with other reliability activities, processes for management of corrective actions and for their closure, and milestones are to be integrated into the overall program plan.

2.2.2 The FMEA analysis method and standard to be used are to be determined, which may be described briefly.

2.2.3 This plan is to contain the following points:

(1) clear definition of the specific purposes of the analysis and expected results;

(2) determination of the scope of FMEA by carrying out discussion with the client/shipowner;

(3) description of how the present analysis supports the overall project dependability;

(4) establishment of an analysis team including design experts;

(5) key project schedule milestones clearly marked to ensure the analysis is executed in a timely manner;

(6) manner of closure of all actions identified in the process of mitigation of identified failure modes that need to be addressed.

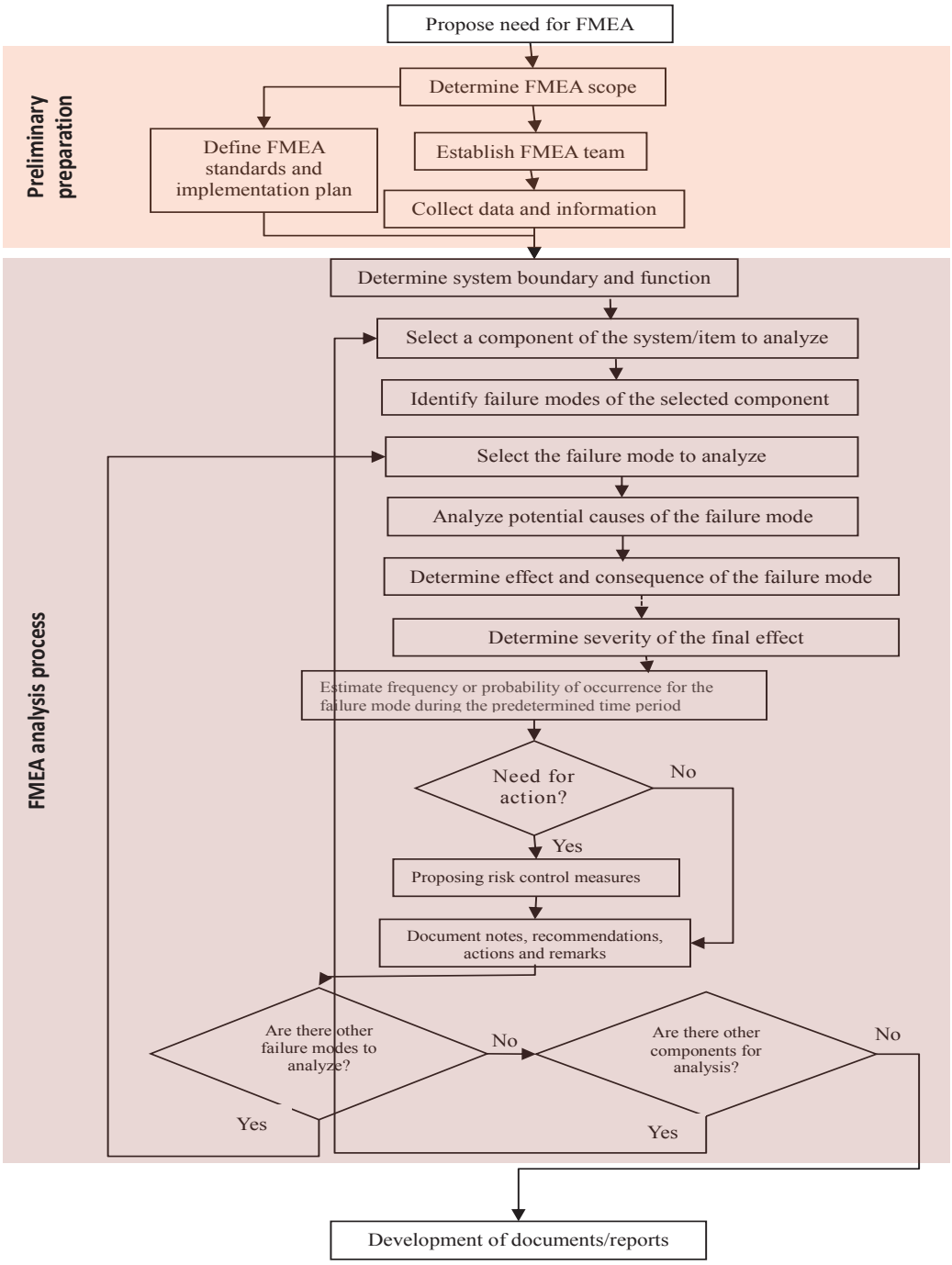


Figure 2.1.2 Analysis Flowchart

2.2.4 The plan is to reflect the consensus of all participants and is to be approved by project management.

2.3 Preparation of data and relevant information

2.3.1 FMEA needs data and information about the elements of the system in sufficient detail for meaningful analysis of the ways in which each element can fail.

2.3.2 Data and information may include:

(1) drawings or a flow chart of the system being analysed and its components, or the steps of a process;

(2) an understanding of the function of each step of a process or component of a system;

(3) details of environmental and other parameters, which may affect operation;

(4) an understanding of the results of particular failures;

(5) historical information on failures including failure rate data where available.

2.4 FMEA process

2.4.1 Define the system boundary (including physical boundary and operational boundary) and system function, divide the system into elements or steps and draw functional diagrams.

2.4.2 For listed elements or steps, confirm the following:

(1) judgement criteria of defining the failure;

(2) analysis of the failure mode, i.e. the way in which the failure manifests itself: how does each part have obvious failures?

Example of a set of general failure modes Table 2.4.2

No.	Failure mode
1	Failure during operation
2	Failure to operate at a prescribed time
3	Failure to cease operation at a prescribed time
4	Premature operation

Note: This listing is an example only. Different lists would be required for different types of systems.

(3) analysis of failure causes: what is the specific mechanism giving rise to these failure modes?

(4) analysis of failure effects: consequences caused by failure, including the local effects on the element itself, effects at the system level and effects at the global level (ship).

(5) identification of failure detection methods: how is the failure detected?

2.4.3 Once the failure mode and mechanism are determined, possible preventative and improvement measures may be proposed, including:

(1) redundant items that allow continued operation if one or more elements fail;

(2) alternative means of operation;

(3) monitoring or alarm devices;

(4) any other means of permitting effective operation or limiting damage.

2.4.4 A top down method is generally used in the system FMEA. A top down FMEA starts from the overall system level and progresses to the next level down, or subsystem level, and on down to the equipment item and component level. However, if it can be justifiably shown that at a certain level between overall system level and component level that there is no further effect on the overall system if a failure occurs, then it is not necessary to continue to the next level down.

2.5 Criticality analysis

2.5.1 When needed, FMEA may be further expanded to carry out the criticality analysis when it is allowed by the analysis cost, time and resources. The purpose is to quantify the relative magnitude of each failure effect as an aid to decision making, so that with a combination of and severity and probability of failure modes, priority for action to mitigate or minimize effect of certain failures may be set. This criticality analysis is usually qualitative or semi-quantitative. The most common method is risk level.

2.5.2 The risk level of failure mode is obtained by the combination of failure severity and failure probability. Such method is applicable to different consequences of different failure modes and can be applied to equipment, system or process.

$$\text{Risk} = \text{Probability of failure} \times \text{Severity}$$

$$\log(\text{risk}) = \log(\text{probability}) + \log(\text{consequence})$$

$$\text{Risk index（RI）} = \text{Probability index（PI）} + \text{Severity Index（SI）}$$

The criticality can be represented by a risk matrix as shown in Figure 2.5.2. The probability of occurrence of failure and degree of severity are divided into several levels. The probability and degree of severity are placed in a matrix, i.e. risk matrix. A risk matrix may be divided into three areas: high risk area, low risk area and critical area between those two areas. It is to be noted that although criticality is not uniformly defined, it is to be defined by the analysis personnel, subject to approval by project or procedure management.

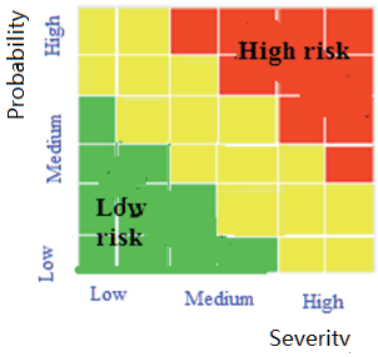


Figure 2.5.2 Risk Matrix

2.5.3 The following examples demonstrate the definition and level division of probability of occurrence, severity and risk of failure modes. Tables 2.5.3.1 to 2.5.3.3 are only examples. For specific application, different level divisions can be used to represent the criticality of failure modes.

Example of Division of Probability Level Table 2.5.3.1

PI	Probability	Definition
5	10^{-1}	Likely to occur frequently
4	10^{-2}	Probable – may occur several times in the life of an item
3	10^{-3}	Occasional – may occur sometime in the life of an item
2	10^{-4}	Remote – unlikely to occur but possible
1	10^{-5}	Improbable – unlikely to occur at all

Example of Division of Severity Level Table 2.5.3.2

SI	Severity	Definition
4	Catastrophic	Failure causes complete system loss with a high potential for fatal injury and major pollution
3	Major	Major damage to system with a potential for serious injury to personnel and minor pollution
2	Critical	Failure will probably occur without major damage to system, pollution or serious injury
1	Minor	Functional failure of part of a machine or process with no potential for injury, damage or pollution

Example of Division of Failure Risk Level Table 2.5.3.3

	PI	1	2	3	4	5
SI		Improbable	Remote	Occasional	Probable	Frequent
4	Catastrophic	5	6	7	8	9
3	Major	4	5	6	7	8
2	Critical	3	4	5	6	7
1	Minor	2	3	4	5	6

2.5.4 Rating of failure detection probability: for some FMEA application, the likelihood that a failure will be detected has to be estimated; that is, the probability that the design features/aids or verification procedures will detect potential failure modes in time to prevent a system-level failure. For a process application, this refers to the probability that a set of process controls currently in place will be in a position to detect and isolate a failure before it gets transferred to the subsequent processes or to the ultimate product output.

2.5.5 Assessment of risk acceptance criteria: after obtaining the risk matrix formed by risk index of various failure modes, the risk acceptance criteria needs to be defined, i.e. under which risk index the failure mode is acceptable, tolerable or unacceptable. The risk acceptance criteria may be qualitatively defined and is driven by professional and financial decisions and varies in different industry types. Generally the following need to be considered:

(1) relevant requirements of rules of classification societies and regulations;

(2) system operation criteria provided by the system or equipment manufacturer;

(3) for engines, reference may be made to Appendix 3 “Design” of IACS UR M44. E.g. single propulsion engine installation is to have stricter acceptance criteria than multi-engine installation, e.g. higher redundancy and fault tolerant requirement and design, which means the system can maintain safe operation under a number of and certain type of failure modes.

2.6 FMEA tests

2.6.1 Some assumptions made during FMEA and conclusions drawn by analysis are to be verified and confirmed by relevant tests, in order to demonstrate that the identified risk and its consequence have been eliminated or effectively controlled, or that measures taken to control the impact of risk are effective.

2.6.2 Tests are part of the FMEA process and are not to be treated in isolation. The FMEA will use the results of the tests in the final analysis and usually include the test sheets in the report.

2.6.3 The design of FMEA tests is to reflect the performance of the whole system in failure mode, and at the same time tests are to be through and complete so that any unacceptable failure mode is uncovered during trials insofar as practicable.

2.6.4 The FMEA test programmes are to describe the purpose of the test, the vessel and equipment setup for the test, how the equipment failure is to be induced or simulated, and the possible effects of the failure.

2.7 Preparation of FMEA report

2.7.1 Through FMEA, the identified failure modes and their causes and possible effects are listed, and recommendations for further analysis are listed.

FMEA Worksheet **Table 2.7.1**

Time: _____					Page:_____ of _____							
Ship: _____					System:_____							
References:_____					Team members_____							
No.	Equipment	Function	Failure modes	Failure causes	Failure effects		Criticality analysis (if applicable)			Failure detection methods	Recommended action	Remark/ test
					Local	Failure severity Global	Failure probability	Failure risk				

2.7.2 The FMEA report may be included in a very large research project or may be self-contained. In any case, the report contents are to include detailed analysis records and summaries, as well as functional diagram and block diagram defining system structure. The contents of the report are to include:

(1) Executive Summary

(2) Introduction

.1 FMEA Introduction;

.2 Scope of Work;

.3 FMEA Procedure or Methodology;

.4 Vessel Application and Particulars;

.5 Any Assumptions Made in the Analysis, e.g. the operational mode the vessel is in when the analysis is carried out;

.6 Documentation.

(3) Method of analysis:

.1 Block diagrams;

.2 FMEA Worksheet;

.3 If criticality analysis is carried out, criticality (risk index) and the method to define criticality;

.4 FMEA improvement work report.

(4) Description of Systems, for example:

.1 DP Control System;

.2 Electrical Systems;

.3 Machinery Systems;

.4 Safety Systems.

Each section is to include details of any significant failure modes identified together with the FMEA recommendations put forward.

(5) Recommendations, recommendations on further analysis, any design alteration or any feature planned to be included in the testing plan, and actions.

(6) Conclusions.

(7) Appendices, e.g.:

.1 Worksheets;

.2 Trials Test Sheets;

.3 Question and Answer ("Q&A") Punchlist;

.4 FMEA Report Sheets;

.5 List of Shipyards and Equipment Suppliers.

2.8 Updating of FMEA

2.8.1 FMEA is a process of repetitive updating with the development of design. Due to design change, relevant parts of FMEA are required to be reviewed and updated. As a result, upon completion of the above analysis, the system needs to be assessed by another round of FMEA if appropriate.

2.9 Output results

2.9.1 The primary output of FMEA is a list of failure modes, the failure mechanisms and effects for each component or step of a system or process (which may include information on the likelihood of failure). Information is also given on the causes of failure and the consequences to the system as a whole.

2.9.2 The output from criticality analysis includes a rating of importance based on the likelihood that the system will fail, the level of risk resulting from the failure mode or a combination of the level of risk and the 'detectability' of the failure mode. Criticality analysis can give a quantitative output if suitable failure rate data and quantitative consequences are used.

2.10 Application of FMEA in risk assessment

2.10.1 Based on different assessment objects, FMEA can be used in the following application:

(1) design (or product) FMEA which is used for components and products;

(2) system FMEA which is used for systems;

(3) process FMEA which is used for manufacturing and assembly processes;

(4) service FMEA;

(5) software FMEA.

2.10.2 FMEA can be used alone. As a systematic inductive method of analysis, FMEA is most often used to complement other approaches, especially deductive ones, such as FTA.

2.10.3 Risk assessment is the overall process of risk identification, risk analysis and risk evaluation. As a tool and technique of risk assessment, FMEA is very applicable to risk identification of risk assessment.

2.10.4 The main consideration in selecting the method of analysis is to depend on the particular requirements of the project, not only with regard to technical requirements but also timescale, cost, efficiency and usage of the results. General guidelines are as follows:

(1) FMEA is appropriate when comprehensive knowledge of the failure characteristics of an item is required.

(2) FMEA is more appropriate for smaller systems, modules or assemblies.

(3) FMEA is an essential tool at the research and development or design stage when unacceptable effects of failures need to be identified and solutions found.

(4) FMEA can be necessary for items that are of innovatory design and their failure characteristics cannot be known from previous operational experience.

(5) FMEA is usually more applicable to systems having large numbers of components to be considered that are related by predominantly series failure logic.

(6) FTA is generally more suitable for the analysis of multiple failure modes and dependency involving complex failure logic and redundancy. FTA can be used at the higher levels in the system structure early in the design stage and can help in identifying the need for detailed FMEA at lower levels during detailed design.

CHAPTER 3 FMEA APPLICATION OF HIGH-SPEED CRAFT

3.1 General requirements

3.1.1 FMEA is to be conducted for each high-speed craft, before its entry into service, in respect of directional control systems, mechanical systems and their control devices, electrical systems and stabilisation systems

3.1.2 For craft of the same design and having the same equipment, one FMEA on the lead craft will be sufficient, but each of the craft is to be subject to the same FMEA conclusion trials.

3.1.3 FMEA for high-speed craft is based on a single-failure concept under which each system at various levels of a system's functional hierarchy is assumed to fail by one probable cause at a time. The effects of the postulated failure are analysed and classified according to their severity. Such effects may include secondary failures (or multiple failures) at other level(s). Any failure mode which may cause a catastrophic effect to the craft is to be guarded against by system or equipment redundancy unless the probability of such failure is extremely improbable. For failure modes causing hazardous effects, corrective measures may be accepted in lieu. A test programme is to be drawn to confirm the conclusions of FMEA.

3.1.4 FMEA procedures, basic methods and requirements for high-speed craft are to be in accordance with Chapter 2 of the Guidelines and Appendix 4 of the International Code of Safety for High-Speed Craft (2000).

3.1.5 With regard to FMEA systems (devices) of high-speed craft specified in this Chapter, it does not mean independent analysis has to be carried out in accordance with specified systems (devices). FMEA systems may be determined in accordance with the practical conditions of the craft, especially in case of different functions achieved by the same system (device), e.g. directional control and propulsion are the same system.

3.2 System failure mode and effects analysis

3.2.1 Before proceeding with a detailed FMEA into the effects of the failure of the system elements on the system functional output it is necessary to perform a functional failure analysis of the craft's important systems. In this way only systems which fail the functional failure analysis need to be investigated by a more detailed FMEA.

3.2.2 When conducting a system FMEA the following typical operational modes within the normal design environmental conditions of the craft are to be considered:

(1) normal seagoing conditions at full speed;

(2) maximum permitted operating speed in congested waters; and

(3) manoeuvring alongside.

3.2.3 The functional interdependence of these systems is to also be described in either block diagrams or in a narrative format to enable the failure effects to be understood. As far as applicable, each of the systems to be analysed is assumed to fail in the following failure modes:

(1) complete loss of function;

(2) rapid change to maximum or minimum output;

(3) uncontrolled or varying output;

(4) premature operation;

(5) failure to operate at a prescribed time; and

(6) failure to cease operation at a prescribed time.

Depending on the system under consideration, other failure modes may have to be taken into account.

3.2.4 If a system can fail without any hazardous or catastrophic effect, there is no need to conduct a detailed FMEA into the system architecture. For systems whose individual failure can cause hazardous or catastrophic effects and where a redundant system is not provided, a detailed FMEA is to be followed. Results of the system functional failure analysis are to be documented and confirmed by a practical test programme drawn up from the analysis.

3.2.5 Where a system, the failure of which may cause a hazardous or catastrophic effect, is provided with a redundant system, a detailed FMEA may not be required provided that:

3.2.5.1 the redundant system can be put into operation or can take over the failed system within the time-limit dictated by the most onerous operational mode in 3.2.2 without hazarding the craft;

3.2.5.2 the redundant system is completely independent from the system and does not share any common system element the failure of which would cause failure of both the system and the redundant system. Common system element may be acceptable if the probability of failure complies with specified probability criteria (see section 13, Appendix 4 of HSC 2000); and

3.2.5.3 the redundant system may share the same power source as the system. In such case, an alternative power source is to be readily available with regard to the requirement of 3.2.5.1.

3.2.5.4 The probability and effects of operator error to bring in the redundant system are also to be considered.

3.3 Equipment failure mode and effects analysis

3.3.1 The systems to be subject to a more detailed FMEA investigation at this stage are to include all those that have failed the system FMEA and may include those that have a very important influence on the safety of the craft and its occupants and which require an investigation at a deeper level than that undertaken in the system functional failure analysis. These systems are often those which have been specifically designed or adapted for the craft, such as the craft's electrical and hydraulic systems.

3.4 FMEA requirements for systems (devices)

3.4.1 Directional control systems

3.4.1.1 A directional control system includes any steering device or devices, any mechanical linkages and all power or manual devices, controls and actuating systems.

3.4.1.2 FMEA is to be completed for the directional control system in accordance with the provisions of 3.2 and 3.3, taking into account typical operational modes within the normal design environmental conditions of the craft as specified in 3.2.2.

3.4.1.3 The FMEA results (as verified by test) of the directional control system are to satisfy the requirement that "the probability of total failure of all directional control systems shall be extremely remote when the craft is operating normally, i.e., excluding emergency situations such as grounding, collision or a major fire".

3.4.1.4 The construction of the directional control systems is to be analyzed by FMEA so that a single failure in one drive or system, as appropriate, will not render any other one inoperable or unable to bring the craft to a safe situation. The Administration may allow a short period of time to permit the connection of a secondary control device when the design of the craft is such that such delay will not, in their opinion, hazard the craft.

3.4.1.5 Directional control devices involving variable geometry of the craft or its lift system components are to be verified by FMEA so that that any failure of the drive linkage or actuating system will not significantly hazard the craft.

3.4.2 Machinery systems and their associated controls

3.4.2.1 FMEA is to be completed for machinery systems and their associated controls in accordance with the provisions of 3.2 and 3.3.

3.4.2.2 Special consideration is to be given by FMEA to the reliability of single essential propulsion components. For a separate source of propulsion power, the redundancy is to be analyzed by FMEA.

3.4.2.3 FMEA is to be conducted for the essential auxiliaries (systems) of craft in order to demonstrate that the normal operation of propulsion machinery can be sustained or restored even though one of the essential auxiliaries becomes inoperative. Special consideration is to be given to the malfunctioning of:

(1) a generating set which serves as a main source of electrical power;

(2) the fuel oil supply systems for engines;

(3) the sources of lubricating oil pressure;

(4) the sources of water pressure;

(5) an air compressor and receiver for starting or control purposes; and

(6) the hydraulic, pneumatic or electrical means for control in main propulsion machinery, including controllable-pitch propellers.

3.4.3 Electrical systems

3.4.3.1 FMEA is to be completed for electrical systems in accordance with the provisions of 3.2 and 3.3.

3.4.3.2 In cases where faults can occur without being detected during routine checks on the installations, FMEA is to take into account the possibility of faults occurring simultaneously or consecutively.

3.4.3.3 FMEA of the electrical system is to verify that the electrical system is designed and installed so that the probability of the craft being at risk of failure of a service is extremely remote.

3.4.3.4 Where the failure of power supply would cause serious risk to the craft, corrective actions are to be provided, e.g. starting the standby power supply within a specified time, in order to eliminate or mitigate the consequence of failure.

3.4.3.5 Where loss of particular essential service would cause serious risk to the craft, the service is to be fed by at least two independent circuits to eliminate or mitigate the consequence of failure.

3.4.4 Stabilization system

3.4.4.1 Stabilization control system is a system intended to stabilize the main parameters of the craft's attitude: heel, trim, course and height and control the craft's motions: roll, pitch, yaw and heave, mainly including devices, power drives actuating stabilization devices and stabilization equipment for accumulating and processing data for making decisions and giving commands.

3.4.4.2 For an automatic control system or a combined system incorporating elements of both automatic and manually assisted control systems, FMEA is to be completed in accordance with the provisions of 3.2 and 3.3, taking into account typical operational modes within the normal design environmental conditions of the craft as specified in 3.2.2.

3.4.4.3 The FMEA results (including limiting measures and as verified by test) of the stabilization system are to satisfy the requirement that "in case of failure of any automatic equipment or stabilization device, or of its power drive, the parameters of craft motion shall remain within safe limits".

3.4.4.4 For lateral and height control systems, consideration is also to be given to the safety levels as given in section 2.4 of annex 3 of HSC 2000 and of the safe values of motions appropriate to the particular craft and service.

3.5 FMEA report and example

3.5.1 The FMEA report is to be a self-contained document with a full description of the craft, its systems and their functions and the proposed operation and environmental conditions for the failure modes, causes and effects to be understood without any need to refer to other plans and documents not in the report. The analysis assumptions and system block diagrams are to be included, where appropriate. The report is to contain a summary of conclusions and recommendations for each of the systems analysed in the system failure analysis and the equipment failure analysis. It is also to list all probable failures and their probability of failure, where applicable, the corrective actions or operational restrictions for each system in each of the operational modes under analysis. The report is to contain the test programme, reference any other test reports and the FMEA trials.

3.5.2 Based on the requirements of 3.5.1, the report is to contain the following contents:

(1) plans and documents, including particulars of the craft and descriptions of the following systems and functional requirements: general description of system operation and structure, functional relationship between system components, acceptable functional limitation and system constraints of systems and components in each typical operation mode;

(2) analysis assumptions and system block diagram, analysis explanation and conclusion summary;

(3) if needed, a list of all possible failures and their probability, corrective actions or operational limitations for each system in each operation mode under analysis;

(4) testing procedures, all the other testing reports and FMEA tests used as references;

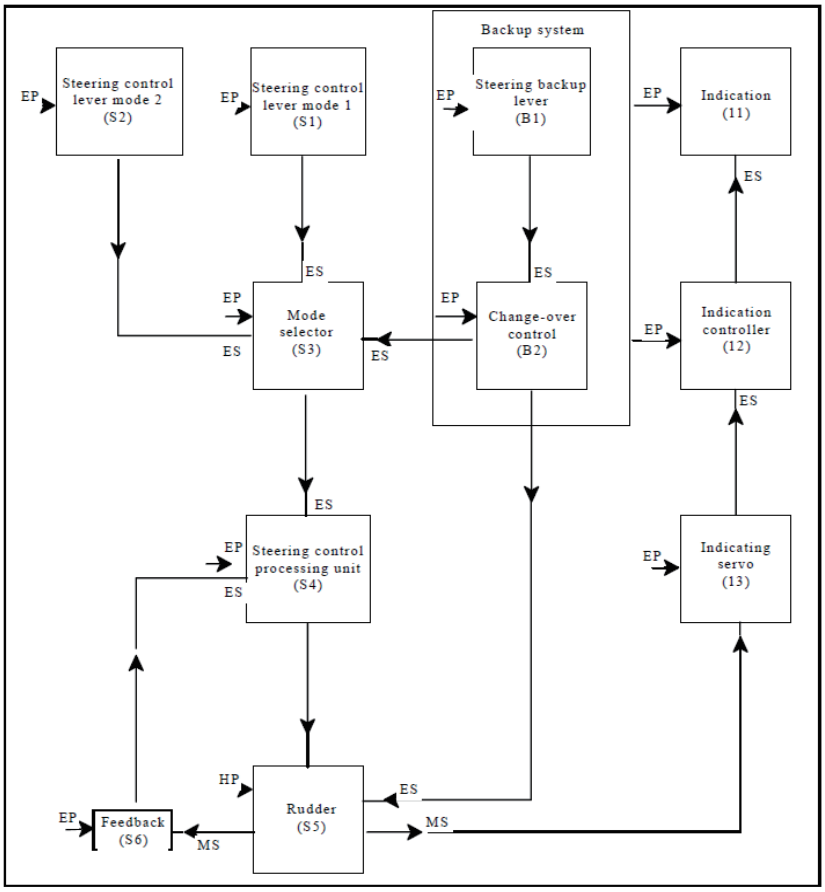
(5) worksheet.

3.5.3 Report example

3.5.3.1 System block diagram

Steering controls system Date:_____

Analyst:_____



where:EP - electric power
HP - hydraulic power
ES - electric signal
MS - mechanical signal

3.5.3.2 FMEA worksheet

FMEA worksheet **Table 3.5.3.2**

Name of system: _____ References: _____

Mode of operation: _____ System block diagrams: _____

Sheet No: _____ Date: _____

Name of analyst: _____ Drawings: _____

Equipment Failure effect name or number	Function	Ident. No.	Failure mode	Failure cause	Failure effect		Failure detection	Corrective action	Severity of failure effect	Probability of failure (if applicable	Remarks
					Local effect	End effect					

CHAPTER 4 FMEA APPLICATION OF DYNAMIC POSITIONING SYSTEM

4.1 General Requirements

4.1.1 For vessels applying for the class notations of DP-2 and DP-3, FMEA is to be carried out for the whole dynamic positioning system. The purpose of FMEA is to give a description of the different failure modes of the equipment related to functions of the DP system. Special attention is to be paid to the analysis of systems of which a certain piece of equipment may have a number of failure modes and thus induce a number of different effects on the dynamic positioning system.

4.1.2 The FMEA procedures, basic methods, requirements and criteria of dynamic positioning system may refer to the provisions of Chapter 2 of the Guidelines and IMO MSC/Circ.645.

4.2 FMEA Report of Dynamic Positioning System

4.2.1 The FMEA of dynamic positioning system onboard is to provide the ship's particulars, (including main parameters, designer, shipyard, shipowner, name of ship and identification, type of ship, main purpose, characters of classification, main equipment supplier, FMEA supplier and other related information) and acceptance criteria.

4.2.2 The FMEA of dynamic positioning system is to involve all DP working conditions onboard the ship (such as pipe-laying, drilling, ROV, etc.), and describe the whole technical status under each working condition of the ship.

4.2.3 FMEA is to cover all systems and main components thereto as detailed as possible, generally including, but not limited to the following items:

(1) All thruster system (thruster control system, thruster hydraulic system, thruster cooling system, control mode selection, power supplies to control and auxiliary pumps);

(2) Power system (high voltage systems, low voltage distributions, emergency power, battery and UPS systems and distributions);

(3) Machinery system (diesel engines/diesel generator sets, fuel oil system, lubrication oil system, seawater/freshwater cooling system, compressed air system, engine room ventilation);

(4) DP control system (DP control computer system, joystick system, ship and position reference system, mode selection, DP UPS power system, sensor system);

(5) Integrated automation system, power management system, generator voltage control system, diesel engine governor control;

(6) Emergency stop/shutdowns;

(7) Fire and flooding separation arrangements (DP-3);

(8) Other relevant systems (fire-fighting system, ventilation system, ESD system, cooling system in computer rooms, etc.);

(9) Conclusions/findings/recommendations (if applicable);

(10) Test program.

4.2.4 The FMEA report is to be prepared to include description of all main components of the system and functional block diagram showing interactions between them, redundant group, all major failure modes, the main cause that can be anticipated of each failure mode, the transient effect of each failure on the vessel's position, the method of detecting failures, the effects of failures on the ability of the system and the analysis to probable common failure mode.

4.3 Redundancy and Other Requirements for Dynamic Positioning System

4.3.1 Redundancy requirements

4.3.1.1 "Redundancy" means ability of a component or system to maintain or restore its function, when a single failure has occurred. Redundancy can be achieved for instance by installation of multiple components, systems or alternative means of performing a function. The redundant component or system is to be immediately available and the transfer to redundant component or system is to be automatic as far as practicable, and operator intervention is to be kept to a minimum①.

The transfer is to be smooth and within acceptable limitations of the operation.

4.3.1.2 Redundancy of components for dynamic positioning system will normally be necessary as followings:

(1) For DP-2 class notation, redundancy of all active components (such as generators, thrusters, switchboards, communication networks, remote valves, etc.);

(2) For DP-3 class notation, redundancy of all components, including cabling and piping, and A-60 physical separation out of the components. Physical separation with two A-0 class divisions may be acceptable in low fire risk space.

4.3.1.3 All independence of technical functions is to be taken into account. When it is considered unnecessary for certain components of the system to be redundant or redundancy cannot be achieved, their reliability or mechanical maintenance are to be further taken into consideration. If these components have sufficiently high reliability or low fault effect, the corresponding arrangement may be acceptable.

4.3.1.4 Three situations for redundant components or systems to be organized to perform the same function are as followings:

(1) All the redundant components or systems are completely independent;

(2) All the redundant components or systems are cross connected with intersecting components or subsystems;

① If a single failure does not impact the ship's capabilities to maintain its position or heading immediately, proper human intervention is to be taken to avoid the loss of position, and such intervention may be acceptable subject to FMEA analysis and test verification.

(3) All the redundant components or systems are connected by a common component or system.

4.3.1.5 The following four failure modes for redundant system are not to be accepted:

(1) A certain common cause failure will affect all redundant components/systems and common components/systems;

(2) When the redundant components/systems intended to realize the same function are cross connected, the intersecting component or subsystem failures will affect all redundant components/systems;

(3) When the redundant components/systems intended to realize the same function are connected by a common component or system, the common component or system failures will affect all redundant components/systems;

(4) When the redundant components/systems intended to realize the same function are connected by a common component or system, a failure in one of the redundant components or systems will propagate to other redundant components or systems (e.g. short circuit).

Where these above-mentioned failures cannot be avoided, compensating measures are to be taken, e.g. failure detection, protective functions, stand-by start, re-start, change-over, etc. The FMEA is to describe and analyze these compensating measures.

4.3.1.6 Each redundant group is to be described by figures, tables, block diagrams and texts in FMEA report, in which it is to define whether the redundant components or systems intended to realize the same function are completely independent, cross connected, connected by common component or system, and illustrate the changeover time between components/systems (including switching time and recovery time, etc.) in case of a single failure in redundant components/systems, and possible effects that may be caused.

4.3.2 Other requirements

4.3.2.1 Systems which are not directly part of the DP system, but may lead to DP system fault in the event of failure, such as common fire-fighting system, ventilation system for engines, shutdown system, etc., are also to be subject to FMEA.

4.3.2.2 Where the component or system has hidden failures, and the operator is not reminded by the system, further significant failure may be caused to affect the ship's positioning functions, leading to inability of automatically maintaining the ship's position and heading within the specified operation range under specified environmental conditions, which is to be considered as a single failure. Therefore, monitoring and alarming (such as audible and visual alarm equipment, automatic sensor device, etc.) are to be taken for such hidden failures, or other measures are to be taken to mitigate or prevent the effects brought by these hidden failures, and indicated in FMEA report.

4.3.2.3 Effects caused by operator's inadvertent negligence, if reasonable and most likely to occur, are to be taken into account in FMEA.

4.4 Ship's Systems in FMEA Report and Examples①

① Examples provided in 4.4 are only for reference, not the requirements for FMEA. Detailed analysis is to be made for each specific case.

4.4.1 Thruster system

4.4.1.1 Thruster system includes control system, hydraulic system and cooling system for thruster, control mode selection device, power supply of control and auxiliary pumps, etc. The allocation and redundancy of these systems are to be described in FMEA report and relevant analysis is to be carried out.

4.4.1.2 A certain vessel provided with four thrusters is shown in the following figure and table.

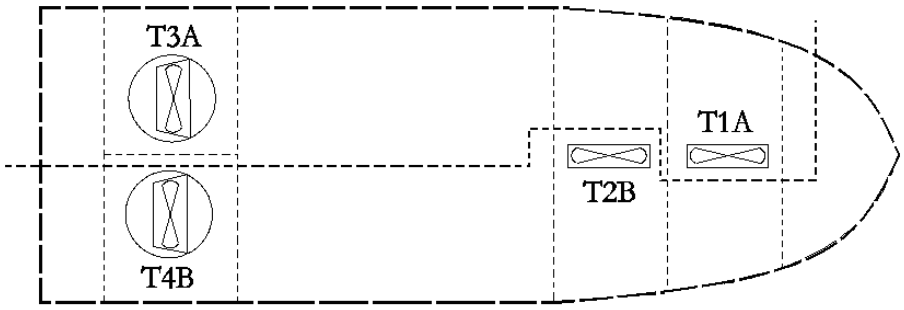


Figure 4.4.1.2 A Certain Vessel Provided with Four sets of Propulsion Units

Redundant Group Design for Propulsion Unit Table 4.4.1.2

Condition	Maintaining ship's position and heading	Redundancy type/description
Normal DP working condition	Group A (T1A and T3A) and Group B (T2B and T4B)	Active redundancy, no drift off, and no drive off caused by any thruster[1]
After single failure	Group A (T1A and T3A) and Group B (T2B and T4B)	

4.4.1.3 A certain vessel provided with five thrusters is shown in the following figure and table:

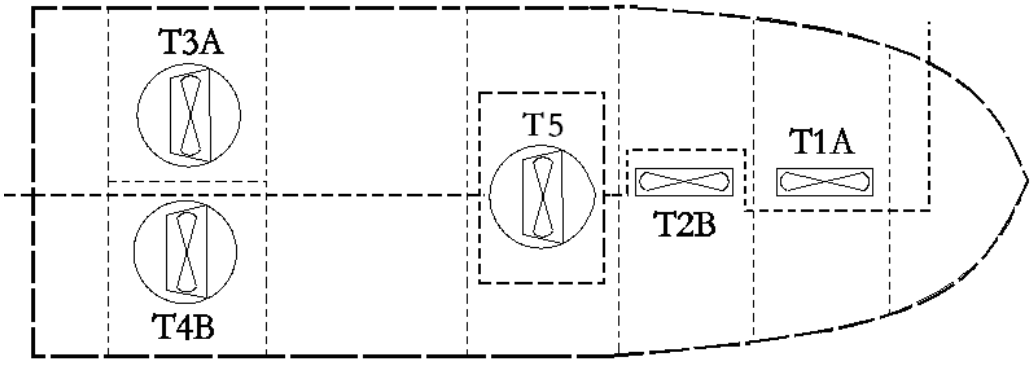


Figure 4.4.1.3 A Certain Vessel Provided with Five Sets of Propulsion Units

① Drift off means that the vessel cannot maintain its position and heading due to that the combined thrust is less than environmental force; and drive off means that vessel cannot maintain its position and heading due to the unbalance between combined thrust and environmental force caused by partial thruster unable of outputting the expected thrust and DP control system unable of kicking out the corresponding thruster.

Redundant Group Design for Propulsion Unit Table 4.4.1.3

Condition		Maintaining ship's position and heading	Redundancy type/description
Operation mode I	Normal DP working condition	Group A (T1A and T3A) and Group B (T2B, T4B and T5)	Active redundancy, no drift off, and no drive off caused by any thruster
	After single failure	Group A (T1A and T3A) and Group B (T2B, T4B and T5)	
Operation mode II	Normal DP working condition	Group A (T1A, T3A and T5) and Group B (T2B and T4B)	Active redundancy, no drift off, and no drive off caused by any thruster
	After single failure	Group A (T1A, T3A and T5) and Group B (T2B and T4B)	

4.4.1.4 A propulsion system for a certain vessel is shown as the following diagram, and the main propulsion unit includes independent power supply and control circuit, fresh water cooling system, etc. FMEA carried out for each components of main thruster system is shown in the following table.

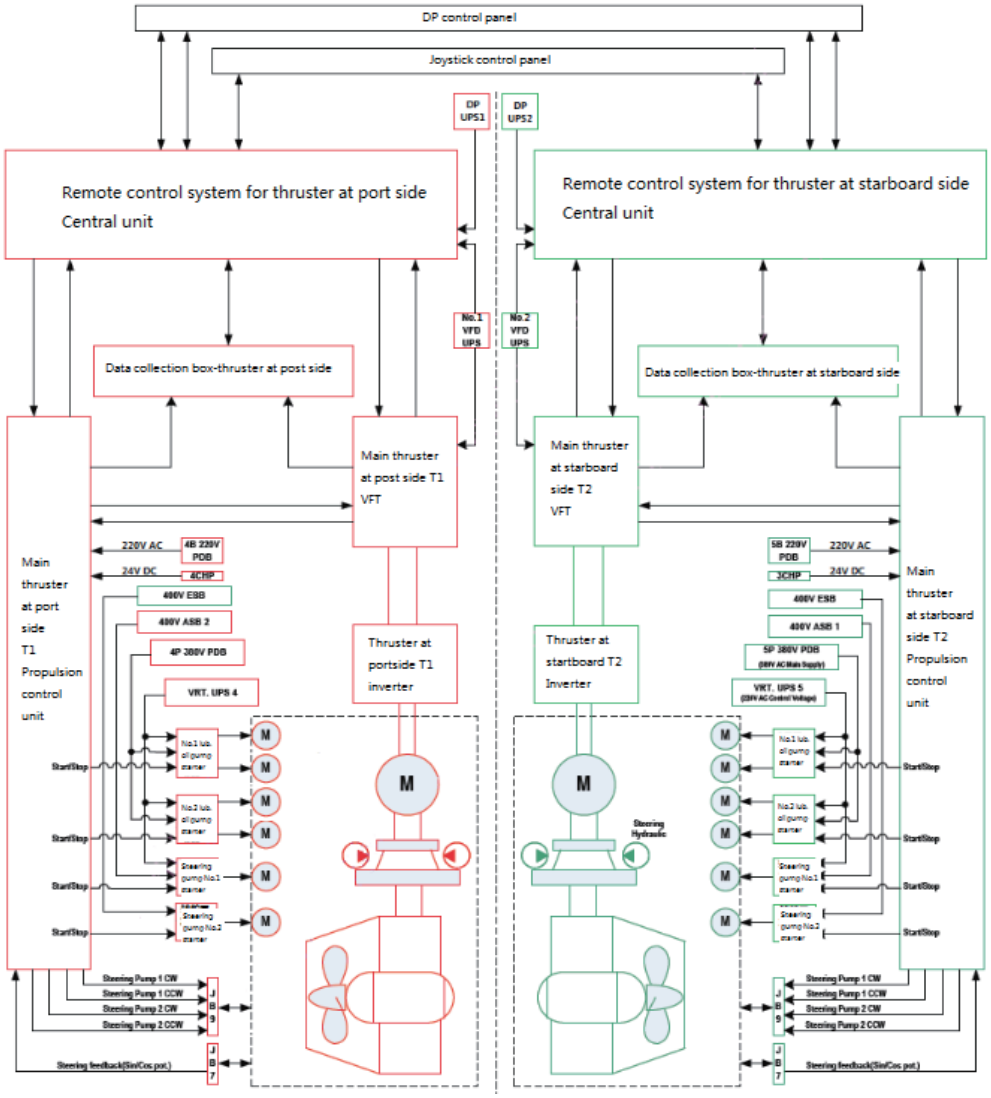


Figure 4.4.1.4 Diagram of Main Propulsion System for a Certain Vessel

FMEA for Main Thruster System

Table 4.4.1.4

Driving unit for main thruster								
No.	Component / failure mode	Cause of failure	Effect of failure	Detection method	DP effect	Probability	Danger level	Recommended action or others
1	Rectifier failure	Fuse failure Internal fault	Thruster switch- off	Alarm in AMS, and thruster not ready alarm displayed in DP control	Loss of relevant thruster, position and heading kept by remaining thruster s	Small	Small	None
2	Inverter failure	Internal fault	Tripping of inverter, stopping of thruster	Alarm in AMS, and thruster not ready alarm displayed in DP control	Loss of relevant thruster, position and heading kept by remaining thruster s	Small	Small	None
3	CPU failure	Internal fault	Tripping of inverter, stopping of thruster	Alarm in AMS, and thruster not ready alarm displayed in DP control	Loss of relevant thruster, position and heading kept by remaining thrusters	Small	Small	None
…	…	…	…	…	…	…	…	…
Thruster control units:								
1	AC230V main power source supply failure	Short circuit, earth fault, overload or wire break	Loss of one power source and automatically switched to stand-by power source	Power failure alarm in AMS	No immediate effect on DP, and the affected main propulsion still available in DP	Small	Small	None
2	DC24V stand-by power source supply failure	Short circuit, earth fault, overload or wire break	Loss of one power source	Power failure alarm in AMS	No immediate effect on DP, and the affected main propulsion still available in DP	Small	Small	None
3	Main PLC failure	Power supply fault, internal fault	Loss of PLC redundancy and switched to stand-by PLC	Alarm in AMS	No immediate effect on DP, and the affected main propulsion still available in DP	Small	Small	None
4	Stand-by PLC failure	Power supply fault, internal fault	Loss of PLC redundancy	Alarm in AMS	No immediate effect on DP, and the affected main propulsion still available in DP	Small	Small	None

5	CW signal failure for steering pump 1	Wire break and component fault	The steering of affected main thruster frozen, deselect from DP control	Thruster not ready alarm displayed in DP control thruster	Loss of relevant thruster, position and heading kept by remaining thrusters	Small	Small	None
6	CW signal failure for steering pump 2	Wire break and component fault	The steering of affected main thruster frozen, deselect from DP control	Thruster not ready alarm displayed in DP control thruster	Loss of relevant thruster, position and heading kept by remaining thrusters	Small	Small	None
7	CCW signal failure for steering pump 1	Wire break and component fault	The steering of affected main thruster frozen, deselect from DP control	Thruster not ready alarm displayed in DP control thruster	Loss of relevant thruster, position and heading kept by remaining thrusters	Small	Small	None
8	CCW signal failure for steering pump 2	Wire break and component fault	The steering of affected main thruster frozen, deselect from DP control	Thruster not ready alarm displayed in DP control thruster	Loss of relevant thruster, position and heading kept by remaining thrusters	Small	Small	None
9	Steering feedback signal failure	Wire break and component fault	The steering of affected main thruster frozen, but still follow DP command	Steering signal false alarm	No immediate effect on DP	Small	Small	None
…	…	…	…	…	…	…	…	…
Main thruster remote control system/data collecting units:								
…	…	…	…	…	…	…	…	…
Thruster auxiliary system:								
1	Steering hydraulic motor failure	Mechanical damage of main components	…	…	No immediate effect on DP	Small	Small	None
2	Steering control valve failure	Mechanical damage or loss of power source, etc.	Loss of steering control and affecting relevant thrusters	Alarm in AMS	No immediate effect on DP	Small	Small	None
3	Hydraulic oil system failure	…	…	…	No immediate effect on DP	Small	Small	None
4	Lubrication oil system failure	…	…	…	No immediate effect on DP	Small	Small	None
…	…	…	…	…	…	…	…	…

4.4.2 Electrical power system

4.4.2.1 Electrical power system includes shaft generator (if any), diesel generator, switchboard, distribution box, cable and cable channel (DP-3), UPS and batteries, power management system, etc.

4.4.2.2 A certain vessel provided with four thrusters and four main generators is shown as the following figure and table:

Redundant Group Design for Electrical Power System Table 4.4.2.2

Sub-system	Redundant group A	Common group X	Redundant group B
Thruster	T1A, T3A		T2B, T4B
Diesel oil generator	DG1, DG2		DG3, DG4
Power distribution	SWBA		SWBB

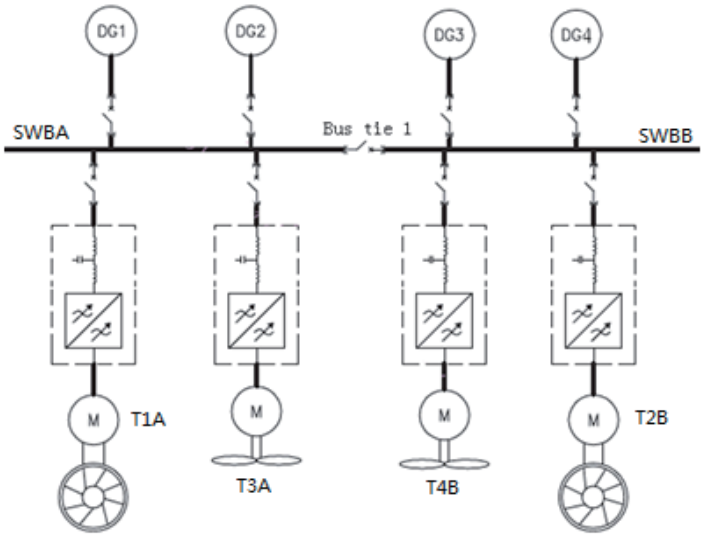


Figure 4.4.2.2 A Certain Vessel Provided with Four Thrusters and Four Generators

Bus tie 1 is assumed to be open in the above-mentioned DP mode, and redundant groups A and B are completely independent. The electrical power system FMEA is to take the consideration of false operation likely to occur as a single failure. The bus tie is to be kept open in DP mode, however, closing of bus tie mentioned above due to false operation may reduce the system redundancy, interlock or other proper measures are to be taken.

Where the above-mentioned case occur in DP mode and bus tie 1 is closed, redundant groups A and B have the common group of bus tie 1, special consideration is to be taken (such as full-scale short-circuit current testing or other valid documents).

4.4.2.3 Where the generators running in parallel are electrically connected, or generator control and protection systems have a certain common failure modes, it is to ensure that one generator failure cannot lead to power supper interruption of other generators running in parallel. The redundant groups for whole electrical power system are to be listed. The whole electrical power system for a certain vessel applying for class notation DP-2 is described in the following figure and table.

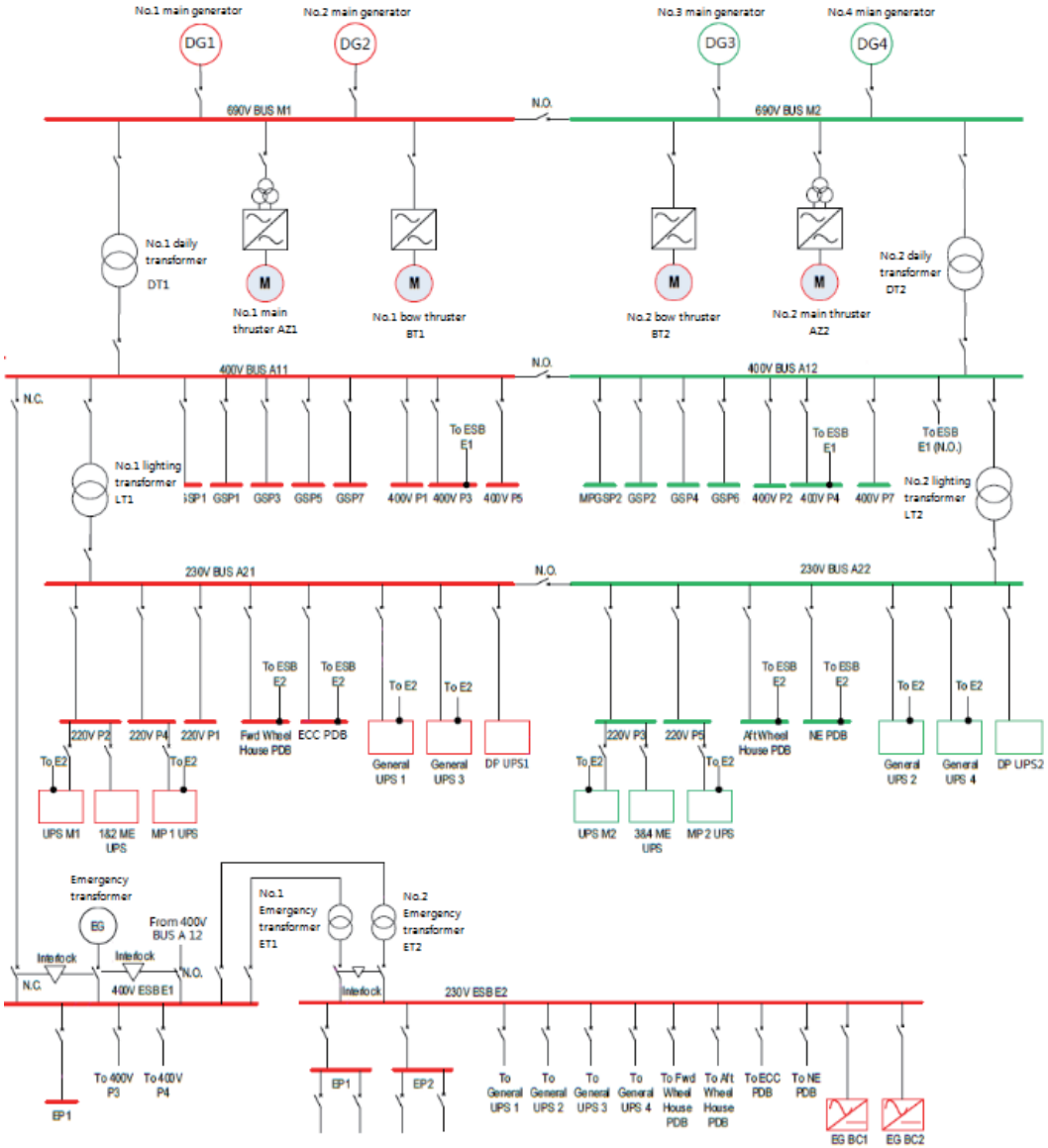


Figure 4.4.2.3 Electrical Power System of a Certain Vessel Applying for Class Notation DP-2

Redundant Group for Electrical Power System Table 4.4.2.3.1

Sub-system	Redundant group A	Common group X	Redundant group B
Diesel oil generator	DG1, DG2		DG3, DG4
AC690V system	690V BUS M1	Bus tie 1	690V BUS M2
AC400V system	400V BUS A11 and associated consumers and distribution box 400V ESB E1	Bus tie 2	400V BUS A12 and associated consumers and distribution box
AC230V system	230V BUS A21 and associated consumers and distribution box 230V ESB E2	Bus tie 3	230V BUS A22 and associated consumers and distribution box
DC24V system	…	…	…

For electrical power distribution system, the different failure mode of each voltage level may be

analyzed either by the same table or individually. Components or systems in the common group X are to be analyzed as detailed as possible. For emergency switchboard power supply loads, all the equipment used in DP mode are to be listed in the failure mode analysis table.

Power System FEMA Worksheet **Table 4.4.2.3.2**

Generators								
No.	Component / failure mode	Cause of failure	Effect of failure	Detection method	DP effect	Probability	Danger level	Recommended action or others
1	DG1 failed	Fuel oil, lubricating oil, cooling system or power source failures, low speed tripping, low pressure tripping, safety stopping, emergency stopping, etc.	Tripping of DG1, but not affecting other generators and thrusters	DG1 tripping alarm	No effect on DP, all thrusters are available	Medium	Small	Nil
2	DG2 failed	Ditto	Ditto	Ditto	Ditto	Ditto	Ditto	Ditto
3	DG3 failed	Ditto	Ditto	Ditto	Ditto	Ditto	Ditto	Ditto
4	DG4 failed	Ditto	Ditto	Ditto	Ditto	Ditto	Ditto	Ditto
AC690V electrical power distribution system:								
1	690V BUS M1failed	Short circuit or earth fault	Loss of BT1 and AZ1; power supply interruption of 400V BUS A11, 230V BUS A21, 400V ESB and 230V ESB	BT1 and AZ1 deselect from DP control; Bus-bar power interruption alarm in AMS	No loss of position and heading keeping, loss of redundancy	Medium	Small	Reminding DPO to pay attention
2	690V BUS M2 failed	Short circuit or earth fault	Loss of BT2 and AZ2; power supply interruption of 400V BUS A12 and 230V BUS A22	BT2 and AZ2 deselect from DP control; Bus-bar power interruption alarm in AMS	No loss of position and heading keeping, loss of redundancy	Medium	Small	Reminding DPO to pay attention
3	No.1 day transformer failure	Component fault	Loss of relevant loads	Alarm in AMS	No loss of position and heading keeping	Medium	Small	Verified by testing
…	…	…	…	…	…	…	…	…
AC400V electrical power distribution system:								

1	400V BUS A11 failed	Short circuit or earth fault	Loss of BT1 and AZ1, power supply interruption of 400V BUS A11, 230V BUS A21, 400V ESB and 230V ESB	BT1 and AZ1 deselect from DP control; Bus-bar power interruption alarm in AMS	No loss of position and heading keeping, loss of redundancy	Medium	Small	Reminding DPO to pay attention
2	400V BUS A12 failed	Short circuit or earth fault	Loss of BT2 and AZ2, power supply interruption of 400V BUS A12 and 230V BUS A22	BT2 and AZ2 deselect from DP control; Bus-bar power interruption alarm in AMS	No loss of position and heading keeping, loss of redundancy	Medium	Small	Reminding DPO to pay attention
3	MPGSP1 failed	Short circuit or earth fault	Loss of MP1 fan	Alarm in AMS	No loss of position and heading keeping	Small	Small	Nil
4	GSP1 failed	Short circuit or earth fault	Loss of BT1 fan	Alarm in AMS	No loss of position and heading keeping	Small	Small	Reminding DPO to pay attention
…	…	…	…	…	…	…	…	…
AC230V electrical power distribution system:								
…	…	…	…	…	…	…	…	…
Emergency switchboard:								
…	…	…	…	…	…	…	…	…
DC24V electrical power distribution system:								
…	…	…	…	…	…	…	…	…

4.4.3 Power management system

4.4.3.1 Power management system is to be analyzed in FMEA report, refer to the documents provided by PMS equipment suppliers. The PMS system provided onboard a certain DP-2 vessel is listed as the following figure.

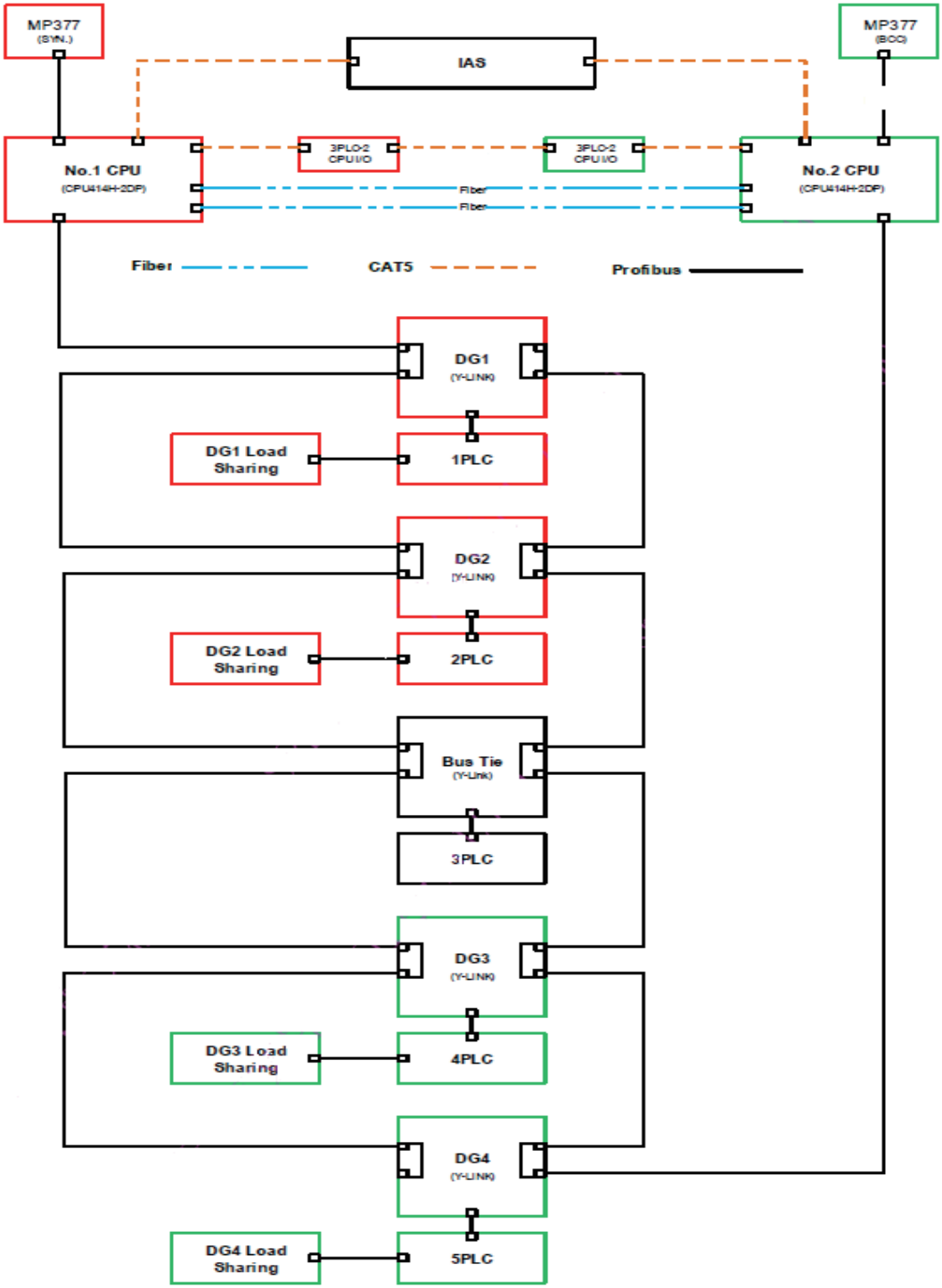


Figure 4.4.3.1 PMS System for a Certain Vessel

Redundant Group for PMS **Table 4.4.3.1.1**

Sub-system	Redundant group A	Common group X	Redundant group B
CPU	No.1 CPU		No.2 CPU
Y-Link	No.1 DG, No.2 DG	Bus tie	No.3 DG, No.4 DG
Load Sharing	No.1 DG, No.2 DG		No.3 DG, No.4 DG
Screen	No.1		No.2

Power Management System FMEA Worksheet **Table 4.4.3.1.2**

No.	Component / failure mode	Cause of failure	Effect of failure	Detection method	DP effect	Probability	Danger level	Recommended action or others
1	CPU failed	Component failure	Loss of CPU redundancy	Alarm in AMS	No loss of position and heading keeping	Medium	Small	Nil
2	PLC failed	Component failure	Loss of affected PLC	Alarm in AMS	No loss of position and heading keeping	Medium	Small	Nil
3	PPU failed	Component failure	Affected generators deselect from DP	Alarm in AMS; Alarm on power limits in DP control station	No loss of position and heading keeping	Medium	Small	Nil
4	Network failed	Component failure, wire break	Loss of communication between CPUs	Alarm in AMS	No loss of position and heading keeping	Medium	Small	Nil
…	…	…	…	…	…	…	…	…

4.4.4 DP control system

4.4.4.1 DP control system FMEA includes DP control computer system, joystick system, ship and position reference system, mode selection switch, relevant power supply unit, etc. Each hardware module, network frame and power source supply are to be analyzed for DP control system FEMA with the reference of approved FMEA for relevant product plan approval.

4.4.4.2 The redundancy design of DP control system for a certain vessel is described in the following figure and table.

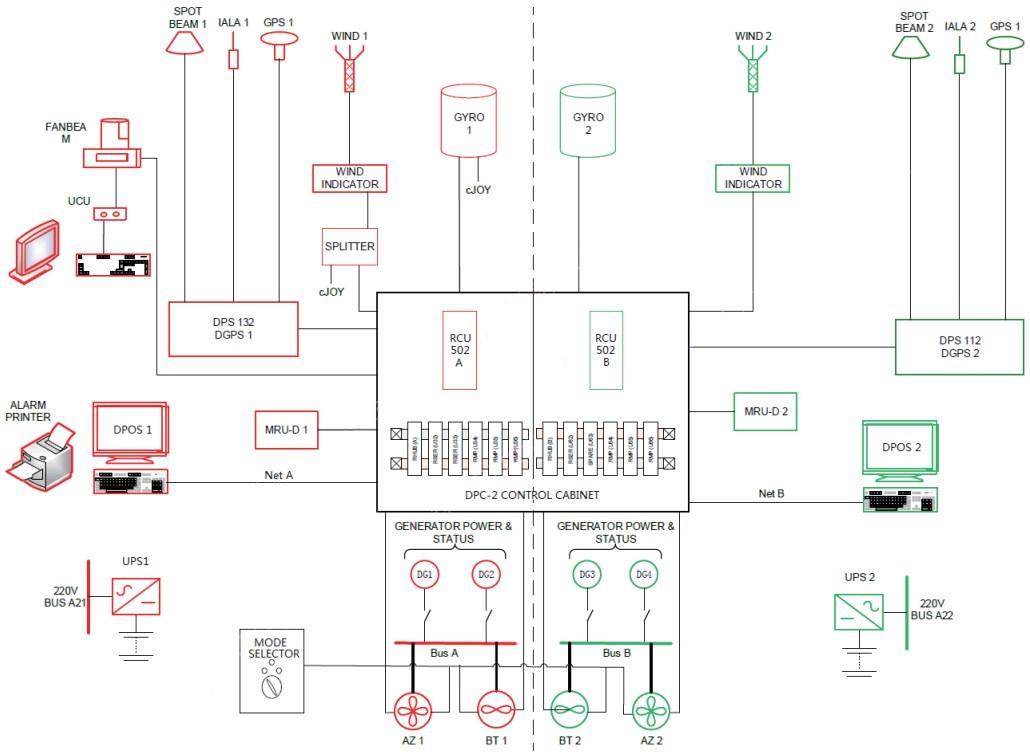


Figure 4.4.4.2.1 DP Control System for a Certain Vessel

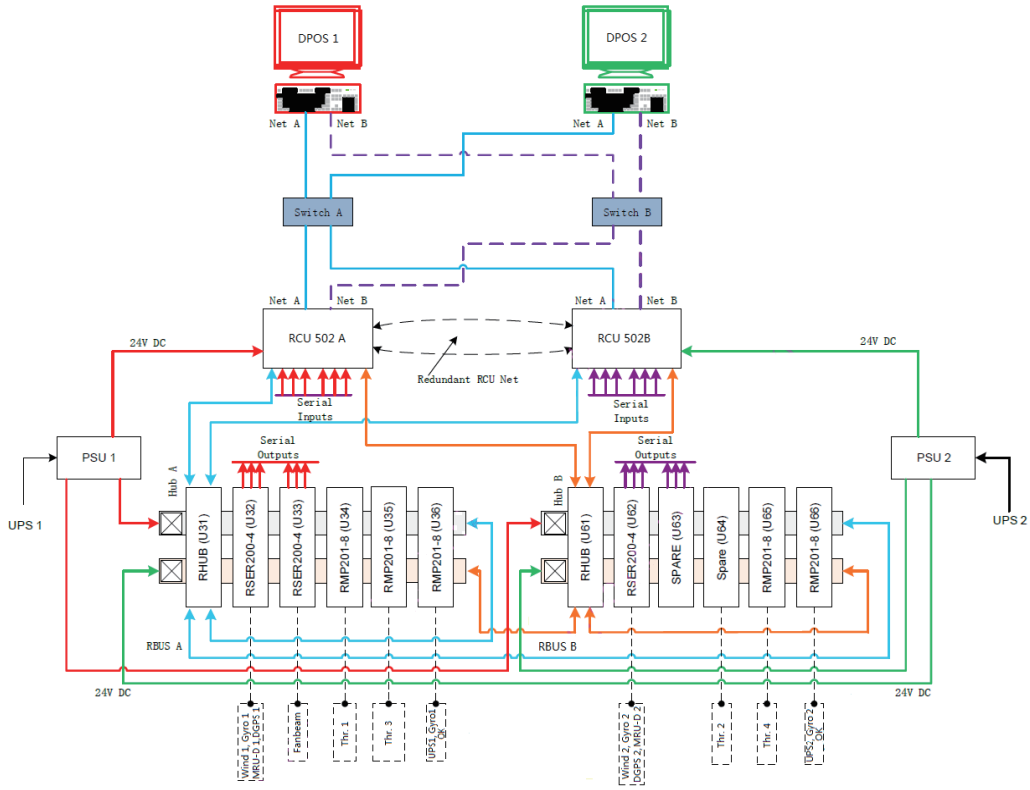


Figure 4.4.4.2.2 DPC-2 Control Box Provided onboard the Vessel

Redundant Group for DP Control System Table 4.4.4.2.1

Sub-system	Redundant group A	Common group X	Redundant group B
Control station	DPOS1		DPOS2
DP main control box (DCP-2)	PSU1	DP control software RCU 501A (main) RCU502B (stand-by) Mode selection switch Network communication line RMP/RSER/RHUB module	PSU2
UPS	DP UPS1		DP UPS2
Sensor	Gyro 1, Wind 1, MRU 1 DGPS 1, Fanbeam		Gyro 2, Wind 2, MRU 2 DGPS 2
Network	Switch A	DPOS1 Net A DPOS2 Net B RCU A Net B RCU B Net A	Switch B
Thruster	T1, T3		T2, T4

DP Control System FMEA Worksheet Table 4.4.4.2.2

Sensors:								
No.	Component / failure mode	Cause of failure	Effect of failure	Detection method	DP effect	Probability	Danger level	Recommended action or others
1	DGPS failed	Component fault	Loss of affect position reference	Alarm in DP control station	No loss of position and heading keeping	Small	Small	Nil
2	Fenbeam failed	Component fault	Loss of affect position reference	Alarm in DP control station	No loss of position and heading keeping	Small	Small	Nil
3	Wind speed sensor failed	Component fault	Loss of affect wind speed sensor	Alarm in DP control station	No loss of position and heading keeping	Small	Small	Nil
4	Wind speed signal dismatch	Signal disorder	Selected wind speed sensor used	Alarm in DP control station	No loss of position and heading keeping	Small	Small	Nil
5	Gyro failed	Component fault	Loss of relevant Gyro signal	Alarm in DP control station	No loss of position and heading keeping	Small	Small	Nil
6	MRU failed	Component fault	Loss of relevant vertical reference	Alarm in DP control station	No loss of position and heading keeping	Small	Small	Nil
…	…	…	…	…	…	…	…	…
Controllers:								

1	Ethernet network A or B	Component failure	Loss of a communication network	Alarm in DP control station	No loss of position and heading keeping	Small	Small	Nil
2	Master controller failed	Component failure	Stand-by controller takes command	Alarm in DP control station	No loss of position and heading keeping	Small	Small	Nil
3	Stand-by controller failed	Component failure	No effect	Alarm in DP control station	No loss of position and heading keeping	Small	Small	Nil
4	DPC-2 power source failed	Loss of power source supply	Loss of one power source	Alarm in DP control station	No loss of position and heading keeping	Small	Small	Nil
5	RHUB A or B failed	Component failure	Loss of one RBUS communication link	Alarm in DP control station	No loss of position and heading keeping	Small	Small	Nil
6	Serial module failed	Component failure	…	Alarm in DP control station	No loss of position and heading keeping	Small	Small	Nil
7	I/O failed	Component failure	…	Alarm in DP control station	No loss of position and heading keeping	Small	Small	Nil
…	…	…	…	…	…	…	…	…
Joystick system:								
1	Gyro 1 failed	Component failure	Automatic heading function is not activated	Alarm in DP control station	No effect on DP	Small	Small	Nil
2	Wind speed sensor 1 failed	Component failure	Joy wind speed compensate function is not activated	Alarm in DP control station	No effect on DP	Small	Small	Nil
…	…	…	…	…	…	…	…	…

4.4.5 Ship auxiliary system

4.4.5.1 The following case shows two fuel oil transfer system onboard a certain vessel both on port side and starboard side. Each side has common fuel oil supply pipeline, which is capable of supplying fuel oil to Main Engine by each daily service fuel oil tank. Each pair of Main Engine has their individual return lines arranged to mirror the supply lines such that they return to their own daily service fuel oil tanks. Isolating valves (FOV71) are arranged on fuel oil supply line in parallel. These isolating valves are usually closed in DP2 mode so that two systems maintain isolation and then redundancy is kept. Each main engine is to be provided with one electric fuel pump and to be used as a stand-by one for each other.

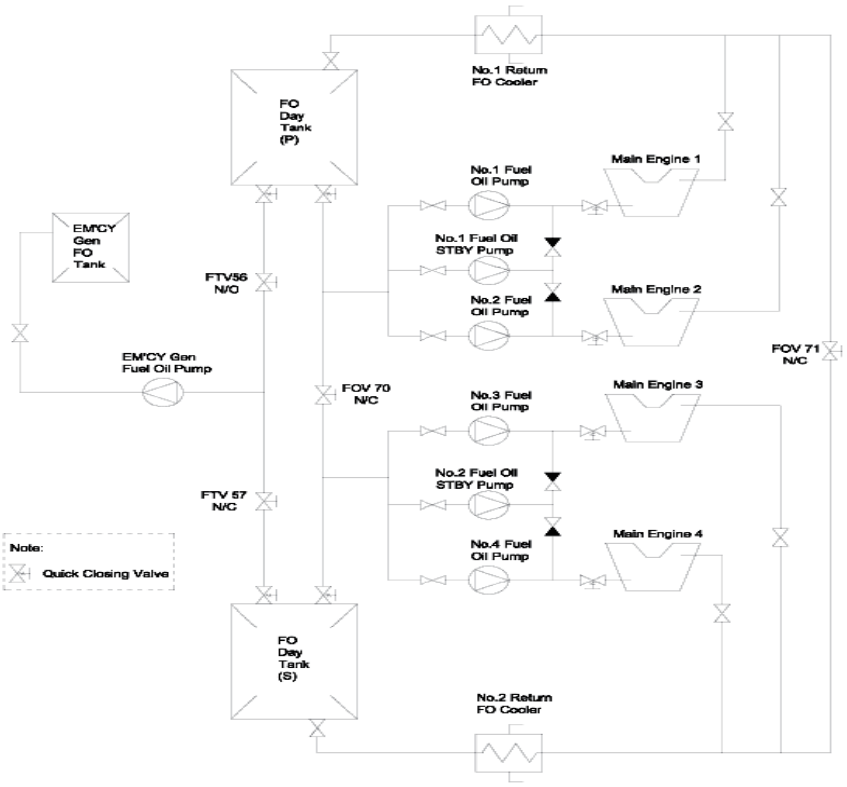


Figure 4.4.5.1 Fuel Oil Transfer System of a Certain Vessel

Fuel Oil Transfer System FMEA Worksheet Table 4.4.5.1

Fuel oil supply system:								
No.	Component / failure mode	Cause of failure	Effect of failure	Detection method	DP effect	Probability	Danger level	Recommended action or others
1	Main fuel oil pump	Fuel oil pump failure or low pressure alarm	Loss of main fuel oil pump	Sensor detection	No loss of positioning capability	Medium	Small	Stand-by fuel oil pump automatically starts and continuously supplies fuel oil to main engine
2	Stand-by fuel oil pump	Hidden fault	Loss of stand-by fuel oil pump	NIL	No loss of positioning capability	Medium	Small	Stand-by fuel oil pump is not used
…	…	…	…	…	…	…	…	…

4.4.5.2 The following case shows a sea water cooling system provided onboard a certain vessel, which includes two sea chests connected by main sea water pipelines, isolated valve (CSV10) is provided between the pipelines, the valve is to be kept closed in DP operation mode. The first main cooler is served for No.1 and No.2 main engines while the second main cooler is served for No.3 and No.4 main engines. Three main sea water cooling pumps are provided, two for daily service and one for stand-by.

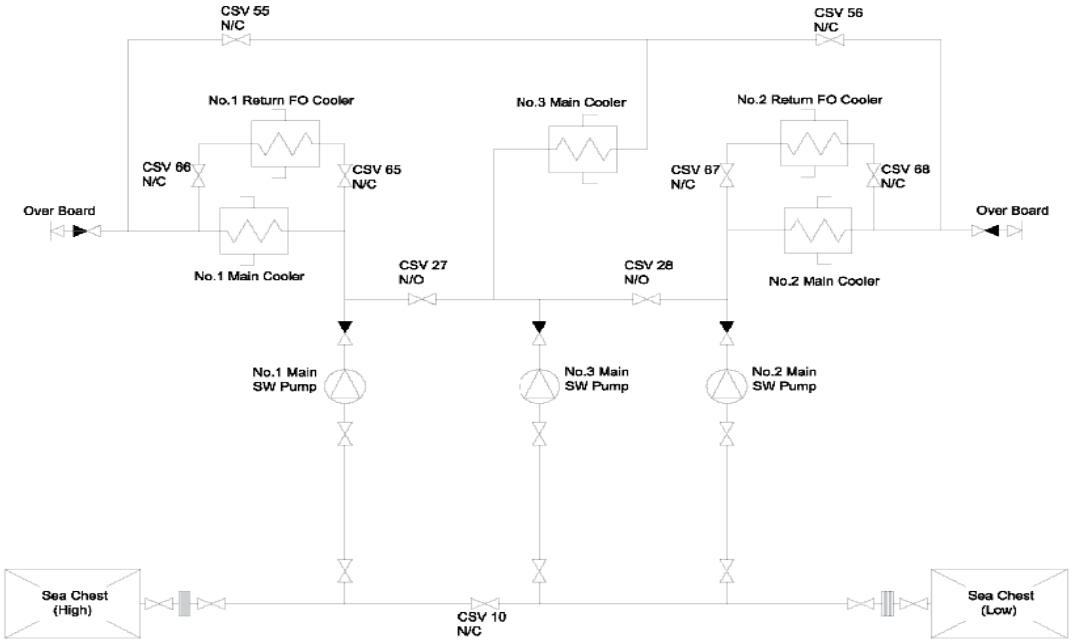


Figure 4.4.5.2 Sea Water Cooling System of a Certain Vessel

Sea Water Cooling System FMEA Worksheet **Table 4.4.5.2**

Sea water cooling system:								
No.	Component / failure mode	Cause of failure	Effect of failure	Detection method	DP effect	Probability	Danger level	Recommended action or others
1	Sea water cooling system for main engine	Sea water pump failure or low pressure alarm	Loss of sea water cooling for main engine	Sensor detection	No loss of positioning capability	Medium	Small	After valve on pipeline is opened, the stand-by pump is started
2	Sea water cooling system for ruder stock device	Sea water pump failure or low pressure alarm	Loss of sea water cooling for rudder stock device	Sensor detection	No loss of positioning capability	Medium	Small	After valve on pipeline is opened, the stand-by pump is started
…	…	…	…	…	…	…	…	…

4.4.5.3 The following case shows a fresh water cooling system provided onboard a certain vessel, each main engine is provided with an independent fresh water cooling system, which is consisted of low temperature pipeline and high temperature pipeline. The low temperature fresh water pipeline includes engine-driven low temperature fresh water cooling pump, low temperature air cooler and lubricating oil cooler. The main engine shares main cooler, high temperature fresh water expansion box and temperature control valve. The high temperature fresh water pipeline includes engine-driven high temperature fresh water cooling pump, high temperature air cooler and temperature control valve. Such arrangement is to ensure that any single failure of fresh water cooling system for main engine will not cause other faults in any time.

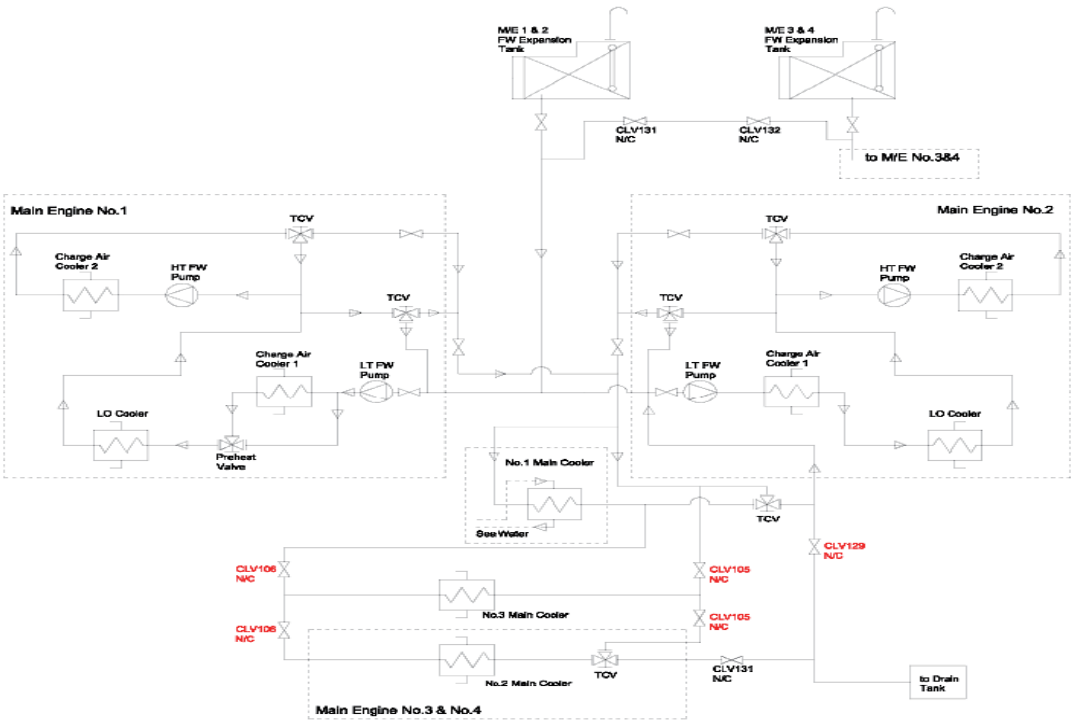


Figure 4.4.5.3 Fresh Water Cooling System of a Certain Vessel

Fresh Water Cooling System FMEA Worksheet Table 4.4.5.3

Fresh water cooling system:								
No.	Component / failure mode	Cause of failure	Effect of failure	Detection method	DP effect	Probability	Danger level	Recommended action or others
1	Low temperature fresh water cooling pump for main engine (engine-driven pump)	Fresh water pump failure or low pressure alarm	Loss of low temperature fresh water cooling pump for main engine. Power reduced due to loss of one main engine and loss of one generator	Sensor detection	Position keeping by action of all thrusters	Medium	Small	
2	High temperature fresh water cooling pump for main engine (engine-driven pump)	Fresh water pump failure or low pressure alarm	Loss of high temperature fresh water cooling pump for main engine. Power reduced due to loss of one main engine and loss of one generator	Sensor detection	Position keeping by action of all thrusters	Medium	Small	
3	Main cooler	Block of cooler or high temperature alarm due to leakage	Loss of operating cooler	Sensor detection	No loss of positioning capability	Medium	Small	After valve on pipeline is opened, the stand-by pump is started
…	…	…	…	…	…	…	…	…

4.4.5.4 The following case shows an air control system provided onboard a certain vessel. Compressed air is sent to two starting air bottles by two main air compressors and supply starting air for four main engines. Control air and service air are to be provided through pressure reducing valves. The starting air bottle at port side is to provide starting air for No.1 and No.2 main engines while the starting air bottle at starboard side is to provide starting air for No.3 and No.4 main engines. Isolating valve is to be kept closed in DP-2 operation mode.

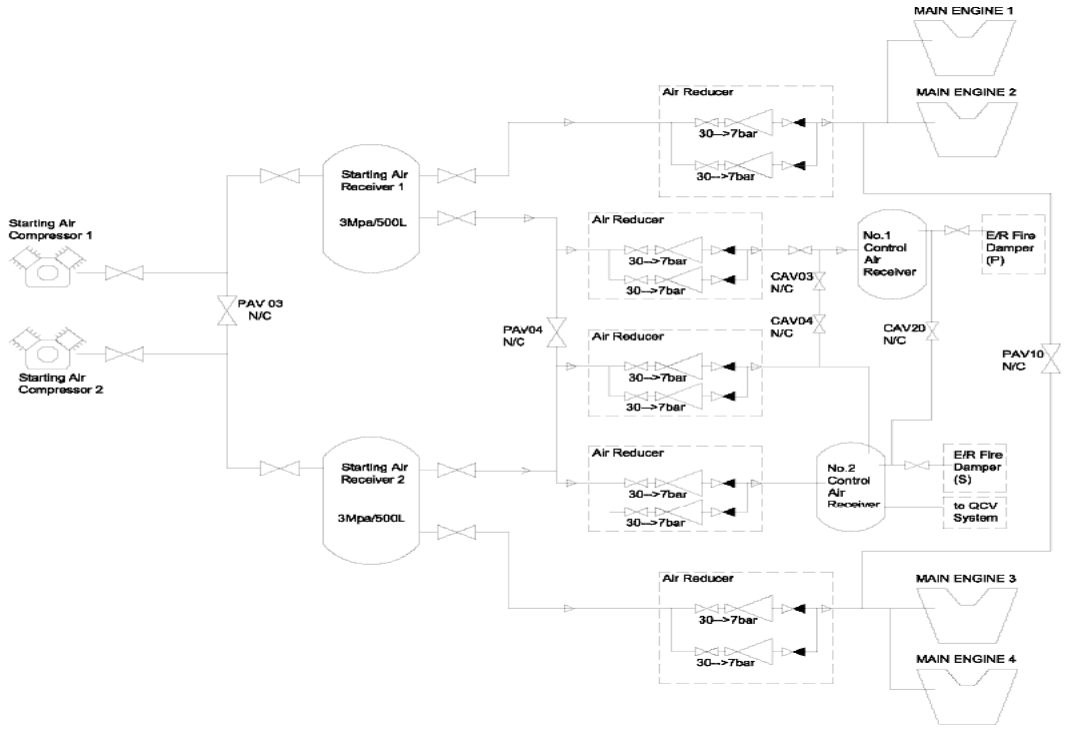


Figure 4.4.5.4 Starting Air System of a Certain Vessel

Starting Air System FMEA Worksheet Table 4.4.5.4

Starting air system:								
No.	Component / failure mode	Cause of failure	Effect of failure	Detection method	DP effect	Probability	Danger level	Recommended action or others
1	1# air compressor	Air compressor failure	Loss of 1# air compressor	Sensor detection	No loss of positioning capability	Medium	Small	2# air compressor put into service
2	1# starting Air bottle	Leakage, block, valve failure …	Loss of 1# starting air bottle	Sensor detection	No loss of positioning capability	Medium	Small	2# starting air bottle put into service
3	1# control air bottle	Leakage, block, valve failure …	Loss of control air for pneumatic damper at port side. Closing of damper at port side, reducing of unpowered ventilation capability in engine room	Sensor detection	No loss of positioning capability	Medium	Small	
…	…	…	…	…	…	…	…	…

4.4.6 Protection for fire and flooding (class notation DP-3)

4.4.6.1 Vessels applying for class notation DP-3 are to take into consideration the failures caused by fire or flooding of DP control stations, power distribution rooms, shared cable channels, main/auxiliary engine rooms, engine control rooms which might affect the ship's positioning capability.

4.4.6.2 For vessels applying for class notation DP-3, cable laying, equipment arrangement in possibly immersed compartments and physical separation with A-60 class divisions are to be described in detail in FMEA report.

4.5 FMEA test programmes

4.5.1 The test of system redundancy is to be tested under each failure mode. The redundancy test program is to be based on the simulation of failure modes, and the tests are to be carried out in the realistic condition as far as practicable. Details of the redundancy test program are to be submitted for examination.

4.5.2 FMEA and redundancy test programmes are to be available onboard the ship. FMEA, test procedures and test report must be kept valid and updated during the whole ship's operation stages. Evaluation is to be carried out in time in the following cases:

(1) where additional FMEA is required;

(2) where test programs need to be updated;

(3) where functional test and/or failure test is required;

(4) where other parts in the document need to be updated.

CHAPTER 5 FMEA APPLICATION OF GAS FUEL ENGINES

5.1 General requirements

5.1.1 Chapter 9, PART THREE of CCS Rules for Classification of Sea-going Steel Ships and Rules for Natural Gas Fuelled Ships put forward the requirements of FMEA for gas fuel engines. This Chapter provides the requirements for the scope, method, procedure and process of gas fuel engine FMEA.

5.1.2 The gas fuel engine is generally developed on the basis of mature conventional fuel oil engines. According to the definition of diesel engine types, the diesel engine is to be added with gas supply, injection, monitoring, control and safety systems by improving design. The pilot oil supply, injection and control systems are added to ignite the natural gas in the cylinder. Other auxiliary systems such as sealing oil system and inert gas system may be added to ensure the safe use of gas. In addition, for the gas fuel engine operating stably and safely under different fuel modes, special control, monitoring and safety systems are needed to control the gas supply, gas injection, gas-air mixing ratio, ignition in the cylinder, etc. As the gas fuel engine belongs to a new type of engine, the approval, type test, inspection and certification are to be carried out again.

5.1.3 As mentioned above, the gas fuel engine is generally developed on the basis of mature fuel oil engines. The corresponding risk analysis has been carried out during the design process of the original fuel oil engine and continuous design improvement and operational experience verification have been conducted, so it has sufficient reliability. When the FMEA is carried out for gas fuel engine, the detailed analysis of basic engine is unnecessary while it is necessary to consider the additional potential risks of basic engine and auxiliary systems (fuel oil system, lubricating oil system, cooling water system, air intake system, exhaust system, hydraulic control system, starting air system, etc.) due to the use of gas fuel, e.g. ignition failure or incomplete combustion of gas fuel in cylinder, explosion risk resulted from the escaped unburned gas into the exhaust system, etc.

5.1.4 There are various designs of gas fuel engines, e.g. dual fuel engine with high pressure direct injection in the cylinder, dual fuel engine for which gas is injected into air inlet channel port, gas fuel only engine for which gas is mixed with air before turbo-charger, etc. The potential risks and hazards vary greatly due to different design concepts and operating modes, so the FMEA is to be carried out by combining the system design.

5.1.5 The effects of consequences resulting from failure are different for the different engine applications on board, so the acceptable safety standards for FMEA need to be treated differently and the corresponding risk control measures (e.g. redundant configuration, safety protection requirements, etc.) may also differ.

5.1.6 The safety and reliability of gas fuel engines is not to be lower than that of fuel oil engines.

5.1.7 The FMEA of gas fuel engine is to be carried out in accordance with Chapter 2 of the Guidelines.

5.1.8 The FMEA of gas fuel engines is to be based on the single failure principle, i.e., only one failure is to be considered at the same time and the possibility of simultaneous occurrence of two or more failures is not considered. Failures of any component directly caused by a single failure of another component are also to be considered. In addition, both detectable and non-detectable failures are to be considered.

5.2 Scope of FMEA

5.2.1 When the gas fuel engine is applied to the ship, the risks associated with the use of gas fuels are not only limited to the engine equipment itself, but the failures of engine external systems (e.g. fuel storage system and fuel supply system) are to require additional safety protection actions from the engine control and monitoring system.

5.2.2 The FMEA of gas fuel engines is to consider at least the following scope:

(1) A failure or malfunction of any system or component involved in the gas mode operation of the engine;

(2) A gas leakage downstream of the gas valve unit in the gas fuel supply system;

(3) The safety of the engine in case of emergency shutdown or blackout, when running on gas;

(4) The inter-actions between the engine and the gas fuel system.

5.3 Design and application description of gas fuel engine system

5.3.1 As a basis and precondition for the FMEA, the design and application of gas fuel engine system is to be determined through reference to drawings and equipment manuals. The system design, operational modes, boundaries and functional requirements are to be explained in the form of text and chart.

5.3.2 The possible applications of gas fuel engine are to be described, which may affect the type approval scope and limitation of product applications in the certificate in the future. The purposes of engine mainly include:

(1) Single main engine propulsion, including direct-driving fixed pitch propeller or controllable pitch propeller, etc.;

(2) Multiple engines, including diesel-electric and diesel-mechanic;

(3) Auxiliary engine;

(4) Emergency engine.

5.3.3 Description of design characteristics of gas fuel engine and its system. There are various forms of gas fuel injection for gas fuel engine systems, mainly including:

(1) Cylinder direct injection;

(2) Gas injection into inlet manifold, scavenge box and air inlets of each cylinder;

(3) Gas and air premix before the supercharger.

5.3.4 Functional description of gas fuel engine and its system operation, structure and boundaries, including:

(1) Description of various operating modes and design objectives;

(2) The relationship between functional elements of the system is to be explained through the method of block diagram. The gas fuel engine system is to be decomposed into subsystems and components, and the input, output and identification number of each subsystem are to be properly numbered. Figures 5.3.4.1 and 5.3.4.2 are the functional block diagram and block diagram of each element described for the dual fuel engine of a company.

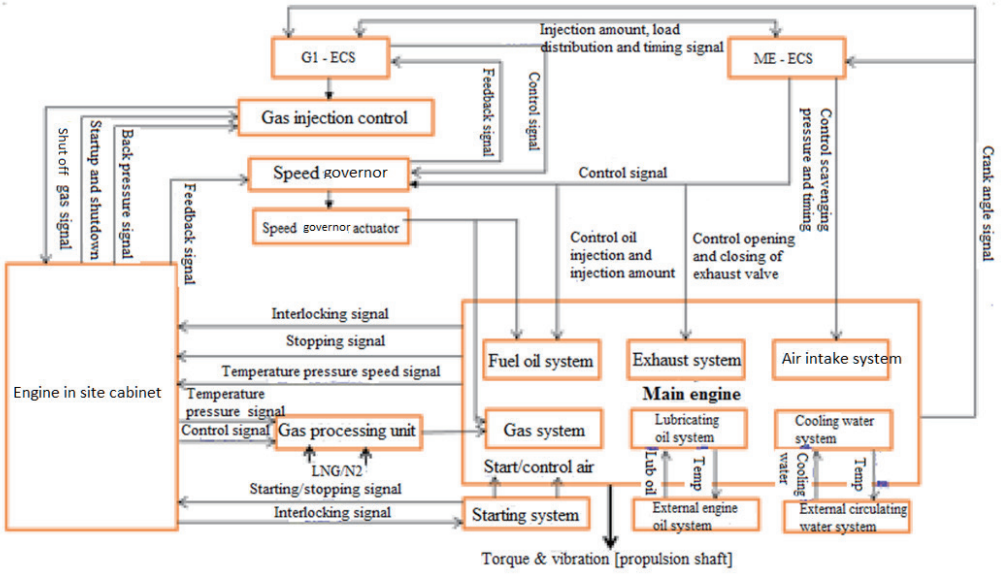


Figure 5.3.4.1 Functional block diagram of dual fuel engine

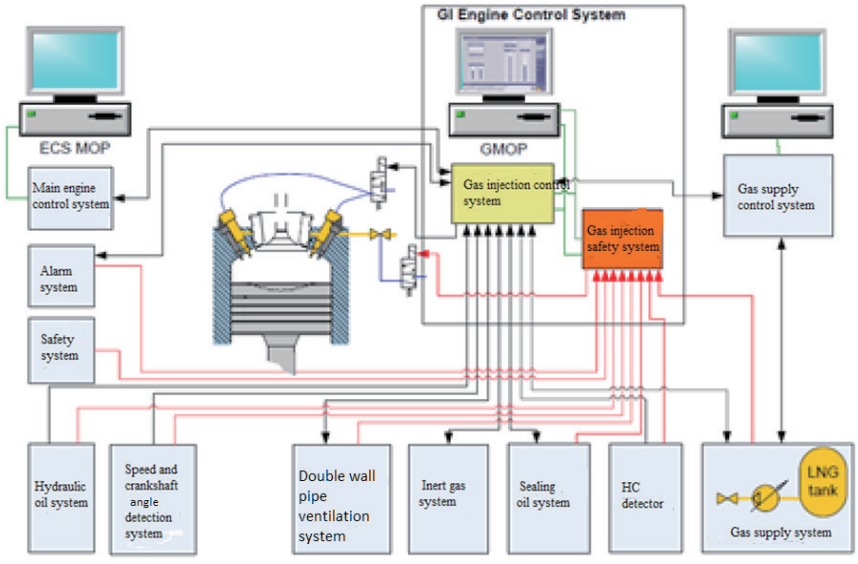


Figure 5.3.4.2 Block diagram

5.4 FMEA Procedure

5.4.1 FMEA is to be carried out in accordance with the following procedures:

5.4.1.1 Identify all the possible failures in the concerned equipment and systems which could lead:

(1) to the presence of gas in components or locations not designed for such purpose, or;

(2) to ignition, fire or explosion.

5.4.1.2 Evaluate the consequences;

5.4.1.3 Identify the failure detection method;

5.4.1.4 Where the risk cannot be eliminated, identify the corrective measures: in the system design, such as redundancies or safety devices, monitoring or alarm provisions which permit restricted operation of the system; in the system operation, such as initiation of the redundancy or activation of an alternative mode of operation.

5.4.2 The results of the risk analysis are to be documented.

5.5 Gas-related systems, equipment and operation

5.5.1 Failure of the gas-related systems or components, in particular gas piping and its enclosure, cylinder gas supply valves, etc. Failures of the gas supply components not located directly on the engine, such as block-and-bleed valves and other components of the gas valve unit, are not to be considered in the FMEA of gas fuel engines.

5.5.2 Failure of the ignition system, e.g., oil fuel pilot injection failure for dual fuel engines and sparking plug failure for gas fuel only engines.

5.5.3 Failure of the air to fuel ratio control system including charge air by-pass, gas pressure control valve, etc.

5.5.4 For engines where gas is injected upstream of the turbocharger compressor, failure of a component likely to result in a source of ignition (hot spots).

5.5.5 Failure of the gas combustion or abnormal combustion (misfiring, knocking).

5.5.6 Failure of the engine control, monitoring and safety systems.

5.5.7 Leakage of gas in the engine components and external systems connected to the engine. Normally no gas exists in the engine auxiliary system. However, gas fuel may leak into the lubricating oil, cooling water, exhaust, starting air and air intake/scavenging systems due to aging, fatigue, stress concentration of components and materials while the gas fuel is used for operation.

5.5.8 Presence of combustible gas in the spaces inside of gas fuel engines such as crankcase, space below the piston, scavenge box, etc.

5.5.9 Gas fuel related operation such as starting, reversing, stopping (normal or emergency stopping), etc.

5.5.10 Changeover between different operating modes for dual fuel engines, including changeover between fuel oil mode, gas fuel mode or other operating modes.

5.5.11 Hazard potential for crankcase fuel gas accumulation, for engines where the space below the piston is in direct communication with the crankcase.

5.6 Verification of analysis results

5.6.1 Some assumptions and analysis conclusion of FMEA are to be verified and supported through a series of tests so as to prove that the identified risks and consequences have been eliminated or controlled, or measures taken to control risk influence are effective.

5.6.2 The conclusions of FMEA are to be the input and basis of the type test programme and factory test programme of gas fuel engines.

5.6.3 Take the dual fuel engine FMEA of a company for example. According to the analysis results, the following items are proposed for the type test of the dual fuel engine:

(1) Software version and parameter verification;

(2) Fuel gas /fuel oil mode changeover simulation test, including gas mode unavailable, interruption of starting, etc.;

(3) Emergency stopping test in gas mode;

(4) Low gas pressure simulation test;

(5) Low hydraulic oil pressure simulation test;

(6) High concentration of gas in the double wall pipe and detector failure simulation;

(7) Shut-off of gas supply system;

(8) Cylinder pressure and gas injection valve pressure monitoring;

(9) Failure of gas fuel injection control valve and gas fuel regulating valve;

(10) Failure of cylinder control unit, gas supply safety unit and cylinder gas safety unit module;

(11) Network failure;

(12) Power failure;

(13) Failure of electrical control system signal;

(14) Failure of main control panel;

(15) Key sensor failure simulation test, simulating single sensor data error and no signal such as speed sensor;

(16) Gas pipe component failure simulation test.

CHAPTER 6 FMEA APPLICATION OF DIESEL ENGINE ELECTRONICALLY CONTROLLED SYSTEMS

6.1 General requirements

6.1.1 Chapter 9, PART THREE of CCS Rules for Classification of Sea-going Steel Ships requires the submission of FMEA report of diesel engine electronically controlled system. This Chapter specifies the requirements for the method, process and report of FMEA for diesel engine electronically controlled systems.

6.1.2 The primary objective of an FMEA for the diesel engine electronically controlled system is to provide a comprehensive, systematic and documented analysis, which establishes the important failure conditions and assesses their significance with regard to acceptable safety and performance criteria. The FMEA is to demonstrate that single failure of the control system will not result in the operation of the engine being degraded beyond acceptable performance criteria for the engine. Single failure is related to the consideration of only one component failure mode at a time, i.e. no combination of failure modes; however, it considers the possibility of common-cause failures.

6.1.3 General acceptable performance and safety criteria for the engine, as well as criteria specific to the engine application (see 6.2.1.1), are to be stated in the FMEA report and all identified failure modes evaluated against the corresponding performance and criteria. From this point of view, the analysis method of diesel engine electronically controlled systems in this Chapter is rather similar to an extended analysis of FMEA, that is, hazardous analysis is carried out; however, the objective to demonstrate the compliance with acceptance criteria can efficiently be met by using the analysis method provided in this Chapter.

6.1.4 The safety and reliability of electronically controlled diesel engines are not to be lower than those of non-electronically controlled diesel engines.

6.1.5 This Chapter focuses on the diesel engine control system FMEA and related documentation requirements. Refer to Chapter 2 of the Guidelines for the FMEA process and procedure.

6.1.6 The diesel engine control system FMEA is to be performed as a system FMEA.

6.1.7 A system FMEA is carried out in a top-down manner, i.e. it starts from the overall system level and progresses to the next level down, or subsystem level, and further down to the equipment item or component level. However, if it can be justifiably shown that at a certain level there is no further effect on the overall system if a failure occurs, then it is not necessary to continue to the next level down. In this case, it would not be necessary to continue to analyze all of the system levels down to component level.

6.1.8 The FMEA for diesel engine control systems is to be based on a single-failure concept under which a subsystem or equipment item at various levels of the system's functional hierarchy is assumed to fail by one probable cause at a time. The effects of the postulated failure are analyzed and classified according to their severity. Any failure mode which may cause an effect on the system beyond previously agreed acceptance criteria are to be mitigated by measures (such as system or equipment redundancy).

6.1.9 A test programme is to be drawn up to verify the assumptions and confirm the conclusions made in the FMEA.

6.2 FMEA process

6.2.1 Define and describe the system and engine application. As a basis for the FMEA, the system to be analyzed is to be described through narrative text, use of drawings and reference to equipment manuals. The narrative description of the system, its operational modes, boundaries and functional requirements are to address the following:

(1) Description of the engine application, primarily defining:

.1 Single main engine propulsion (limitations of application, e.g. controllable pitch propeller only);

.2 Multiple engines (diesel-electric and diesel-mechanic);

.3 Auxiliary engines;

.4 Emergency engines.

(2) Functional description of system operation, structure and boundaries, including:

.1 Description of system boundaries (physical, e.g. diesel engine and control system elements considered in the analysis as well as operational boundaries, e.g. performance parameters):

- I/O signal specification, sensors and actuators;
- Interface signal specification;
- Monitoring system, including human-machine-interfaces;
- Network connection, e.g. CAN bus, Ethernet;
- Protection, e.g. galvanic isolation;
- Hardwired safety circuits;
- Power supply arrangement;
- Definitions of interactions with engine external systems (e.g. ship alarm system, gear box, controllable pitch propeller automation, power management, gas detection, exhaust, ventilation, lube oil supply, fuel supply systems)
- Definition of limiting performance parameters influenced by the control system, e.g. temperatures, pressures, power, speed

.2 Design intents and operational modes for the electronically controlled system

- Description of manual operation;

- Description of local/remote mode;

- Alarms/warnings.

.3 Any interface to the engine safety system, if applicable

.4 Illustration of the interrelationships of functional elements of the system by means of block diagrams. The block diagrams are to provide a graphical representation of the system and its components for the subsequent analysis. It may be necessary to develop a different set of block diagrams for each operational mode. As a minimum, the block diagrams are to contain:

- Breakdown of the system into major sub-systems or components;

- All appropriately labelled inputs and outputs and identification numbers by which each sub-system is referenced;

- All redundancies, alternative signal paths and other engineering features, which provide "fail-safe" measures

(3) Functional relationships among the system elements, including:

.1 Listing of all component units and components within the control system boundary (part list, names, functions);

.2 Redundancy level and nature of the redundancies, separation, independency;

.3 Description of multiple CPU operation from a concept/system architecture perspective;

.4 Distributed control system architecture.

(4) System requirements and function with acceptable functional performance limits of the system and its constituent elements in each of the typical operational modes.

.1 Acceptance criteria for the electronic control and safety system performance depending on engine application.

(5) System constraints.

6.2.2 Establish safety and performance acceptance criteria. The acceptable performance criteria are to be established in accordance with the requirements of 2.5.4 and to meet the following requirements:

(1) The acceptable performance criteria need to be stated in a manner, which enables the evaluation of each failure mode against these criteria. It is recommended to apply a risk matrix, using a severity index, reflecting the impact of a failure mode to the safety and to the engine performance, and a frequency index reflecting the frequency of occurrence of the event.

(2) The assumptions made in the evaluation of the severity and frequency indices are to be documented.

(3) Refer to 2.5.3 for the definition and value of frequency index, severity index and risk index of failure mode. The risk matrix (Table 2.5.3.3) can be divided into three areas: an area with an acceptable risk index (here lower left with indices 2 and 3), the area with not-acceptable risk indices (here upper right with indices 6, 7, 8 and 9), and the area between the before mentioned two (here the diagonal with indices 4 and 5), where the acceptance depends on further description of the event, for instance means of detection of the failure and the possibility of a manual mode of operation after a failure has occurred. In this area every effort is to be made to make the risk as low as reasonably practicable.

6.2.3 Identify all potential failure modes and their causes. A failure mode is the specific effect by which a failure is observed. When used in conjunction with functional performance specifications governing the inputs and outputs on the system block diagram, all potential failure modes can be thus identified and described.

6.2.3.1 Each (sub-) system is to be considered in a top-down approach. Starting from the system's functional output a failure is to be assumed by one possible cause at a time. Since a failure mode may have more than one cause, all potential independent causes for each failure mode are to be identified.

6.2.3.2 Identify all potential common cause failures. It is not sufficient to consider only random and independent failures. Some common-cause failures (CCF) can occur, that cause system performance degradation or failure through simultaneous deficiency in several system components, due to a single source, environmental stresses, or human error. CCFs are those failures, which defeat the fundamental assumption that the failure modes under consideration in the FMEA are independent. The CCF will cause more than one item to fail simultaneously, or within a sufficiently short period of time as to have the effect of simultaneous failures. Typically, sources of CCF include environmental influences, such as electrical interference, temperature cycling, vibration, as well as human factors like incorrect operating or maintenance actions.

6.2.4 Evaluate the effects for each failure mode. The consequence of a failure mode on the operation, function, or status of a component or a system is called a 'failure effect'. The failure effects are to be evaluated regarding safety and availability in two respects locally, i.e. related to the engine, considering effects to the engine safety system as well, if applicable; and globally, i.e. related to the engine application, e.g. single prime mover in a ship or multiple engine installation.

6.2.5 Identify failure detection methods. A failure detection method can be a visual or audible warning device, automatic sensing devices, sensing instrumentation, manual inspection or other unique indications. These are to be identified for every failure mode and its causes, as appropriate.

6.2.6 Assess the severity and frequency of occurrence. The severity of each failure effect, as well as the frequency of occurrence of each failure mode is to be assessed (according to the index table specified in 2.5.3). Local and global effects on safety and availability are to be considered when determining the severity index.

6.2.7 Evaluate the established risk index. The risk index for each failure mode is to be evaluated in accordance with the requirements of 2.5.3 and Table 2.5.3.3.

6.2.8 Identify corrective measures for failure modes. The response of any back-up equipment, or any corrective action (manual or automatic) initiated at a given system level to prevent or reduce the effect of the failure mode of a system element or component is to be identified and evaluated.

6.2.9 Document the analysis. The FMEA is to be analyzed according to the worksheet as shown in 2.7.1. The worksheet is to start with the highest system level and then proceed down through the system hierarchy.

6.2.10 Describe input to test programme. A test program is to be developed to support the conclusions from the FMEA analysis and to verify any assumptions made. The FMEA is to be an input to the development of test specifications in general and particularly for identification of relevant test to be done during Type Approval Test (TAT) and Factory Acceptance Test (FAT) respectively.

6.3 FMEA report

6.3.1 The FMEA report is to be developed in accordance with the requirements of 2.7 for diesel engine electronically controlled system and at least include the following aspects:

(1) Description of the diesel engine control system;

(2) Subsystems and functions;

(3) Operating and environmental conditions for the failure modes;

(4) Causes and effects;

(5) Analysis assumptions;

(6) System block diagrams;

(7) Performance acceptance criteria;

(8) Worksheets (ref. to 2.7.1);

(9) Test programme and any other test reports.

6.3.2 The report is to contain a summary of the main conclusions, such as the results of the evaluation against the acceptance criteria.

BIBLIOGRAPHY

[1] IEC 60812-2006: Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)

[2] IEC/ISO 31010-2009: Risk management – Risk assessment techniques

[3] GB/T 7826-2012: Analysis Techniques for System Reliability – Procedure for Failure Mode and Effects Analysis (FMEA)

[4] IACS REC.138: Recommendation for the FMEA process for diesel engine control systems, 2014

[5] The International Marine Contractors Association (IMCA). Guidance on Failure Modes & Effects Analyses (FMEAs), 2002

[6] International Code of Safety for High Speed Craft, International Maritime Organization, 2000 Translated by China Classification Society, Beijing: China Communications Press, 2002

[7] International Maritime Organization. MSC/Circ.645: Guidelines for Vessels with Dynamic Positioning Systems, 1994

[8] Rules for Classification of Sea-going Steel Ships, 2015, China Classification Society, China Communications Press Co., Ltd.