INDEX OF REVISIONS

REV	DESCRIPTION AND/OR PAGES REVISED
0	ORIGINAL

	REV. 0	REV. A	REV. B	REV. C	REV. D	REV. E	REV. F	REV. G	REV. H
DATE	15/11/2022								
PROJECT	ESUP								
EXECUTION	CMH4								
VERIFICATION	B79G								
APPROVAL	EK9U								

SUMMARY

1. INTRODUCTION

The Failure Mode Effects and Criticality Analysis (FMECA/FMEA) are structured and inductive method to identify and analyze potential failures, failure modes, causes and effects on system and equipment performance, indicating measures to reduce the occurrence of failures and/or mitigation of its consequences. The two methods of failure analysis are practically identical, however FMECA additionally addresses the evaluation of the criticality of failures.

FMECA/FMEA analysis should be applied in addition to other risk analysis techniques when new systems, equipment or technologies are used on the installations, which allows a better investigation of the fail and fault modes of these systems and to evaluate their effects on the installations. The application should seek means to reduce failures and their criticality.

In the planning and execution of the analysis by FMECA/FMEA, as well as in the management of its recommendations, the following requirements should be met for risk analysis process: National Agency for Petroleum, Natural Gas and Biofuels - ANP, Regulatory standard NR 37, Petrobras standard N-2782 - Techniques Applicable to Industrial Risk Analysis and Safety Engineering Guideline DR-ENGP-M-I-1.3.

The application of FMECA/FMEA is more effective in the design phases where there are already more details and information about the systems and equipment under analysis. Therefore, it is recommended to apply in the detailing design phase or in the operational phase of the installation.

In cases of the lack of failure rate data of the systems and/or equipment during the analysis, data base sources of failure rates recognized in the industry can be used as reference, provided that they are agreed with Petrobras.

2. OBJECTIVES

This Technical Specification (TS) is intended to define the methodology for the Failure Mode Effects and Criticality Analysis of systems or equipment in addition to the requirements contained in the corporate technical Petrobras standards N-2781 and N-2782 and the Safety Guideline DR-ENGP-M-I-1.3 in force on the date of signing the contract. This TS has as main objectives, the following:

2.1 Define scope and criteria for performing the FMECA/FMEA analysis for the Detailing Project phase off the Maritime Production Units, hereinafter designated as Production Unit. This TS can be used optionally as a guide for applying the methodology in the operation phase of the Production Units.

2.2 Guide the dynamics for planning, development, and monitoring of the analysis by the parties involved until its final approval.

2.3 Define the standardization, content, and minimum requirements for the technical report of the analysis.

3. SCOPE OF FEMECA/FMEA ANALYSIS

3.1 The systems or equipment that are selected for the analysis with FMECA/FEMEA, due to the need for greater knowledge of the failure modes and their criticality, shall have the analysis boundaries defined prior to the application of the selected fault analysis method (FMECA or FMEA). FMECA should be selected whenever failure criticality assessment is required.

3.2 The analysis should cover the systems, equipment within the boundaries of analysis previously defined in the scope of the study and according to the objective and scope of the analysis, in some special cases, can even reach the level the components of systems and equipment.

3.3 When more than one system is integrated or has interfaces, the analysis shall evaluate the effects of failures among the systems and on their own interfaces. The effects of failures on systems upstream and downstream of the boundaries of the system under review shall also be assessed.

3.4 During the analysis, for each identified failure mode should be evaluated the need to include other measures or devices to reduce the probability of failure, such as including redundancies, means to stop the evolution of failure events before the undesired consequences occur and means to reduce criticality if failures occur. The fault detection modes and measures to mitigate their consequences should also be identified or recommended to be included, considering that predicted failures may occur.

3.5 General aspects of analysis

3.5.1 The final report of the analysis shall be issued in Portuguese (Brazil). If the contractual language of the project is English, the report shall also be issued in English.

3.5.2 The analysis shall be based on data contained in the technical design documentation of the Production Unit itself. The documentation to be used as the basis for the analysis shall have the condition of "released by Petrobras", according to this TS.

If outstanding or incomplete information is identified in the project documents, prior to the realization of the analysis, or during its development, the responsible to perform the analysis shall request it from the Designer company, in accordance with the Project Communication Management Plan. These requests shall be reported to Petrobras.

3.5.3 It is the responsibility of the Designer to research and obtain all the information necessary to perform the analysis, including engineering documentation, updated technical data relevant to the analysis of failures, reliability data of systems, equipment or components obtained from manufacturers or reliability

databases recognized in the industry. If the project is executed internally to Petrobras, the area responsible for the project will have the same responsibility as the Designer.

3.5.4 The final report of the analysis shall contain the complete list of reference documents, with the indication of the revision of each document used in the analysis, and it is the responsibility of the performer of the analysis to verify the completeness of the list of documents.

3.5.5 It is the responsibility of the Designer to carry out the management of changes (MOC) of the project and the reference documents for the realization of the analysis and its impacts (changes) in the result of the analysis, being at its responsibility to review and updating the analysis and the final report.

3.5.6 The final report of the analysis shall be submitted for formal approval by Petrobras.

4. DEFINITIONS

4.1 Human Reliability Analysis (HRA) - Method used to qualitatively and quantitatively analyze the human actions, tasks and services required by a system.

4.2 Common Cause Failure Analysis - Technique that assesses the occurrence of failures on two or more equipment resulting from a common cause (see Common Cause Failure).

4.3 Failure Modes, Effects and Criticality Analysis (FMECA) - Structured inductive technique to identify failure modes of systems, equipment or components and qualitatively evaluate the criticality of their respective effects. Criticality is obtained by combining the probability of occurrence with the severity of the consequence of each failure.

4.4 Task Analysis - Method of human error analysis that consists of dividing tasks into subtasks. It involves the detailed determination of the required performance of people and equipment and the determination of environmental effects and conditions, malfunction, and other unexpected events.

4.5 Block Diagram Analysis - Graphical and analytical method used to represent the logical combination of the elements of a system and calculate its reliability, availability, and maintainability.

4.6 Safety Barriers – These are all physical and non-physical means designed to prevent, control, or mitigate accidental events. Barriers include design safeguards and safety operational procedures.

4.7 Causes – Are the initiators of the deviation, the reasons why deviations can occur. They may include equipment failure, human error, unforeseen changes in operating conditions, and others.

4.8 Reliability - Probability of a system, subsystem or component successfully performing its specific functions over a period of time, within normal conditions of use and operation.

4.9 Consequence - Manifestation of how physical effects impact human, environmental and/or material resources caused by fires, explosions, or leaks of toxic or hazardous products, expressed in the form of damage to health, economic loss and impacts on the environment.

4.10 Deviations - Divergences from project intentions or normal operating conditions. The list of applicable deviations is obtained from the combination of process parameters (variables) with guide words.

4.11 Availability - Ability of a component to be able to perform a certain function at a given time or for a given time interval, considering the combined aspects of its reliability, maintainability, and maintenance support, assuming that the required external resources are assured.

4.12 Effects - Consequences arising from the occurrence of a failure mode, which may affect operation, function and could result in consequences for the facilities, people, environment, and image of the Company.

4.13 Human Error - Actions, tasks or activities performed by people, which may contribute or result in accidents by exceeding acceptability limits defined by the system.

4.14 Responsible for performing FMECA/FMEA (Analysis Performer) - Company responsible for the execution of FMECA/FMEA and may be a company contracted by Designer.

4.15 Failure - Cessation of an element's ability to perform the required function.

4.16 Function - is a description of the design intent for a system, subsystem, or component.

4.17 Common Cause Failure (CCF) - Failures of different systems, equipment or components resulting from the same direct cause.

4.18 Fault - State of an element characterized by the inability to perform a required function, excluding disability during preventive maintenance or other planned actions or due to lack of external resources.

Note: A fault is often the result of an element failure, but it can occur without failure.

4.19 Failure Frequency - Number of failure events occurred, divided by the "calendar" time or operating time in which such events occur or by the total number of demands.

4.20 Maintainability - Probability that a particular repair can be performed in a given period.

4.21 Detection modes - These are devices, systems or other means already existing in the Production Unit or foreseen in the project, used to identify the occurrence of the deviation. Examples: level control loops, pressure control loops, alarms, fire and gas detectors etc.

4.22 Failure Mode - Effect by which a failure is observed on a system, equipment, or component of a system. A failure mode can be identified as:

a) loss of the function, over function, under function, intermittent function or Unintended Function.

b) function without demand.

c) condition out of specification; or

d) a physical characteristic, such as a leak (incipient failure mode) observed during inspection.

A process failure is the manner in which a system, subsystem or part fails to meet its intended purpose.

4.23 Hazard - condition or property inherent to a substance, activity, system, or process, with the potential to cause damage to the physical integrity of the company's persons, environment, property, or image.

4.24 Designer - company responsible for the preparation of the engineering project of the Production Unit that can be a Conceptual Project, Basic, Executive Project or technical assistance of pre-operation, and may be Petrobras itself or contracted company.

4.25 Recommendations - Proposed measures to reduce the likelihood of accidental scenario occurrence or mitigate its consequences whenever existing safeguards are considered insufficient.

4.26 Risk - Combination of the expected frequency of occurrence of an accidental scenario with the severity of the consequence of this scenario.

4.27 Safeguards - Safeguards are considered only those means existing or already provided for in a project that are adequately sized and in operational conditions that allow the effective prevention or mitigation of the analyzed accidental scenario.

4.28 Failure Rate - Correlation between the number of failures that occur on a component, equipment, or system, and the operating time or "calendar" time or total number of demands on which those failures occur.

5. REFERENCE DOCUMENTATION

They are the documents necessary for the preparation of the Analysis. The following documents should be considered, in their most up-to-date version and with status of released by Petrobras in any electronic document management system defined in the contract. The revision of each document to be used shall be clearly indicated on the report of the analysis.

a) Process Flow Diagrams (PFDs).
b) Engineering Flow Diagrams (P&IDs).
c) Cause and Effect Matrix.
d) Risk Analysis Reports already conducted for the Unit, including risk analyses carried out for marine systems and subsea systems, when applicable.
e) Descriptive Memorial of systems and equipment.
f) Data sheets of systems and equipment.
g) Manuals of operation and maintenance of equipment systems, whenever necessary.
h) Industry-recognized reliability data of the systems, equipment, and components.

Depending on the systems or equipment to be analyzed, the documents cited above may not be available or are not applicable to the analysis, in this cases Petrobras shall be consulted about its relevance and applicability for the preparation of the analysis.

The documentation shall be available to the technical responsible for conducting the analysis and to the participants of the analysis at least 10 days before the start date of the analysis.

6. REQUIREMENTS FOR DEFINING THE PARTICIPANTS

The following are the main requirements for the professionals involved in the analysis:

6.1 The Analysis shall be prepared by a multidisciplinary team involving professionals from the Designer and Petrobras. The Designer team shall be composed by experienced professionals in the area who engage in the project and represent the following disciplines: process, equipment/ mechanics, instrumentation / automation and control, safety, naval and submarine systems, according to the characteristics of the system or equipment under analysis.

The Petrobras team may be composed by professionals from all disciplines mentioned or in part, however there should be full participation of technical professionals who have knowledge of the operation of the systems, equipment, and components under analysis. It is also indicated the participation of maintenance professionals and operation of the systems or equipment under analysis.

6.2 The technical responsible for conducting the FMECA/FMEA analysis shall have proven training in the methodology and conduction this activity. It shall also have

participated in at least 2 (two) to FMECA/FMEA analysis of industrial systems or equipment.

6.3 In the preparation of the Analysis the defined team shall have its composition, function and attributions performed by each one, as described on Table 1 below:

Table 1 - Basic composition of the elaboration team of the analysis

Function	Activities
Coordinator	Professional of the Designer Company responsible for the event and who shall: • convene the team. • gather up-to-date information such as: Design documentation, technical specifications of the project, etc. • distribute documentation to the team. • prepare and manage the plan, schedule the meetings, and provide the resources for their realization.
Analysis performer - Technical professional responsible for the conduction FMECA/FMEA analysis	Professional responsible to perform the FMECA/FMEA analysis, who shall: • explain the methodology to the participants. • conduct the meetings and define the pace of progress of the meetings. • manage pendencies from previous meetings. • pre-evaluate the documentation to be used in the analysis, defining the limits of scope of the analysis, preparing the block diagrams of the systems/subsystems and fill out the spreadsheet of the analysis. • prepare the final complete report of the analysis.
Participants	Professionals of the Designer, suppliers of systems or equipment and Petrobras that are designated to attend the meetings. It is recommended that at least one representative of each discipline have more than 3 years of experience in the area they represent.
Experts	Technical professionals of the Designer, suppliers or even Petrobras who have advanced or specialized knowledge about specific equipment, technologies or systems may participate on demand, according to the need.

7. PLANNING

Prior to the analysis, a planning stage shall take place, when the objectives and scope of the analysis, the schedule of the meetings, the identification of the necessary documentation, the location of the meetings and the participating team in accordance with item six (6) shall be defined.

The invitations to the scheduled meetings shall be sent by the coordinator to the participants. All technical documentation to be used in the analysis and this technical specification (TS) shall be sent in advance to the participants.

The language for conducting and for the notes of the meetings of the analysis should be defined on the planning stage.

During planning, all interfaces between systems shall be identified and included in the scope of the analysis.

8. METHODOLOGY

The methodology of FMECA/FMEA shall consider at least the following aspects.

8.1 The spreadsheet or program (software) of the analysis shall cover at least the following information:

a) identification of the item.

b) function.

c) failure mode.

d) cause of failure.

e) effect of failure.

f) detection mode.

g) frequency (of failure mode).

h) severity (of the effect of failure).

i) criticality.

j) actions, observations, and recommendations.

Each item, failure modes, or causes of failure shall always be presented in distinct lines of the worksheet and have unique identification.

8.2 The aspects of the analysis and the assumptions to be adopted:

a) All documentation used as a source of data for the FMECA/FMEA analysis shall be attached to the analysis report. The documentation of systems considered as "package" shall also be added to the documentation of the analysis and later attached to the body of the final analysis report.

b) Systems and subsystems shall previously undergo hierarchical decomposition with division into functional blocks to facilitate analysis by block diagrams, with the proper correlations of inputs and their outputs of each block. All interfaces among systems that are within the boundaries of analysis should be considered.

c) FMECA/FMEA analysis shall consider all causes of failures including and those of common cause failure modes.

d) Visual detection, auditory detection and local instrumentation can be considered as effective detection modes in cases of assisted operation.

e) Existing routine operating procedures and maintenance plans shall not be considered as safeguards in FMECA/FMEA.

f) Systems or equipment that are identical and operate in exactly the same conditions may have the typical analysis of one of them that will serve the other.

g) The analysis shall identify and cover the interfaces between systems within the scope of the analysis.

h) All modes of operation in which the system or equipment are involved shall be considered.

i) Human errors may be considered as possible causes of failures, when related to assisted operations, operations that require manual performance or associated with a possible incorrect or improper operation of a valve and other manually actuated elements. For these cases, HRA and Task Analysis may be used.

j) Alarm giving by instruments can be considered as detection modes, but not as safeguards.

k) Spurious actions of protective devices should be considered as causes of failures.

l) All systems and equipment analyzed shall be clearly identified, including instruments, valves, and other components. Each one shall have its tags registered in the analysis worksheet.

8.3 Identification of systems and subsystems to be analyzed

It consists in the determination of the system to be analyzed and its indication in the P&ID or PFDs with demarcation of systems and subsystems and equipment indicating the limits of the borders under analysis.

In the analysis worksheet, the number of documents with the revision, the succinct description of the system and the subsystem shall be indicated.

8.4 The identification of the item to be analyzed

Each item to be analyzed, system/subsystem component shall be identified and indicated in the analysis worksheet. Each item shall have a unique numeric identification.

8.5 As for the function of each item

Each item under analysis shall have its function described in the analysis worksheet. If the item has different function in another mode of operation, then it shall appear in another line of the analysis worksheet. The modes of operation and function shall be clearly identified on each line.

8.6 As for failure modes

Each item shall have the failure modes indicated in the analysis worksheet. If there are distinct failure modes for the same item, they shall be represented in distinct lines of the worksheet.

8.7 As for detection modes

Detection modes are the devices, systems or other means already existing in the installation design documentation or foreseen in the project, used to identify the occurrence of the failure. Examples: detectors, transducers, analyzers, etc. They shall be identified on the worksheet and described.

8.8 As for Safeguards

Safeguards are the devices, systems or other means already existing in the installation design documentation or foreseen in the project that aims to reduce the frequency of occurrence or criticality of the accidental scenarios caused by failures. The safeguards will be considered as Preventive Safeguard (PS) when reduces the frequency of occurrence of the failure and they will be considered Mitigating Safeguard (MS) when reducing the criticality of the failure results.

Each safeguard shall be identified, describing the means available to eliminate the cause of faults, or to reduce its frequency of occurrence or to reduce its criticality.

When the analysis is identified the need for a safeguard and it is not present in the project documentation under analysis, even if provided for in a design standard or guideline, it should be included as a recommendation, so that it can be managed and implemented on the design documentation.

Typical examples of system safeguards:

- PSHH with closing action of the vessel inlet valve.
- Relief and safety valves (PSVs).
- Interlock actions shall be recorded in the safeguard column.

The operating procedure contemplating the operator's response associated with a process variable alarm can be considered as a safeguard in an accidental scenario, provided that it meets all the following requirements:

- The alarm shall be generated in a place where the operator is present continuously (permanently assisted control station) and can recognize it.
- Field alarm and response devices shall have initiators independent of the interlocking system devices.

- The response time to the alarm shall be sufficient for the operator to take the planned actions to interrupt the scenario.
- The action taken is effective to minimize risk without exposing the operator performing the response.

Thus, the alarm, the element to be acted and the operational procedure, are integral parts of the safeguard "operator response to the alarm". Operating procedures and alarm, without taking into account the above, cannot be considered as safeguards.

8.9 As for Identification of additional recommendations, observations, and comments

Recommendations are proposed measures to prevent the failure and the occurrence of the accidental event or mitigate its criticality of the consequences whenever existing safeguards are considered insufficient. Recommendations shall be clear, succinct, well defined and preceded by verb with action. Terms such as planning, designing, elaborating, identifying, specifying, installing, etc. shall be complemented by conclusive actions.

The Designer shall manage the implementation of the recommendations generated in the analysis, including the impact on reviews of reference documents used. For each recommendation, the company, or the body responsible for its implementation should be identified according to ET-3000.00-5400-947-P4X-002 - Management of Safety Study Recommendations.

Observations are complementary information that can be recorded in order to clarify the analyzed scenario, without, however, demanding any action.

Comments are general or specific information that may contribute to clarification of aspects considered in the analysis, but that do not fit as recommendations or observations.

The recommendations generated in the analysis shall be identified as Rxxx, the observations shall be identified as Oxxx, and the Comments will be identified as Cxxx, where xxx corresponds to sequential numbering.

8.10 As for classification of risks

In the phases of detailing and operation project, the risks shall be classified according to the risk matrix presented on the Safety Guidelines – DR-ENGP-M-I-1.3 of Petrobras.

For scenarios that generate recommendations, risk classification shall be presented without recommendations and also presents the risk classification with their implementation (residual risk).

For the scenarios that have as a consequence the loss of containment, they shall be considered the possible effects for the classification of severity, as example: possibility of fire, intoxication of people, explosion, among others. The categorization of the

severity of residual risk, used in the PHA, shall be used as an initial estimate for the analysis of the severity of these scenarios.

9. REQUIREMENTS FOR REVIEW MEETINGS

The schedule of the meetings and provision of the resources for their realization are in charge of Coordinator and shall comply with the following guidelines:

9.1 Planning Meeting

This meeting is intended to briefly present the project in question, define the objectives and scope of the contracted analysis, as well as evaluate and make the necessary adjustments in the work schedule proposed by the Analysis Performer, where the minimum agenda should be:

- To dimensioning of Designer team, Petrobras team and to prepare the list of participants for issuing invitations.
- To clarify the objectives and scope of the analysis.
- To check the documentation necessary for the execution of the analysis and preparation of a pending list, if any, for supply by the Designer.
- To present the proposal schedule of meetings by the Analysis Performer and evaluation to meet the project schedule.
- Definition of the locations, necessary resources, and duration of meetings.

Participants: Designer Coordinator, Petrobras Representatives, and Analysis Performer (mandatory the participation of the leader of the Analysis).

9.2 Initial meeting of the analysis and other meetings

In the initial meeting of the analysis, the Analysis Performer Leader will address the following topics:

- *Safety* briefing on the place of realization.
- Presentation of participants.
- Presentation of the objective and scope of the analysis.
- Presentation of the meeting schedule.
- Brief presentation of methodology and premises.
- Brief description of the Production Unit.
- Presentation of a summary of the historical analysis of incidents that occurred in the Unit or other similar Units.
- Description of the systems or equipment that will be analyzed.

The other meetings on the planed schedule should address the following topics:

- Presentation of new participants, if any.
- Description of the systems that will be analyzed.

Participants: Designer and Petrobras professionals designated team, and analysis Performer.

10. REVIEW THE ANALYSIS

The analysis should be reviewed in the following cases:

a) when changes occur in the project (MOC) that alter the systems or equipment analyzed.

b) when systemic or critical deviations in the reports in relation to this specification are detected by Petrobras.

c) in the operational phase in the cases established in the Company's operational safety management procedures.

11. REPORT CONTENT

The report shall be submitted complying with Petrobras Standard N-1710 encoding and Petrobras Standard N-381 formatting. The final report shall be issued within ten working days after the conclusion of the meetings.

Reports shall contain at least the following items:

1. Objective and Scope of Analysis
   Description of the objectives targeted with the application of the technique, the scope covered by the analysis, and the structure of the report.

2. List of participants
   The list of participants shall contain the general data of each participant (full name, company, department, technical specialty, contact email, discipline that represents and time of experience in it).

   A daily attendance list shall also be generated and shall be signed by each of the participants.

3. Executive summary

4. Introduction

The introduction should contain the description of the Unit, its capacity (POB – people on board) description of the analyzed systems, considering modes of operation, and any relevant aspects related to the analysis.

5. Justification and description of the applied technique

6. List of reference documents - all documents that were used for the analysis shall be related, with their respective revisions.

7. Assumptions considered in the analysis.

8. List of recommendations

   It shall be presented in a table in order to enable the management of the implementation of the recommendations. It shall be listed in this table, the person responsible for implementing each recommendation as well as the corresponding node and scenario number.

9. List of observations

   It shall be presented in a table, the scenario number, and the corresponding node.

10. List of Considerations

    They shall be presented in a table together with the identification of those responsible.

11. Conclusions

This item shall contain at least the following information:

- Total systems and equipment evaluated.
- Total recommendations and observations generated.

12. References: Documents and bibliography

13. Attachments

A. Completed Analysis Worksheets and Block Diagrams.

B. Documents analyzed

C. Daily signed attendance list.

D. List of Barriers.

A list of safety barriers relating to each of the accidental scenarios respective barriers (Safeguards) should be issued and attached to the final report, classifying them between Preventive Safeguards (PS) or Mitigating Safeguards (MS).