INDEX OF REVISIONS

REV.	DESCRIPTION AND/OR REVISED SHEETS
0	ORIGINAL
A	Revised Item 5 - Added “Comments added”.
B	REVISED WHERE INDICATED
C	ITEMS 1, 3, 4, 5, 6, 8 AND 11 REVISED TO ALIGN WITH HUMAN FACTORS ENGINEERING REQUIREMENTS, TO ADEQUATE THE PHA METHODOLOGY TO THE STANDARD N-2782 AND TO INCORPORATE SUGGESTIONS FROM CONTINUOUS IMPROVEMENT PROCESS.

	REV. 0	REV. A	REV. B	REV. C	REV. D	REV. E	REV. F	REV. G	REV. H
DATE	28/01/2020	03/13/2023	05/12/2023	01/MAR/2024					
DESIGN	ESUP	ESUP	ESUP	ESUP					
EXECUTION	DANIELA	CWFS	ABKC	DXVM					
CHECK	IGORG	U4BA	B79G	B79G					
APPROVAL	PAOLO	EK9U	EK9U	EK9U					

SUMÁRIO

1. INTRODUCTION

The Preliminary Hazard Analysis (PHA) is a structured inductive technique used to identify hazards and accidental situations, their possible causes and consequences; qualitatively assess their risks; analyze existing safeguards and propose recommendations, when necessary, for risk reduction.

In the execution of PHA, the requirements of the National Agency for Petroleum, Natural Gas and Biofuels – ANP; Regulatory Standards (NRs) of Ministry of Labor and Employment; Petrobras standard N-2782 - Applicable Techniques to Industrial Risk Analysis; and Safety Engineering Guidelines - DR-ENGP-M-I-1.3 shall be complied with.

This Technical Specification (TS) complements the hazard identification requirements of standard N-2782 and Safety Engineering Guidelines DR-ENGP-M-I-1.3, in force on the date of signature of the contract. It also aims at guiding the development of PHA and the execution of its respective report.

The risk assessment related to the hazards identified in the PHA shall be used to make decisions regarding the adoption of prevention and control measures necessary to maintain the risks in accordance with the tolerability criteria established in the N-2782 standard and Safety Engineering Guidelines DR-ENGP-M-I-1.3, and the measures that make the project inherently safer shall be prioritized.

2. PURPOSE

This specification has the following objectives:

2.1 Define scope and criteria for conducting PHA for project phases of Concept Design, Basic Design, Detailing Design and Assisted Operation of Maritime Floating and Fixed Production Unit, hereinafter referred to as the Unit. This TS can optionally be used as a guide in the Unit Operation phase.

2.2 Guide the dynamics for the planning, development and follow up of the analysis by the parts involved and final approval thereof.

2.3 Define the model, minimum content, and minimum requirements for submission of the PHA report.

3. SCOPE

3.1 The PHA analysis shall cover hazardous events which have their causes originated in the Unit analyzed or in external causes inherent in its operation, identifying the main risk situations and establishing control measures considering component or system failures, as well as operational or maintenance errors (human errors).

3.2 The analysis shall seek primarily to identify hazards in the Unit, not intended to be used to implement operational improvements.

3.3 General

3.3.1 The final PHA report shall be issued in English and then in Portuguese, including all appendices and spreadsheets which shall be presented in both languages.

3.3.2 Analyzes shall be based on the data, released by Petrobras, contained in the design documentation of the Unit used as reference, according to this TS.

3.3.3 If pending or incomplete information is identified in the project documents, prior to the PHA or during its development, the PHA Consulting shall request them from the Designer. These requests shall be informed to Petrobras.

3.3.4 The Project Designer is responsible for searching and obtain all information necessary to carry out the PHA in administration, whether public or not, including engineering documentation, updated technical data, technical standards, and applicable legislation. If the project is executed internally at Petrobras, the department responsible for the project will have the same responsibility as the Designer.

3.3.5 The final report of PHA shall contain the complete list of reference documents, indicating the revision used in the analysis. It is PHA Leader's responsibility the verification of completeness of the list of documents.

3.3.6 The final PHA report shall be submitted to formal approval by Petrobras.

4. DEFINITIONS

4.1 Safety Barriers - all physical and non-physical means designed to prevent, control, or mitigate accidental events. Barriers include project safeguards, safety, and operational procedures.

4.2 Causes - event initiating an incident that can result from equipment failures, human errors, unforeseen changes in operating conditions, external factors, among others.

4.3 Scenario - specific sequence of unintended events that have undesirable consequences.

4.4 Effects - consequences from an accidental scenario, which may affect the persons, environment, asset, and image of the Company.

4.5 PHA Consulting - responsible for the execution of PHA, which may be a contracted company, either by Designer or Petrobras. It can be also an internal Petrobras workforce.

4.6 Frequency - physical quantity indicating the number of occurrences of an event in each time interval.

4.7 Detection modes - devices, systems or other means already existing in Unit or provided in the design, used to identify the occurrence of the accidental scenario. Examples: alarms, fire, and gas detectors, through visual, auditory, olfactory, etc.

4.8 Assisted Operation - support activity to the operation and maintenance teams to ensure that the operation start up is the safe continuation of the pre-operation and operation phases.

4.9 Hazard - condition or property inherent to a substance, an activity, a system, or a process with potential to cause harm to people, environment, asset, or image of the Company.

4.10 Designer - company responsible for the elaboration of the engineering project, which may be conceptual design, basic design, or detailing design, being Petrobras itself or contracted company.

4.11 Recommendations - proposed measures to prevent the occurrence of the accidental event or mitigate its consequences, whenever the existing safeguards are considered insufficient. In PHA, mitigating measures shall be prioritized.

4.12 Risk - Combination of the expected frequency of occurrence of an accidental scenario with the severity of its consequence.

4.13 Safeguard - Any device, system, or action, already planned in the project or existing in the Unit, capable of interrupting the chain of events that occurs from an initiating event, reducing the probability of occurrence of the undesirable scenario or reducing the severity of its consequences.

4.13.1 Preventive Safeguard - any device, system, or action capable of interrupting a chain of events that occurs from an initiating event (cause of the deviation), reducing the probability of the undesirable scenario occurrence (loss of containment). Preventive safeguard does not affect the probability of the initiating cause occurrence, but rather the probability of the undesirable scenario occurrence, given that an initiating cause has occurred.

4.13.2 Mitigation Safeguard - any device, system, or action capable of reducing the severity of the consequences of the undesirable scenario, that is, reducing the impacts of the top event. Ex: Confirmation of methane gas in a zone, generating an alarm and initiating interlocking actions.

NOTE: Firewalls and Passive Fire Protection (PFP), which are prescribed by the Safety Guidelines (DR-ENGP-M-I-1.3) to protect equipment, structures, piping, etc., shall be considered as mitigating safeguards in PHA. Those PFP or firewalls, which depends on the recommendations of consequence studies, shall not be considered as safeguard of the analysis.

4.14 Severity - represents the magnitude of the consequences of each of the accidental scenarios.

4.15 Cancelled.

4.16 Safety Critical Procedures (SCPs) - procedures which rely on the human intervention and whose failure or omission may contribute to the occurrence or the consequences of an accidental scenario classified as “Non-Tolerable” or “Moderate” risk level, with severity category “IV” or “V” for people or environment, or “V” for asset, including those ones which (i) encompasses operational maneuvers of safety critical equipment or systems; (ii) encompasses functional tests or integrity assurance activities of safety critical equipment or systems; and (iii) are prescribed as safety critical procedures based on previous events or learned lessons as per described on item 8.11.

4.17 Human Factors (HF) - individual, technological, and organizational factors which influence the human behavior during the execution of activities and may affect the Unit’s operational safety.

4.18 Cancelled.

4.19 ALARP (As Low As Reasonably Practicable) - a concept which seeks to ensure that the magnitude of the risk is reduced, through the application of appropriate prevention and control measures, to a level as low as reasonably practicable, and that additional measures to reduce it would be disproportionately costly compared to the potential benefits of these measures.

4.20 Small release - loss of containment without the possibility of detecting the pressure drop. Typically, a small release occurs due to leaks in flanges, connections, piping, instrument sockets, or small holes.

4.21 Large Release - loss of containment with the possibility of detection through variable pressure. Typically, a large release occurs due to rupture of piping, flanges, fittings, or equipment.

Note: Small or large release has no relation to the total volume released (referring to the inventory of the section being analyzed). The total volume released shall be considered to determine the consequences of the scenario, depending on the estimated fluid released between the beginning of the loss of containment and the interruption of the leakage (released inventory), through the actuation of mitigating safeguards.

4.22 Hazard event - it is the realization of a hazard.

5. REFERENCE DOCUMENTATION

5.1 As inputs for the elaboration of PHA, the following documents shall be considered, in its up-to-date revision with status of COMMENTS ADDED or

RELEASED by Petrobras at SIGEM or another electronic document management system defined in a contract. For detailing design, it shall be considered P&IDs, at least, in revision A. The revision of each document to be used shall be clearly indicated in the analysis report.

a) Process Flow Diagrams (PFDs);

b) Process and Instrumentation Diagrams (P&IDs);

c) Cause and Effect Matrix;

d) Safety data sheets;

e) General arrangement of the Unit and the specific equipment layout of accommodations, process plant; utilities and hull compartments such as engine room, pump room, bow compartments;

Note: In arrangement drawings, the location of equipment with its respective identification (TAGs) shall be indicated, including also the location of: pipe racks, risers arrival, diving areas, cranes and laydown areas, helideck, helicopters refueling stations, chemical storage, offloading stations, among others. The arrangements shall have the wind rose with the indication of prevailing winds, north of design and true north.

f) Metocean Data;

g) Safety Plan that indicates the installation/location of Fire and Gas detectors - F&G, firefighting system, escape routes, lifesaving appliances, muster stations, passive fire protection, etc.;

h) Hazardous Areas Classification Plan;

i) Mechanical handling of the Unit;

j) Risk Analysis Reports already performed for the Unit, including those carried out for hull systems and subsea systems.

k) Updated 3D Model available. If there is no 3D Model in the project, only 2D layout drawings will be used.

l) Subsea arrangement;

m) Material Safety Data Sheet (MSDS);

n) Operational or maintenance procedures from reference Units.

5.2 Additional documents shall be provided for the identification of the following aspects of the project:

a) Containment and drainage for equipment handling flammable / combustible liquid and hazardous substances (toxic, corrosive).

b) Location of air intakes for closed spaces; process equipment vents; flammable / combustible / chemicals product storage vents, as well as discharges of internal combustion equipment (turbomachinery). All hot surfaces must be indicated (equal to or greater than 60°C).

c) Type of floor that separates the decks (plated or grid floor);

5.3 Depending on the design phase for which the PHA is being prepared, some of the documents cited above may not be available. In this case, Petrobras shall be consulted about its relevance to the preparation of the study.

6. REQUIREMENTS FOR THE PARTICIPATING TEAM DEFINITION

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

6.1 The PHA shall be elaborated by a multidisciplinary team involving professionals from the Designer and Petrobras. The team shall be formed by professionals involved in the project and that are experienced in the area they represent, with representatives of the following disciplines, as applicable: process, naval system, safety, operation, arrangement, instrumentation/automation and control, mechanics, electrical, architecture, maintenance naval*, and subsea* systems.

**Applicable when the analyzed system interfaces with naval or subsea systems*.

6.2 The analysis leader shall have formal training in the PHA tool and the PHA leadership activity.

6.3 The defined PHA team shall have composition, function and attributions performed as follows:

Table 1 - Basic composition of the PHA team

Function	Activities
Coordinator	Professional of the Designer responsible for the event and who shall: • organize the team, • gather up-to-date information, such as P&IDs, technical specifications, etc., • distribute material to the team, • schedule meetings.
PHA Leader	Professional of the PHA Consulting who knows the technique, responsible for: • complying with the schedule of planned meetings, • explaining the technique to be employed to the other participants and making them aware of the need to consider human factors in the analysis, facilitating meetings and defining its progress status, • asking participants for pending information from the previous meetings, if in case,

	• prior evaluation of the documentation to be used in the analysis, defining the sections to be evaluated, • preparing the final analysis report.
Participants	Professionals of the Designers/Suppliers and Petrobras, who have knowledge about the design of the Unit or system to be analyzed, or experience acquired in similar systems/Units. At least one representative from each discipline shall have at least 2 years of experience in the area they represent. Each discipline shall have a professional with this experience, not necessarily the same professional, for full-time participation during PHA.
Specialists	Professionals from the Designer, Suppliers or even Petrobras who have advanced knowledge about specific equipment, technologies or systems that can participate on demand, according to the need.

7. PLANNING

Prior to the PHA, a planning stage shall occur, when shall be defined 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 team involved, in accordance with item 6.

In addition, invitations shall be sent and all the documentation to be used shall be previously available to the participants.

The language for conducting and recording PHA meetings shall be defined.

During planning, all interfaces between systems shall be identified, which shall be included in PHA scope, to guarantee their integrated analysis.

8. METHODOLOGY

The PHA methodology shall follow the guidelines in Annex D of standard N-2782 (represented on Figure 1) and the aspects presented below.

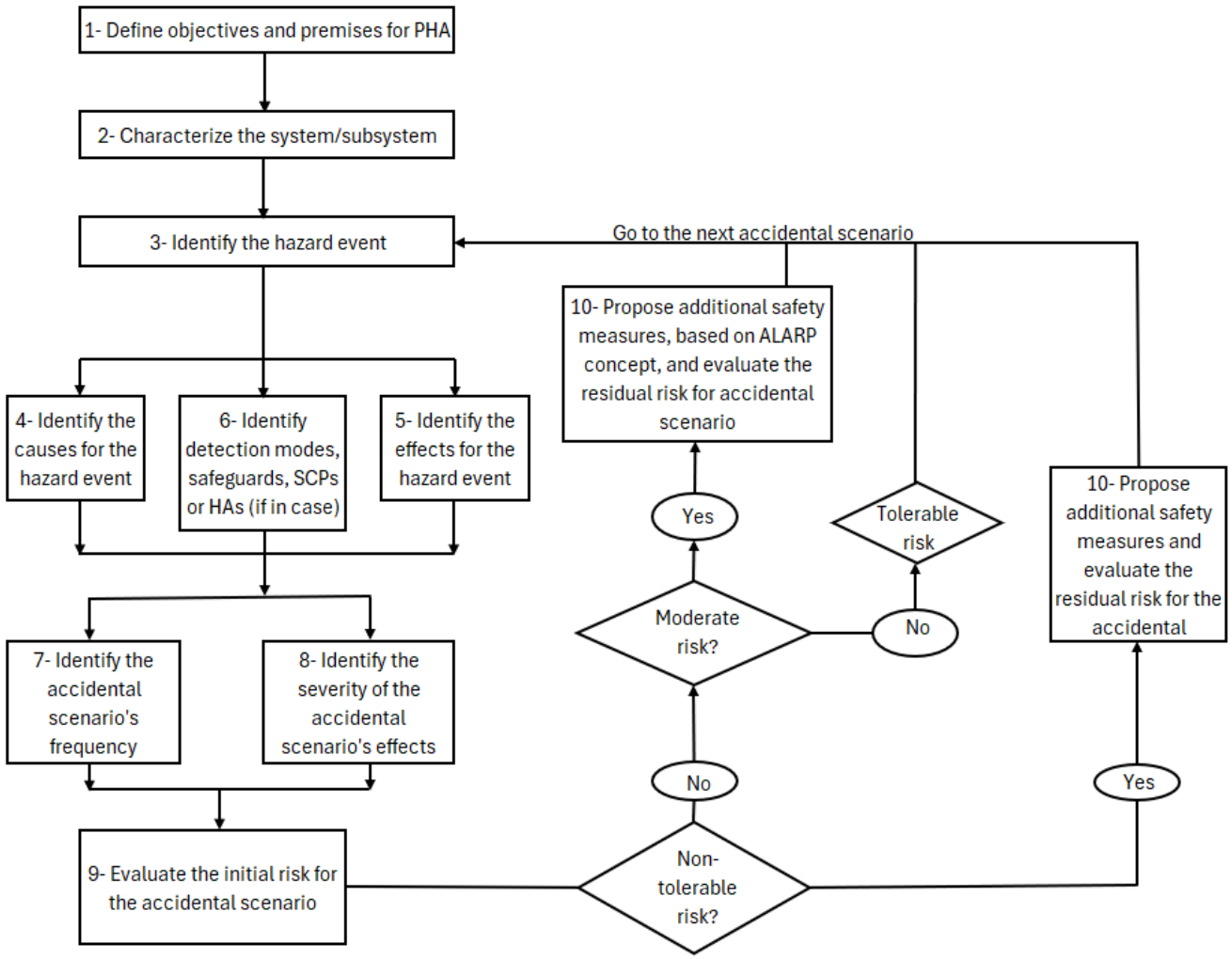


Figure 1: Flowchart with steps of PHA methodology (based on Annex D of standard N-2782).

8.1 Step 1 - Regarding the objectives and premises definition

This step consists of clearly defining the objective with the PHA application and the premises which will be considered along the analysis. The PHA shall consider:

a) All scenarios, observations and recommendations raised during the basic design shall be re-evaluated in the detailing design, considering the treatment given to the recommendations of the previous phases of the project. For the recommendations, which implementation is ongoing or incomplete, they shall be retained in the PHA review. In this case, the description of the recommendation shall reference the original recommendation number and the phase of the study to maintain traceability.

b) The documents of systems considered as a "package" shall be included in the documentation of the analysis in the detailing design phase, or in an earlier stage, if the "package" information is already available.

c) Hazards related to new technologies, unusual process conditions in the industry or unknown to the analysis team shall be evaluated considering the precautionary principle. This principle can be described as the adoption of special caution in cases of dangers linked to technical and scientific uncertainties in processes, technologies, or innovative operations, with little known impacts and little evaluated by previous risk analyzes. In addition, this principle must be observed when the associated risk cannot be assessed with sufficient confidence for decision making, depending on the level of uncertainty as to the possibility of undesirable events and harmful effects to people or environment.

d) All scenarios identified and recorded in the PHA spreadsheet shall have their risks categorized even if they have no impact on people, asset, or environment. This approach considers that the risk is composed of the combination of frequency and severity. Since there is a chance of the scenario occurring, the risk shall be categorized even if all severity dimensions are considered negligible.

8.2 Step 2 - Regarding the system/subsystem characterization

a) All systems of the Unit that have relevant hazards shall be included in the analysis. For those considered not relevant, the reasons for not including them in the analysis shall be technically justified through premise of the analysis.

b) The Unit shall always be divided into systems/subsystems, which shall be preferentially segregated by SDVs, being accepted other valves of remote automatic closure. The definition of each system/subsystem shall consider the change in fluid composition, fluid phase, or in module. The causes of the accidental scenario shall be identified within the system/subsystem, while the consequences should be identified inside and outside of the system/subsystem.

c) Consideration shall be given to the interfaces between Topside, naval systems (oil transfer, loss of containment at FPSO pump room, other marine systems which may be sources of hazards) and subsea systems (e.g., leakage between boarding SDV and riser balcony, considering the impacts of such leaks to the integrity of the Unit).

d) The analysis shall verify possible interfaces between analyzed systems and other modules / packages. Whenever this is not possible, depending on the design phase (e.g., documentation not available for a package systems), a premise shall be included in the analysis informing and technically justifying why the interfaces are not verified. In the case of the example, the premise shall inform that this analysis will be carried out in the next phase of the project.

e) The systems/subsystems selected for analysis shall be described on PHA spreadsheet and marked up on the related document (e.g., Process Plant

Overview, PFD, P&ID, etc.) in a manner that it is possible to easily understand what they include and exclude.

8.3 Step 3 - Regarding hazards events identification

a) The hazards events identified in the PHA shall be associated with loss of primary containment and be listed in the "HAZARD" field of the PHA spreadsheet. Examples of hazards events to be considered:

- Small release of flammable liquid (e.g., leakage on flanges, connections, etc.);
- Large release of flammable liquid (e.g., line rupture, equipment, etc.),
- Small release of flammable gas (e.g., leakage on flanges, connections, etc.),
- Large release of flammable gas (e.g., lines ruptures, equipment, etc.),
- Release of toxic gas or liquid (e.g., H_2S, CO_2, etc.),
- Release of substance under high temperature,
- Release of heated gases and vapors in inappropriate areas,
- Release of pressurized fluids,
- Presence of flammable mixture in the gas line,
- Small or large release of chemical product,
- Presence of substance subject to spontaneous combustion.

b) Deviations in process variables (e.g., higher/lower pressure, higher/lower flow, higher/lower temperature, etc.), and scenarios of contamination, reverse flow, and overpressure (higher pressure) in piping and equipment shall not be included as hazard of PHA. These deviations/scenarios shall be analyzed through the HAZOP technique.

c) Cargo transfer (dropped objects, load swing, etc.) shall not be considered as hazard event in PHA. Instead, it shall be considered as possible causes of large release of hazardous fluids (oil, gas, oily water, condensate, hot water, etc.) to assess the consequences of the accidental scenario, the safeguards, and the risk classification.

8.4 Step 4 - Regarding causes identification

a) For each identified hazard event, their respective causes shall be related. These causes can comprehend inherent failures of equipment (leaks,

ruptures, instrumentation failures, etc.), as well as human errors during execution, testing, operation, or maintenance activities.

b) PHA shall not consider causes that depend on the occurrence of two or more simultaneous events. However, these causes may be considered if there are reported accidental scenarios or if they lead to consequences of critical or catastrophic severity, as defined in N-2782.

c) Cancelled.

8.5 Step 5 - Regarding effects and accidental scenarios identification

a) For each hazard event identified on step 3, the possible consequences shall be listed without considering the existence of any safeguards. For example, for a hazard of small gas release, the possible effects could be fire and explosion, among others.

b) In the context of PHA, an “accidental scenario” is defined as a group formed by the identified hazard, its causes and each of its effects. An example of a possible accidental scenario would be large release of toxic substance (hazard) due to pipe rupture (causing) leading to the formation of a toxic cloud (effect) and causing damage to people, environment, asset and image (severity).

NOTE: In the context of PHA for Unit's design phase, the identified hazard is not related to operational tasks. These hazards shall be evaluated during the operational phase.

8.6 Step 6 - Regarding detection modes and safeguards identification

a) When the safeguard aims to reduce the frequency of occurrence of the accidental scenario, it will be considered as Preventive Safeguard (PS) and when it reduces the severity of the consequence, it will be considered as Mitigating Safeguard (MS). The safeguards in PHA are mainly related to the loss of primary containment, while the safeguards in HAZOP are mainly related to process deviations.

b) Human actions and procedures, such as use of personal protective equipment (PPE), following operating procedures, inspection/maintenance plans, emergency response plans, vessel approach protocols, monitoring environmental conditions, training program, etc., shall not be considered as safeguards to reduce the risks of the analyzed accidental scenario. Also, devices, systems, or actions applicable to outside the Unit’s boundaries, and specific information about an equipment, operation mode or system, shall not be considered as safeguards for the analyzed accidental scenario. Instead, they should be cited as observation of the accidental scenario if the PHA team deems as relevant.

c) Alarm that allows the response of the operator for the control action of the accidental scenario can be considered as safeguard. Other alarms shall only be considered as a detection mode.

d) An alarm with response from the operator shall be considered a safeguard under the following additional conditions:

- The alarm shall be generated in a location where the operator is present continuously (control point permanently assisted) and can recognize it,
- The alarm and the respective on-site response devices are independent of the initiating cause of the accidental scenario,
- The response time to the alarm shall be enough for the operator to take the actions planned to interrupt the scenario,
- The action taken is effective to minimize risk without exposing the responding operator.

e) To clearly identify elements regarding their function in the accidental scenario in the PHA spreadsheet, they shall be followed by indication letters, or separated and written in specific columns (for instance, a “detection mode” column and a “safeguards” column). The indication letters are the following:

- (D), to indicate a Detection mode,
- (PS), to indicate a Preventive Safeguard,
- (MS), to indicate a Mitigating Safeguard,
- (SCP), to indicate a Safety Critical Procedure,
- (HA), to indicate a non-safety critical procedure.

f) In cases of assisted operation, visual or auditory detections can be considered as effective detection modes.

g) All possible operation modes of the process plant shall be considered.

h) The following characteristics of the design project shall not be considered as safeguard, but included as an observation of the analyzed accidental scenario: redundancy of moorings, double hull, redundancy of equipment, etc.

8.7 Step 7 - Regarding frequency identification

According to the PHA technique, accidental scenarios shall be classified into frequency categories, which shall be estimated considering:

a) The frequency categories allow an assessment of the frequency of the accidental scenario and not of the initiating event.

b) To classify the frequency of the accidental scenario, the performance of existing or planned preventive safeguards shall be considered.

c) The frequency of accidental scenarios shall be classified according to the following Table 1.

d) In some situations, the frequency of the accidental scenario may be different, for example, in relation to people, asset or environment. In these cases, these scenarios shall be deployed and recorded on different lines.

Table 1: Frequency of accidental scenario.

A EXTREMELY REMOTE	B REMOTE	C NOT LIKELY	D PROBABLE	E FREQUENT
Conceptually possible, but with no references in the industry (never occurred worldwide).	Not expected to occur, although there are references in similar facilities in the industry (already occurred at least once worldwide).	Not likely of occurring during the lifetime of a group of similar units (already occurred at least once at Petrobras).	Possible of occurring once during the Unit lifetime.	Possible of occurring many times during the Unit lifetime.

8.8 Step 8 - Regarding severity identification

Each accidental scenarios identified shall be classified into severity categories that allow an assessment of the physical effects consequences' magnitude (over pressure, toxic concentration, thermal radiation, etc.) and provide a qualitative indication of the severity level regarding its consequences. Severity shall be estimated considering:

a) The presence of mitigating safeguards, existing or foreseen in the project.

b) The severity of the consequences shall be assessed for damages to people, assets, environment, and the image of the company's department responsible for the asset and Petrobras. For this categorization, the risk tolerance matrix presented in Table 2 of N-2782 and Annex I of the Safety Engineering Guidelines shall be used. The severity classification shall reflect what is described in the consequence or effect column.

NOTE: Depending on the objectives of the PHA, it may be unnecessary to consider all dimensions: personal safety, asset, environment, and image. In this case, a premise shall be issued for registering it.

8.9 Step 9 - Regarding risk evaluation

a) The risk analysis is performed via Risks Matrix (Table 2 of standard N-2782) through combination of the frequency and severity categories, which provides a qualitative indication of the risk level for each accidental scenario identified upon the analysis.

b) The risk level can be evaluated as “Tolerable”, “Moderate” or “Non-Tolerable”. The term “Non-Tolerable” may be replaced by the term "Intolerable" without prejudice for understanding. Adoption of measures is expected for each risk level to have the desired effect, as Table 3 of standard N-2782.

c) Cancelled.

d) The scenarios with a “Non-Tolerable” initial risk level, in any of the dimensions for people, assets, environment, or image, indicate that additional control measures and / or mitigating actions shall be adopted to reduce risks, so they shall have recommendations to reduce the residual risk level to “Moderate”. In general, “Non-Tolerable” scenarios should not have a procedure as the only recommendation proposed. In this case, the PHA team may discuss the possibility of proposing another recommendation, considering the ALARP concept.

e) The scenarios with a “Moderate” risk level, in any of the dimensions, indicate that additional control measures and / or mitigating actions shall be adopted to reduce risk, based on the application of ALARP (*As Low as Reasonably Practicable*) concept as per described on item 8.12.

f) The scenarios with a “Non-Tolerable” initial risk level, and "Moderate" initial risk level with severity categories “IV” and “V” for people and asset shall be evaluated by consequences analysis for the definition of protections to be adopted in the project (type of protection, quantity, location). In case of the gas dispersion analysis, all scenarios involving gas leakage shall be evaluated by this consequence analysis independently on the risk classification.

g) The PHA team, when identifying scenarios classified with severity “IV” and “V”, shall consult the existing consequence analysis of this project to verify if these scenarios are already quantitatively analyzed.

h) The scenarios with a “Non-Tolerable” initial risk level, and "Moderate" initial risk level with severity categories “IV” or “V” for people or environment or “V” for asset, which are associated to safety critical procedures (SCP) or human actions (HA), are considered as accidental scenarios associated with human factors and shall be evaluated by human reliability analysis for human errors identification and reduction.

i) In the final review of the PHA, before start of operation, the risk classification shall be revised considering the adoption of preventive or mitigating measures.

8.10 Step 10 - Regarding recommendations, additional comments, and notes

a) Recommendations are proposed measures to prevent the occurrence of the accidental scenario or mitigate its consequences whenever the existing safeguards are considered insufficient. The recommendations shall:

a. Seek to eliminate the scenario throughout solutions inherently safer,

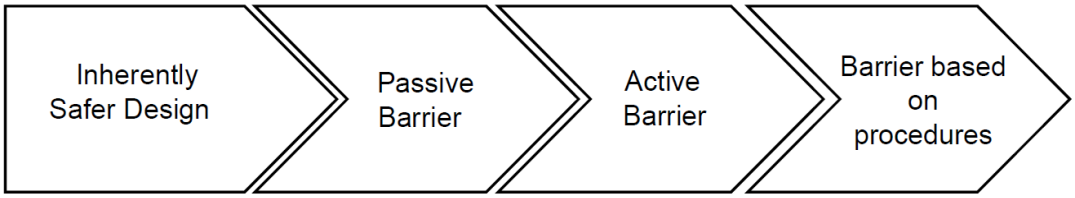
b. Seek to prevent the undesired events, reducing the probability of their occurrence,

c. Consider mitigation and control of the accidental scenario evolution, seeking to reduce the extent, duration, and magnitude of their consequences.

After the recommendation is proposed, PHA team shall check whether it reduces the frequency (chance of occurrence) of the event or mitigates their effects with the purpose of evaluate the recommendation effectiveness in risk reduction of the accidental scenario and estimate the residual risk.

NOTE: There may be an accidental scenario in which, even with a recommendation proposed, the residual risk remains the same of the initial risk. In this case, it is understood by PHA team that the recommendation is necessary to maintain the risk within the ALARP concept.

b) The PHA team shall consider the following hierarchy of barriers/protection layers for recommendations proposal:



c) Recommendations shall be clear, concise, well-defined, and preceded by action verb, so that whoever reads it understands what they should do. Terms such as plan, design, elaborate, identify, specify, install, etc. shall be complemented by conclusive actions.

d) For each recommendation originating from the PHA, the company or organization responsible for its implementation shall be identified. The planning and management of recommendations shall consider the risks classification for the definition of their prioritization.

e) The designer shall manage the implementation of these recommendations generated in the analysis, including the impact on the revision of reference documents used in the PHA. If any recommendation is not implemented, or an alternative solution is indicated, it shall be justified and submitted to Petrobras' approval.

f) For pre-operational PHA, the recommendations resulted from other risk analyses/studies along the project, and which are confirmed as implemented shall be considered as safeguards of the current PHA and registered on “safeguard” column as preventive (PS) or mitigating (MS) safeguard as per item 8.3 of this TS.

g) Interfaces identified during the execution of the analysis that depend on the analysis in another system/subsystem shall be recorded as recommendations of PHA for future verification.

h) Observations are complementary information that can be recorded to clarify the scenario analyzed, without, however, requiring any action. They can be used to justify, for example, the criteria or considerations adopted by the PHA team to estimate a certain frequency or severity category for the accidental scenario. The text of the observations shall not be written with action verbs, such as "should", "must", "shall", etc. If there is a need for an action, it constitutes the need for a recommendation and nor an observation.

i) Whenever a Human Action (HA) or a Safety Critical Procedure (SCP) were listed on the “safeguards” column of an accidental scenario, an observation shall be registered informing that the respective accidental scenario is associated to human factors and will be evaluated within a human reliability analysis.

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

k) The PHA recommendations will be identified as Rxxx, the observations will be identified as Oxxx, and the additional comments will be identified as Cxxx, where xxx corresponds to the sequential numbering.

8.11 Regarding the identification of Safety Critical Procedures (SCPs) and Human Actions (HAs)

a) The Safety Critical Procedures (SCPs) are the procedures listed in accidental scenarios classified as “Non-Tolerable” initial risk level, or “Moderate” initial risk level with severity category “IV” or “V” for people or environment, or “V” for asset (“accidental scenarios associated with human factors”).

b) Considering the project’s procedures are elaborated and issued at the end of detailing phase, the procedures identified and listed in accidental scenarios, throughout the analysis, shall not be considered as preventive or mitigating safeguards.

c) When a SCP is identified as related to an accidental scenario associated with human factors, the operations representative shall indicate an existed procedure to be considered as reference for the project’s human reliability analysis. The reference procedure shall be registered in the safeguard column and indicated as “(SCP)”, as per described on item 8.6.e of this TS, and a recommendation shall be registered to project elaborate its own procedure at the end of detailing phase and classify it as safety critical procedure.

d) When a procedure is indicated in an “accidental scenario associated with human factors” and there is no existed procedure to be considered as

reference for the project's human reliability analysis, it shall be registered in the safeguard column and indicated as "(SCP)", as per described on item 8.6.e of this TS, and two recommendations shall be registered to the project: (i) elaborate at basic design a proposal of procedure, including tasks sequencing and responsibilities, for the human action to be evaluated on the project's human reliability analysis; and (ii) elaborate its own procedure at the end of detailing phase and classify it as safety critical procedure.

e) As output of PHA, it shall be issued a List of Safety Critical Procedures (SCPs) which will be used as input to the project's human reliability analysis.

f) When a procedure is indicated in an "accidental scenario non-associated with human factors", it should be registered at safeguard column and indicated as "(HA)", as per described on item 8.6.e of this TS, since it is a non-safety critical procedure. In this case, no recommendation is required to be registered to the project and this procedure shall not be part of the List of Safety Critical Procedures (SCPs) which will be used as input to the project's human reliability analysis.

8.12 Application of the ALARP Concept in PHA

a) It is recommended, as good practice, the application of ALARP concept in qualitative and quantitative risk analyses with the purpose of risk reduction to a level as low as reasonably practicable through the adoption of proper preventing and control measures, when additional measures for risk reduction are disproportionally expensive if compared to their benefits.

b) This concept shall be applicable only to the scenarios classified as "Moderate" initial risk level, because all scenarios with "Non-Tolerable" initial risk level shall be reduced to lower risk levels.

c) The ALARP concept includes the following four concepts:

1. Good Practice - adoption of good practices can serve as an appropriate indicator to demonstrate that the ALARP region has been achieved. However, it should be emphasized that "good practice" evolves over time, requiring updates by risk study and project teams due to the need for continuous improvement.

2. Precautionary Principle - it can be described as exercising special caution in cases involving hazards linked to technical scientific uncertainties in innovative processes, technologies, or operations with little known and assessed impacts on HSE (Health, Safety, and Environment). This principle should be observed when the associated risk cannot be confidently assessed for decision making due to the level of uncertainty regarding the possibility of undesirable events and detrimental effects on people or the environment.

3. Disproportionate Effort - if a measure is feasible and the implementation effort is not considered disproportionate to the benefit of risk reduction, then the measure will be considered "reasonably practicable", and its implementation is recommended.

4. Inherently Safer Process - it applies to a design or process in which risks associated with it are reduced or eliminated by incorporating one or more of the following principles: substitution, minimization, simplification, and moderation. Examples include:

   - Substitution: using aqueous solvents instead of organic ones and employing safer chemical routes.

   - Minimization: reducing the use, storage, and transport of hazardous substances.

   - Simplification: using fewer complex systems with lower failure rates and greater error tolerance.

   - Moderation: reducing process severity or criticality, diluting reagents, and using cooling to lower the pressure of stored products.

d) The questions which are potentially applicable along the qualitative analysis are:

   - Was the "Good Practice" principle applied?

   - Was the "Precautionary Principle" applied when relevant?

   - Was the "Disproportionate Effort" principle applied?

   - Was the "Inherently Safer Process" principle applied?

e) For scenarios with “Moderate” initial risk level, that the analysis team has not suggested any additional risk reduction measures, the following sentence shall be included as scenario’s observation: “During the evaluation of the present scenario, the concepts of Good Practice, Precautionary Principle, Disproportionate Effort, and Inherently Safer Design were considered”. The observation shall only mention concepts that are relevant and applicable to the scenario and shall be mentioned only concepts that were assessed by the team during the analysis.

9. REQUIREMENTS FOR PHA MEETINGS

Meetings shall follow as described below:

9.1 Planning Meeting

The scope of this meeting is to summarize the project to be assessed, 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 PHA Consulting, where the minimum agenda shall be:

- Define Petrobras, designer, and executor of PHA teams (preparation of list of participants to issue invitations),
- Clarifications on objectives and scope of the analysis,
- Prior analysis of all necessary documentation for the execution of the PHA and elaboration of hold list, if any, to be completed by the Designer,
- Presentation of proposal meetings schedule by the PHA Consulting and evaluation regarding the project schedule,
- Definition of locations, resources needed and duration of meetings,
- Participants: Representatives of Petrobras, designer and PHA Consulting (mandatory participation of the PHA leader).

9.2 Initial PHA meeting and others study development meetings

At the initial PHA meeting, the Leader shall address the following topics:

- Safety briefing,
- Participants presentation,
- Presentation of analysis objective and scope,
- Presentation of the meetings schedule,
- Brief presentation of the methodology and premises,
- Short description of the Unit,
- Presentation of a summarized historical analysis of incidents occurring in the Unit or others similar installations,
- Description of the systems to be analyzed,
- Assumptions/premises to be considered throughout the analysis.

The others PHA meetings shall address the following topics:

- Presentation of new participants, if any,
- Description of the systems to be analyzed,

- Additional assumptions/premises to be considered throughout the analysis.

Participants: Professionals from Petrobras, designer and PHA Execution (including the PHA Leader), as defined in item 6 of this TS.

10. PHA REVIEW

The PHA shall be reviewed in the following cases:

- At each project phase,
- When there are changes in the project that led to new accidental scenarios and/or change the risks previously considered. This analysis shall be carried out by the Project Designer with the participation of Petrobras,
- When Petrobras detects systemic or critical deviations from reports in relation to this specification,
- In the pre-operation phase; and during operation, according to Petrobras's safety management standards.

11. REPORT CONTENT

The PHA Report shall include at least the following items:

1. Purpose and scope of the analysis

Description of the objectives, 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, position, contact email, project discipline representing and time of experience in it).

A daily presence list shall also be generated.

3. Executive summary

4. Introduction

The introduction shall contain the description of the Unit, description of the analyzed systems, considering modes of operation, and any relevant aspects related to the analysis.

5. Justification and description of the PHA technique

6. List of documents

All the documents that were used for the analysis with their respective revisions shall be listed.

7. Historical Analysis

Evidence shall be presented that the occurrence of accidental scenarios in similar units, especially Petrobras, with the respective Reports of Treatment of Anomalies (RTA), when applicable, were used for definition of scenarios and classification of their frequency. National and international database events can be used, considering the applicability of the data to the project (facility type and complexity, sea conditions, modes of operation of the unit / equipment, etc.).

The historical analysis shall be presented to all participants on the first meeting day, before the start of PHA, and shall be registered through a document with a code that allows traceability and be attached to the PHA report.

References that can be used to elaborate the historical analysis:

a) Hydrocarbon Release Data Base (HCRD - HSE);

b) WOAD - World Offshore Accident Database - https://www.dnvgl.com/services/world-offshore-accident-database-woad-1747;

c) Report Blowout and Well Release Characteristics and Frequencies, 2014 - SINTEF Technology and Society - Safety Research 2014-12-30;

d) Accident Statistics for Floating Offshore Units on the UK Continental Shelf 1980-2005. HSE Research Report RR 567 2007;

e) Process Release Frequencies, IOGP Report 434-01, 2021;

f) Accident Statistics for Fixed Offshore Units on the UK Continental Shelf 1980-2005, HSE Research Report RR 566 2007 - http://www.hse.gov.uk/research/rrhtm/rr566.htm;

g) Reports of Treatment of Anomalies (RTA) from Petrobras;

h) ANP Incidents Database - https://www.gov.br/anp/pt-br/assuntos/exploracao-e-producao-de-oleo-e-gas/seguranca-operacional/incidentes.

8. Analysis Development

9. Assumptions/premises defined for the analysis.

10. Information on the hazardous substances involved;

In this item, shall be reported which hazardous substances involved in the analysis (those in which the loss of containment resulted to the scenarios analyzed). The

characteristics and risks that such substances may offer to people, asset and environment shall be identified.

11. List of recommendations

It shall be presented in a table to allow management of the implementation of the recommendations. It shall be listed in this table the corresponding scenario number(s), the department responsible for each recommendation and the implementation phase.

12. List of observations

It shall be displayed in a table, with the corresponding accidental scenario number.

13. Table of Safety Critical Procedure (SCP)

The SCPs identified along the analysis shall be displayed in a table, with the corresponding accidental scenario number. In case of SCPs which have a reference procedure related, the table shall also present the number of the reference procedure listed on PHA spreadsheet.

14. Additional considerations

These shall be presented in a table along with the identification of those responsible.

15. Conclusions

It shall contain, at least, the following information:

a) Total systems and scenarios evaluated;

b) Total of scenarios classified as Tolerable, Moderate and Not Tolerable, considering the aspects people, asset, environment and image;

c) Total number of recommendations and observations;

d) Identification of interfaces between Naval and Subsea disciplines, indicating the PHA scenarios in which such interfaces were analyzed. The studies of Naval and Subsea disciplines that also contain analysis of these interfaces shall be related, when applicable.

e) Statistics of the scenarios for each aspect considered (people, asset, environment, and image).

f) Identification of scenarios for elaboration of safety critical elements list:

- All the safeguards of scenarios classified with severity IV and V for dimensions People and Environment; and severity V for Image and Asset shall be considered as safety critical elements. After consolidating the critical elements of the PHA scenarios, the safety critical elements list may be complemented by other

elements defined by technical criteria or other analyzes that identify other safety functions relevant to the Installation.

- The elements are considered critical when essential to prevent or mitigate risks or, in case of its failure, it may cause or contribute to the occurrence of an operational accident.

g) Total of Safety Critical Procedures (SCPs) and the “accidental scenarios associated with human factors” identified during the PHA and which will be evaluated in the project’s human reliability analysis.

16. References used in the analysis.

17. ANNEXES

A. Filled out PHA spreadsheet

All completed worksheets shall be presented, as shown in Figure D.2 of N-2782. The scenarios shall be numbered to facilitate their identification, considering that scenarios related to different systems of the Facility cannot have the same numbering. They shall be identified as "SS.XXX", where "SS" is the PHA subsystem and "xxx" refers to the sequential numbering."

B. Documents analyzed

An annex shall be included in the report with all analyzed P&IDs, including their identified and highlighted segments, among other relevant documents.

C. Presence list.

The daily presence lists shall be attached. The lists shall inform which systems were analyzed at each meeting.

D. List of Barriers.

A list of barriers shall be annexed to the final report, which lists their respective safety barriers for each of the accidental scenarios and classifies them as preventive or mitigating barriers.