PETROBRAS	**TECHNICAL SPECIFICATION**	**Nº:** I-ET-3000.00-5400-947-P4X-008	
	CLIENT:		**SHEET:** 1 of 35
	JOB: -		-
	AREA: -		-
SRGE	**TITLE:** **BOW-TIE ANALYSIS**		INTERNAL
			ESUP

MICROSOFT WORD / V. 2016 / I-ET-3000.00-5400-947-P4X-008_A.DOCX

INDEX OF REVISIONS

REV.	DESCRIPTION AND/OR REVISED SHEETS
0	ORIGINAL
A	REVISED WHERE INDICATED

	REV. 0	REV. A	REV. B	REV. C	REV. D	REV. E	REV. F	REV. G	REV. H
DATE	28/12/2023	JUL/22/2024							
DESIGN	ESUP	ESUP							
EXECUTION	B79G	B79G							
CHECK	ABKC	ABKC							
APPROVAL	CMH4	EK9U							

SUMÁRIO

1. INTRODUCTION

The Bow-Tie Analysis (BTA) is a diagram that shows how various threats can lead to a loss of control of a hazard and allow this unsafe condition to develop into several undesirable consequences.

The diagram is able to show all the barriers and degradation controls deployed.

Its presentation in the form of a diagram has the advantages of facilitating the communication of accident scenarios, presenting the definition of roles and responsibilities of those who operate and maintain the barriers, and facilitating risk management in cases of barrier degradation.

In the execution of BTA, the requirements of the National Agency for Petroleum, Natural Gas and Biofuels – ANP and Safety Engineering Guidelines - DR-ENGP-M-I-1.3 shall be complied with.

2. PURPOSE

This specification has the following objectives:

2.1 Define scope and criteria for conducting BTA for project phases of 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 parties involved and final approval thereof.

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

3. ABBREVIATION

ANP – *Agência Nacional do Petróleo, Gás Natural e Biocombustíveis* (National Agency for Petroleum, Natural Gas and Biofuels)

BDV – Blowdown valve

BT - Bow-Tie

BTA - Bow-Tie Analysis

CCTV – Closed-circuit Television

CCS - Call Conversion Station

C&E M - Cause and Effects Matrix

FCV – Flow Control Valve

FWP – Firewater Pump

HAZOP – Hazard and Operability Study

HPU – Hydraulic Power Unit

HVV - High Velocity Vent

LOPA - Layers of Protection Analysis

LOPC - Loss of Primary Containment

LPS - Lightning protection system

MOC – Management of Change

PCV – Pressure Control Valve

P&ID - Piping and Instrumentation Diagrams

PHA - Preliminary Hazard Analysis

PLC - Programmable Logic Controller

PSV – Pressure Safety Valve

SDV – Shutdown valve

SIGEM - *Sistema Integrado de Gerenciamento de Empreendimentos* (Integrated Enterprise Management System)

SOPEP – Ship Oil Pollution Emergency Plan

TS – Technical Specification

TSL - Telephone Signaling Lamp

UPS - Uninterruptible Power Supply

4. ESCOPE

4.1 The BTA analysis shall cover hazardous events from the Unit's reference Preliminary Hazard Analysis (PHA), HAZOP and LOPA (if applied), according to

the definition of relevant process safety accidental scenarios presented in the DR-ENGP-M-I-1.3.

4.2 The categories of severity and risk mentioned in the criterion presented in the DR-ENGP-M-I-1.3 consider the initial risk, i.e., the one estimated considering the safeguards and without considering the recommendations. Safeguards recommended by risk studies shall be included in the BT diagram once implemented.

4.3 The final BT shall consider all the recommendations from risk studies implemented.

4.4 General

4.4.1 The final BTA report shall be issued in English and Portuguese (Brazil), according to the specified in contractual documentation.

4.4.2 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.

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

4.4.4 The Project Designer is responsible for searching and obtaining all information necessary to carry out the BTA 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.

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

4.4.6 The final BTA report shall be submitted to formal approval by Petrobras.

5. DEFINITIONS

5.1 Accidental Scenario - An accidental scenario is the description of a risk event related to the operation, activity, or material with the potential to cause injury to people, damage to asset, impact to the environment, or to the image of the Company. Each scenario is associated with an analysis of the possible causes and consequences of the undesirable event.

5.2 Top Event - In the Bow tie, the top event is a central event situated between a threat and a consequence corresponding to the moment when there is a loss of control or loss of containment of the hazard.

5.3 Threat - A threat is any action or condition that, in isolation, has the potential to initiate an accidental scenario, loss of control or containment of a hazard.

5.4 Consequences - undesirable results of an accidental scenario, which may affect people, asset, environment and image of the Company.

5.5 Safety Barriers - A control measure, or grouping of control elements that, on its own, can prevent a threat from developing into a relevant process safety accidental scenario (prevention barrier) or can mitigate the consequences of a relevant process safety accidental scenario after it has occurred (mitigation barrier).

5.6 Escalation Factor - Escalation factor is a situation, condition, defect or error that compromises the function of a barrier through any loss or reduction of its effectiveness, i.e., leading to insufficient and unwanted performance. If a barrier degrades, then the associated risks can increase or escalate.

5.7 Escalation Factor Control - It is a measure that helps prevent the degradation factor from harming or degrading the barrier. It is also called the Escalation Control Requirement, as it refers to the measures and controls, especially management, implemented to eliminate or reduce actions and omissions that can degrade preventive and mitigating barriers.

5.8 Barrier Management - It is a systematic management process that monitors the Integrity and Reliability of the Preventive and Mitigating Barriers of Process Safety, defining responsibilities for this management in order to ensure that the integrity requirements of the barriers are met and thus ensure that the scenarios are in the risk categories mapped in the risk analyses in the preparation of the bow ties.

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

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

6. REFERENCE DOCUMENTATION

6.1 As inputs for the elaboration of BT diagrams, the following documents shall be considered, in its most 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. The revision of each document to be used shall be clearly indicated in the analysis report.

a) PHA;

b) HAZOP;

c) LOPA – if applicable;

d) P&ID;

e) Cause and Effects Matrix

f) Safety Plans

g) Close Out Reports

h) Critical Items List

i) Fire and Gas Layout

j) Passive Protection Documents

k) Any other risk analysis reports already performed for the Unit, including those carried out for hull systems and subsea systems – if applicable.

6.2 In case some of the documents cited above are not available, Petrobras shall be consulted about its relevance to the preparation of the study.

6.3 Petrobras can provide any other document, if necessary and requested.

6.4 Item 14.2 brings some clarification upon each barrier and related documentation.

7. REQUIREMENTS FOR THE PARTICIPATING TEAM DEFINITION

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

7.1 The BT diagrams shall be evaluated by a multidisciplinary team composed of 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: process, instrumentation/automation and control, process safety, mechanics, electrical, ergonomics/human factors, operation, maintenance naval* and subsea* systems.

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

7.2 The professional from Process Safety shall have knowledge in BTA methodology.

7.3 The analysis leader shall have formal training in the BTA tool and the BTA leadership activity.

7.4 The defined BTA team shall have composition, function and attributions performed as follows:

Table 1 - Basic composition of the BTA 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.
BTA Leader	Professional of the BTA Consulting who knows the technique, responsible for: • comply with the schedule of planned meetings; • explain the technique to be employed to the other participants, facilitate meetings and define its progress status; • ask participants for pending from the previous meetings; • prior evaluation of the documentation to be used in the analysis, defining the bow-tie diagrams 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 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 BTA.
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.

8. PLANNING

Prior to the BTA, 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 7.

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

The bow-tie diagrams shall be populated previous to the meetings.

9. METHODOLOGY

The BTA methodology shall follow the aspects presented below:

9.1 Regarding the accidental scenarios:

a) Information for the construction of the Bow Tie diagram shall be obtained from APR, HAZOP and LOPA studies (if any).

b) The relevant process safety accidental scenarios to consider are those involving physical effects of overpressure, thermal radiation, toxic or flammable releases, whose initial risk categorizations for the "People" or "Asset" dimensions are classified as Moderate in severity categories IV or V, or Non-Tolerable, according to the Risk Tolerability Matrix of DR-ENGP-M-I-1.3.

c) In a bow-tie type structure, the cause-consequence-safeguard information needs to be completely aligned with the hazard being considered. The categorization of risk is different depending on the cause-consequence pair, as each cause will generate a specific final consequence, challenging existing barriers.

d) The PHA has the information of the Consequences of a Top Event and the Mitigating Barriers, associated with a hazard or hazardous event.

e) HAZOP has the information of the Threats of a Top Event and the Preventive Barriers.

9.2 Regarding bow-tie diagrams construction:

a) Initially, the PHA and HAZOP scenarios shall be selected according to the criteria in item 9.1.

b) Next, an APRxHAZOP Scenario Association table is generated to map the Bow tie diagrams.

c) Prepare bowtie diagram(s) / safety barrier management for the highest risk scenarios (relevant process safety accidental scenarios) for the Unit, identifying the hazard (system) in question, top event, threat, escalation factors with their respective requirements/controls of escalation factors, the barriers (with their respective elements and requirements) and the consequences.

9.3 Regarding barriers classification

Characterize the preventive and mitigating barriers according to the criteria defined by Petrobras (B1 to B10 presented in item 14 - ANNEX)

9.4 Regarding elements identification

Identify the elements that constitute each safety barrier from the risk analysis and referenced documentation (e.g. Risk Analysis (PHA, HAZOP and LOPA, this one when available), List of Critical Elements and other project documents such as

Safety Plan, P&IDs and Plans of deluge/fire suppression systems, Cause and Effect Matrix, Fire and Gas Layout, Passive Protection Documents, Ex Equipment List (Area Classification Documents), Gas Dispersion Study, Dropped Object Study, Drainage System Documents, among others.

10. REQUIREMENTS FOR BTA MEETINGS

Meetings shall follow as described below:

10.1 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 BTA Consulting, where the minimum agenda shall be:

- Define Petrobras, designer and executor of BTA 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 BTA and elaboration of hold list, if any, to be completed by the Designer;
- Presentation of proposal meetings schedule by the BTA Consulting and evaluation regarding the project schedule;
- Definition of locations, resources needed and duration of meetings;
- Participants: Representatives of Petrobras, designer and BTA Consulting (mandatory participation of the BTA leader).

10.2 BTA meetings

At the initial BTA 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;
- Assumptions/premises to be considered throughout the analysis.

For the regular meetings, Leader shall address the following topics, as a minimum:

- For each relevant process safety accidental scenario, threats, barriers, top event and consequences shall be presented to provide an overview.
- For each threat, barriers, critical elements, escalation factors and escalation controls shall be validated and confirmed.
- For each consequence, mitigation measures, critical elements, escalation factors and escalation controls shall be validated and confirmed.

– After all escalation factors and controls have been discussed, determine if any shortfall exists for the relevant process safety accidental scenario. Recording of action items as determined by the workshop team.

11. BTA REVIEW

The BTA shall be reviewed in the following cases:

– When there are changes in the project that lead 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.

– After the implementation of risk study recommendations that generate new safety barriers to the mapped scenarios.

– After review of the risk studies that were used in the construction of the BT.

– 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.

12. SOFTWARE

The workshop discussions shall be undertaken using illustrative bow ties generated from a bow tie tool. The software to be used shall be validated with Petrobras before the beginning of the BTA.

All information generated in BT shall also be available in spreadsheet, to manage the implementation on the system.

13. REPORT CONTENT

The BTA Report shall include at least the following items:

a) Purpose and scope of the analysis;

Description of the objectives, the scope covered by the analysis, and the structure of the report.

b) 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.

c) Executive summary

d) 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.

e) Justification and description of the BTA technique

f) List of documents

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

g) Analysis Development

h) Assumptions/premises defined for the analysis.

i) List of action items / recommendation (if applicable)

j) List of observations: It shall be displayed in a table, with the corresponding scenario number.

k) List of critical elements

l) A load sheet of elements by barriers/bow ties/threats/consequences shall be generated with the respective installation location.

m) Conclusions

It shall contain, at least, the following information:

- Total number of top events/BT diagrams evaluated.
- Total number of scenarios mapped, according to the above criteria, per risk study.
- Total number of recommendations and observations.
- Identification of interfaces between Naval and Subsea disciplines (if applicable).

n) References used in the analysis.

o) ANNEXES

A. APR x HAZOP Scenario Association table

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 Classified Barriers.

E. Elements sheet: the spreadsheet mentioned in item 13, letter l).

14. ANNEX

14.1 BARRIERS CLASSIFICATION

A list of classified barriers shall be annexed to the final report, according to the Table 2 below. The list shall have the correlation of safety barriers and the respective accidental scenarios.

Table 2 – Barriers, systems and elements

Barriers		Systems	Elements
Preventive Barriers	Barrier 1 (B1)	Primary Containment	Static and dynamic equipment, piping, connections and instruments.
	Barrier 2 (B2)	Basic Process Control	Automatic process controls, equipment form supervisory control, its components and source of power.
	Barrier 3 (B3)	Alarms and Human Intervention	Instrumentation related to process' alarm referred in operational procedures, source of power and qualified operator.
	Barrier 4 (B4)	Safety Interlock	Instrumentation / automation system components, final elements and source of power.
	Barrier 5 (B5)	Relief Systems	Mechanical relief devices, flare system.
Mitigating Barriers	Barrier 6 (B6)	Post-release Protection System - ESD	Comprises the passive mitigation elements and the elements that detect and mitigate automatically the consequences related to the top event, reducing the inventory released.
	Barrier 7 (B7)	Control of ignition sources	Comprises the elements that shall have integrity requirements not to become ignition sources.
	Barrier 8 (B8)	Operational Emergency Response	Operational maneuvers that mitigate or limit the consequences of the top event, equipment needed to those maneuvers and qualified operator.
	Barrier 9 (B9)	Brigade Emergency Response	First actions taken, as defined at Emergency Response Plan, equipment, inputs necessary to those actions and brigade members.
	Barrier 10 (B10)	Evacuation, Rescue and Abandonment	Last actions of Emergency Response Plan, equipment and qualified people.

14.2 Elements for each barrier

Barrier 1 (B1) - Primary Containment

Purpose or Safety Function: To ensure the containment of process fluids and to guarantee that the process fluid design requirements within process conditions.

This barrier is related to the integrity of the equipment, pipes and valves present in the pipe section. It considers the quality of the project, capacity parameters, materials used, equipment sizing, and equipment integrity status.

Element:

- The installation site of pipes and dynamic or static primary containment equipment related to the mapped scenarios shall be considered in this Barrier, according to the respective threats.
- For Hazop process deviations, in which higher or lower pressure occurs, if possible, include only the equipment and piping affected by the process deviation.

Points of Attention and Additional Clarifications

- The elements (equipment, pipes and valves) of this barrier shall be considered according to the expected threat of the scenario. Therefore, for the causes of loss of containment identified in the PHA, the equipment, pipes and valves of the entire section of the PHA shall be mapped. For Hazop threats, if possible, only the section that will be affected by the process deviation and that may generate the loss of containment should be considered, even if it covers areas beyond the analyzed system.

- Identify the TAG of piping present in the section (for the causes foreseen in PHA). Try to locate the piping in SAP; if it does not exist, contact the support area responsible for the SAP tree.

- For the threats of dropped objects, sections of pipe and equipment that are unprotected (that are directly under the reach of the crane and may suffer the impact of the fall) shall not be included as Barrier 1, since they are not designed to withstand the impact of collision and/or dropped objects.

Barrier 2 (B2) - Basic Process Control

Purpose or Safety Function: Perform the automatic control of the process, through the detection of deviation of process variable and command in valves or other control elements, in order to keep the process within the conditions foreseen in the project.

Element:

- For Barrier 2, as three basic functions are assumed (detection; decision; action) for the Barrier to be effective, the TAGs and/or installation location shall be considered: of the sensor elements (which identify the deviation of the process); of the elements responsible for the "decision" (when it involves a Control PLC or other decision-making or action mechanism); of the final element actuated; in order to fully comply with the concept of Barrier.
- The control loops that are the cause of the process deviation shall not be considered in this Barrier.

Points of Attention and Additional Clarifications

- In the case of MOC that foresees the mirroring of control in the safety interlock loop (as may occur in case of degradation/unavailability of the control loop), the elements of the Interlock loop to which this function have been assigned shall have their statuses also impacting Barrier 2. The temporary adjustment shall be made on the tool for the duration of the mirroring. This aspect shall be considered during operation with the tool by the Monitoring Team. In the preliminary stage of Bow Ties Elaboration, this condition shall be considered only if the Management of Change is Permanent.

- Warnings associated with the autoresponder control loop shall not be included in Barrier. In case of alarms to which there is an established response procedure, these alarms, as well as the associated procedures, shall be considered in Barrier 3.

Essential and Emergency Electrical Power Generation, Storage and Distribution Systems (*)

Purpose or Safety Function: Ensure the supply of energy to essential and emergency consumers in situations that require the action of barriers.

Elements:

- UPS Essential Power System Load delimiters and circuit breakers
- Emergency Loads System UPS
- Emergency System battery banks
- Emergency loads system distribution panels

Points of Attention and Additional Clarifications

- (*) The system for the generation, storage and distribution of essential and emergency electrical power shall be provided whenever there are elements in the barrier that depend on energy sources. If there are only passive elements in the barrier, the elements of this system shall not be provided for.

Barrier 3 (B3) - Alarms and Human Intervention

Purpose or Safety Function: Alert the operation that there has been a deviation of a process variable and that human action is necessary to return to normal conditions (return the process to the operational range) foreseen in the project.

Elements:

- The sensors elements (XT/XIT, XSH-HH / XSL-LL - where X represents the process variable) that are sensitized as a result of the process deviation (Preventive Barrier) and that have operational response procedures associated with them.
- The Procedure associated with the actuated sensor element, in which the actions that shall be performed by the operation in response to the process deviation are established.
- The actuated end element (manual valve, pushbutton, etc.), as set out in the Associated Procedure.
- Procedures indicated by the Unit (*).

Points of attention and additional clarifications:

- The sensors or final elements associated with the control loops that are the cause of the process deviation shall not be considered as a barrier.

- Warnings associated with the autoresponder control loop shall not be included in Barrier. In case of alarms to which there is an established response procedure, these alarms, as well as the associated procedures, may be considered in Barrier 3.

- (*) In the case of procedures associated with the threat (e.g., the threat of dropped loads and the procedure related to the mechanical handling), these procedures may be provided for in this Barrier 3, even if dissociated from alarm, when the training is sufficient to be considered as barrier (human response to circumstances that could lead to a deviation and/or accident). The Unit shall provide a spreadsheet with the procedures that will be monitored in the barrier management, indicating the respective scenarios and applicable barriers, as well as the criteria (integrity rules, such as OP1, OP2, etc.) to which they refer.

<u>HC Blanketing System</u>

Elements:

- Procedures and set of sensors elements and final elements actuated for the release of cargo tanks for inspection and return to operation.

Points of attention and additional clarifications:

This system is being considered in Barrier 3 in the case of alarms and procedures that require intervention of the operation.

Essential and Emergency Electrical Power Generation, Storage and Distribution Systems (*)

Purpose or Safety Function: Guarantee energy supply for essential and emergency consumers in situations that require the action of barriers.

Elements:

- UPS Essential Power System Load delimiters and circuit breakers
- Emergency Loads System UPS
- Emergency System battery banks
- Emergency Loads System distribution panels

Points of attention and additional clarifications:

- (*) The system for the generation, storage and distribution of essential and emergency electrical power shall be provided whenever there are elements in the barrier that depend on energy sources. If there are only passive elements in the barrier, the elements of this system shall not be provided for.

Barrier 4 (B4) - Safety Interlock

Equipment shutdown (ESD-1) or Process shutdown (ESD-2) subsystems

Purpose or Safety Function: (according to DR-ENGP-M-I-1.3):

(ESD-1) Ensuring the shutdown of an equipment or part of a system due to some deviation in the normal operation of the equipment or system.

(ESD-2) Ensuring the total process shutdown without affecting the Unit's utility areas. Occurs when a process variable, such as pressure, temperature, level, exceeds the design limits.

Elements:

- Sensors and interlock switches that generate ESD-1 listed as a preventive safeguard in the reference study (Hazop).
- Final actuation elements triggered in ESD-1 (as per Points of Attention below).
- Sensors and interlock switches that generate ESD-2, listed as a preventive safeguard in the reference study (Hazop).
- Final actuation elements triggered in ESD-2 (SDV, BDV, etc.), according to the Cause and Effects Matrix (C&E M).
- Associated PLC.
- High Integrity Pressure Protection System (HIPPS), when foreseen – Consider all elements of the protection system.

Points of attention and additional clarifications:

- The updated C&EM of the facility shall be considered to identify what is effectively in terms of loop, in order to verify whether it is a preventive or mitigating loop, and the final elements actuated and necessary to prevent the development of the chain of events.
- Only the loops associated with the Safety PLC shall be considered in Barrier 4. If the loop is associated with the Control PLC, even if it is a "mixed" PLC (as, for example, occurs in Packages, where the control and safety loops are in the same PLC), the loop, the PLC and the final elements shall be considered in Barrier 2.
- When an interlock causes a compressor or pump to stop, the final element to be considered for monitoring purposes will be the electrical panel associated with the equipment, which electrically supplies it and performs command functions for starting and stopping (panel in which the relay and delimiter are located).
- The shutdown of a piece of equipment, whatever it may be, shall only be foreseen as a safeguard if it is effective to prevent the chain of events and prevent the occurrence of the top event. If the planned interlock is only for the protection of the equipment and does not prevent the occurrence of loss of containment, it shall not be foreseen as a barrier of the loss of containment scenario.
- In the case of MOC that foresees the mirroring of the safety interlock (preventive) in the control loop (as may occur in case of degradation/unavailability of the safety interlock loop), the elements of the control loop shall have their status also impacting Barrier 4. The temporary adjustment must be made to the tool for the duration of the mirroring.
- Very low pressure switches (PSLL) identified in the PHA shall not be included in Barrier 4. If the PSLL promotes the isolation of the section, according to the C&EM, preventing the feed of the loss of containment, it shall be included in Barrier 6.
- In Hazop scenarios of inadvertent or spurious valve closure, position switches that are interlock initiators can be mapped to Barrier 4 when independent of the cause of the deviation.

Essential and Emergency Electrical Power Generation, Storage and Distribution Systems (*)

Purpose or Safety Function: Ensure the supply of energy to essential and emergency consumers in situations that require the action of barriers.

Elements:

- UPS Essential Power System Load delimiters and circuit breakers
- Emergency Loads System UPS
- Emergency System battery banks
- Emergency Loads System distribution panels

Points of Attention and Additional Clarifications

- (*) The system for the generation, storage and distribution of essential and emergency electrical power shall be provided whenever there are elements in the barrier that depend on energy sources. If there are only passive elements in the barrier, the elements of this system shall not be provided for

Barrier 5 (B5) - Relief Systems

Purpose or Safety Function: Ensure overpressure relief of the protected equipment/section and safe routing of the fluid. In this case, the valve (actuated in the event of overpressure), the related elements (according to the subsystem listed below) necessary for the safe disposal of the inventory and its adequate performance are interdependent.

Flare Relief Subsystem

- Initial Element:
  - PSV (*)
  - Pin valve (*)
  - Quick Open Valve Set for Closed Flare (**)
  - Rupture Disc(**)
- Other elements for the safe disposal of the inventory and the system's compliance (****):
  - Piping involved in the disposal of gas to the Flare (****)
  - Level Transmitter (LT/LSHH) with interlocking of the HP and LP Flare vessels
  - Flare Ignition System
  - Flare Purge System
  - Emergency Shutdown System interlock assembly (flow meter, pressure gauge, and concentration meter, where applicable) (**)
  - N_2 generation system for flare, when existing (**)
  - Inert Gas Purity Analyzer (**)
  - Oxygen Analyzer (**)
  - Quick-open valves and their actuators (**)
  - Gas Dilution System (***)

- Orifice plates (responsible for flow and time according to the design criteria, if individualized in SAP)

Points of Attention and Additional Clarifications

(*) Only equipment connected to the Flare (those that discharge to the Flare and those that serve to protect the Flare).

(**) Applicable for Closed Flare and/or Flare with receiving high CO_2 currents.

Rupture discs are present in closed flare systems and act if quick-opening valves fail.

(***) Applicable for flare that receives gas streams with high CO_2 concentration.

(****) For scenarios in which the top event occurs in the Flare System, the elements shall be considered in the barriers that are best applicable for protection, not restricted to barrier 5.

<u>High Velocity Vent (HVV) Relief Subsystem</u>

- Initial Element:
  - PSV
  - Rupture disc
  - HVV stage actuation valves
  - Pin valve
- Other elements for the safe disposal of inventory or for the protection of the HVV system (*):
  - Level Gauge (LT/LSHH) of HVV drum
  - Purge System of HVV
  - Emergency Shutdown interlock assembly of the system (pressure gauge, temperature gauge, where applicable)
  - Lightning protection system (LPS)
  - Flame arresters
  - CO_2 Snuffing System of the atmospheric vent
  - Piping involved in the destination of gas for the HVV

Points of Attention and Additional Clarifications

- Only equipment that discharges to the HVV and those that serves to protect the HVV shall be considered.

- Regardless of the size of the PSV for fire, this element shall be provided for in Barrier 5, as it is foreseen to avoid overpressure. Therefore, its prediction, even if LOPC (Loss of Primary Containment) has occurred in some part of the installation, when provided for the protection of certain equipment, is in order to prevent this equipment from losing its primary containment.

- The LPS, flame arresters and CO_2 snuffing system are necessary to ensure the safe disposal of inventory and the protection of this system. The LPS protects against a possible source of ignition in the vent. If there is an ignition, the flame arrester protects against the return of flame and the CO_2 snuffing system fights this fire. Thus, the unavailability of these elements can compromise the function of the vent system.

(*) The elements for the protection of the system itself are provided for in Barrier 5 when they are necessary to ensure the effectiveness of the relief system and safe disposal of the inventory. If the mapped event occurs in the relief system itself (such as, for example, the flame return scenario by the HVV), the protection elements will be mapped as independent of the relief system provided for herein.

Oil Cargo Tank Relief Subsystem

- Initial Element:

- Relief and vacuum valves (PVSV)
- Pressure/Vacuum Breaker (P/V breaker)
- Piping involved in the destination of gas to the cargo tanks vent post
- Serial check valves may be included when registered in the Hazop as safeguards for reverse flow scenarios of liquids fluids (at least two valves in series and dissimilar). However, check valves should not be provided as a barrier when the deviation generates overpressure.
- Siphon, when provided as a preventive Safeguard in Hazop.

Points of Attention and Additional Clarifications

- Check Valves and siphons are elements provided for in Hazop to avoid worse consequences due to the possibility of reverse flow from one system to another. As established in API STD 521, check valves are devices designed to limit reverse flow, but they can fail, in addition to not being effective measures to prevent overpressure due to reverse flow. In this case, check valves shall only be provided as a preventive barrier if there is no threat or consequence of overpressure.

Barrier 6 (B6) - Post-release Protection System - ESD

Barrier 6 involves a set of elements that, together or separately, achieve a certain purpose. Thus, according to the objective, the elements are grouped.

Production shutdown and inventory isolation (ESD-2) by process deviation subsystem

Purpose or Safety Function: Detection of large loss of containment, which causes deviation in process variables, acting the trigger of safety interlocking and inventory isolation (inlet and outlet of the affected section).

Elements:

- Sensors and interlock switches (very low pressure and/or level, as applicable) that generate ESD-2, listed as mitigating safeguard in the reference study (PHA), if they are actuated due to loss of containment.
- Final elements actuated in ESD-2, which have automatic inventory isolation safety function (SDV, etc.)

Points of Attention and Additional Clarifications

- The objective of this subsystem, when considered as mitigating safeguard, is to isolate the segment and prevent the loss of containment from being fed. To consider the interlocking loop in Barrier 6, as well as the XSLL (where X is any process variable sensitized by the loss of containment), it is necessary that the interlocking promotes the reduction of the system's inventory from the closure of the inlet and outlet SDVs of the segment under consideration. The C&EM shall be consulted to confirm the actions of the instrument.

- In cases of ESD-2, any incongruence identified between the provisions of the C&EM regarding the SDVs acted and the Unit Safety Guidelines (total shutdown of the process without affecting the utility areas of the Unit), shall be communicated to the Focal Point of the Unit for internal verification of the implemented logic.

<u>Fire and Gas detection subsystem generating emergency shutdown (ESD-3), isolation and depressurization</u>

Purpose or Safety Function: Ensure the detection of fire and toxic and/or flammable gases arising from loss of containment, with the activation of emergency shutdown actions, isolation of the segment and depressurization of inventory automatically (commands to be confirmed with the unit's MCE).

Elements:

- CH_4 detectors (****)
- H_2 detectors (****)
- CO_2 detectors (****)
- H_2S detectors (****)
- Final elements activated in ESD-3 (SDV, among others that have a safety function)
- Depressurization system
  - BDV
  - Piping from BDV to flare
  - BDV restriction orifice (*)

  - Accumulators (**)
  - Mechanical time delay system, when foreseen (***)
- Flame detectors (any type, according to leakage location)
- Smoke detector (*)
- Fusible plug of the affected location, according to opened ADVs
- Low pressure sensor of fusible plug loop

Points of Attention and Additional Clarifications

- (*) In case that it is individualized in SAP
- (**) Air or hydraulic fluid accumulators for the BDVs
- (***) In conformity with Petrobras' standards (PE-2SMS-00068 - DEFINIÇÕES DE SMS PARA OPERAÇÃO DOS SISTEMAS DE DESPRESSURIZAÇÃO and PE-2E&P-01013 -TESTES FUNCIONAIS DE VÁLVULAS AUTOMÁTICAS DE SEGURANÇA DO TIPO BDV).
- (****) Depending on the composition of the leaked process fluid and the consequences foreseen in the scenario. The indication of the sensors shall take into account the expected consequences and the correspondence of the sensor to the consequences.
- Gas detectors are designed to identify the leak before it ignites. For leaks in which there is predicted to have gas release in an open place, the gas detectors positioned in the module of origin of the leak (or of the modules, according to the APR section) must be provided as a means of detection as follows:
  - In an area with metal floor and ceiling ("closed"), only gas detectors (all types, according to the composition of the gas and expected consequences) at the level of the module of the section under consideration shall be provided as means of detection.
  - In an area with metal floor ("closed") and a graded ceiling ("open"), only gas detectors (all types, according to the composition of the gas and expected consequences) of the level and levels above (if any) of the module of the section under consideration shall be provided as means of detection.
  - In an area with a graded floor and ceiling ("open"), gas detectors (all types, according to the composition of the gas and expected consequences) of the level and levels above and below the module of the considered section shall be provided as means of detection.
  - In an area with a grated floor ("open") and plate ceiling ("closed"), only gas detectors (all types, according to the composition of the gas and expected consequences) of the level and levels below the module of the considered stretch shall be provided as means of detection.

System for the collection, pressurization and distribution of firefighting water, according to project parameters

- Driver (motor and respective starting system) of the firefighting water collection and pressurization system
- HPU of the lift pump of diesel-hydraulics FWPs
- Primary pump set
- Start-up painel of the primary pump set (automation and control of the pump unit)
- Device(s), set(s) or system(s) for protection during an accident or spurious activation (PCV and PSV of the ring and overspeed sensor).
- Firewater distribution piping
- Pressurization element of the distribution subsystem (jockey pump)
- Jockey pump driver (motor and respective start-up system)
- ADVs
- Deluge System network
- Deluge nozzles, according to the most updated hydraulic balance of the Unit.

Storage, pressurization, mix, (with firewater) and distribution of foam concentrate

Elements:

- Pump
- Diaphragm
- Dosing
- Eductor
- Foam concentrate aligning automatic tank outlet valve
- Automatic water alignment valves for foam system
- Automatic pump alignment valves
- PCV
- Foam concentrate distribution system piping
- Foam concentrate nozzle network
- Water and foam concentrate ADV Skids of foam system

Points of Attention and Additional Clarifications

- The updated C&EM of the facility shall be considered to identify what is effectively in terms of loops, in order to identify the final elements actuated.

- As provided for in Barrier 4, when an interlock causes the stop of a compressor or pump, the final element to be considered for monitoring purposes will be the electrical panel associated with the equipment, which electrically powers it and performs command functions for start and stop. In the future, when Performance Standards are created, new considerations may be made in relation to this premise.

Water Mist System

Purpose or Safety Function: The water mist (high-pressure) firefighting system is applicable indoors for the purpose of fire extinguishing.

Elements:

- Automation and control panel
- Propellant set – N_2 cylinder actuation valve
- Propellant set – water mist system control and flow valves (PCV/FCV)
- Pneumatic pump (when applicable)
- Cylinders battery – main and stand-by N_2 cylinders
- Piping
- Fix temperature detector (process area, engine room, pump room, water mist actuation)

Open drainage system

Purpose or Safety Function: Ensure the flow to safe place of flammable liquid or condensate or combustible from loss of containment. This system shall not be considered when the leak is only gas.

Elements:

- Fixed containment barriers (skids, trays, coamings and module / equipment containment basin) that contemplate pool fire scenarios resulting from releases of liquid or condensate.
- Hazardous area open drainage piping

Points of Attention and Additional Clarifications

- It does not include existing drain boxes or drain pit in an area served by other open drainage points sized for the system or module.

Passive Fire Protection System

Purpose or Safety Function: Ensure thermal protection and integrity of the structure, areas and equipment in the event of a hydrocarbon fire. As informed in item 8 of the General Clarifications, passive protections shall be provided for together with their protected elements.

Elements:

- Unit or equipment support structures passive protection
- Division between process areas or between process area and non-classified area (fire wall)
- Passive protection of equipment and valves (SDV, BDV and other equipment that are in this Barrier)

Essential and Emergency Electrical Power Generation, Storage and Distribution Systems (*)

Purpose or Safety Function: Ensure energy supply for essential and emergency consumers in situations that require the action of barriers

Elements:

Emergency Generator

- Diesel engine
- Generator automation panel
- Emergency Generator Drive System Battery Charger & Battery Bank
- Starter air compressor (**)
- HPU key elements

Essential Power Distribution System

- UPS essential power system load disconnectors and circuit breakers
- UPS Emergency Cargo System
- Emergency System Battery Bank
- Distribution panels of emergency consumers system

Points of Attention and Additional Clarifications

- (*) According to the Safety Guideline, Emergency Generation Systems are only required if ESD-3T or ESD-4 is triggered, since only these systems are capable of generating an interruption of the main electrical system. The elements that can generate the ESD-3T are the manual pushbutton (CCR) or the confirmed fire or gas signal in areas that compromise all the main generators or the power distribution, that is, in the turbogenerator module. In this sense, ESD-3T is not expected to occur in the processing modules except by manual activation (Barrier 8). Therefore, only in the case of accidental scenarios in the turbogenerator module should the Emergency Generation System be in Barrier

6. In other cases, when provided, the Emergency Generation System shall be at Barrier 8 (ESD-3T) and/or 10 (ESD-4) together with the pushbutton, as applicable. In all cases, UPS does not fit into the previous determination, and must be provided for in the respective Barriers regardless of the type of ESD.

- (*) The emergency power generation and distribution system shall be provided whenever there are elements in the barrier that depend on energy sources. If there are only passive elements in the barrier, the elements of the essential electricity generation and distribution system shall not be foreseen.
- (**) Only if it is dedicated equipment for the emergency generator.

Inert Gas System

Purpose or Safety Function: Ensure non-explosive atmosphere in storage tanks.

Elements:

- Inert gas insufflation oxygen analyzer and its associated interlocks, where applicable, including valves.
- Inert gas system relief or vacuum valves (PVSVs).
- Pressure/Vacuum Breaker (P/V breaker)
- Seal tank low pressure sensor that interlocks the operation of inert gas generators and their associated interlocks, where applicable, including valves.
- Low-level switch of the sealing tank and its associated interlocks, where applicable, including valves

HC Blanketing System

Elements:

- Set of valves, piping, compressors and control and safety loops components of the HC Blanketing gas generation and supply/recovery system to/from cargo tanks.

Ventilation and Exhaustion System

Purpose or Safety Function: Ensure safe indoor atmosphere control.

Elements:

- Fan (*)
- Fan motor (*)
- Fan delimiter (*)
- Exhaust fan (*)
- Exhaust fan motor (*)
- Exhaust fan delimiter (*)
- Differential pressure or flow sensor (**)

- Gastight damper (**)
- Fire damper (**)

Points of Attention and Additional Clarifications

- (*) Only fans/exhaust fans required for maintenance of safe condition of the compartment.

- (**) For the following cases: compartments protected by fixed gaseous firefighting systems; dampers in the air intake to the inhabited compartment; dampers in rooms that have emergency attend action and dampers in the oil/gas process area.

Other anti-ignition safety elements:

- Flame Arrest Protection Valves
- Lightning Protection System (LPS) Equipment
- Vent Flame Arrester

Barrier 7 (B7) - Control of ignition sources

It comprises the elements that shall have integrity requirements in order not to become sources of ignition or that can generate an explosive atmosphere in contact with an ignition source.

Equipment certified for explosive atmospheres (Ex)

Purpose or Safety Function: Ensure that equipment certified to operate in environments with potential explosive atmospheres (Ex Equipment) has full protection and are not possible sources of ignition for scenarios of loss of containment of combustible or flammable material.

Elements: For the consideration of equipment with Ex protection, the foreseen consequence (types of fire) and the equipment that would be a possible source of ignition must be analyzed. For cloud fire scenarios, the gas cloud has the possibility of hitting neighboring modules before ignition. For jet fire, explosion, or pool fire scenarios, the released gas is ignited closer to the leak source.

- For scenarios in which is foreseen pool fire, cloud fire, jet fire or explosion, all the equipment provided for in the List of Ex Equipment of the Module in which the LOPC took place shall be selected as elements of Barrier 7.

Barrier 8 (B8) - Operational Emergency Response

Comprises the elements and procedures related to the operation's response to a loss of containment event. The elements associated with the essential and emergency generation systems necessary for the proper functioning of the planned electrical equipment are also foreseen.

Elements:

- CH_4 detectors (all types)
- H_2 detectors
- CO_2 detectors
- CO detectors, if applicable
- H_2S detectors
- Alarms associated to the detectors (gas, flame, smoke, heat)
- CCTV (visual detection to control room)
- The procedure associated with the actuated alarm, in which the actions that shall be performed by the operation in response to the process deviation are established.
- The final elements actuated (valve, pushbutton, etc.), as established in the Procedure. In case of activation of a pushbutton, the elements controlled by it shall also be included here.
- Emergency phone (from the module where the release occurs), satellite phone (landline and portable).
- CCS (Call Conversion Station) and TSL (Telephone Signaling Lamp) of the module where the LOPC occurs
- Fire extinguishers, in the vicinity of the leak site

Points of Attention and Additional Clarifications

- Alarms associated with gas, flame or smoke detectors may be included in Barrier 8 if there is an operational response procedure associated with them. In these cases, the alarms, as well as the procedures, should only be considered in Barrier 8. Otherwise, the alarm must be mapped to Barrier 6.

Water Mist System

Purpose or Safety Function: The water mist (high-pressure) firefighting system is applicable indoors for the purpose of fire extinguishing.

Elements:

- Propellant assembly - N_2 cylinder trigger valve
- Propellant assembly - Water Mist System (PCV/FCV) control and flow valves
- Pneumatic pump (when applicable)
- Cylinder battery - N_2 main cylinders and reserve
- Piping
- Pushbutton

Points of Attention and Additional Clarifications

- SOPEP kit can be used in case of small leaks contained in the platform. As Dynamic Barrier Management focuses on larger scenarios, in which large inventory losses occur with severe consequences, it is not applicable to map the SOPEP Kit as a Barrier element, since it does not have any effectiveness for these scenarios.

Emergency Power Generation, Storage and Distribution Systems (*)

Purpose or Safety Function: Ensure energy supply for essential and emergency consumers in situations that require the action of barriers.

Elements:

Emergency Generator

- Diesel Engine
- Generator Automation Panel
- Battery Charger & Battery Bank Emergency Generator Drive System
- Starter air moto-compressor (**)
- Main Elements of the HPU

Essential Power Distribution System

- UPS essential power system load delimiter and circuit breaker
- Essential power loads system UPS
- Essential system battery banks
- Essential load system distribution panels

Points of Attention and Additional Clarifications

- (*) According to the Safety Guideline, Emergency Generation Systems are only required if ESD-3T or ESD-4 is triggered, since only these systems are capable of generating an interruption of the main electrical system. The elements that can generate the ESD-3T are the manually activated pushbutton (CCR) or the confirmed fire or gas signal in areas that compromise all the main generators or the distribution of electricity, that is, in the turbogenerator module. In this sense, ESD-3T is not expected to occur in the processing modules except by manual activation (Barrier 8). Therefore, only in the case of accidental scenarios in the turbogenerator module shall the Emergency Generation System be in Barrier 6.

In other cases, when provided, the Emergency Generation System shall be at Barrier 8 (ESD-3T) and/or 10 (ESD-4) together with the pushbutton. In all cases, UPS does not fit into the previous determination, and shall be provided for in the respective Barriers regardless of the type of ESD.

- (*) The emergency power generation and distribution system shall be provided whenever there are elements in the barrier that depend on energy sources. If there are only passive elements in the barrier, the elements of the essential power generation and distribution system shall not be foreseen.

- (**) Only if it is dedicated equipment for the emergency generator.

Ventilation and Exhaustion System

Purpose or Safety Function: Ensure safe indoor atmosphere control.

Elements:

- Fan (*)
- Fan motor (*)
- Fan delimiter (*)
- Exhaust fan (*)
- Exhaust fan motor (*)
- Exhaust fan delimiter (*)
- Differential pressure or flow sensor (**)
- Gastight damper (**)
- Fire damper (**)

Points of Attention and Additional Clarifications

- (*) Only fans/exhaust fans required for maintenance of safe condition of the compartment.

- (**) For the following cases: compartments protected by fixed gaseous firefighting systems; dampers in the air intake to the inhabited compartment; dampers in rooms that have emergency attend action and dampers in the oil/gas process area.

Barrier 9 (B9) - Brigade Emergency Response

It comprises the elements and procedures related to the brigade's response to a loss of containment event. The elements associated with the essential and emergency generation systems necessary for the proper functioning of the planned electrical equipment are also foreseen.

System of collection, pressurization, distribution and final elements of the firewater firefighting system, according to design parameters

Elements:

- Firewater distribution piping
- Distribution subsystem pressurization element (jockey pump)
- Jockey pump driver (motor and its starting system)
- HPU (FWP hydraulic lift pump unit)
- Main FWP unit
- Drive panel (pumping unit automation and control)
- Battery charger and starter system batteries, if applicable
- Device(s), set(s) or system(s) for protection during an accident or spurious activation (PCV and PSV of the ring and overspeed sensor).
- Fire hydrant (*)
- ADVs
- Fixed moniotrs (*)

Points of Attention and Additional Clarifications

- (*) Consider only fixed monitors and hydrants in areas adjacent to the accident site, since only these will be accessible by the brigade. These elements are not provided for in Barrier 6 because they require human action.

Foam concentrate storage, pressurization, mixing (with firefighting water) and distribution system

Elements:

- Moto-pump
- Diaphragm
- Proportioner
- Eductor
- Foam concentrate aligning automatic tank outlet valve
- Automatic water alignment valves for foam system
- Automatic pump alignment valves
- PCV
- Foam concentrate distribution system pipinge
- Foam concentrate nozzles network
- Fixed foam concentrate monitors
- Water/foam ADV skids of foam system
- Activation buttons (if it is the only way to activate the foam system)

Fixed Gaseous Firefighting systems

Purpose or Safety Function: Ensure safe firefighting with gaseous agents.

Elements:

- Cylinder batteries segregated by zone or group
- Directional valves (segregation by zone or group)
- Status light
- Horns (audible alarm)
- High pressure sensors for triggering the warning system (PSHs, PIT)
- Battery trigger solenoid valves (zone or group segregation)
- Flood time delay device
- Pushbuttons
- Pipes

Points of Attention and Additional Clarifications

- As provided for in Petrobras' standards, the orientation is for the brigade to activate the triggering pushbuttons.

Other safety elements

- Brigade procedures associated with Emergency Response.

Barrier 10 (B10) - Evacuation, Rescue and Abandonment

Elements: For Barrier 10 to be effective, the elements of communication, the means for evacuation, rescue and abandonment, and the associated procedures shall be considered.

- ESD-4 Push Button
- Priority microphone
- Fixed Radio and VHF DSC Antenna
- Fixed Radio and MF/HF Antenna
- GMDSS Portable VHF Radio
- Inmarsat C Terminal & Antenna
- Radar Transponder
- EPIRB
- Radio communication repeaters
- Radiant system
- Fixed Radio
- Satellite Phone (**)
- Visual and audible alarm activation pushbutton (general and abandonment)
- Intercom Center
- Lifeboats
- Inflatable liferafts

- Rescue boat
- Davit (lowering system, includes cables) (*)
- Escape Chute or transshipment basket (*)
- Procedures related to Evacuation, Rescue and Abandonment
- Crane (*)

Points of Attention and Additional Clarifications

- (*) When provided for in the project and in the unit's ERP (Emergency Response Plan).

- (**) According to the characteristics of each Unit, communications outside the unit can be reevaluated considering the existence of at least two communication options outside the unit without a common failure mode.