PETROBRAS | N-2595 | REV. D | ENGLISH | 12 / 2016

CONTEC
Comissão de Normalização Técnica

SC-10
Instrumentation and Industrial Automation

Criteria for Design, Operation and Maintenance of Safety Instrumented Systems in Industrial Units

1st Erratum

This is the 1st Erratum to PETROBRAS N-2595 REV. D and it is used to alter the text of the Standard in the part(s) indicated below:

NOTE 1 The new page with the performed amendment is placed in its corresponding position.
NOTE 2 The corrected pages, indicated the date of the erratum, are placed at the end of this standard, in chronological order, and shall not be used.

CONTENTS OF THE 1st ERRATUM - 12/2016

- Subsection 7.11.3.3:

Alteration of the text.

PETROBRAS | N-2595 | REV. D | ENGLISH | 03 / 2015

Criteria for Design, Operation and Maintenance of Safety Instrumented Systems in Industrial Units

Procedure

This Standard replaces and cancels its previous revision.

The CONTEC - Authoring Subcommittee provides guidance on the interpretation of this Standard when questions arise regarding its contents. The Department of PETROBRAS that uses this Standard is responsible for adopting and applying the sections, subsections and enumerates thereof.

Technical Requirement: A provision established as the most adequate and which shall be used strictly in accordance with this Standard. If a decision is taken not to follow the requirement ("non-conformity" to this Standard) it shall be based on well-founded economic and management reasons, and be approved and registered by the Department of PETROBRAS that uses this Standard. It is characterized by imperative nature.

Recommended Practice: A provision that may be adopted under the conditions of this Standard, but which admits (and draws attention to) the possibility of there being a more adequate alternative (not written in this Standard) to the particular application. The alternative adopted shall be approved and registered by the Department of PETROBRAS that uses this Standard. It is characterized by verbs of a nonmandatory nature. It is indicated by the expression: **[Recommended Practice]**.

Copies of the registered "non-conformities" to this Standard that may contribute to the improvement thereof shall be submitted to the CONTEC - Authoring Subcommittee.

Proposed revisions to this Standard shall be submitted to the CONTEC - Authoring Subcommittee, indicating the alphanumeric identification and revision of the Standard, the section, subsection and enumerate to be revised, the proposed text, and technical/economic justification for revision. The proposals are evaluated during the work for alteration of this Standard.

CONTEC
Comissão de Normalização Técnica

SC - 10
Instrumentation and Industrial Automation

Introduction

PETROBRAS Technical Standards are prepared by Working Groups - WG (consisting specialized of Technical Collaborators from Company and its Subsidiaries), are commented by Company Units and its Subsidiaries, are approved by the Authoring Subcommittees - SCs (consisting of technicians from the same specialty, representing the various Company Units and its Subsidiaries), and ratified by the Executive Nucleus (consisting of representatives of the Company Units and its Subsidiaries). A PETROBRAS Technical Standard is subject to revision at any time by its Authoring Subcommittee and shall be reviewed every 5 years to be revalidated, revised or cancelled. PETROBRAS Technical Standards are prepared in accordance with PETROBRAS Technical Standard N-1. For complete information about PETROBRAS Technical Standards see PETROBRAS Technical Standards Catalog.

Summary

Figures

Tables

Foreword

This Standard is the English version (issued in 10/2015) of PETROBRAS N-2595 REV. D 03/2015. In case of doubt, the Portuguese version, which is the valid document for all intents and purposes, shall be used.

1 Scope

1.1 This Standard aims to provide guidelines and establish the minimum conditions required for design, operation and maintenance of Safety Instrumented Systems - SIS in PETROBRAS' onshore facilities.

1.2 Fire and gas detection systems are not considered in this Standard.

1.3 Any function with exclusively manual actuation does not fit the Safety Instrumented Systems (SIS). For example: inventory insulation and depressurization.

1.4 This Standard sets forth conditions required for projects started as of its issue.

1.5 This Standard contains Technical Requirements and Recommended Practices.

2 Normative References

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document applies.

Norma Regulamentadora N° 10 (NR-10) - Segurança em Instalações e Serviços de Eletricidade;

PETROBRAS N-329 - Bateria de Acumuladores;

PETROBRAS N-332 - Uninterruptible Power System - Continuous Current for Industrial Use;

PETROBRAS N-858 - Construction, Assembly And Conditioning of Instrumentation;

PETROBRAS N-1219 - Colors;

PETROBRAS N-1756 - Passive Fire Protection Design and Application on Onshore Facilities;

PETROBRAS N-1883 - Presentation of Instrumentation/Automation Design;

PETROBRAS N-2782 - Applicable Techniques to Industrial Risk Analysis;

IEC 61131-3 - Programmable Controllers, Part 3: Programming Languages;

IEC 61508-1 - Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems - Part 1: General Requirements;

IEC 61508-2 - Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems - Part 2: Requirements for Electrical / Electronic / Programmable Electronic Safety-Related Systems;

IEC 61508-3 - Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems - Part 3: Software Requirements;

IEC 61508-4 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Part 4: Definitions and Abbreviations;

IEC 61511-1 - Functional Safety - Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, Definitions, System, Hardware and Software Requirements;

IEC 61511-3 - Functional Safety - Safety Instrumented Systems for the Process Industry Sector - Part 3: Guidance for the Determination of the Required Safety Integrity Levels;

IEC 62337 - Commissioning of Electrical, Instrumentation and Control Systems in the Process Industry - Specific Phases and Milestones;

IEC 62381 - Automation Systems in the Process Industry - Factory Acceptance Test (FAT), Site Acceptance Test (SAT) and Site Integration Test (SIT);

ISO TR 12489 - Petroleum, petrochemical and natural gas industries — Reliability Modelling and Calculation of Safety Systems;

API STD 521 - Pressure-relieving and Depressuring Systems;

ISA TR 84.00.03 - Guidance for Testing of Process Sector Safety Instrumented Functions (SIF) Implemented as or Within Safety Instrumented System (SIS);

ISA TR 84.00.04 Part 1 - Guideline for the Implementation of ANSI/ISA-84.00.01 (IEC 61511);

ISA 84.91.01 - Identification and Mechanical Integrity of Safety Controls, Alarms, and Interlocks in the Process industry;

ISA TR 96.05.01 - Partial Stroke Testing of Automated Block Valves.

NOTE For documents referred in this Standard and for which only the Portuguese version is available, the PETROBRAS department that uses this Standard should be consulted for any information required for the specific application.

3 Terms and Definitions

For the purposes of this document, the following terms and definitions apply.

3.1
Layers of Protection Analysis (LOPA)
semi-quantitative technique for assessing risks, the purpose of which is to determine if the layers of protection associated to an accidental scenario are sufficient to reduce its frequency of occurrence to a level considered tolerable

3.2
Process Hazard Analysis (PHA)
systematized and organized effort using one or more techniques listed on PETROBRAS N-2782 (APR, HAZOP etc.) to identify and assess the relevance of the potential hazards associated with the processing or handling of hazardous products focusing on equipment, instrumentation, utilities, human actions, and external conditions that may affect the process

3.3
protection layer
resource specifically adopted, designed or developed to reduce the risk associated with one or more scenarios

NOTE 1 The resource adopted may be a process engineering technique, such as the dimensioning of a vessel containing a hazardous product; a mechanical piece of equipment, such as a safety valve; a Safety Instrumented Function; or even an administrative procedure, such as an emergency plan for situations of imminent danger.
NOTE 2 A protection layer may be preventive, when it aims to reduce the expected frequency of occurrence of a scenario; or mitigating, when it aims to reduce the severity of the scenario consequence.
NOTE 3 A protection layer may be passive (when it does not need to execute an action to fulfill its protection function), or active (when it needs to change from a particular state to another in response to a change in the measurable property of the process in question). In the second case, its actuation may be automatic or by human action.

3.4
Independent Protection Layer (IPL)
protection layer that keeps its preventive or mitigating function autonomously, without taking into account the initiating cause or the action of any other protection layer associated with the scenario

3.5
initiating cause
equipment failure, inappropriate human action or external event that triggers a scenario

3.6
scenario
sequence of unintended events that culminates in some harm

NOTE For the purposes of LOPA application, a scenario consists of a cause-consequence pair. Therefore, events that may result in different consequences shall be analyzed as distinct scenarios.

3.7
safety life cycle
set of activities involved in the SIFs implementation during the time interval that starts in the conceptual design phase and ends when these SIFs are disabled

3.8
Enabling Event (EE)
action or state that does not cause the scenario directly, but needs to exist so that the scenario happens

3.9
consequence
demonstration of how the accidental scenario may have an impact on human, environmental and/or material resources, expressed in the form of harm to health, environmental impacts and/or economic loss

3.10
Programmable Electronics (PE)
programmable controller designed and developed specifically to act as SISs Logic Solver

NOTE The CP safety denomination replaces the former term PES, which was used by Petrobras, in order to eliminate conflict with IEC 61508-4 and IEC 61511-1, in which the term PES designates the entire set of devices (sensors + Logic Solver + final elements) of SIS.

3.11
harm
impact, achieved consequence or final outcome of a hazardous event on human beings, environment and/or property, expressed in terms of fatalities, environmental damage, property destruction, production loss, etc.

NOTE 1 Environmental impacts may include expenses with facilities cleaning and environmental decontamination, fines from supervision bodies, civil and labor reparation, difficulties in obtaining new licenses, harm to the company's image etc.
NOTE 2 Property is understood as equipment, facilities, products, and processes.

3.12
fault
abnormal condition that may lead to the reduction or loss of a device ability to perform its function

3.13
demand
hazardous condition or event that requires the action of a SIF

3.14
device
equipment capable of performing a specific function

3.15
final element
device that integrates the SIS and implements the physical action required to achieve a safe state

NOTE The most common examples are:

a) valve, including actuator and solenoid;
b) control circuit, interposing relay and circuit breaker or contactor to disconnect the electric motor.

3.16
Safety Requirements Specification (SRS)
documentation containing all the requirements that each SIF shall present when implemented in the SIS

3.17
safe state
state of a process or equipment of which risk is within the limits defined as tolerable

3.18
Hazards and Operability Study (HAZOP)
inductive and structured technique to identify process hazard and potential operational problems, associating, in a systematic way, a set of keywords to the process variables; for each deviation identified, its causes, consequences, detection modes, and existing safeguards are listed, and additional measures are recommended, when necessary

3.19
logic solver
device that integrates the SIS and receives signals from the sensors, processes programmed functions and sends commands to the final elements

3.20
failure
event characterized by the cessation of a device's ability to perform its function

NOTE The disabilities caused by planned actions, such as preventive maintenance, are excluded from this concept.

3.21
random hardware failure
failure that occurs on an unpredictable moment because of a variety of degradation processes acting on the internal components of a device

NOTE 1 Due to the manufacturing tolerances, such degradation processes have different dynamics in distinct components, giving a random character to the failure instant.
NOTA 2 Due to its nature, the random hardware failure may be quantified in a statistic way. For example: by observing various identical devices, operating under the same conditions, the respective failure rate may be determined.

3.22
common cause failure
failures in more than one device, component or system, as a result of a same direct cause, in a relatively short period of time, not being such failures a consequence of one another

NOTE 1 The items that fail due to a same cause normally fail in the same functional mode. Therefore, the term “common mode” is used sometimes. However, it is not considered a precise term to communicate features that describe a common cause failure.
NOTE 2 As examples of common causes, one can mention the action of corrosive atmosphere, electromagnetic interference, mechanical vibration, clogging of stand-pipe taps, loss of electrical power, loss of pneumatic or hydraulic pressure, fire, explosion, lightning, improper (manufacturing, installation, pre-commissioning, operation, or maintenance) procedure, inadequate training (ditto), design fault or limitation.

3.23
failure on demand
non-actuation of a SIF when it is subjected to an actual demand

3.24
undetected failure
failure that is only noticed when a SIF is demanded or tested

3.25
dangerous failure, unsafe failure, fail-to-function failure
failure that has the potential to prevent a safety function from activating when there is an actual demand

NOTE A single dangerous failure is often insufficient to prevent a redundant safety function from activating when required.

3.26
safe failure, spurious trip failure, nuisance trip failure, false trip failure, fail-to-safe failure
failure that has the potential to cause the activation of a safety function when it is not required

NOTE A single safe failure is often insufficient to cause a spurious trip in a redundant safety function.

3.27
systematic failure
failure related, in a deterministic way, to a certain cause

NOTE 1 Three main types of errors may lead to systematic failures:

— design error (wrong or omissive specifications, such as: incorrect equipment sizing, improper selection of materials);
— equipment failure (error in the manufacturing process, improper installation, inappropriate maintenance or operation procedure);
— program error (software programming or change).

NOTE 2 A systematic failure can only be eliminated through appropriate changes in its cause. Corrective maintenance interventions without the implementation of these modifications do not eliminate the systematic failure.
NOTE 3 Due to its nature, the causes of systematic failures cannot be easily predicted or quantified in a statistical way.

3.28
coverage
number that ranges from 0 to 1 (100 %) and that indicates the percentage of undetected failures that are found when a SIS device is subject to a certain test or diagnostic

3.29
Risk Reduction Factor (RRF)
measurement of the performance of a protection layer, given by the ratio between risks with and without the implementation of this protection layer; it may be mathematically expressed as the inverse of the PFD_{avg} of the protection layer considered: $RRF = 1/ PFD_{avg}$

3.30
Modification Factor (MF)
specific condition that may alter the consequence of a scenario

3.31
Initiating Cause Frequency (ICF)
expected frequency of occurrence of the cause that may lead to the scenario considered

3.32
frequency of consequence (F^{C})
expected frequency of occurrence of the undesired consequence, taking into account the frequency of the initiating cause, the probability of occurring the enabling event, the average probabilities of failure on demand of the non-SIF protection layers and the applicable modification factors

3.33
scenario risk tolerance criteria (F^{TOL})
risk tolerability criterion given by the frequency above which a scenario with certain consequence severity is not tolerated

3.34
Safety Instrumented Function (SIF)
protection function to which a SIL is required, and which aims to reach or maintain a safe state of a process or equipment through a specific automatic action against a certain operational deviation

NOTE A SIL and a MTTFS are associated to each SIF.

3.35
risk graphs
technique for qualitative assessment of the risk reduction that uses graphical representations of the risk tolerability criterion

3.36
sensor
device or combination of devices that provide information to the Logic Solver on the value or state of process variables or of monitored equipment that initiate the SIF activation

NOTE 1 The most common examples are:

a) transmitters, including connections to the process, sensors and complete wiring;
b) limit switches, including complete wiring;
c) manual trip switches and complete wiring.

NOTE 2 The term sensor, as defined in this standard, is equivalent to the term “initiator" used in the Portuguese version.

3.37
operator interface
means by which communication is established between the human operator and the SIS. The operator interface is also known as Human-Machine Interface (HMI)

NOTE As examples of operator interface, one can mention: video monitors, indicator lamps, push-buttons, sirens and alarm speakers.

3.38
Safety Integrity Level (SIL)
discrete indicator of the performance of a SIF, in terms of its PFD_{avg} and its RRF, expressed in a scale of integer numbers from 1 to 4

NOTE The SIF design shall consider all failures (random hardware and systematic ones) that may prevent the safe state from being reached. For random hardware failures, the SIL is related to the quantified PFD_{avg} of the SIF. For systematic failures, it is necessary to use specific approaches, such as FMEA, FMECA, fault trees, etc.

3.39
hazard
condition or property inherent to a substance, activity, system or process, with potential to cause harm to people’s physical integrity, to the environment and to property, or production loss

NOTE The term includes hazards that are presented in short time intervals (e.g., fire or explosion) and in long periods of time (e.g., release of toxic products).

3.40
Probability of Failure on Demand (PFD)
probability that a protection layer fails to perform its specific function in response to a demand

3.41
average probability of failure on demand (PFD_{avg})
indicator of the reliability of a protection layer, given by the average probability, in a given time interval, that such layer fails when demanded

NOTE The time interval considered in the calculation of the average is usually the interval between periodic tests (normally equal to the plant or equipment campaign period).

3.42
application software
specific program for user application; it generally contains logic sequences, permissions, limits and expressions necessary to meet its functional requirements

3.43
embedded software
specific program that is an integral part of the programmable electronic system, supplied by the respective manufacturer, and that is essential to the operation and not accessible for modifications by the user; also known as firmware or software of the system

3.44
utility software
set of programming tools required for the creation, modification and documentation of the application software; these programming tools are not necessary for the programmable electronic system operation

3.45
redundancy
existence of more than one way to perform the same function, usually to increase the reliability and/or availability of a system

NOTE Redundancy may be implemented through identical devices (identical redundancy) or different devices (diverse redundancy).

3.46
diverse redundancy
resource usually used to reduce the influence of common cause failures through the use of different technologies, designs, manufacturing, programming, etc. to perform a same function

NOTE Some examples of usual methods for obtaining diverse redundancy are:

a) measurement of different process variables, such as pressure and temperature, in the cases where the correlation between these variables is well established and known;
b) measurement of a single process variable by means of different technologies, such as flow measurement through vortex and coriolis;
c) use of aerial and underground routes with different paths for redundant means of communication;
d) use of different controller models in a redundant architecture, programmed with distinct methods, by technicians with different specializations.

3.47
risk
combination of the expected frequency of occurrence of a scenario with the consequence severity of this scenario

NOTE 1 The risk can be expressed mathematically as the product of the expected frequency of occurrence of a scenario by the severity of its consequence Risk = frequency x severity.
NOTE 2 The expected frequency of occurrence is usually expressed in terms of the number of events per year.
NOTE 3 The consequence severity is normally expressed in terms of monetary value (production losses and/or property harm) and/or number of fatalities.

3.48
process risk
risk inherent to the process or equipment conditions caused by abnormal events (including faults in the BPCS), without taking into account the layers of protection

NOTE 1 In the context of this Standard, the process or equipment risk is the specific risk to which a protection layer provides reduction.
NOTE 2 Process hazards include fire, explosion, toxic release, and exposure to ionizing radiation, but they do not include hazards not related to the process, normally controlled by other means, such as hearing protection, gloves, safety goggles, guardrail, or housekeeping, and occupational hazards such as slips, stumbles and falls.

3.49
tolerable risk
risk defined as acceptable in a given context

NOTE In the context of this Standard, the term “acceptable” refers to a consensus between the society, risk analysts and specialized agencies (e.g., HSE) in dealing with a particular risk so as to obtain certain benefits, trusting that this risk is being properly controlled and, therefore, these benefits compensate the risk assumed

3.50
consequence severity
qualitative or quantitative measurement of harm to people, to the environment and to the property

3.51
Safety Instrumented System (SIS)
system used to implement one or more safety instrumented functions; a SIS is composed of a set of sensors, logic solvers and final elements

3.52
Basic Process Control System (BPCS)
system that responds to input signals from the process, associated equipment and/or operator, generating output signals that cause the process to operate as desired

NOTE 1 The BPCS typically implements various functions, such as continuous and discrete (on-off) process controls, monitoring, alarms, sequencing and interlocking.
NOTE 2 The BPCS does not perform any SIF.

3.53
SIF response time
time interval between the appearance of a demand and the completion of a SIF actuation; this time includes the rise time of the demand condition by the sensor(s), the signals processing time in the Logic Solver, the delay time of the SIF, and the actuation time of the final element(s)

3.54
SIF delay time
time delay intentionally added to the processing of a SIF logic, which is not sufficient to check the harm to be avoided against an actual demand, and necessary to avoid spurious trips due to normal/expected process oscillations that do not represent any hazard, but may reach the SIF actuation threshold

3.55
process safety time
time interval between the appearance of an actual demand and the hazard

3.56
failure on demand tolerance
capacity of a SIF to perform its function when demanded, even in the presence of dangerous failure(s)

NOTE As an example of architecture that has tolerance to failure on demand, one can mention the voting type 1 of 2.

3.57
spurious trip tolerance
capacity of a SIF not to cause a spurious trip, even in the presence of dangerous failure(s)

NOTE 1 As an example of architecture that has tolerance to spurious trip, one can mention the voting architecture type 2 of 2.
NOTE 2 The voting architecture type 2 of 3 is generally used in SIS devices when one wishes to achieve, simultaneously, failure on demand tolerance and spurious trip tolerance.

3.58
trip
actuation of the final element(s) of a SIF, due to either actual demand, manual forcing, or SIF failure (spurious trip)

3.59
spurious trip
trip occurred without an actual demand or intentional forcing (manual trip) of this condition; it usually occurs due to the failure of one or more SIF devices

NOTE Not all spurious trips may be categorized as safe failure, since the total or partial spurious actuation of some SIFs may be initiating causes of risk scenarios.

3.60
validation
activity for demonstrating that the SIS installed effectively meets the specifications of its SIFs, including all aspects of their functionalities and performance requirements

3.61
high integrity backflow prevention device
device especially designed and built to ensure, with high reliability, a tight shut-off for backflow

NOTE These devices have seat and internals precisely machined that ensure a tight metal-metal shut-off, and a special design (e.g., venturi type) that provide them with a set of characteristics, such as: laminar axial flow, full bore, low load loss in the bore, smooth and stable response against flow variations, fast (assisted by a spring or pneumatically) and smooth (non-slam) closing, which minimize harm caused by erosion, vibration, abrupt closing and high cycling.

3.62
verification
activity of demonstrating for each SIS life cycle phase, through analyses and/or tests, that, for the specified conditions, all objectives and requirements established in the functional specification for that phase are achieved

NOTE Examples of verification activities include:

— reviews of the products (e.g., documents) of all phases of the safety life cycle to ensure the compliance with each phase's objectives and requirements, taking into account their specific entries;
— design reviews;
— tests performed with the products designed in that phase to ensure that their performance is in accordance with their specification;
— integration tests performed with the different parts of a system that operate together, and with the performance of environmental tests to ensure that all parts work together in the specified manner.

4 Symbols and Abbreviations

ABNT - "Associação Brasileira de Normas Técnicas";
AIChE - American Institute of Chemical Engineers;
ALARP - As Low As Reasonably Practicable;
ANSI - American National Standards Institute;
API - American Petroleum Institute;
PHA - Preliminary Hazard Analysis;
CCPS - Center for Chemical Process Safety;
PC - Programmable Controller;
EE - Enabling Event;
EEL - Enabling Event Likelihood;
F^{C} - Frequency of Consequence;
FCC - Fluid Catalytic Cracking;
F^{TOL} - Tolerable Frequency;
HART - Highway Addressable Remote Transducer;
HAZOP - Hazards and Operability Study;
HSE - UK Health & Safety Executive;
ICF - Initiating Cause Frequency;
IEC - International Electrotechnical Commission;
HMI - Human-Machine Interface;
IPL - Independent Protection Layer;
ISA - The Instrumentation, Systems, and Automation Society;
LOPA - Layers of Protection Analysis;
MF - Modification Factor;
MTBF - Mean Time Between Failures;
MTTF - Mean Time to Fail;
MTTFS - Mean Time to Fail Safe;
MTTR - Mean Time to Repair;
NFPA - National Fire Protection Association;

DCP - Direct Current Panel;
PFD - Probability of Failure on Demand;
PFD_{avg} - Average Probability of Failure on Demand;
RRF - Risk Reduction Factor;
SDV - Shut Down Valve;
SIF - Safety Instrumented Function;
SIL - Safety Integrity Level;
SIS - Safety Instrumented System;
SRS - Safety Requirements Specification;
BPCS - Basic Process Control System;
FAT - Factory Acceptance Test;
UPS - Uninterruptible Power Supply.

5 Assessment of the SIS Need and Basic Design Structuring

The assessment of the need to implement one or more SIFs is an integral part of the design practices, and shall be performed during the elaboration of the plant's basic design, through the application of one or more risk analysis techniques, followed by the adoption of appropriate protection layers.

5.1 Risk Analysis

5.1.1 Among the various techniques for assessing process risks mentioned in PETROBRAS N-2782, the HAZOP application by a multidisciplinary team is recommended. This team is composed of professionals from the following areas: process, instrumentation and control, industrial operation and safety, who use as reference design documents that allow the scenarios of and the assessment of risks associated with each scenario **[Recommended Practice]**.

5.1.2 The boundary conditions imposed by the plant or equipment installation place, as well as by its operational philosophy, shall be defined upon the analysis of the impacts arising from a risk scenario. Typical examples are equipment remotely or manually operated in the field and plants located in isolated areas or near inhabited areas.

5.1.3 Once the risk associated with a scenario is determined, it shall be evaluated whether such risk is tolerable, taking as basis the corporate policies expressed in PETROBRAS N-2782 criteria, the local legislation and the applicable regulations.

NOTE The following may also be considered when determining the tolerable risk: international standards and references, information from insurance companies, and agreements between stakeholders, eventually allowing the involvement of the local community. **[Recommended Practice]**

5.1.4 Table 2 of PETROBRAS N-2782 makes it clear that the risk of a scenario not being tolerable (being out of the T - tolerable - zone) is different from not being tolerable (being in the NT - unacceptable - zone). However, it shall be emphasized that leaving the final risk in the M (moderate) zone shall be justified after having used all resources to reduce it, in accordance with the ALARP concept.

5.2 Protection Layers

5.2.1 If the assessment of a scenario indicates that its frequency is greater than the limit established as tolerable, the reduction of the expected frequency of occurrence, or the severity of the consequence associated with this scenario, shall be sought. Such reduction is achieved through the application of risk reduction measures, often referred as safeguards or protection layers (see Figure 1).

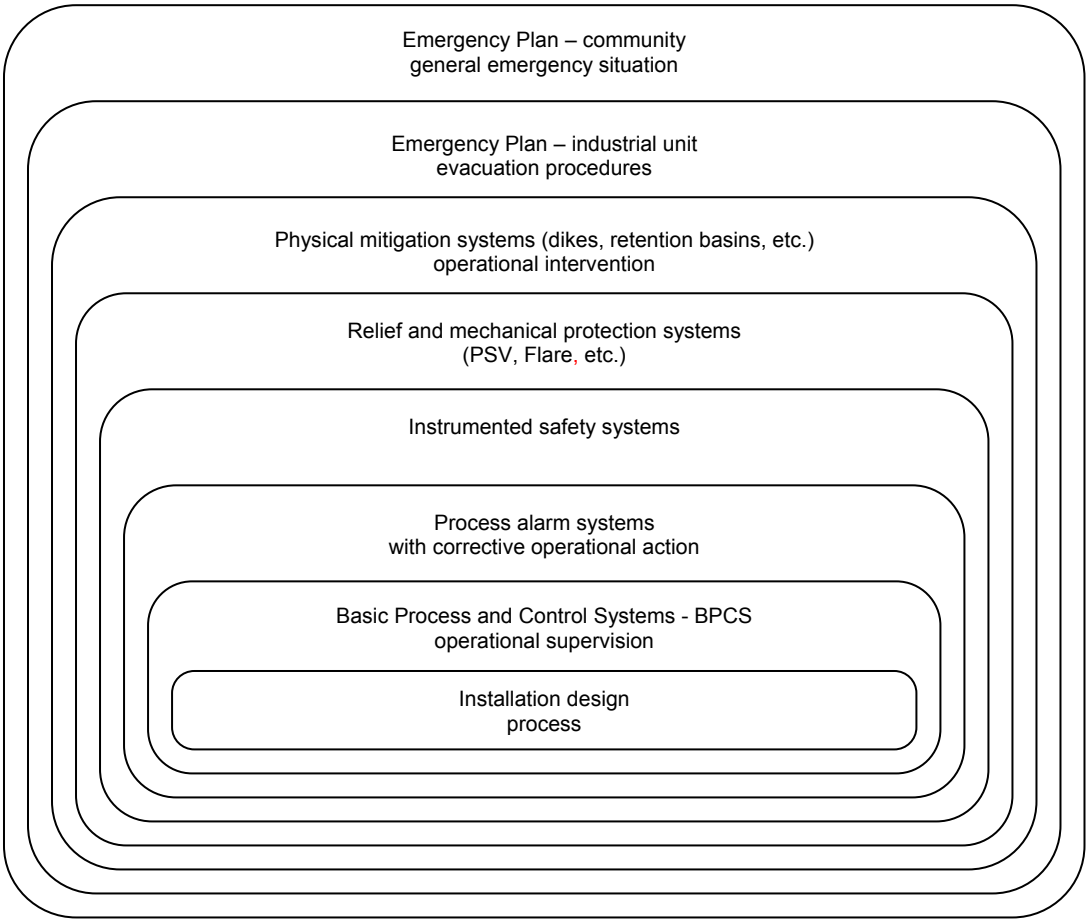

Figure 1 - Typical Layers of Protection

5.2.2 As the first protection layer, a scenario associated with the operation of equipment and/or processes may have its risk significantly reduced, or even completely eliminated, through specific design techniques or through an inherently safer design. Examples: risks due to excessive pressure may be reduced through the proper specification of the pipeline thickness or through the limitation of the pump head below the design pressure of the vessel to which it discharges; risks due to high temperatures may be reduced through appropriate design of heat exchangers; risks due to vibrations may be reduced considering appropriate supports for the pipelines; risks to people may be greatly reduced through the installation of the plant in a non-inhabited location; fire or explosion risks may be eliminated if it is possible to change the product by a non-flammable one.

5.2.3 As the second protection layer, there are generally automatic control systems available for the process or equipment. So, as a third layer is likely to be attained a proper alarm system, with continuous supervision by qualified operation personnel.

5.2.4 The next protection layer, consisting of a SIS, the main object of this Standard, usually accompanies another one, formed by relief and prevention systems based on mechanical devices, such as safety valves, rupture discs and check valves.

5.2.5 The adoption of a SIS is only recommended if, after the application of the other risks reduction measures mentioned, the residual risk remains higher than the tolerable risk (see Figure 2). **[Recommended Practice]**

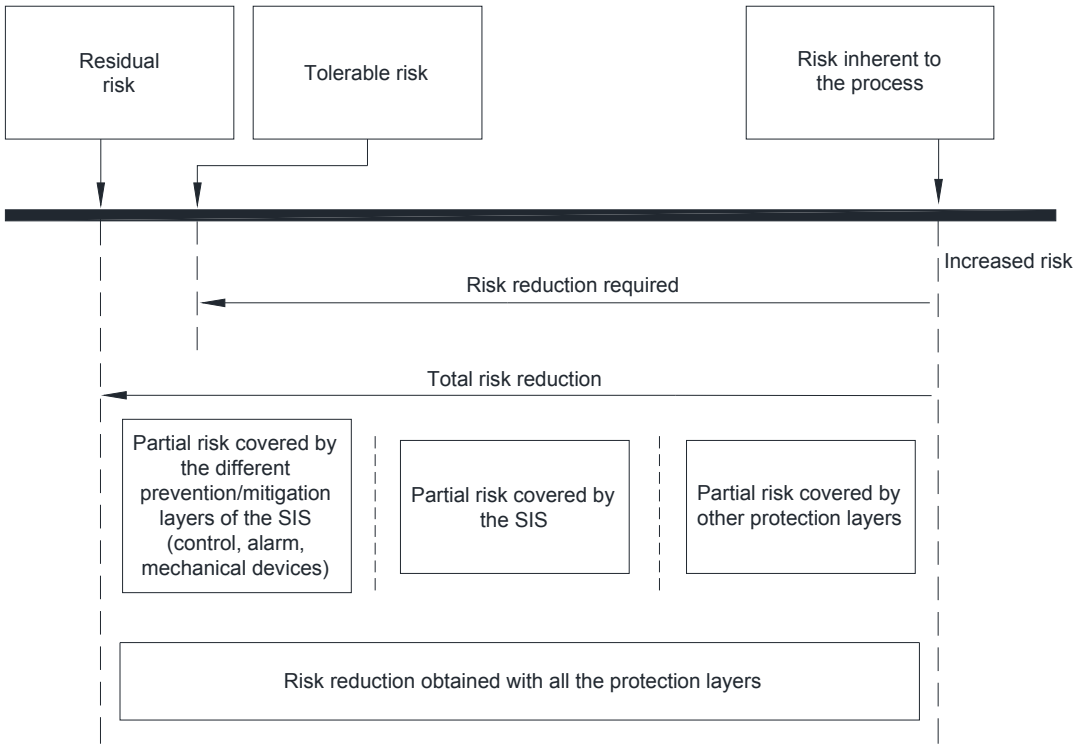

Figure 2 - Graphical Representation of the Risk Reduction

5.3 SIS Life Cycle

5.3.1 Once the need for one or more SIFs is confirmed, its application now constitutes a SIS itself. The steps required to implement a SIS include conception, design, installation, operation, maintenance and deactivation, and are called SIS life cycle (see Figure 3).

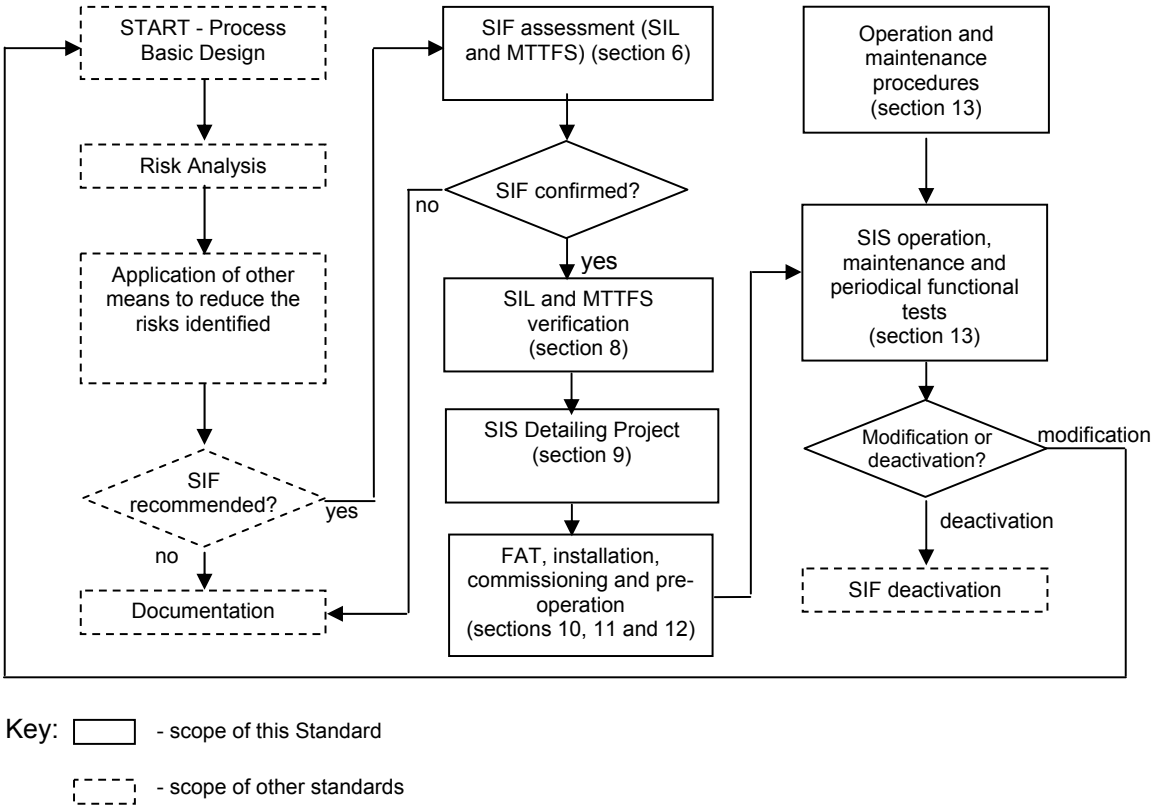

Figure 3 - SIS Life Cycle Model

5.3.2 To enable the application and operationalization of a SIS, the existence of a management system implemented to its life cycle is required, based on a Safety Plan according to IEC 61511-1, capable of ensuring that:

a) the people and organizations involved in each phase of the life cycle are identified, and their respective responsibilities are assigned;
b) the training programs required are applied;
c) each phase foreseen is performed and documented;
d) the documents generated are distributed, controlled and kept up to date;
e) control verifications are periodically performed.

5.4 SIS Basic Design Structuring

5.4.1 The SIS basic design shall establish and record, in an organized and systematic way, the technical specification requirements necessary for each of the SIFs that are part of the SIS, including those created during the process basic design (usually recorded in engineering flowcharts, and cause and effect matrices), and those created as recommendations of the hazard identification technique, applied during the plant risk analysis phase.

5.4.2 The process engineering discipline is responsible for defining, during the SIS basic design stage, the adjustment values (trip and alarm set point) and the process safety time for each SIF.

5.4.3 All SIFs shall be executed by the SIS logic solver. The SIF execution by the BPCS is not allowed.

5.4.4 Only the implementation of SIFs in the SIS is recommended. **[Recommended Practice]**

5.4.5 The SIFs should only include devices and solvers required to reduce risks in the respective scenarios. **[Recommended Practice]**

5.4.6 Each SIF shall have an exclusive alphanumeric identification (tag).

5.4.7 Each SIF shall be documented on a data sheet that gathers the main SIF specifications, composing a set of information equivalent to the Safety Requirements Specification (SRS) defined in IEC 61511-1.

5.4.7.1 The use the model presented in Annex D is recommended to document SIFs data. **[Recommended Practice]**

5.4.7.2 At the end of the basic design, at least the set of information listed on the SIF Data Sheet form, suggested in Annex D, shall be defined and documented.

5.4.8 The SIS basic design documentation shall form a distinct set separate from the other project documents not related to the SIS (see ISA.84.91.01)

5.4.9 The SIS basic design documentation will follow the SIS throughout its life cycle, and shall be filed in the technical documentation system of the respective industrial facility, being always up to date, in a traceable and auditable way, due to eventual reviews in the plant.

5.4.10 The elaboration of the SIS basic design shall consist, fundamentally, on execution of the following tasks, which are detailed in the next sections:

a) SIFs identification (not covered by this Standard);
b) SIFs assessment (see Section 6);
c) definition of the SIS implementation requirements (see Section 7);
d) verification of the SIL and of MTTFS required for each SIF (see Section 8).

6 SIS Basic Design - SIFs Assessment

6.1 General Considerations

6.1.1 The assessment phase consists, basically, of determining two important performance parameters, in order to elaborate the SIS specification, namely:

a) Safety Integrity Level (SIL);
b) Mean Time to Fail Safe (MTTFS).

6.1.2 The SIFs assessment shall be performed during the basic design phase of a new plant and during reviews that might be performed in the design of an existing plant.

6.1.3 The SIFs assessment shall not replace the risk analysis study, but it shall complement its execution, assisting in the specification of an appropriate SIS.

6.1.4 The SIFs should be assessed by the same team that did the risk analysis, together with or immediately after the risk analysis completion. **[Recommended Practice]**

6.2 SIFs Assessment Team Composition

6.2.1 The team assigned to assess the safety instrumented functions shall be multidisciplinary, composed, throughout the entire execution of this activity, of a team leader and of professionals representing at least the following areas:

a) process;
b) instrumentation and control;
c) operation;
d) safety.

6.2.2 Specialists from specific areas, such as static, thermal, dynamic or electrical equipments, shall be consulted by the assessment team, whenever it needs, to confirm premises assumed in the risk estimates involving such specialties.

6.2.3 The representative from the process area shall have participated in the specific basic design to be analyzed, so as to ensure a good knowledge about it.

6.2.4 The representative from the instrumentation and control area shall know the instrumentation design and the plant automation architecture, as well as shall be experienced and/or trained specifically in Safety Instrumented Systems (SIS).

6.2.5 The representative from the operation area shall:

a) be experienced in process concerned;
b) be linked to the future operation of the plant concerned.

6.2.6 The representative from the safety area shall:

a) be familiar with the health, safety and environmental policies, guidelines, standards and laws applicable to the plant concerned;
b) be linked to the future operation of the plant concerned.

6.2.7 The leader of the assessment team shall be experienced in risk analysis, shall be trained specifically in the method to be used, and shall have previously anticipated in other SIF assessment processes.

6.2.8 It is admissible that the leader of the assessment team accumulates the function of representative from any of the areas listed in 6.2.1, provided that he/she meets the requirements for this post.

6.2.9 The leader of the assessment team shall ensure the organized, systematic and consistent application of the method used, guiding the other team members in this sense.

6.2.10 Before starting the analysis, the leader of the assessment team should promote a leveling of the understanding about the method to be used by all participants, in order to ensure the minimum familiarity with the technique and its specific terminologies. **[Recommended Practice]**

6.2.11 At the end of the study, the report shall be prepared and agreed to by the entire team. As to the items for which a consensus could not be reached, the reasons shall be recorded.

6.3 Preparation for SIFs Assessment

6.3.1 The following documents shall be available, in their latest reviews, for use in the safety instrumented functions assessment process:

a) engineering flowcharts;
b) automatic actions description (cause and effect matrix, logic diagram, or other equivalent document);
c) risk analysis report, if issued.

6.3.2 Additional information about failures, hazardous events and accidents related to the process or equipment under the SIF protection may also be used, provided that their sources are properly documented on the SIF Data Sheet.

6.3.3 Among the scenarios identified by the risk analysis, shall be selected for assessment those in which there is interlocking as safeguard or recommendation. Other scenarios may be assessed at the team's criteria.

6.4 Assessment of the Safety Integrity Level required for a SIF

6.4.1 For each SIF, a SIL shall be attributed in accordance with the risk reduction required for such SIF (see Table 1).

NOTE For SIFs operating in continuous mode or with high demand (more than one demand per year, or two or more demands at each interval between tests), the SIL is correlated with a frequency of dangerous failures per hour. For example, SIL 1 is equivalent to a frequency between 10^{-6} and 10^{-5} per hour (see Table 4 of IEC 61511-1).

Table 1- SIL Scale for SIF in Demand Mode

RRF	PFD_{avg}	SIL
> 10 to ≤ 100	≥ 10^{-2} to < 10^{-1}	1
> 100 to ≤ 1,000	≥ 10^{-3} to < 10^{-2}	2
> 1,000 to ≤ 10,000	≥ 10^{-4} to < 10^{-3}	3
> 10,000 to ≤ 100,000	≥ 10^{-5} to < 10^{-4}	4

6.4.2 The assessment of the SIL required for a SIF shall consider the consequences about:

a) personal safety (S);
b) environment (E);
c) company property (L).

6.4.3 The SIL required for the SIF shall be the highest among those determined for each of these three aspects.

NOTE If the risks associated with the personal and environmental aspects are both considered worthless, causing the SIL to be determined only by the risk associated with the company property aspect, the cost-benefit analysis is recommended to determine if it is worth implementing the SIF or not. This analysis shall confront the costs of the harm to be prevented by the SIF with the implementation, maintenance and spurious trips costs of the SIF throughout its life cycle. **[Recommended Practice]**

6.4.4 If a single SIF is the safeguard for several scenarios, the required SIL shall be the highest among those obtained for each scenario.

6.4.5 In this Standard two distinct methods to assess the SIL required for a SIF are presented, namely:

a) risk graphs (Annex A): qualitative method, with a simpler and more immediate application, that, therefore, usually leads to more conservative results, with higher SILs and a larger number of SIFs;
b) LOPA (Annex B): semi-quantitative method that takes into account risk reductions by other protection layers different from the SIS, allowing more consistent assessments of the scenarios and producing a more complete documentation.

6.4.6 When choosing the most appropriate assessment method, the following shall be taken into account: the complexity of the process; the nature and severity of the consequences; the availability of information about the hazard scenarios; the qualification and experience of people available for the assessment work.

6.4.7 The use of the LOPA method is recommended. **[Recommended Practice]**

6.4.8 Once the required safety integrity level is determined, this SIL shall be recorded on the respective SIF Data Sheet.

6.4.9 If the result of SIF assessment indicates a required SIL greater than 3, other means of risk reduction shall be applied, in order for the SIF to have its required safety integrity level under SIL 4. Guidance and precautions to be taken aiming to reduce the required SIL in a safe way can be found in ISA TR 84.00.04 Part 1.

6.4.10 In case of the assessment result indicates there is no requires SIL, the provisions of 5.4.4 shall be observed.

6.5 Assessment of a SIF´s Spurious Trips Frequency

6.5.1 Aiming not to jeopardize the availability of plant or equipment under the SIF protection, a minimum value, considered acceptable in the application, shall be stipulated for the SIF Mean Time to Fail Safe (MTTFS), related to spurious trips.

6.5.2 The use of Table 2 is recommended to determine the minimum acceptable MTTFS. **[Recommended Practice]**

Table 2 - Criteria for Determining the Acceptable MTTFS

Spurious trip cost (US$)	Acceptable MTTFS (years)
≤ 10 000	Spurious trip tolerance not required
> 10 000 to ≤ 100 000	25
> 100 000 to ≤ 1 000 000	50
> 1 000 000	Reassess the SIF due to the significant impact caused by its spurious trip
NOTE 1 Besides the production loss (lost profit), the spurious trip cost also takes into account the costs associated with other possible consequences related to the unexpected shutdown and to the subsequent plant startup, such as: harm to equipment (breaking of refractories, pipes coking, etc.), contract penalties due to production interruption, environmental harm (excessive relief for a flare, noise when opening safety valves), harm to the company image etc.	
NOTE 2 The tolerance to the spurious trip, even when not justified by Table 2, may be implemented to minimize risks associated with these trips and with the subsequent startups.	

6.5.3 If the spurious actuation of a SIF leads to a new accidental scenario, the associated risk shall be tolerable. For example, a relief system of toxic or flammable material shall be directed to a safe place.

6.5.4 It shall be taken into account that the actuation of a SIF may originate other protection actions. For example: the low flow rate of gas causes a trip in the compressor, which in turn, causes a trip in the charge pump.

6.5.5 Once the MTTFS is determined, it shall be recorded on the respective SIF Data Sheet.

7 SIS Basic Design - Implementation Requirements

7.1 Segregation between SIS and BPCS

7.1.1 SIFs shall have their physical implementations separated from the BPCS loops. Therefore, at least the following components shall be segregated:

a) process taps (see Note 1);
b) impulse lines;
c) sensors;
d) signal wirings;
e) junction boxes;
f) multicables;
g) terminal blocks;
h) control and marshalling panels;
i) fuses and circuit breakers;
j) Logic Solver;
k) final elements (see Note 2).

NOTE 1 It is admissible to share process taps or nozzles of the BPCS instruments with redundant SIS sensors. If it is necessary to use more than two SIS sensors for a same orifice plate, the assessment of one of the following solutions is recommended:

a) use of the “T” fitting in the taps for clean fluids;
b) use of special flanges capable of resisting the additional number of drillings required;
c) use of two orifice plates when the pressure drop is not relevant.

NOTE 2 For shutdown of electric machines (motors, generators), the entire shut off circuit, including circuit breakers and contactors, is considered as final element of the SIS.

7.1.2 It is admissible to share between SIS and BPCS for the following components:

a) primary flow rate elements of the types orifice plate, venturi or v-cone;
b) gears (rotation measurement);
c) thermometric wells;
d) air supply branches.

7.1.3 The shared use of a control valve as the second final element of a SIF is only admitted in the cases in which all items below are met:

a) the installation of a second stop valve has a very high cost or is not usual;
b) the control valve cannot be an integral part of another IPL;
c) the SIL obtained shall be verified using a quantitative method that takes into account the cases in which the failure in the control valve is the initiating cause;
d) the tightness of the control valve is compatible with the SIF requirements;
e) the failure mode of the control valve is the same as the block valve;
f) when the safety position is closed, the by-pass valve is kept locked, and its position is continuously monitored by the SIS Logic Solver with the use of a limit switch;
g) the safety actuation on the control valve is made by the SIS Logic Solver by means of a dedicated solenoid valve.

7.2 Segregation between Different SISs

7.2.1 Plants that operate independently or have independently scheduled maintenance shutdowns shall have separated SISs.

7.2.2 For process equipments located within the same plant, which have independently scheduled maintenance shutdowns, it is recommended to segregate the following components of each respective SIS: junction boxes, multicables, I/O modules and application programs. **[Recommended Practice]**

7.2. The SIS should be segregated from other safety systems ruled by specific standards. **[Recommended Practice]**

EXAMPLE
— ABNT NBR 12712 for gas pressure reduction stations;
— ABNT NBR 17240 for fire alarm detection systems;
— API 670 for machine protection systems.

7.3 Segregation Among Redundant Channels of a SIF

7.3.1 For SIFs with redundancy of sensors and/or final elements, it is recommended to segregate the following components of each respective channel: **[Recommended Practice]**:

a) process taps;
b) impulse lines;
c) signal wirings;
d) junction boxes;
e) multicables;
f) terminal blocks;
g) fuses and circuit breakers;
h) I/O modules.

7.3.2 In case of redundant temperature measurement, the use of one single well for more than one sensor is admitted.

7.4 Power Supply

7.4.1 The electric power supply for the SIS shall be provided from a redundant direct current system consisting of two sets of chargers, two battery banks and two distribution panels (DCP) with circuit breakers for interconnection, being one DCP equal to the other (mirror), and each one of these sets powered by independent feeders.

7.4.2 This system shall distribute the electrical power to:

a) Logic Solver power supply modules;
b) power supply of analogic sensors;
c) energization of the discrete sensor circuits;
d) energization of the final element circuits.

7.4.3 The requirements established in PETROBRAS N-329 shall be observed for the design of accumulator batteries, and those in PETROBRAS N-332 shall be observed for charges design.

7.4.4 The Logic Solver power supply modules, as well as the power supplies for the sensors and final elements shall be redundant.

7.4.5 It is recommended that the Logic Solver power supply modules, as well as the power supplies for the sensors and final elements, have independent electric power inputs, each one being supplied by a distinct DCP. **[Recommended Practice]**

7.5 Communication between the Field Devices and the Logic Solver

7.5.1 The use of digital communication protocols for transmitting process signals in safety functions is not allowed.

7.5.2 The use of HART digital communication protocol is only allowed for diagnostic purposes, and the remote configuration functionality shall be inhibited.

7.5.3 The use of marshalling panels, intrinsic safety barriers, isolators, signal converters, or other elements between the field devices and the Logic Solver is not recommended. **[Recommended Practice]**

NOTE 1 In case of electric machines (motors) actuation circuits, the interposing relay is considered an integral part of the final element.

NOTE 2 If there are intermediate elements, they shall be recorded on the SIF data sheet as an integral part of the sensor or final element, and considered in the reliability calculations.

7.5.4 If the application of intrinsic safety barriers and/or signal isolators is required, such elements shall be:

a) installed in the same panel as the Logic Solver, and not distributed in other locations/panels;
b) supplied by the power sources located in the Logic Solver panel.

7.6 Sensors

7.6.1 The sensors shall be implemented by transmitters operating in analog mode at the range of 4 mA to 20 mA, directly powered by the respective SIS Logic Solver panel.

7.6.2 In cases where the use of transmitters is not technically feasible, techniques that reduce undetected failures shall be used, such as: line supervision, energized signal circuits under normal operating condition of the plant or equipment.

7.6.3 Aiming to minimize the occurrence of spurious trips, it is recommended that the transmitters' internal diagnostic is configured in order to lead the output signal to the following values in case of failure, being items 7.8.8 and 7.8.14 also observed: **[Recommended Practice]**

a) below 3,6 mA (under-range) for cases where the trip actuation occurs towards the increase of the transmitter output signal;
b) over 21 mA (over-range) for cases where the trip actuation occurs towards the decrease of the transmitter output signal.

7.6.4 It is recommended that the SIS sensors and the sensors used in the BPCS to measure the same variables have the same range and compatible uncertainties, so as to allow their direct comparison, being the deviation alarms likely to be implemented in the BPCS. **[Recommended Practice]**

7.6.5 The sensors shall be painted in safety orange, in accordance with PETROBRAS N-1219. The partial painting of the sensor body is acceptable. Example: only the transmitters' covers are painted.

7.6.6 For the SIFs sensors assessed as SIL 3, the use of diverse redundancy is recommended. **[Recommended Practice]**

7.7 Final Elements

7.7.1 It is recommended that the SIS valves use pneumatic actuators. Electric or hydraulic actuators may be used in the cases where pneumatic actuators are not practicable. For example, unavailability of instrument air. **[Recommended Practice]**

7.7.2 SIS valve actuators shall operate normally pressurized or energized, and the lack of such pressurization or energization shall cause the valve to return to the position established as safe, by means of the energy storage device (e.g.: previously compressed spring, hydraulic accumulator, etc.).

NOTE In some cases, the risk of spurious trip may be high, which justifies the use of normally de-energized actuation mode. However, it is necessary to demonstrate that the safety integrity level required is reached and kept throughout the installation life cycle.

7.7.3 The SIS valves shall not have hand wheels for manual actuation.

7.7.4 For SIS valves and their respective actuators, at least the following aspects shall be specified:

a) adequacy of the valve type and of its materials to the process and operation conditions (especially for low demand);
b) tightness required;
c) failure modes of the valve actuator;
d) normal flow direction that tends to take the valve to the safety position;
e) opening and closing times of the valve and actuator set, compatible with the SIF requirements;
f) device for monitoring the safety position.

7.7.5 In case the SIF final elements are actuation circuits of electric machines (motors), the status of such equipment shall be displayed in the operation interface.

7.7.6 For the SIF assessed as SIL 3, of which actuation is made in an electric motor, the engine status confirmation should occur through the monitoring of variables such as axis rotation or electric current. **[Recommended Practice]**

7.7.7 In applications involving the protection of essential equipment, driven by electric motor, is recommended the use of the Break Failure (BF) function in the electric protection relay of the motor circuit breaker. **[Recommended Practice]**

NOTE The impacts of the shutdown of the remaining electric loads affected by the BF actuation shall be assessed.

7.7.8 It is recommended that the interposing relays are installed in the terminal boxes that make an interface with electric equipment. **[Recommended Practice]**

7.7.9 For solenoid valves that command pneumatic actuators, the following aspects shall be specified:

a) normal operating condition: energized coil;
b) minimum operating air pressure;
c) flow rate capacity suitable to the required actuation time;
d) protection of air leaks against clogging by dirt, insects and frost.

7.7.10 The use of solenoid valves with mechanical manual reset is not recommended. **[Recommended Practice]**

7.7.11 In case the SIF Data Sheet indicates the need for performing valve partial stroke tests (see ISA TR 96.05.01), these tests shall be implemented by devices specially designed for this application and with a certification adequate to the SIL required, in accordance with IEC 61508-1. The certificate shall be submitted for PETROBRAS' approval. The application restrictions indicated in the respective safety manuals and reports accompanying the compliance certificates shall be observed.

7.7.12 The SIS final elements shall be painted in safety orange, in accordance with PETROBRAS N-1219. The partial painting is acceptable, e.g.: only solenoid valves covers and valve actuator casings are painted.

7.7.13 For the SIFs final elements assessed as SIL 3, the use of diverse redundancy is recommended. **[Recommended Practice]**

7.8 Logic Solver

7.8.1 The Logic solver shall meet all technical requirements expressed in the Specification Data Sheets of the SIFs composing the SIS.

7.8.2 The Logic Solver shall have a certification of compliance with IEC 61508-1 for applications with safety integrity level equal or higher than the highest SIL required among the SIFs allocated on it. The certificate shall be submitted for PETROBRAS' approval. The application restrictions indicated in the respective safety manuals and reports accompanying the compliance certificates shall be observed.

7.8.3 The Logic solver shall be physically implemented through a Safety CP in all applications where the total amount of sensors and final elements is equal or greater than 20.

7.8.4 Upon the express agreement of the Company's Organizational Unit, the Logic Solver may be physically implemented through a non-programmable electronic technology, in which the total quantity of sensors and final elements is less than 20, and the logic required has low complexity.

7.8.5 The use of a safety CP adequate to SIL 3 applications as SIS Logic Solver is recommended, even though SIL 3 is not required for any of the respective associated SIFs. This practice enables a greater flexibility in the SIFs design. **[Recommended Practice].**

7.8.6 All CP safety modules (input and output modules, power supplies and processors) related with the SIFs logic solving shall:

a) not cause a spurious trip by simple failure;
b) enable maintenance interventions without the need for deenergizing or interrupting the logic solving (hot swapping).

7.8.7 It is recommended that the logic solver has resources to detect a signal indicating that the sensor is out of the normal operational range, and to attribute to the sensor a failure status (out of specification) when below 3,6 mA or above 21 mA. **[Recommended Practice]**

7.8.8 The Logic solver and its auxiliary equipment shall be installed on a panel exclusive for this purpose. This set shall be compatible with the specific environmental and electric conditions of the installation site.

7.8.9 The Logic solver panel and the SIS junction boxes shall have identifications different from the others. The partial painting of the panel and boxes in safety orange color and the inscription "SIS" on the panel nameplate are suggested.

7.8.10 In case of interaction between distinct logic solvers, their actions shall be coordinated so as to ensure the conduction of the process as a whole to a safe state.

7.8.11 The SIF solving through a digital communication link between distinct safety CPs is conditional upon the certification of the safety integrity level achieved by the whole set, including the respective communication link, according to IEC 61508 - Parts 1, 2 and 3. The certificate shall be submitted for PETROBRAS' approval. The application restrictions indicated in the respective safety manuals and reports accompanying the compliance certificates shall be observed.

7.8.12 The application program shall:

a) be developed in accordance with the logic diagram of the SIS detailing design;
b) be developed considering the adequate restrictions regarding the use of the utility program, compatible with the required integrity level, as indicated in the safety manual of the CP selected;
c) have a scan time compatible with the SIFs need, limited to 250 ms in the safety CP;
d) provide the BPCS with information, according to 7.12.

NOTE 1 It is recommended to use the Function Blocks programming language (see IEC 61131-3). **[Recommended Practice]**
NOTE 2 It is not recommended to use the text-type or Ladder diagram programming languages. **[Recommended Practice]**

7.8.13 In order to minimize the occurrence of spurious trips, sensors identified as in failure state should be automatically bypassed by the application program, respecting the limitations imposed by 7.11.3. **[Recommended Practice]**

NOTE 1 The duration of this automatic by-pass shall be defined in the detailing design phase, and cannot exceed 8 hours. During this period, the unit operation shall decide whether actuating the manual by-pass for the maintenance of the sensor concerned or not.
NOTE 2 The total duration of the by-pass (automatic + manual) shall comply with the limit established in the specific procedure for the SIF concerned.
NOTE 3 If the automatic by-pass timer ends without the manual actuation of the maintenance by-pass according to 7.11.3.5, the application program shall assign the trip status to the sensor in failure, with the consequences programmed in the SIF logic.

7.8.14 It is recommended that the application program treats the cases of SIFs with redundant sensors, in order to avoid spurious trips by the false diagnosis of simultaneous failure in all sensors, due to the real excursion of the process variable outward the normal operational range in the direction opposite to the trip. **[Recommended Practice]**

EXAMPLE

Reassess the operational range and/or consider the possibility of extending the under/over-range limits beyond those established in 7.6.3.

NOTE The possible implementation of a specific logic to avoid this type of spurious trip shall be preceded by a careful evaluation of the common cause failure possibilities of the sensors.

7.9 Manual Trip Command

7.9.1 The amount and coverage of manual trip commands of the plant or equipment shall be defined in the process basic design phase, and shall be described on the respective SIF Data Sheets.

7.9.2 The manual trip commands should be implemented through electromechanical pull to activate buttons, with a double contact normally closed, connected in series, installed on a place of easy access by the operation team and provided with a protection against improper activation. **[Recommended Practice]**

7.9.3 The signals of the manual trip command should be processed by the SIS Logic Solver. **[Recommended Practice]**

7.10 SIF Reset

7.10.1 Every SIF shall have a reset command to enable the controlled restart of the plant or equipment operation, protected by the SIF, when, after a trip event, no demand condition is verified.

7.10.2 After the occurrence of a demand and the consequent actuation of the respective SIF, the command signal to the final element shall remain in the activated state until the receipt of a manual reset command by the operator.

7.10.3 The SIF automatic reset is not allowed.

7.10.4 The manual reset command shall only be implemented through a physical button located in the field when required on the SIF Data Sheet.

7.10.5 The SIF reset signal shall be of type short-duration pulse.

7.11 SIF By-Pass

7.11.1 General Considerations

7.11.1.1 The by-pass purpose is to restrict the actuation of a SIF, whether due to the need for operation start or for a maintenance intervention during the plant or equipment operation.

7.11.1.2 Every by-pass manually activated shall be done through screens pre-configured in the BPCS HMI, having necessarily a signaling for status confirmation.

7.11.1.3 It is not allowed to by-pass the SIF Logic Solver outputs.

7.11.1.4 It is not allowed to by-pass the manual trip command.

7.11.1.5 It is not allowed to force variables in the safety CP application program for SIF by-pass purposes.

7.11.2 Operation Startup By-Pass

7.11.2.1 Only the SIFs that, due to the initial process status, prevent the plant or equipment subject to protection from starting shall have a by-pass command for the operation startup. Examples: low pressure in the gas header to the furnace, low rotation speed of the compressor, low load flow rate, etc.

7.11.2.2 The by-pass commands for operation start should be deactivated through automatic functions, avoiding the use of manual command to this end. **[Recommended Practice]**

EXAMPLE

— process condition: monitors the process variable value until the end of the operation startup condition;
— time: adjustment for a time period not much higher than the necessary for the normal execution of the startup procedure;
— combination of the above.

7.11.2.3 The by-pass commands for operation start shall be kept deactivated when the plant or equipment subject to the SIS protection are not in startup procedure.

7.11.3 Maintenance By-Pass

7.11.3.1 It is recommended that no more than one SIF, belonging to a same plant or equipment, be by-passed at the same time. **[Recommended Practice]**

7.11.3.2 The duration of the maintenance by-pass shall be the lowest possible. If the by-passed device is not repaired within the MTTR assumed in the reliability calculations, the actions predefined in the specific procedure shall be taken in order to keep the plant or equipment in the safe state. The most common example of procedure is the adoption of a special operational regimen (reduction of the process unit charge, operation in state of alert, etc.), with the possibility of culminating in the manual activation of the safety function.

NOTE 1 It is not recommended initiate a startup of plant or equipment with a SIF in by-pass for maintenance. **[Recommended Practice]**
NOTE 2 The startup of a plant or equipment with a SIF in by-pass for maintenance leads to the immediate execution of the actions defined in the specific procedure.

7.11.3.3 For the SIFs that have redundancy on its sensors, the maintenance by-pass shall degrade the respective voting architectures as follows:

a) from 1 out of 2 to 1 out of 1;
b) from 2 out of 2 to 1 out of 1;
c) from 2 out of 3 to 1 out of 2.

NOTE If there is the by-pass of more than one sensor in a same SIF, the specific procedure shall be adopted, as per 7.11.3.2.

7.11.3.4 For the SIFs that do not have redundancy on its sensors, there shall be a maintenance by-pass command only in the SIFs that satisfy both the following requirements:

a) existence of another mean to monitor the process variable concerned;
b) the process dynamics allows the operator to timely activate the manual trip command.

7.11.3.5 The SIF shall be by-passed according to a specific procedure and it shall be developed for this purpose during the SIS detailing design phase. This procedure shall include the control of the by-pass duration (see 13.1.5), and shall comply with the plant or equipment operational standards, subject to the SIS protection.

EXAMPLE

After being authorized, the operator activates a by-pass request command, specific for the respective intended sensor, by means of the BPCS HMI. Then, the maintenance technician shall activate a physical switch in the SIS Logic solver panel, which enables the respective bypass command. While the by-pass is active, an alert may be periodically announced.

7.12 Operator Interface

7.12.1 It is considered that the plant or equipment subject to SIS protection is monitored and controlled by a BPCS, of which HMI also serves as interface between the SIS and the plant operator. Therefore, the following SIS information shall be presented in the BPCS HMI:

a) SIFs actuation indication (trip events);
b) indication of the first event in a trip sequence;
c) indication of status (valve open/closed, motor turned on/off) and diagnostic of the final elements (good/ in failure);
d) graphical representations of the logic, showing the Logic Solver inputs and outputs statuses, in real time with trip values (example: animated cause and effect matrices);
e) supporting texts;
f) sensors by-pass status (see Note);
g) summary of the Logic Solver alarms (electrical power failure, high panel temperature, modules in failure, wiring disruption, safety CP hardware failures, safety CP software errors, etc.);
h) indications and diagnostics of analogical sensors;
i) discrete sensors statuses;
j) alarms that precede the SIFs actuation (pre-trip alarms);
k) safety CP communication failure.

NOTE For temporized by-passes is recommended to show of the remaining time interval for deactivation. **[Recommended Practice]**

7.12.2 The following commands shall be previously configured and sent from the BPCS operation interface to the SIS Logic Solver:

a) acknowledgement of the first event;
b) acknowledgement of alarms;
c) operation startup by-pass;
d) maintenance by-pass;
e) SIF reset.

7.12.3 Every failure automatically identified in a SIS device, either by a specific diagnostic function, by deviation in the monitored variable value, or by any other method, should generate an alarm in the BPCS operation interface. **[Recommended Practice]**

NOTE Deviation in the monitored variable value means a difference greater than twice the total error probable between the SIS and BPCS analogical sensors values, for the same process variable.

7.12.4 The synchronization between the internal clocks of the BPCS and of the SIS Logic Solver is recommended, in order to enable analyses of sequences of events. **[Recommended Practice]**

7.12.5 It is acceptable a maximum delay of 3 seconds between the occurrence of a trip action activated by a SIF and the respective indication in the BPCS operation interface.

7.12.6 There shall be a pre-trip alarm whenever there is sufficient time for the corrective action by the operator.

7.12.7 The visual identification for the first event of a trip sequence shall be outstandingly presented in the operation interface.

7.13 Maintenance and Engineering Interface

7.13.1 The interface for maintenance and engineering shall be performed in an industrial PC microcomputer, and shall have the following functions:

a) safety CP configuration and storage of its configuration;
b) diagnostic with all details on failures detected in the Logic Solver;
c) storage of the auditable history of actions/interventions in the SIS, with TAG, date, time and personal identification, so as to allow the posterior analysis of the occurrences.

7.13.2 The maintenance and engineering interface shall be provided with a password for access.

7.13.3 There shall be at least one engineering/maintenance station networked for the various safety CPs of an industrial site.

7.13.4 The existence of a local communication port in each safety CP is recommended, for network unavailability cases. **[Recommended Practice]**

7.14 Communication Interface with the BPCS

The use of redundant communication cables and modules between the Logic Solver and the BPCS is recommended. **[Recommended Practice]**

7.14.2 The communication protocol used should block commands different from those previously defined in 7.12.2 from the BPCS to the Logic Solver. **[Recommended Practice]**

7.14.3 In case of a failure, the communication interface shall:

a) not compromise SIFs execution;
b) not cause spurious trip;
c) announce the failure in the operation interface.

7.15 Response and Delay Times

7.15.1 The SIF response time should equal or be under half the process safety time informed by the process discipline. **[Recommended Practice]**

7.15.2 The use of the delay time in the SIFs should be assessed so as to reduce the spurious trips frequency of occurrence. **[Recommended Practice]**

8 SIS Basic Design – Verification of the SIL and MTTFS Required for Each SIF

8.1 The verification phase aims to provide the basic design with greater consistency, avoiding significant changes during the detailing design.

8.2 Reliability calculations shall be made in order to verify the compliance with the SIL and MTTFS values required of each SIF. Example, methodology presented in ISO TR 12489.

8.2.1 The simple voting architecture (1 of 1) with components for general use shall be initially considered. If necessary, redundant components, components with higher reliability, or partial test devices may be adopted.

NOTE The indication, after the calculations, that the tolerance to failure is not required does not invalidate the application of other redundancy criteria, such as operational flexibility, including the execution of SIF tests during the plant or equipment operation.

8.2.2 For the SIFs of which the required SIL equals 3, the application of the tolerance to failure is compulsory for the demand and for all SIF components.

8.3 The reliability calculations of each SIF shall be recorded in a specific calculation memory containing the following information:

a) voting architecture of the SIF devices;
b) devices used (description, brand and model);
c) failure rates of the devices used in the process conditions considered (see Notes 1 and 2);
d) device diagnostic coverage factor;
e) tests coverage factor;
f) common cause factor;
g) MTTR considered in the industrial site concerned;
h) time interval considered between periodic tests;
i) calculation method adopted;
j) identification of the sources of the failure data used;
k) requirements and means to conduct tests during the normal operation campaign, if needed; e.g.: partial stroke tests in valves;
l) special requirements applicable; examples: use of an intrinsic safety barrier (see Note 3), energization for trip (see Note 4);
m) calculation criteria considered. Example: all failures detected during the tests are corrected, the devices fixed are as good as new, the failure rates are constant in time, etc.

NOTE 1 The devices failure rates to be used shall be obtained from databases established by the Operating Unit, and the parameters adopted shall be recorded.

EXAMPLE

EXIDA - Safety Equipment Reliability Handbook;
SINTEF - Reliability Data for Control and Safety Systems;
IEEE - STD 500 Reliability Data.

NOTE 2 The Operating Unit should choose a single database and use it in all its SIS applications, so as to maintain a coherence among the verification results of the SIL reached. **[Recommended Practice]**

NOTE 3 When using the failure rates informed by manufacturers, the correction factor should be added in order to cover the failures caused by the installation (tap clogging, for example) and by the process conditions (operation temperature, corrosive liquids, aggressive environment, etc.). **[Recommended Practice]**

NOTE 4 In case the use of any element between field devices and the Logic Solver (intrinsic safety barrier, isolator, signal converter, interposing relay, etc.) is required, its failure rate shall be considered in the SIF SIL and MTTFS calculations.

NOTA 5 Typically, a UPS failure causes a spurious trip, but its failure rate shall not be taken into account in the MTTFS calculation. On the other hand, if a SIF demands electric power to operate, the UPS failure rate shall be taken into account when calculating its PFD.

8.4 The MTTR assumed in the reliability calculations shall include the time (i) for the problem notification to the Maintenance Management, (ii) for the conduction of the repair itself and of post-repair tests, and (iii) for the device restoration to its normal operating condition.

8.5 The time interval between periodical tests shall be equal to or greater than the campaign period foreseen, being understood as the time interval between scheduled periodical shutdowns for the plant or equipment maintenance.

NOTE For the Units that do not have a defined campaign period, the time interval between periodical tests shall not be under 6 months.

8.6 A time interval between tests lower than the campaign period shall only be adopted in the cases where it is demonstrated with proofs that the SIL required cannot be achieved otherwise.

8.7 If a time interval between tests lower than the campaign period of the plant or equipment is adopted, the respective SIF shall be provided with resources/facilities that enable periodic tests during the normal operation campaign. These tests shall be performed without compromising the integrity of the plant/equipment, or the availability required for the plant (production losses). Such resources/facilities are part of the SIF design.

8.8 The calculation of the SIL obtained shall only consider the automatic safety actions indicated on the SIF Data Sheet. Secondary actions and manual trip commands shall not be considered in the SIF performance calculations (SIL or MTTFS).

NOTE The manual activation is a form of activation of the final elements of a SIF by the operator, provided for in the process design, but it is not part of the automatic protection function.

9 SIS Detailing Project

This Section establishes requirements for the preparation and presentation, in an organized and systematic way, the set of documents that enable the SIS correct physical and functional deployment.

9.1 General Requirements

9.1.1 The implementation of SIS detailed project shall consider the implementation requirements set forth in Section 7 of this Standard.

9.1.2 The following documents shall be available to start the detailed design stage:

a) SIF data sheet;
b) checking calculation memory of SIL and MTTFS and SIF;
c) process data sheet of SIS instrument process.

9.2 Documentation

9.2.1 The following referenced documents shall be produced during the phase of SIS detailed design and comply with the PETROBRAS N-1883 PETROBRAS, forming a distinct whole and out from the other detailed design documents (see ISA 84.91.01):

a) list of SIFs and SIS instruments (see Note 1);
b) datasheet of SIS instruments;

c) list of the SIS set points;
d) checking calculation memory of SIL and MTTFS SIF (Note 2);
e) SIS logical diagram;
f) SIS mesh diagram;
g) SIS interconnection diagram;
h) SIS communication list;
i) list of inputs and outputs of SIS Logic Executor;
j) list of electric charges of SIS (see Note 3);
k) technical specification of the SIS Logic performer;
l) technical specification of the SIS panels;
m) technical manual (manufacturer) of SIS Logic Executor (see Note 4);
n) technical manuals (manufacturers) of SIS sensors (see Note 4);
o) technical manuals (manufacturers) of SIS final elements (see Note 4);
p) application program of SIS Logic Executor (listing);
q) SIS panel designs;
r) SIS FAT plan (see Note 5);
s) SIS operation manual (see Note 6);
t) SIS maintenance plan (see Note 7).

NOTE 1 The list of SIFs and SIS instruments is a document divided into two parts: the first part shall list in numerical order each SIS SIF ("tag", description and SIL required) with the "tags" of the instruments (primers and final elements) that compose it. The second part shall list in alphabetical order each instrument of SIS ("tag", service, or flowchart source drawing and data sheet) with the "tags" of SIFs of which they are part.

NOTE 2 The checking calculation memory of SIL and MTTFS in the detailed project stage shall have the same calculations made during the phase of basic project. However, considering the voting architectures and specific models of primers, performer Logic and final elements effectively adopted, and include the response time of calculation of SIF and the delay time, if necessary.

NOTE 3 The list of electric charges of SIS will be required if the power to the SIS is unique.

NOTE 4 The technical manuals shall include, where applicable, the relevant certificates and compliance reports with the safety integrity level as the IEC 61508-1.

NOTE 5 The contents of the SIS FAT plan is defined in 10.2.

NOTE 6 The content of the SIS operation manual is defined in 13.1.

NOTE 7 The content of the SIS maintenance plan is defined in 13.2.

9.2.2 The SIF data sheets shall be reviewed in accordance with the consolidated information in the documents listed in a), b), c) and d) of 9.2.1.

9.2.3 After completion of the project stage, all documents of the SIS, including data sheets SIF, manuals, plans and reports shall be grouped in order to select the Security Instrumented System Manual.

10 Factory Acceptance and Preservation Test

10.1 Factory Acceptance Test - FAT

10.1.1 The SIS FAT shall be run after the completion Performer detailed design of logic and development of its application program and before the installation steps and the Logic Executor conditioning (see IEC 62381).

10.1.2 The objective of FAT is to verify operation compliance of Logic Executor set and application program according to the requirements previously established in SIF data sheets and in the logic diagram. The FAT shall be planned and executed in detail for non-compliance solution, defective equipment and to-do solution.

10.1.3 The SIS FAT shall be comprehensive, covering all SIFs and all possible logical combinations of each SIF.

10.2 Pre-Requirements to Perform FAT

10.2.1 During the step of SIS detailed project, a proper and specific planning shall be established for the FAT. Such planning shall be structured and presented in a document entitled Plan of FAT, which shall include the following items:

a) place of fulfillment;
b) reference documents, among which stands out the SIS Logical Executor Technical Specification;
c) competence of personnel assigned for test supervision and execution;
d) responsibility for test implementation and records;
e) responsibility for monitoring, testimony and release;
f) implementation schedule;
g) description of the test platform and tools;
h) list of tests to be performed;
i) execution procedure designed specifically for each type of test;
j) acceptance criteria;
k) report model of results record - FAT Report;
l) corrective action procedures;
m) classification of disputes and form for registration thereof;
n) reports of internal testing performed (pre-FAT).

10.2.2 The acceptance criteria are part of the test procedure and shall be based on ET Logic performer.

10.2.3 The FAT Plan shall be submitted for review and release by PETROBRAS. Only after releasing the FAT Plan can continue the FAT actual implementation.

10.3 FAT Implementation

10.3.1 The FAT shall be performed with the same equipment and application programs, utilities, and built that will actually be installed in the field.

10.3.2 It is recommended the use of process simulation capabilities with graphical display to aid the implementation of FAT. **[Recommended Practice]**

10.3.3 The FAT shall be conducted in accordance with the FAT Plan, including the completion of testing of the following types:

a) visual inspection;
b) electrical tests: insulation, continuity;
c) functional tests: Logic verification itself;
d) verification of the memory map and agreement with the project;
e) performance tests: Measuring "scan time" etc .;
f) environmental compatibility testing: electromagnetic compatibility, operating under the most specified room temperature etc.;
g) tolerance test failure: operation in degraded mode;
h) interface testing:

— reading and writing all channels, analog and digital input / output, as well as all diagnostic levels; example: 2 mA to 4 mA to 20 mA signal; party cable simulation monitored digital input signal;
— variation of the power supply voltage;
— verification of network communication;
— verification of pressurization, where applicable, the "range" of set pressure.

NOTE 1 The tests of analog inputs shall be carried out in at least five representative points of the measuring range. Example: 0 %, 25 %, 50 %, 75 % and 100 %.
NOTE 2 A temporary terminal to specific graphic displays shall be provided for testing.

10.3.4 For each test run shall be registered:

a) FAT Plan associated document number;
b) "tag" the SIF and its functionality test object;
c) of the associated test procedure document number;
d) identification of equipment and tools used;
e) description of the activities;
f) the results obtained for each individual SIF;
g) according to the acceptance criteria and to-do relationship;
h) signature of the performer and those responsible for the witness.

10.3.5 Records of tests shall be grouped into a document entitled FAT report, which shall be submitted for review and release by PETROBRAS.

10.3.6 In the case of running a test not be successful, the relevant event shall be recorded in the report, analyzed and applied the planned corrective actions.

10.3.7 During the implementation of the FAT shall not be made modifications to the application program that changes the functionality or integrity of SIFs. Any modification shall be made in accordance with 13.4 of this Standard.

10.3.8 For a better analysis of the implemented logic functionality, we recommend the inclusion in the monitoring team and witness the FAT, the operating personnel of the plant or equipment for which the performer Logic will be installed. **[Recommended Practice]**

10.4 Preservation

10.4.1 The purpose of this step is to provide information to maintain the physical integrity of the Logic performer during periods of transport and storage, before the onset of step.

10.4.2 A document entitled Preservation Plan shall be prepared, which shall include the following items:

a) description of the packaging for transport, including handling recommendations;
b) extreme conditions to which the equipment may be subjected, such as acceleration, temperature, humidity, pressure etc .;

NOTE If the sensitivity of the acceleration equipment is a critical factor, the use of shock detectors for transport shall be evaluated.

c) description of the receipt and inspection procedures on the mounting base;
d) description of the procedures for preservation in the pre- and post installation.

11 Installation and Conditioning for SIS Operation Starting

11.1 Installation

11.1.1 The installation step is to assure that all SIS devices are actually installed in accordance with its technical specifications and other requirements established in the design stage.

11.1.2 A document entitled Installation Plan shall be prepared, which shall contain:

a) list of materials and equipment to be installed;
b) description of installation activities which shall include checking the conditions of preservation plan;
c) procedures and techniques to be used at the facility;
d) implementation schedule of installation activities;
e) personal relationship responsible for supervising the activities of installation;
f) corrective action procedures.

11.1.3 The SIS shall be installed according to the Installation Plan, which shall comply with these requirements by PETROBRAS N-858.

11.1.4 During the execution of the installation any impediment to follow the planned project (eg. physical interference, reduced space, insufficient length of electric cable, etc.) shall be registered in installation report and forwarded for review of those responsible for preparing the project, which shall indicate solution to be adopted which does not degrade the technical requirements set out in the SIS project. The design documentation shall be updated accordingly.

11.2 Conditioning

11.2.1 The conditioning step is to assure that all SIS devices are operating individually in order to facilitate the realization of the pre-operation stage (see IEC 62337).

11.2.2 A document entitled conditioning plan shall be prepared, containing:

a) list of equipment to be conditioned (primers, Logic Executor, final elements etc.);
b) list of pending issues raised in the FAT has not remedied;
c) description of conditioning activities;
d) procedures and techniques to be used in conditioning (calibration, leak test etc.);
e) execution schedule of fitness activities;
f) personal relationship responsible for the supervision and registration of fitness activities.

11.2.3 The conditioning activities shall include the following tasks:

a) visual inspection;
b) check connections and electrical grounding resistance;
c) verification of sources of electricity, pneumatics and hydraulics;
d) parameterization and calibration of the primers and final elements;
e) checking the electrical interconnections between sensors and final elements with the Logic Executor panel, including continuity and insulation;
f) verification of all the stop valves and drain in the normal operating position;
g) check all energized SIS devices and internal diagnostics indicating good operational status;
h) checking the correct sending and receiving information from the operator interface (HMI);

i) measuring the operating times of the final elements;
j) confirmation of immunity to electromagnetic interference.

11.2.4 The SIS devices shall be conditioned according to the conditioning plan, which shall meet the requirements of PETROBRAS N-858. During the execution of conditioning activities shall be made records and prepared report conditioning in order to demonstrate compliance with the technical requirements of the SIS project.

12 SIS Pre-Operation and Final Acceptance

12.1 Pre-Operation

12.1.1 The pre-operation step shall be performed after completion of the installation steps and conditioning. The completion and successful this step is requisite for the start of operation of the plant or object of protection equipment for the SIS.

12.1.2 Pre-operation stage is designed to validate SIS through simulations and comprehensive functional testing, covering not only the joint operation of all SIS devices, but also with these other systems and / or equipment interconnected and effectively installed in the field.

12.1.3 A document entitled Plan for Pre-operation of the SIS shall be prepared, including:

a) Validation Checklist, including all relevant modes of operation of the process or equipment associated with the SIS (starting, steady, stop, maintenance etc.);
b) procedures and techniques to be used;
c) execution schedule of validation activities;
d) list of persons and organizations responsible for implementation, registration and monitoring of validation activities;
e) project list of documents to be used as a reference standard for validation (SIF data sheets, of cause and effect matrix logic diagram etc.).

12.1.4 It is recommended that the Pre-Operation Plan does not impose too many demands during the testing of final elements. **[Recommended Practice]**

12.1.5 The list of validation activities shall include at least:

a) simulation of the performance of each SIF, showing the functionality of Primer set designs, performer and logic element ends, including voting architectures;
b) confirmation of the limit values for performance of each SIF (set points to trip), as well as the delay time values;
c) simulation step by step starting sequence of the plant or equipment, including border controls and the performance of each SIF;
d) performance tests, including the SIFs response time;
e) confirmation of proper operation of the starting commands and manual stop;
f) confirmation of proper operation of the contour commands (Bypass) for maintenance;
g) confirmation of proper operation of the reset command;
h) confirmation of correct communication with the operator interface, including indications, alarms generated by the SIFs, event logging, cause matrix and lively effect etc.;
i) expected behavior of the confirmation of each SIF in cases of occurrence of: measuring off range, lack of energy, loss of pneumatic or hydraulic pressurization.

12.1.6 The activities performed in the SIS Pre Operation step shall be recorded in a validation report.

12.2 SIS Final Acceptance

12.2.1 The purpose of this step is to record conclusively the end of the pre-operation of SIS step, freeing it to start operation.

12.2.2 A document entitled Declaration of Acceptance SIS shall be prepared, which shall include the following records:

a) number of SIS Pre-Operation Plan used;
b) validated version of the application program;
c) tools and test equipment used;
d) identification of each SIF examined and the results of their tests;
e) test results with other interconnected systems (BPCS, other SIS);
f) description of the observed discrepancies;
g) name and signature of those responsible for plant operation or equipment.

12.2.3 Any discrepancy found between the result obtained and expected to be subjected to analysis, by those responsible for preparing the project, in order to decide correctly whether SIS can be accepted, or is due a revision in the documents project. The analysis report and the decision on the treatment to be given to the discrepancies shall be an integral part of the Declaration of Acceptance of SIS.

12.2.4 All pending that degrades technical requirement of the SIS design shall be treated.

12.2.5 As a final inspection activities shall be performed in the SIS to ensure that:

a) all the boundary functions were left at their normal operating positions;
b) all the final elements (stop valves, contour, etc.) are in their locked position;
c) all materials and testing devices are removed;
d) all variables or conditions "forced" in the application program have been removed.

13 Operation, Maintenance, Periodic Tests and Modifications

13.1 Operation

13.1.1 The purpose of this subsection is to establish requirements that contribute to the proper operation of the SIS throughout its life cycle.

13.1.2 During the detailed design shall be prepared a document entitled SIS operation manual, which shall present an organized manner the following content:

a) functional and detailed description of each SIF, addressing:
   — dangerous event that the SIF is designed to protect;
   — potential consequences associated with the hazardous event;
   — likely causes demand for the SIF;
   — description of the safe state and the correct operation of the SIF;
   — values "set point" alarm and "trip";
   — description of alarms and presentation of interfaces (screens, light and sound announcers, etc.) associated;
   — specific operating procedures when operating with the SIF in outline;
b) step by step description of the starting sequence of the process or equipment associated with the SIS, explaining:

— contour commands;
— process conditions that shall be satisfied in each step and their associated SIFs;
— time intervals to be observed (heating ramp, purge time etc.);
— reset functions;

c) individual description of each contour command, either for starting or maintaining, specifying the conditions under which they are to be used;
d) individual description of each manual stop command, identifying the possible situations in which they are to be triggered;
e) statement on the need to perform Periodic Tests in SIFs to maintain its integrity;
f) procedures associated with the occurrence of SIS diagnostic alarms.

13.1.3 The SIS operation manual shall refer to and comply with other SIS project documents, such as risk analysis reports, SIF datasheets, mother of cause and effect, logical diagram etc.

13.1.4 The personnel responsible for plant operation or object protective equipment by SIS shall undergo training in order to be instructed in the information and procedures contained in the SIS operation manual. The training shall be registered appropriately to ensure traceability.

13.1.5 In the case of a SIF becomes unavailable specific procedure to be used for temporary contour.

NOTE It is recommended that the outline of the registration document contains: **[Recommended Practice]**

a) description of SIF to be circumvented;
b) reasons for the unavailability;
c) envisaged for the time interval boundary;
d) complementary actions of operation during the outline period;
e) signature of the competent authority.

13.2 Maintenance

13.2.1 The objective of this item is to establish requirements that allow the maintenance of the integrity and reliability of the SIS throughout its life cycle.

13.2.2 During the detailed design, a document entitled SIS Maintenance Plan, which shall present an organized manner the following content shall be prepared:

a) ratio of periodic tests to be run for each SIF, addressing:
— functional description of the SIF;
— safety integrity level to be maintained;
— values "set point" alarm and "trip";
— minimum required periodicity;
— the procedures for implementing the periodic test;
b) routine inspections relationship to be held, addressing:
— physical verification of installation: conduits and trays, junction boxes, brackets, tubing, locks and seals in valves and circuit breakers etc.;
— scheduled replacement batteries, fans etc.;
— verification of backups ("back-ups") of the application program;
c) maintenance of registration forms for periodic testing, routine inspections and repair of failures, containing at least the following information:
— description of the task;
— date of the task;
— persons responsible for implementation and employee time;
— fault detection mode and description of corrective action, if applicable;
d) implementation schedule of tests and periodic inspections;
e) description of the tools and the necessary equipment;

f) personal relationship and organizations responsible for implementing the periodic tests of routine inspections and their records.

13.2.3 It is recommended that you adopt a systematic codification of tasks, failures, corrective actions and performances to allow for statistical analysis of SIS occurrences. **[Recommended Practice]**

13.2.4 Performing scheduled maintenance interventions in SIS shall follow the maintenance plan, and the entire execution of registration documentation shall be available for consultation.

13.2.5 TZhe SIS maintenance plan shall refer to and comply with other SIS project documents, such as risk analysis reports, SIF data sheets, mother of cause and effect, logical diagram etc.

13.2.6 It is recommended that other than the SIS layers of protection are included in the SIS maintenance plan, if they have been considered in the risk reduction. **[Recommended Practice]**

13.2.7 The operators of SIS maintenance activities shall undergo training in order to be instructed in the information and procedures contained in the respective SIS maintenance plan. The training shall be registered appropriately to ensure traceability.

13.2.8 Access to the SIS Logic Executor shall be restricted to authorized personnel by the responsible for maintenance. The number of people with access authorization shall be limited and controlled.

13.2.9 All SIS documentation shall be included in a revision control system that ensures their update and distribution, so that your users are always in possession of the last revision.

13.2.10 Periodic audits shall be provided for confirmation of compliance with the following items:

a) procedure adopted for changes implementations;
b) adopted procedure of testing and verification of their periodicity;
c) systematic records and maintenance analysis;
d) training of maintenance personnel;
e) integrity and update the documentation.

13.3 Periodic Tests

13.3.1 The purpose of this subsection is to establish requirements for the implementation of periodic testing in the SIS in order to detect and correct hidden flaws that could compromise the functionality or integrity of the SIFs.

13.3.2 The implementation of periodic tests shall be carried out according to the procedures developed and written specifically for each SIF present in the SIS Maintenance Plan.

NOTE It is recommended to use as reference the ISA TR 84.00.03. **[Recommended Practice]**

13.3.3 The frequency of running the tests shall be such as to maintain the SIL of each SIF, as provided for in SIF data sheet (basic design) and confirmed after the verification step of the SIL (detailed design).

13.3.4 During scheduled maintenance shutdowns all SIFs regardless of SIL and monitoring of existence, shall be tested with coverage factor of 1.

13.3.5 Periodic tests shall cover all the SIF devices, namely primers, Logic Executor and final elements.

13.3.6 Sensors shall be tested simulating up, as close as possible, the actual operating conditions, including impulse lines, primary cells and electrical installation. Example: lock and key level of drainage.

13.3.7 Final elements shall be tested by forcing the performance of the respective outputs of the logic Executor, even for normally energized.

13.3.8 In cases where the full test run of the final element in normal operation regime is not feasible, specific test procedures shall include:

a) run complete test during stop the process or equipment;
b) run part tests during the operating regime of the process or equipment involving the following components: output circuits, interposing relays, solenoid valves and partial dislocation of stop valves.

13.3.9 There shall be contingency action where the final element fails in the safety position during the test.

13.3.10 In case there is the existence of hidden flaw due to the implementation of periodic testing, it shall be repaired in order to restore the integrity of the involved SIFs.

13.3.11 The periodical tests implementation records shall contain the following information:

a) test procedure number;
b) date of the test;
c) name of the person responsible for the test run;
d) tag and serial number of devices subjected to the test;
e) test results as found, including description of the fault (if any);
f) test result as left as acceptance criteria in the procedure;
g) description of the work performed, including the replaced parts (if any) and the time used.

13.3.12 The periodical tests run records shall be maintained throughout the life of the SIS, so that:

a) they can be verified at any time;
b) they allow long-term performance reviews.

13.3.13 At the discretion of the operation, there may be considered real or spurious trips as the SIFs tests, provided that the following conditions apply:

a) the trip event shall be registered in a specific form, containing at least: date and time of the event, SIF actuated, alarms, detection mode, identified cause (process variable misuse, device (s) in failure, human action), subsequent actions and name of the person responsible; the registration form of trip shall be filed in the technical documentation system of Operation, traceable manner;
b) trips with unknown cause cannot be used as SIF test;

c) in a spurious trip caused by failure of the final element none of of SIF devices can be considered as tested;
d) in a spurious trip output module caused by failure of the safety PLC, only the final element can be considered to be tested;
e) in a spurious trip caused by failure of the CPU logic executor, only the safety PLC output module and the final element can be considered as tested;
f) in a spurious trip caused by failure safety PLC input module, all the SIF, except for the sensor and the PLC input module of safety can be considered as tested;
g) in a spurious trip caused by failure of the sensor throughout the SIF, except the sensor, may be considered as tested;
h) on a real trip, only devices that have proven (from event logs) have operated correctly can be considered as tested.

13.4 Changes

13.4.1 The purpose of this subsection is to establish requirements so that changes made to the SIS do not impact the safety of the plant or associated equipment.

13.4.2 All proposed changes to the SIS shall be grounded on facts and data recorded in a document entitled Change Request in SIS, which shall have:

a) description of the proposed change;
b) reasons to implement the change;
c) conditions or related hazardous events.

13.4.3 Any proposed amendment shall be submitted to an initial analysis by the technical team responsible for the SIS in order to be classified the same as:

a) modification type 1: does not change logical structure, SIL or MTTFS of SIF involved. Examples: programming changes parameters such as range values set point alarm or trip or time delays;
b) type 2 modification: you can change functionality, SIL, or MTTFS of SIF involved; examples: addition or removal of sensors or final elements, changes in voting architecture, the type of equipment, or in the application program logic.

13.4.4 The following shall be avoided: **[Recommended Practice]**

a) changes in the logic of the application program during operation of the process or equipment associated with the SIS;
b) firmware changes, except when required for correcting the faults detected by the manufacturer.

13.4.5 After the initial analysis, the change request document in the SIS shall be:

a) subject to approval by the responsible for the operation of the site;
b) filed in order to facilitate consultations during and after the modification process.

13.4.6 If the change request is approved, the responsible technical team review shall issue the relevant technical documents, including procedures for testing, operation and maintenance. The documentation reviewed shall be identified as "PROVISIONAL REVIEW FOR SIS CHANGE" and referencing the corresponding modification request in the SIS.

13.4.7 Prior to the review of documents affected by a type 2 change is to be made revalidation of risk analysis and assessment of SIL and MTTFS.

13.4.8 Prior to the execution of any kind of change in the SIS, the revalidation of verification tests shall be made of the feature SIF involved the change.

13.4.9 Any modification of implementing the SIS shall be planned observing the access authorization procedures and work force in the operation.

13.4.10 The implementation of changes in the application program shall include additional checks to ensure that no changes in the other SIFs not involved in changes thereto.

13.4.11 After completion of the functional verification tests, the description of the review of technical documents affected by the modification shall be changed to "REVIEWED AS A SIS CHANGE REQUEST No. ...".

Annex A - Determination of Required Safety Integrity Level Using Risk Chart Method

A.1 Introduction

A.1.1 This Annex describes the risk of graphic method that allows the safety integrity level of a SIF is determined from the knowledge of the risk factors associated with the process and basic control system process. This is a semi-qualitative method, and was developed from Annex D of IEC 61511-3.

A.1.2 In this approach we use parameters which together describe the nature of the dangerous situation that occurs in the case of absence or SIS failure. Four sets of parameters are used and the selected parameters are combined to determine the level of safety integrity SIF. These parameters represent key factors for risk assessments and allow a tiered risk rating.

A.1.3 This annex provides examples of risk parameters developed graphics and tables to meet the typical criteria of process units. Before use in any project it is important that validated the area responsible for the safety of the plant. This time can be made adjustments to the parameters in order to tailor them to specific situations.

A.1.4 In this Annex we present risk charts related to the safety of people in the process industries and aspects of environmental protection and asset protection.

A.2 Risk Chart Summary

A.2.1 The risk is defined as a combination of the probability of occurrence of harm and the severity of the consequence (see definitions). Typically, in the process industry, the risk is one of the following four parameters:

— severity of the consequence (C);
— occupation or degree of human presence (probability of being exposed area occupied) (F);
— probability to avoid exposure scenario (P);
— demand frequency (number of times per year that the scenario would occur in the absence of instrumented safety function being considered) (W).

Table A.1 - Description of Parameters of Risk Chart

Parameter		Description
Consequence Severity	C	Number of fatalities and/or serious injury resulting from the occurrence of the scenario. Determined taking into account the number of people in the exposed area when the area is busy, and the vulnerability to the scene.
Occupation	F	Probability that the area exposed to the hazard is occupied at the time of occurrence of the scenario. It is determined by calculating the fraction of time occupied area is the occurrence of the scene. It shall be considered to increase presence in the exposed area associated with the investigation of abnormal situations that may exist before the occurrence of the scenario. (this shall be also considered in determining the parameter C).
Probability to avoid exposure	P	Probability of people exposed to danger can prevent damage due to failure on demand of safety instrumented function. It depends on independent methods exist to alert people before the occurrence of the hazardous event and the possibility of evacuation.
Demand frequency	W	The number of times per year that scenario would occur in the absence of the safety instrumented function being analyzed. This can be determined considering all the failures that can lead to hazardous event and estimating the total rate for the occurrence. Other layers of protection analysis may be included.

A.2.2 The risk chart lists specific combinations of risk parameters and safety integrity levels. The relationship between the combinations of risk parameters and safety integrity levels is established considering the tolerable risk associated with specific hazards.

A.3 Documentation Related to Determination of Safety Integrity Level (SIL) Results

It is important that all decisions taken during the SIL determination is recorded in controlled documents. The documentation shall clearly state the reasons why the team selected the specific parameters associated with each security function. The forms to record the results and the assumptions made in each determination of SIL of each safety function shall be compiled in a report. The report shall also include the following additional information:

— the risk chart used along with descriptions of all ranges of parameters;
— the numbers and reviews of all used drawings;
— references to assumptions and possible consequences of studies that were used to evaluate the parameters;
— references to the failures that lead to demands and any failure propagation model used to determine demand rates;
— references to data sources used to determine demand rates.

A.4 Using Risk Chart Related to People Safety

A.4.1 Table A.2 lists descriptions and ranges for each parameter used in Figure A.1 on the safety of individuals.

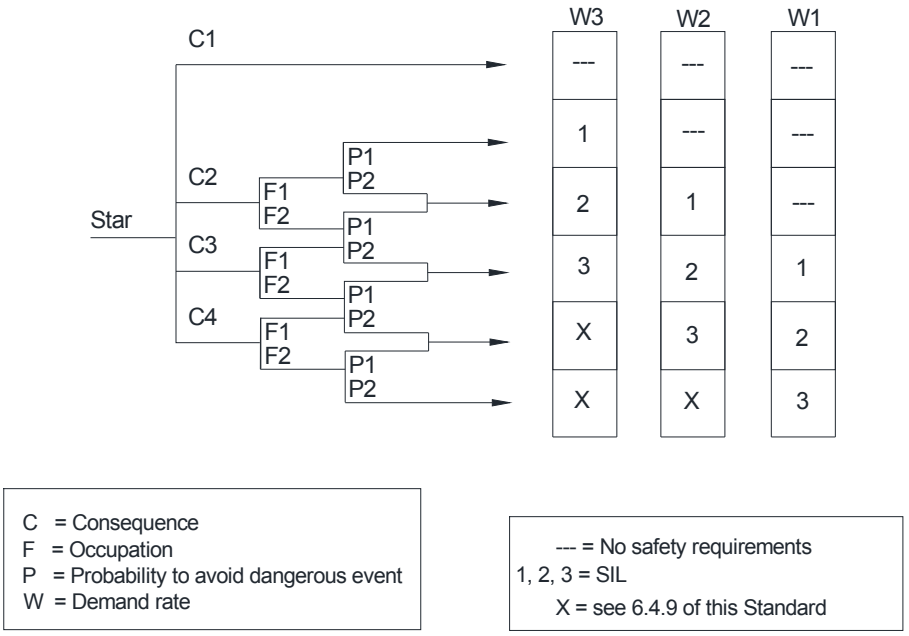

Figure A.1 - Risk Chart Related to Personal Safety

A.4.2 The concept of vulnerability was introduced to modify the parameter of the result, because not always a fault immediately causes a fatality. The vulnerability of a receiver is an important consideration in the risk analysis because the dose received by an individual is sometimes not large enough to cause a fatality. The vulnerability of a receiver is therefore a function of the concentration of the danger he was exposed and the duration of exposure. One example is when a fault causes increased pressure on equipment exceeding the operating pressure, but not reaching the test pressure. The likely result will be normally limited to leakage in flange joints. In such cases, the hazard rate of progression is likely to be slow and operating staff can usually escape the consequences. Even in cases of leaks of large liquid inventories, the worsening situation can be slow enough to allow the operation team can avoid the damage. There are of course cases where a failure can lead to a rupture of pipes or vessels where the vulnerability of the operating staff can be high.

A.4.3 The possibility of increasing the number of nearby people shall be considered when the hazardous event, as a result of verification of symptoms that may occur during the formation of said event. Therefore, shall be considered the worst case scenario.

A.4.4 It is important to stress the difference between "vulnerability" (V) and "probability of avoiding dangerous event" (P) so that it is not considered twice for the same factor. The vulnerability is a measurement that relates to the speed of progression after the danger occurs, while the P parameter is a measurement that relates to the prevention of the danger. The P parameter shall be used in cases where only the danger can be prevented by operator action, after he is aware that their associated SIF has failed.

A.4.5 Some care shall be taken in selecting the occupation parameters. The load factor shall be selected based on the most exposed person and not the average of all exposed.

A.4.6 When unable to frame a parameter in the specified ranges, it is necessary to use other risk mitigation methods.

Table A.2 - Description of Parameters Used in Figure A.1

Risk parameters		Classification	Comments
Severity of Consequence (C) It shall be calculated by multiplying the vulnerability to hazard identified by the number of people present in the area exposed to the hazard (C = NXV). The vulnerability is determined by the nature of the hazard as follows: - V = 0,01 Small release of flammable or toxic material; - V = 0,1 Great release of flammable or toxic material; - V = 0,5 The same release as above, but with a high probability of fire or highly toxic material; - V = 1 Break or explosion.	C1 C2 C3 C4	No relevant damages 0,01 ≤ C < 0.1 0,1 ≤ C < 1.0 C ≥ 1,0	1) The severity of the result is the number of serious injuries and fatalities. 2) C1, C2, C3 and C4 shall be interpreted taking into account also the restoration of the injured conditions.
Occupation (F) This parameter is calculated by determining the proportional length of time in which the area exposed to danger is occupied in a work shift. NOTE 1 If the time in the dangerous area is different depending on the operating shift the maximum value shall be selected. NOTE 2 The use of parameter F is suitable only if it can be shown that the demand rate is random, and is not linked to the period during which the occupancy is higher than normal. This is the case, for example, in batches or during the investigation of abnormalities.	F1 F2	Rare exhibition infrequent in the danger zone Occupation less than 10% of the time (F < 0.1). Permanent frequent exposure in the danger zone Occupation greater than 10% of the time (F ≥ 0.1).	See comment 1 above

Table A.2 - Description of Parameters Used in Figure A.1 (Continued)

Risk Parameter		Classification	Comments
Likely to avoid the hazardous event (P) if the protection system fails.	P1	Adopted if all the conditions are met in the Comments column	3) P1 shall only be selected if all the following conditions are met: - there are means provided to alert the operator that the SIS failed; - there are independent means provided of process stop in order to avoid danger or to allow people to be evacuated to a safe area; - The time between the moment the operator is alerted and time when the event occurs or exceeds 1 hour is enough to take the necessary actions.
	P2	Adopted if one or more of the comments column conditions are not met	
Demand rate (W) The number of times per year that the hazardous event occurs in the absence of SIF under review. To determine the demand rate is necessary to consider all sources of failure that can lead to a dangerous event. In determining the demand rate, limited reliability shall be credited to the control system. The performance of the control system is limited below the performance scales associated with the SIL1.	W1	Demand rate less than 0,1 per year	4) The purpose of the W factor is to estimate the frequency of danger without the existence of the SIS. 5) For demand rates higher than 10 per year, SIL has to be determined by another method.
	W2	Demand rate between 0,1 and 1 per year	
	W3	Demand rate between 1 and 10 per year	

A.5 Using Risk Chart for Environmental Consequences

A.5.1 The required safety integrity level depends on the characteristics of the released substance and environmental sensitivity. Table A.3 shows classes of environmental consequences. During the project stage, there shall be determined what can be accepted at each site for the site.

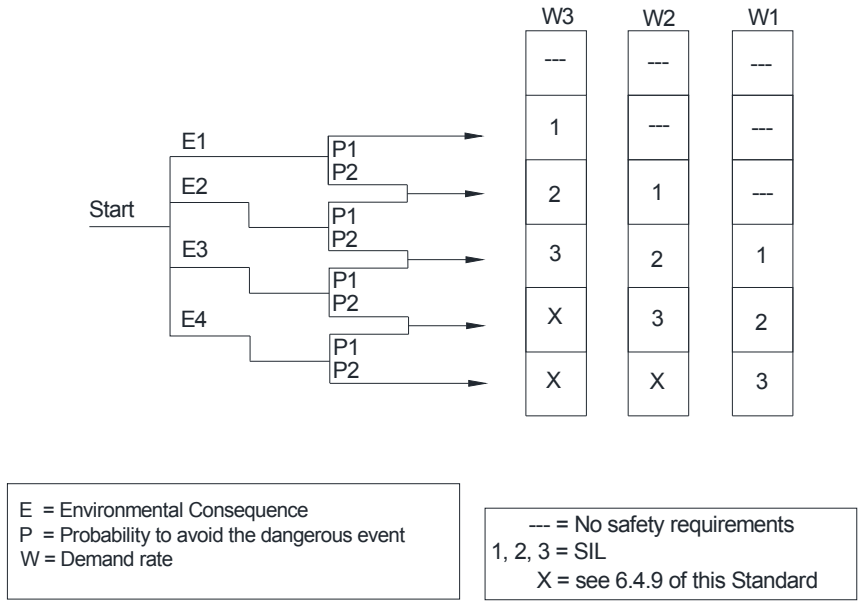

Figure A.2 - Risk Chart Related to Environmental Safety

A.5.2 The consequences above shall be used in conjunction with the risk chart as shown in Figure A.2. It shall be noted that the F parameter is not used in this risk graph because the concept of placement does not apply. P and W parameters apply and the settings can be identical to those used for personal safety chart.

Table A.3 - General Environmental Consequences

Risk Parameters		Classification	Examples
Environmental Consequence (E)	E1	No release or release with minor damage, but large enough to be reported to the plant management	A moderate leak in a flange or valve A small leak of liquid Small soil pollution not affecting the water table
	E2	Release within the company's limits with significant damage	A cloud of steam unhealthy scrolling outside the industrial establishment after flange joint of rupture or compressor seal failure
	E3	Release out of the company's limits with significant damage that can be quickly cleaned without significant lasting consequences	A release vapor or aerosol with or without liquid precipitation, causing temporary damage to the flora or fauna
	E4	Release out of the company's limits with significant damage that cannot be cleaned quickly and with lasting consequences	Significant flow of liquids in a river or the sea; Vapor or aerosol release, with or without liquid precipitation, which causes lasting damage to flora or fauna; Solid release (dust, catalyst, soot, ash); Fluid leak that could affect the water table

A.6 Using Risk Chart for Material Consequences

A.6.1 The use of risk graph to determine the safety integrity level associated with material consequences shall take into account all economic losses resulting from the failure of the demand function. Equipment and facilities repair costs shall be included, loss of production, cleaning and restoration costs, contractual penalties, fines from government agencies etc.

A.6.2 Figure A.3 the risk chart shall be used together with the classes of materials consequences described in Table A.4.

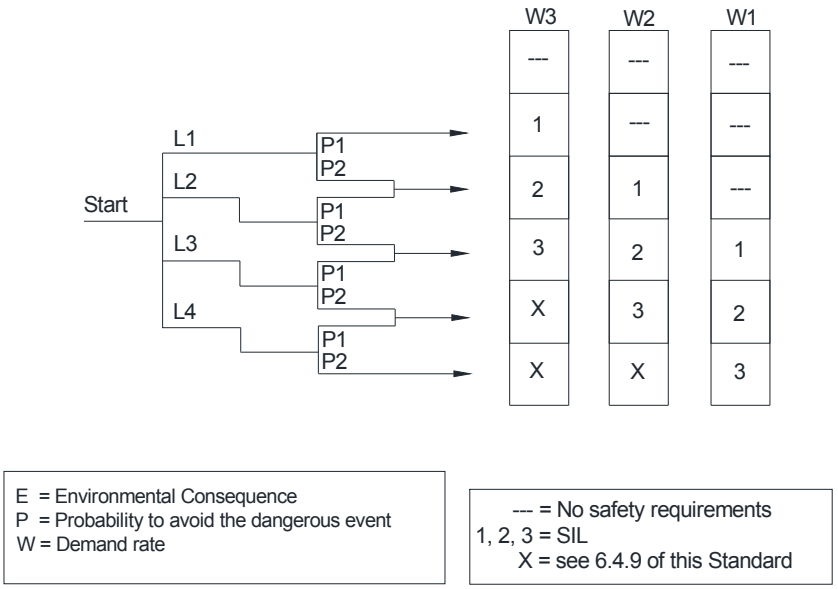

Figure A.3 - Risk Chart for Material Consequences

Table A.4 - Classes of Material Consequence

Risk parameter		Classification	Examples
Material Consequence (L)	L1	Losses between US$ 100,000 and US$ 1,000,000	- production out of specification; - product loss by opening PSV; - cavitation damage in small pumps.
	L2	Losses between US$ 1,000,000 and US$ 10,000,000	- loss of large amounts of goods by opening PSV or reservoir overflow; - cavitation damage in high speed pumps or multistage pumps which have spare ones; - financial damages for delayed production, including fine for delay in delivery.
	L3	Losses between US$ 10,000,000 and US$ 100,000,000	- coking furnace tubes; - sucking liquid damage or blockage of the suction or discharge large compressor; - damage from great product spill, including cleanup costs and fines for environmental audit body; - low cost repairs to essential equipment working without spare ones; - costly repairs in non-essential equipment or have reservations.
	L4	Losses higher than US$ 100,000,000	- reactor explosion; - pressurized system break; - oven explosion; - boiler explosion.

A.6.3 The consequence classes of materials listed in Table A.4 are defined primarily by the given monetary value ranges. The examples are merely illustrative of cases that typically result in financial losses that range and can serve as guidance for the analysis team. It shall be noted that the F parameter is not used in this risk graph because the concept of placement does not apply. P and W parameters apply and the settings can be identical to those in Table A.2.

A.7 Determination of Integrity Level of Safety Instrument Function When its Failure Causes More than One Type of Consequence

When a failure on demand leads to more than one type of result (people, environment and materials), integrity requirements associated with each of the aspects involved shall be determined separately and the largest among them shall be the standard of integrity specified for the function.

Annex B - Layer of Protection Analysis (LOPA)

B.1 Introduction

B.1.1 This annex establishes a standardized procedure to evaluate the Safety Integrity Level (SIL) required for Safety Instrumented Functions (SIFs) using the Layers of Protection Analysis (LOPA) method described in the book-concept AIChE / CCPS.

B.1.2 Layer of Protection Analysis (LOPA) is a semi-quantitative method of risk assessment, whose primary purpose is to determine whether the protection measures present against an unwanted event are enough to reduce its risk to a tolerable level. This is done by assigning numerical values to the frequencies of the possible initiating causes and average probabilities of failure on demand of each existing protection layer, and comparing the risk value obtained with the pre-set tolerable risk.

B.1.3 If the estimated risk for a scenario is not tolerable, other protective layers shall be added in order to achieve the required risk reduction. LOPA does not define protection layers to be added or how to design them, but assists in the evaluation of alternative measures that can be implemented in order to achieve the required risk reduction.

B.1.4 LOPA is not a hazard or accident scenarios identification method. The scenarios to be analyzed with LOPA shall be developed during the application of a HAZOP as a process risk analysis technique to identify accidental risk scenarios, according to PETROBRAS N-2782.

B.2 Procedure

The application procedure of LOPA to determine the SIL required for each SIF is shown in simplified form in Figure B.1 and described in detail in Sections B.2 to B.4 of this Annex, which present some numerical values tabulated to be used in the SIL calculation required at the end of the analysis.

As a general rule, in case of doubt among the tabulated values, the most conservative values shall always be adopted. If the LOPA team decides to use in the analysis some value different from those presented in the tables of this Annex, the values actually adopted shall be based on defensible and documented reasons.

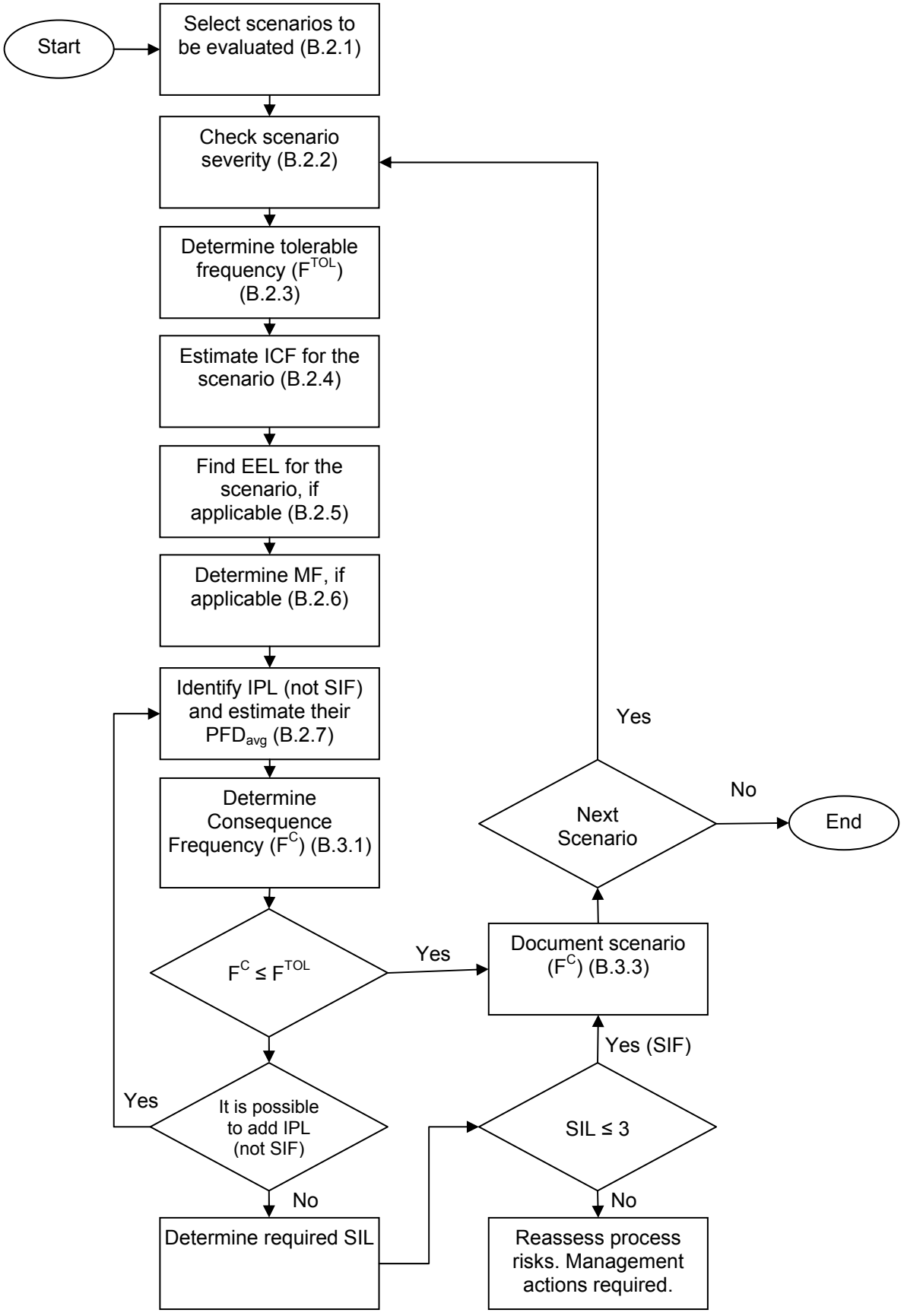

Figure B.1 - LOPA Procedure Flow

B.2.1 Selection of Scenarios to be Analyzed

B.2.1.1 The first activity of the LOPA team shall be selecting among the scenarios identified in the Risk Analysis, those where there is interlock as a safeguard or as a recommendation.

B.2.1.2 Other scenarios can be assessed at the discretion of the team.

B.2.1.3 The LOPA team shall register all scenarios of interest in an analysis worksheet, where the ID (number) and the description of each scenario are copied from the HAZOP.

B.2.1.4 The record of the scenarios shall comply with the requirements of B.3.3.1.

B.2.1.5 For scenarios presenting high occurrence frequency (higher than twice the frequency between IPL tests) or catastrophic severity of consequence, it is recommended to carry out a quantitative risk assessment. **[Recommended Practice]**

B.2.2 Classification of Severity

B.2.2.1 The severity attributed to the consequence of a scenario represents the highest impact among people (S), environment (E) and asset (L). Each pair cause-consequence shall be analyzed separately and considering these three aspects.

B.2.2.2 The classification of the severity of consequence of accident scenarios is a risk analysis activity, which consists in defining for each selected scenario, a severity category for each aspect, according to the tolerability risk matrix of PETROBRAS N-2782, assuming failure in all safeguards.

NOTE In relation to the severity of consequence to the asset, you can use the values given in Table A.4 in Appendix A of this Standard, with the following equivalence: Severity 5 as L4 and so on. **[Recommended Practice]**

B.2.3 Tolerable Frequency (F^{TOL})

The LOPA team shall find in Table B.1 the value of the tolerable frequency for the category of severity of the consequence of the scenario, defined according to B.2.2.

Table B.1 - Tolerable Frequency (F^{TOL})

Severity category	F^{TOL} (event/year)
V	$1x10^{-5}$
IV	$1x10^{-4}$
III	$1x10^{-3}$
II	$1x10^{-2}$
I	$1x10^{-1}$

B.2.4 Initiating Cause Frequency (ICF)

B.2.4.1 The initiating cause corresponds to the reason for the deviation occurrence in the process variable identified in the HAZOP. Each initiating cause shall be analyzed separately in a specific scenario.

B.2.4.2 The LOPA method requires not considering the existence of protective layer or any other factor in determining the frequency of the initiating cause.

B.2.4.3 Failure on demand of protection layers (SIF, PSV etc.) shall not be considered as initiating causes, since other events shall initiate the scenario before these protective layers are demanded.

B.2.4.4 The LOPA team shall select in Table B.2 a frequency for the initiating cause (ICF) of the identified scenario.

Table B.2 - Initiating Cause Frequencies

Initiating cause	ICF (event/year)
BPCS failure	1×10^{-1}
Failure of self-operated control valve in clean service	1×10^{-2}
Failure of static equipment (low vibration)	1×10^{-2}
Failure of static equipment (high vibration)	1×10^{-1}
Failure of dynamic equipment (B.2.4.5.a)	1×10^{-1}
Turbine overspeed / diesel engine with box breaks	1×10^{-4}
Failure of the pressure vessel	1×10^{-6}
Pipe failure - full bore	1×10^{-7} per meter
Leak in pipe - 10% straight section	1×10^{-5} per meter
Atmospheric tank failure	1×10^{-3}
Spurious opening of safety valve	1×10^{-2}
Pump seal failure	1×10^{-1}
Failure of loading / unloading hose (low vibration)	1×10^{-1}
Failure of hose loading / unloading (high vibration)	1
Failure in redundant cooling water system	1×10^{-1}
Packing break	1×10^{-2}
Loss of redundant electrical power supply	1×10^{-1}
Land vehicle impact (truck, excavator, etc.)	1×10^{-2}
Load drop lifted by crane	1×10^{-4} per lifting
Atmospheric electrical discharge	1×10^{-3}
Minor fire	1×10^{-1}
Major fire	1×10^{-2}
Operator's failure to perform routine procedure (well trained operator, not stressed, not fatigued) (B.2.4.5.b)	1×10^{-2} per opportunity
Human error (non-routine task, low stress) (B.2.4.5.c)	1×10^{-1} per opportunity
Human error (non-routine task, high stress) (B.2.4.5.c)	1 per opportunity
Failure in maintenance procedure LOTO type (B.2.4.5.d)	1×10^{-3} per opportunity
SIF spurious action (B.2.4.7)	1×10^{-1}

B.2.4.5 Rules commonly used for initiating causes in Table B.2

a) dynamic equipments refer to pumps, compressors, turbines and similar devices;
b) routine procedures are routinely performed actions in the field or BPCS operation interface that, if performed incorrectly, can result in deviations in the process being analyzed;
c) non-routine tasks are those performed in sporadic situations, such as startup and shutdown of process units, and that if performed incorrectly, can result in deviations in the process being analyzed;
d) considered as a general failure of a safety procedure with multiple steps, called LOTO (Lockout / Tagout) and known by PETROBRAS as LIBRA (Downstream) or PCEP (Transpetro); These designations refer to specific practices and procedures to safeguard workers against inadvertent energizing of equipment, unexpected start-up of machines, or release of hazardous substances during service or maintenance activities; this requires that a designated person turn off and disconnect the machine or equipment from its power supply before performing any service or maintenance and that authorized employees or lock up with padlocks or identify tag energy isolation device, and verify that power has been effectively isolated.

B.2.4.6 The values of Table B.2 are derived from the process industry experience and consider many types of materials and operational failures.

B.2.4.7 For spurious trip of the SIF as initiating cause, it is suggested to adopt an ICF of 10^{-1} spurious trip per year, since at this phase of the procedure, the MTTFS of the SIF is not known yet.

B.2.4.8 Equipment not covered by Table B.2 such as filters (various types), flanges, tank trucks, land and subsea pipelines, manual valves (hand wheel) and block valves with actuator shall have their values of failure frequency based on defensible and documented reasons.

B.2.5 Enabling Event (EE)

B.2.5.1 Enabling event is an action or condition that does not cause the scenario, but that shall exist to allow the initiating cause leading to the unintended consequence considered.

EXAMPLE:

Scenario with enabling event: purge of coke drum to fractionating column is carried out in phases, forcing manually the flow set point gradually to higher values. At the end of the cooling phase, the set point shall return to the operating value before the control is set to automatic.

a) enabling event: set point of the cooling water flow left at a higher flow value in the last cooling phase performed on the drum;
b) initiating cause: inadvertent opening of manual valves of cooling water isolation;
c) consequence: pressure increase in the coke drum due to the sudden vaporization of the injected water, with possible leaks in flanges and fittings, and possible reactor damages.

B.2.5.2 Another possible enabling condition to be considered (perhaps the most common) is the Time at Risk.

B.2.5.3 Time at Risk

Certain hazards exist only in specific stages of the process or during the performance of specific tasks (batch, loading, unloading, start, stop, load variation, wait, regeneration etc.), or in specific operating modes (automatic, manual, remote, maintenance, load monitoring etc.). In such cases, the frequency of the sensor can be adjusted by a factor equal to the enabling event likelihood obtained by dividing the time during which the hazard exists, and the total time interval considered in the analysis (usually 1 year).

EEL = (Time at Risk) / (Total Time)

EXAMPLE:

EEL = 8 times per year x 1 h = 8 h/year x 1 year/8760 h = 0,000913

B.2.6 Modifying Factors (MF)

In some scenarios, it is necessary that certain specific conditions such as the presence of ignition sources or presence of people in the affected area for the damage to occur. In these cases, the probabilities associated with these conditions can be used as adjustment factors of the scenario's risk.

The LOPA team shall ensure that these factors have not been considered previously as enabling condition, or are embedded in the frequency of the initiating cause, especially due to considerations in determining the scenario during the HAZOP, because its accounting in duplicity could significantly affect the analysis results.

A modifying factor shall only be used if deemed condition can be guaranteed throughout the useful life of the installation.

It is noteworthy that in HAZOP, the analyzed effect shall consider the worst case scenario, without taking into account the existence of safeguards, or other mitigating factors.

B.2.6.1 Probability of Ignition

Depending on the product properties and loss of containment conditions (eg. sudden rupture of equipment containing highly reactive product or at high temperature and pressure), the ignition may be spontaneous, regardless of an ignition source.

B.2.6.1.1 Releases of flammable substances not always ignite. The probability that ignition occurs mainly depends on:

a) the existence of ignition sources in the vicinity of the release;
b) the intrinsic properties of the substance and the amount (volume or mass) of material released;
c) the kind of dispersion (jet, pool, light cloud, heavy cloud) of flammable materials in the environment concerned (free or confined atmosphere, water, soil).

B.2.6.1.2 Before adopting a modifying factor to represent the probability of ignition, it shall be noted the considerations made as to the relevant characteristics of the flammable product release and its possible outcomes (jet fire, pool fire, flash fire, explosion, BLEVE). One shall consider the definition of scenario carried out during the risk analysis, especially not to count more than once this reduction factor.

B.2.6.1.3 Tables B.3 and B.4 show some typical ignition probabilities that can be used as modifying factors. The LOPA team can take just one modifying factor for the probability of ignition for each scenario. Therefore, you shall define which of these two tables shall be adopted, according to what is most important in the scenario analysis.

Table B.3 - Modifying Factors of Ignition Probability According to the Amount of Ignition Sources

Number of ignition sources	Modifying Factor (MF)
None readily identifiable (eg dike, empty lot)	0,1
Very few (eg tank farm)	0,2
Few (eg marine terminal, road or rail)	0,5
Many (eg industrial installation)	0,9 (see Note)
NOTE If electrical installations at the scene hit area are suitable for explosive atmosphere, it can be considered a probability of ignition equal to 0,1.	

Table B.4 - Modifying Factors of Ignition Probabilty According to the Type of Flammable Material

Flammable material	Modifying Factor (MF)
Gas or LPG	0,3
Light liquid (flash point < 38 °C)	0,2
Heavy liquid (flash point ≥ 38 °C)	0,1

B.2.6.2 Presence of People

B.2.6.2.1 For environmental or commercial consequences, the presence of people is not a modifying factor. However, for safety-related consequences for people, at least one person shall be present in the area where the incident occurs. It can be used to reduce risk factors related to the time when no one is present in the hazardous area. For example, if a fire occurs due to a leak in a pump seal, an operator has to be close to the pump to be injured. If the operator remain in the area in question only 30 minutes per shift, then the use of a modifying factor is justified.

B.2.6.2.2 If the scenario occurs during a local operational maneuver or during maintenance work, this reduction factor cannot be used.

Table B.5 - Modifying Factors According to the Presence of People

Danger exposure time	Modifying Factor (MF)
Always (more than 4hrs per shift)	1,0
Frequently (2 hrs to 4 hrs per shift)	0,5
Occasionally (1 hrs to 2 hrs per shift)	0,2
Rarely (less than one hour per shift)	0,1

B.2.6.2.3 Other modifying factors such as, for example, higher or lower ease to avoid damage are not considered in this Annex.

B.2.7 Independent Protection Layers (IPL)

This section describes how to proceed to identify the safeguards provided in the project that can be considered independent protection layers (IPL) and determine the risk reduction they provide.

The identification of the IPL is often the most difficult part of this method. It is important to note that all IPL is a safeguard, but not every safeguard is an IPL.

Table B.6 shows some examples of safeguards that are not normally considered IPL.

Table B.6 - Safeguards Generally Not Considered as IPL

Safeguards Generally Not Considered IPL	Comments
Training and certification	These factors can be taken into account in determining the PFD_{avg} actions by the operator, but are not IPL themselves.
Procedures	The existence of good procedures may be considered in determining the PFD_{avg} actions by the operator, but it is not an IPL itself.
Normal tests and inspections	In all hazard assessments it is assumed the perfect execution of these activities, constituting the basis for ICF values in Table B.2 and PFD_{avg} in Table B.7 and Table B.8. Changing the interval between tests and inspections can affect the PFD_{avg} of certain IPLs.
Maintenance	In all hazard assessments it is assumed the perfect execution of this activity, constituting the basis for ICF values in Table B.2 and PFD_{avg} in Table B.7 and Table B.8. Poor maintenance can increase the PFD_{avg} of certain IPLs.
Communications	It is a primary hypothesis that appropriate communications exist in an industrial plant. Poor communications can increase PFD_{avg} of certain IPLs.
Signaling	Signs are not IPLs for themselves. Signs confusing, dubious, misplaced, ignored, etc. can increase the PFD_{avg} of certain IPLs.

Safeguards, whether IPL or not, are linked to an identified scenario in the risk analysis with a specific cause and consequence.

The main feature of an independent layer of protection is that it shall be effective to individually prevent the occurrence of the hazardous event. If just a single layer of protection works, the unintended consequence will not occur. The term "independent" means that the performance of the protective layer is not affected by the initiating cause and that failures shall not disable two or more layers of protection associated with the same scenario at the same time. In addition, it shall be demonstrated through auditable documentation that the protection in question was properly designed and installed, and that is periodically subjected to test and properly maintained to ensure its effectiveness, independence and PFD_{avg} specified.

In short, an independent protective layer shall be:

a) effective in preventing the outcome of a potentially dangerous event;
b) independent from the initiating cause and components from any other IPL considered for the same scenario;
c) auditable through documents proving the compliance of the design, installation, testing and maintenance of this IPL to its specifications.

Additionally, if the spurious actuation of an IPL leads to a new accidental scenario, the associated risk shall be tolerable. For example: For toxic or flammable materials, the relief system shall be directed to a safe place.

The LOPA method is to keep adding protection layers until the obtained risk meets the adopted tolerability criteria.

The decision of which protection layers to add from the possible alternatives can be based on a comparative analysis of their implementation, operation and maintenance costs throughout the life cycle. **[Recommended Practice]**

Before considering adding layers of protection, however, it is recommended that inherently safer design solutions are applied. **[Recommended Practice]**

The adoption of an inherently safer design can effectively eliminate a scenario. Such consideration shall be recorded in the LOPA worksheet. It is noteworthy that other scenarios with the same result (but with other initiating causes) can continue to exist.

In relation to the actuation mode, an IPL can be passive or active.

Passive IPL is that one which does not need not take any action to fulfill its protective function. Table B.7 gives some examples of safeguards that may be considered passive IPLs.

Table B.7 - Pasive IPL and Their Typical PFD_{avg}

Independent Protection Layer (IPL)	Average probability of failure on demand (PFD_{avg})
Basin / dike	1×10^{-2}
Flame arrester (detonation or deflagration)	1×10^{-2}
Rupture panel (“blowout panel”)	1×10^{-2}
Overflow line directed to safe place (B.2.7.2)	1×10^{-2}
Underground drainage system	1×10^{-2}
Open vent (no valve)	1×10^{-2}
Blast-wall or bunker	1×10^{-3}
Passive fire protection (fireproof insulation) [B.2.7.3]	1×10^{-2}

Active IPL is that one which needs to change from a given state to another in response to the change in a measurable property of the process in question. Table B.8 gives some examples of safeguards that can be considered active IPL.

Table B.8 - Active IPL and Their Typical PFD_{avg}

Independent Protection Layer (IPL)	Average probability of failure on demand (PFD_{avg})
Instrumented safety function with SIL 1	1×10^{-1}
Instrumented safety function with SIL 2	1×10^{-2}
Instrumented safety function with SIL 3	1×10^{-3}
Automatic function in BPCS (B.2.7.4.1)	1×10^{-1}
Response of the operator to the alarm (B.2.7.4.2)	1×10^{-1}
Mechanical relief device / safety and relief valve (B.2.7.5)	1×10^{-2}
Multiple independent relief devices (nozzles, discharges, etc.), but more than one needs to act to meet 100 % of the scenario (e.g. multiple partial-load pressure relief valves). (B.2.7.5)	1×10^{-1}
Internal mechanical device of independent safety of SIS and BPCS (e.g. turbine mechanical disarm)	1×10^{-1}
Rupture disk	1×10^{-2}
Check valve (B.2.7.6)	1×10^{-1}
Check valve associated with mechanical pressure relief (B.2.7.6).	1×10^{-1}
Self-operated control valve in clean service (B.2.7.7)	1×10^{-2}
Car sealed valve, frequently listed and checked (B.2.7.8)	1×10^{-2}
Locked valve, (with padlock) frequently listed and checked (B.2.7.8)	1×10^{-2}
Double seal (on pump) with interstitial alarm	1×10^{-2}
Active fire protection (B.2.7.9)	1×10^{-1}

The numerical values in Tables B.7 and B.8 can be used as Average Probability of Fail on Demand (PFD_{avg}) for each IPL. If the LOPA team finds any IPL is more reliable (lower PFD_{avg}) than the numerical values presented in these tables, or identify any different IPL from those presented in these tables, the adopted value for your PFD_{avg} shall be based on defensible and documented reasons.

NOTE Table B.8 expresses PFD_{avg} values for SIF in demand mode. For continuous operation mode, the frequency values of dangerous failure (SIL1 = 10^{-5}/hr, SIL 2 = 10^{-6}/hr, SIL 3 = 10^{-7}/hr) shall be used instead of PFD_{avg}.

To ensure consistency in the application of LOPA, some conditions to guide the decision of when to consider a safeguard as IPL are listed in B.2.7.1 to B.2.7.10.

B.2.7.1 General Conditions

To be considered an IPL, a safeguard shall comply at least with the following general conditions:

a) to be sufficient to prevent the occurrence of the scenario by itself;
b) its failure cannot be the initiating cause of the considered scenario;
c) the scenario cannot lead the IPL to fail or become unavailable;
d) its spurious actuation cannot lead to a new scenario with higher risk than that which it seeks to avoid;
e) it shall not have common components with those of other IPLs;
f) it shall be inserted into an established and auditable maintenance program.

B.2.7.2 Overflow Line

In addition to the general conditions required in B.2.7.1, any valves in the overflow line shall be administratively controlled to ensure that the IPL is available when needed.

B.2.7.3 Fireproof Insulation

In addition to the general conditions required in B.2.7.1, the specific conditions required for a valve (or arrangement of valves) with fireproof insulation to be considered an IPL are:

a) the fire shall be the initiating cause of the scenario, never the unintended consequence;
b) the fireproof insulation shall be able to provide additional time sufficient for an appropriate response to the situation (inventory containment, depressurization, deluge, etc.) in order to effectively prevent the consequences considered in the scenario;
c) the insulation shall remain intact when exposed directly to fire and shall not be displaced by water jets from the fire fighting system;
d) the insulation shall comply with other corporate requirements from PETROBRAS N-1756 and its supporting documents for this type of protection.

B.2.7.4 Basic Process Control System - BPCS

Basic Process Control Systems (BPCS) perform automatic functions such as continuous regulatory controls (PID), discrete controls (such as on-off) and sequential or combinational logic (interlocks). To qualify as an Independent Protection Layer - IPL, an automatic function in the BPCS shall comply with the requirements established in B 2.7.4.1.

Operators respond to process alarms and equipment, implemented in BPCS, through the execution of specific manual procedures. To qualify as an Independent Protection Layer - IPL, operator response to an alarm in the BPCS shall comply with the requirements expressed in B 2.7.4.2.

The risk reduction factor assigned to an automatic function in BPCS or operator response to an alarm in BPCS, considered as IPL shall not be higher than 10.

B.2.7.4.1 Automatic functions in the BPCS

To qualify as an Independent Protection Layer (IPL), an automatic control function in BPCS shall:

a) comply with all the general conditions of IPL described in B.2.7.1;
b) be identified clearly as IPL in the project documentation, especially in engineering flowcharts, distinguishing it from the other automatic control functions in the BPCS not considered IPL;
c) continuously operate in automatic mode. Any contour maneuvers or inhibition shall be treated by specific procedures. Examples of maneuvers to be treated: set the controller to manual mode or direct manual operation in the final element.

NOTE It is recommended to evaluate the application of restrictions on set-points of automatic control functions in the BPCS considered IPL. **[Recommended Practice]**

B.2.7.4.2 Operator's Response to Alarms in the BPCS

The risk reduction for the operator's response to alarm shall not be considered more than once for the same scenario, independently from the number of alarms or actions taken by the operator in response to these.

For operator response to an alarm in the BPCS qualify as an Independent Protection Layer (IPL), the following requirements shall be satisfied:

a) all general conditions described in B.2.7.1;
b) the alarm shall give a clear and immediate indication of the scenario for the operator, without having to perform diagnostics based on indications of other process variables;
c) the operator action in response to the alarm shall be enough to interrupt the scenario in a time interval smaller than the process safety time related to the scenario considered;
d) the alarm shall be clearly identified as part of an IPL in the design documentation, notably in the list of alarms and engineering flowchart, distinguishing itself from other BPCS alarms not considered IPL;
e) the operating unit shall have an alarm management policy and the alarm in question shall be prioritized according to this criterion;
f) the operator shall always be present at the operator interface announcing the alarm (which generally prevents alarms in the field to be considered as IPL);
g) an operational procedure shall define the specific actions to be taken by the operator in response to the alarm, and this procedure shall be known and object of periodic training by operators;
h) the evolution of the considered scenario cannot compromise the effectiveness of the alarm. Example: in a steam line rupture scenario, there may be a false indication of a high level due to formation of bubbles in the liquid phase, so that a low level alarm in the steam generator may not indicate immediately the deviation.

B.2.7.4.3 Assignment of Up to Two IPLs to a BPCS

If the initiating cause of the failure scenario considered is an automatic function in the BPCS, a second automatic function or operator response to alarm in the BPCS can be considered an IPL.

If the initiating cause of the scenario considered is not a failure of an automatic function in the BPCS, two automatic functions or one automatic function and one operator response to alarm can be considered IPLs, and the total RRF associated with the BPCS shall not be higher than 100.

In all cases, the following additional criteria shall be considered:

a) the bypass of the two functions shall not be possible simultaneously;
b) the sensors, I/O modules and final elements associated with each automatic function and alarm considered shall be distinct;
c) it is recommended to use separate controllers for each function **[Recommended Practice]**.

B.2.7.5 Relief Mechanical Device / Safety and Relief Valve

In addition to the general conditions required in B.2.7.1, the following specific conditions are required to consider mechanical relief devices as IPL:

a) the relief system shall be sized to completely mitigate the scenario;
b) relieved fluids shall be clean and not very viscous. If the safety and relief valve is used in a service with corrosive fluids or capable of polymerizing or generate deposits, without any protection, the valve shall not be considered an IPL. However, if the project considers protection measures to ensure the valve operation, one can consider a PFD_{avg} of $1x10^{-2}$. Such measures may include: the use of steam purge, rupture disc installation upstream the valve, installation of two valves in parallel to allow inspection and maintenance, among others;
c) relief shall be done to safe place in order to avoid causing significant consequences.

B.2.7.6 Check Valve

B.2.7.6.1 In addition to the general conditions required in B.2.7.1, the specific conditions required for that check valve to be considered an IPL are:

a) the check valve shall be able to meet the safety requirements for the scenario, such as closing time and permissible leakage;
b) for low demand applications, the service shall be clean, not susceptible to clogging, deposit formation, gums, polymerization, etc.

B.2.7.6.2 Check Valves considered IPL shall be identified with tags, in order to facilitate the records of interventions.

B.2.7.6.3 It is recommended to opt for the use of models which facilitate inspection and maintenance. **[Recommended Practice].**

B.2.7.6.4 A device for preventing reverse flow can be an IPL or not, depending on the process design and the boundary conditions of the considered scenario.

EXAMPLES

a) in a scenario of damaging the pump by reverse flow caused by starting up the spare pump, a simple check valve (e.g. swing type) can be sufficient to avoid the damage with the required reliability and could be considered IPL;
b) a contamination scenario may require the association in series of two different types of check valves to be effective as required by an IPL;
c) in a scenario of excessive pressure upstream the check valve, it is usually necessary to conjugate a PSV dimensioned to leak through the check valve (API STD 521), so that it is considered an IPL;
d) in a scenario of reverse flow in a gas compressor, it may be required to apply a high integrity check valve.

B.2.7.7 Self-Operated Pressure Regulating Valve

Self-operated pressure regulating valves used as IPL shall be identified with TAG to allow the traceability of interventions records.

B.2.7.8 Car-Sealed Valves or Locked Valves

In addition to the general conditions required in B.2.7.1, the specific conditions required for Car-Sealed valves or Locked valves to be considered as IPL are:

a) the persons responsible for plant or equipment operation shall maintain an updated list of all valves locked with seal or with padlock;
b) the persons responsible for plant or equipment operation shall perform periodic inspections to ensure these valves are in the proper position and its seals and locks, intact.

B.2.7.9 Active Fire Protection

In addition to the general conditions required in B.2.7.1, the specific conditions required for active fire protection (for example, fire detection systems commanding the actuation of the deluge system) to be considered an IPL are:

a) active fire protection can be considered as an IPL only for scenarios where the fire is the initiating cause;
b) active fire protection cannot be considered as an IPL for scenarios in which their availability or effectiveness may be affected by fire or explosion that it intended to contain.

NOTE A gas detection system commanding closure of SDV (or inventory isolating valves), may be analyzed similarly, i.e.:

a) this system can be considered a safeguard against events resulting from a gas leak (e.g. fire, explosion), but not against the leak itself, because it will necessarily have occurred when detected;
b) it shall be assessed whether this protective layer can alone prevent the unintended consequence, or depends on other external actions (for example, by the operator) to be effective;
c) it shall be possible to determine (and audit) effectiveness, i.e. RRF = 1 / PFD_{avg} from this layer, taking into account the gas dispersion in the atmosphere at the time of demand.

B.2.7.10 Mitigating IPLs

B.2.7.10.1 Usually IPLs are intended to prevent the unintended consequence. However, some layers of protection, such as dikes, drainage and fire protection system can be considered as mitigating IPLs aimed at reducing the severity of the outcome of a scenario, is limiting their intensity, restricting the area affected, or preventing side effects (eg BLEVE).

B.2.7.10.2 In general, the existence of a mitigating protective layer leads to two entirely new scenarios, which shall be analyzed separately.

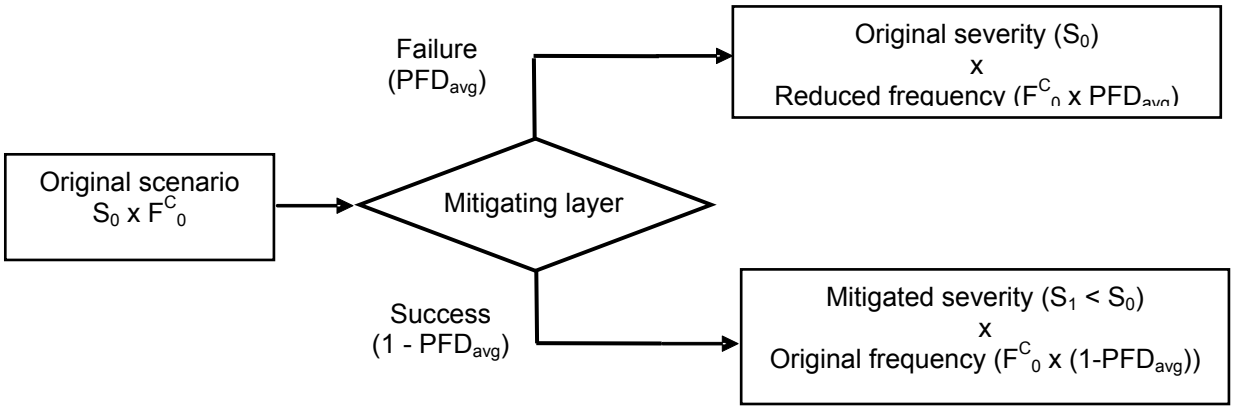

Figure B.2 - Mitigating Protection Layer

B.2.7.10.3 In a simplified way, it is recommended to adopt the following order to include layers of protection: **[Recommended Practice]**

a) inherently safer design;
b) preventive IPLs not SIF;
c) SIFs;
d) mitigative IPLs.

B.3 Analysis Conclusion

B.3.1 Scenario Residual Risk Not Considering Instrumented Function

B.3.1.1 The scenario residual risk not considering Safety Instrumented Functions can be expressed in a simplified manner by the Consequence Frequency (F^C), which is given by the product of the numerical values determined in steps B.2.4 to B.2.7, without any credit for risk reduction due to SIFs:

$$F^C = ICF \times EEL \times \prod_i MF_i \times \prod_j IPL_j$$

Where:

F^C = Consequence frequency;
ICF = Initiating Cause Frequency;
EEL = Enabling Event Likelihood;
MF_i = i-esimal Modifying Factor;
IPL_j = PFD_{avg} of j-esimal IPL (not SIF) associated to Initiating Cause.

B.3.1.2 If F^C is less than or equal to F^{TOL} then the existing protective layers are sufficient.

B.3.1.3 If F^C is greater than F^{TOL}, then additional layers of protection are needed to reduce the residual risk of the scenario to a tolerable level.

NOTE If the F^C indicates that the SIF is demanded more than once per year or in case of two or more demands between test intervals, this SIF is presumed to be operating in continuous mode and thus the SIL is related not with a PFD_{avg}, but with the frequency of dangerous failures per hour, where SIL 1 is equivalent to a frequency between 10^{-6}/hour and 10^{-5}/hour, and so on.

B.3.2 Determination of SIL Required for SIF

B.3.2.1 After exhausting all possibilities of adopting inherently safer design solutions and adding protection layers not SIF, the Safety Integrity Level (SIL) required for the Safety Instrumented Function (SIF) provided in the design or recommended for the scenario can be determined by the total risk reduction factor (RRF) needed to reduce F^C to a value less than or equal to F^{TOL}.

B.3.2.2 If the F^{TOL} has been achieved without the need for a SIF, it is noteworthy that the automatic function provided in the design or recommended by the HAZOP is not critical for safety and shall be performed by the BPCS.

B.3.2.3 If RRF required for SIF is higher than 10 000, the risk and the process design basis shall be re-evaluated, possibly requiring management involvement.

B.3.2.4 It is recommended to evaluate the possibility of replacing a SIF demanded by many scenarios by other SIFs based on process variables more directly related to the deviation of each scenario. **[Recommended Practice]**

EXAMPLE

In a scenario, the failure in the level control of a vessel upstream fractionator column can lead to a discharge of gas through a liquid outlet (gas blow-by), and hence overpressuring the column. A SIF initiated by a PSHH could be replaced by another one, cutting the feed to the column in case of very low level (LSLL) in the vessel.

B.3.2.5 A SIF shall meet the highest SIL required from the scenarios for which it is demanded.

B.3.3 Documentation

B.3.3.1 The LOPA report shall contain sufficient information to support a review of the project by adding, modifying or eliminating safeguards existing or provided in the design, depending on the effectiveness observed during the analysis process to prevent or mitigate undesired effects.

B.3.3.2 In order to record the scenarios considered, it is recommended to use the worksheet provided in Annex C. **[Recommended Practice]**

B.3.3.3 The report shall also record the issues that need to be further detailed or discussed in other forums as well as the actions to be taken and the continuous improvement points of this procedure.

B.4 Results Management

B.4.1 Audit

B.4.1.1 The information included in the documentation of LOPA is related to process safety and, as such, shall be maintained throughout the life cycle of the plant or equipment.

B.4.1.2 The LOPA recommendations shall be included in systematic recommendations management system for the site, which allows analyzing the feasibility of implementing them and properly document these implementations, or even the decision not to implement them, with their respective justifications.

B.4.1.3 All IPL shall be auditable and included in a specific maintenance plan.

B.4.2 Revalidation

Whenever there is some revision in the HAZOP of the installation, it shall be evaluated whether the considerations and assumptions made in the previous LOPA remain valid and, if not, review the LOPA results accordingly.

Annex C - LOPA Spreadsheet Model

PETROBRAS	No.	REV.
	PAGE	of
	TITLE: Layers of Protection Analysis (LOPA)	

Node: | Node Description:

Scenario: | Deviation:

Initiating Cause:

Type: | ICF (/year): | EEL:

Consequence:

Severity:

Modifying Factors:	Personnel	Environment	Property
Ignition probability			
Human presence			
Others			
Others			

Safeguards:	Type:	RRF Personnel	RRF Environment	RRF Property	Remarks / Recommendations:
Residual Risk:					Classif.:

SIF Data: | Consequences of spurious trip: | Spurious trip cost (US$):

MTTR (h): | Process safety time:

Remarks/Recommendations:

Node: | Node Description:

Scenario: | Deviation:

Initiating Cause:

Type: | ICF (/year): | EEL:

Consequence:

Severity:

Modifying Factors:	Personnel	Environment	Property
Ignition probability			
Human presence			
Others			
Others			

Safeguards:	Type:	RRF Personnel	RRF Environment	RRF Property	Remarks / Recommendations:
Residual Risk:					Classif.:

SIF Data: | Consequences of spurious trip: | Spurious trip cost (US$):

MTTR (h): | Process safety time:

Remarks/Recommendations:

PETROBRAS

No. | REV.

SHEET of

TITLE:

Layers of Protection Analysis (LOPA) – Completion Instructions

The spreadsheet LOPA must be completed as per guidance in Appendix B. Details about the completion of each field are listed below:

- **Node** – Complete with the Node number.
- **Node Description** – Complete with the Node description. E.g.: "From XV-6315094 to the entry of tanks TQ-6315051/052, passing through permutators P-6315352/353".
- **Scenario** – Complete with the scenario number. Each scenario shall correspond to a single cause and consequence pair, and shall have a single identification.
- **Deviation** – Process deviation related to one or more scenarios. E.g.: higher level, backflow, higher pressure, lower pressure, etc.
- **Initiating Cause** – Specific description of the initiating cause. Each accidental scenario has a single cause, which may be a primary equipment failure, a mistaken action, or an external event. E.g.: failure in the control loop of UV-102, undue blocking of XV-103, etc.
- **Type (initiating cause)** – Complete with the generic description of the cause, as per table B.2 of PETROBRAS N-2595.
- **ICF (/year)** – Initiating cause frequency (events per year).
- **EEL** – Enabling Event Likelihood, if applicable, as per B.2.5 of PETROBRAS N-2595. Value between 0 e 1.
- **Consequence** – Consequence description. E.g.: leakage outside the dike with environmental contamination; leakage outside the dike with explosion, environmental damage, equipment damage, and death.

The consequence shall reflect the worst possible condition to which the scenario may evolve (1), considering the failure of all safeguards, inexistence of extenuating factors (2) and maximum exposure to damage (3).

(1) Example: In case of leakage of flammable product with the possibility of fire/explosion, consider that they occur. If there is damage even without fire/explosion and the ignition probability modifying factor is applied, divided into 2 scenarios.

(2) Example: If there is a protection (emergency shutdown), or a specific condition in which the damage would be mitigated, they shall not be considered.

(3) Example: In case of damage to people, consider the maximum number that may be present in the area affected during the operation being considered.

- **Severity** – Complete with the severity category of the consequence, according to the risk tolerability matrix of PETROBRAS N-2782. Complete with the values from I to V, in roman numerals.
- **Modifying Factors** – Modifying Factors between 0 and 1, as per Exhibit B of Petrobras N-2595. NOTE: A risk reduction factor may only be taken into account if it is evident to all members of the analysis team that its application does not compromise the safety.
  - **Lines:**

    Ignition probability – Modifying factor that reflects the ignition probability. Apply only if the consequence depends on the ignition. If there are different consequences with and without ignition, they must be represented in 2 distinct scenarios.

    Human Presence – Modifying factor that reflects the human presence level in the place. This modifying factor acts only in the consequence to people.

    Others – Other modifying factors. Specify in the Remarks field.
  - **Columns**:

    Personnel – Modifying factors that apply to the health and physical integrity of people exposed to the risk.

    Environment – Modifying factors that apply to the environmental impact aspects.

    Property – Modifying factors that apply to the damage to the company's physical facilities and/or income.
- **Safeguards** – List the safeguards, either IPLs or not. E.g.: contention dike of TQ-101, PSV in B-02 discharge, PALL-015 alarm, PSHH105 closing XV-102, PSLL202 shutting down the pumps.
- **Type (of safeguard)** – Complete with a generic description of the safeguard (see tables B.7 and B.8). E.g.: PSV, SIF SIL1.
- RRF – Risk Reduction Factor associated to the IPL. Complete only if the safeguard is IPL.
  - **Personnel** – Risk Reduction Factors that apply to the health and physical integrity of people exposed to the risk.
  - **Environment** – Risk Reduction Factors that apply to the environmental impact aspects.
  - **Property** – Risk Reduction Factors that apply to the damage to the company's physical facilities and/or income.
- **Remarks / Recommendations (of the safeguard)** – remarks and recommendations specific to each safeguard.
- **Residual risk** – Residual risk values calculated for personnel, environment and property aspects (in order for the risk to be tolerable, this value must be under or equal to 1; residual risks greater than 100 are classified as intolerable).
- **Classification (of the Residual Risk)** – Classification of the residual risk into Tolerable (T), Moderate (M) and Intolerable (NT), according to PETROBRAS N-2782.
- **SIF Data** – When a SIF is used as safeguard, complete these fields with the SIF data SIF data that are supplied by the risk analysis team and by the process discipline.
  - **Consequence of spurious trip** – Consequence of the SIF spurious trip. Examples: production loss, possibility of tubes coking, damage to refractory materials, etc. This item must be completed by the team performing the risk analysis.
  - **Spurious trip cost** – Cost of the SIF Spurious Trip, in IS$, according to 6.5.2.2 of PETROBRAS N-2595. This item must be completed by the team performing the risk analysis.
  - **MTTR (h)** - Mean time to repair the SIF. This item must be completed by the team performing the risk analysis.
  - **Process Safety Time (s)** – See terms and definitions in PETROBRAS N-2595. This item must be determined by the process discipline.
- **Remarks / Recommendations** – Complete with recommendations and remarks relating to the scenario being analyzed. The recommendations must be numbered.

Annex D - SIF Data Sheet

PETROBRAS	DATA SHEET	No.	
	CLIENT:		SHEET of
	JOB:		
	AREA:		
	TITLE: SIF SPECIFICATION		

INDEX OF REVISIONS

REV.	DESCRIPTION AND/OR REVISED SHEETS

	REV. 0	REV. A	REV. B	REV. C	REV. D	REV. E	REV. F	REV. G	REV. H
DATE									
DESIGN									
EXECUTION									
CHECK									
APPROVAL									

PETROBRAS

DATA SHEET | No. | REV.

SHEET of

TITLE:

SIF Specification

GENERAL INFORMATION

1 Tag:

2 Risk Analysis Report:

3 SIF Description:

4 Demand Causes:

5 Consequences of the Demand Failure:

6 Consequences of the Spurious Trip:

7 Spurious Trip Cost (US$):

RISK ANALYSIS AND PROCESS REQUIREMENTS

8 Process Safety Time (s):

9 Response Time (s):

10 Delay Time (s):

11 Interval Between Periodical Tests (years):

12 MTTR (h):

13

14 Required RRF:

15 Required SIL:

16 Acceptable MTTFS (years):

RESULTS

17 RRF Obtained:

18 RRF Obtained:

19 MTTFS Obtained (years):

INITIATING CAUSES

20 Tag	21 Initiating Causes Description	22 Activation Mode	23 Detection (HH or LL)	24 Trip Value

FINAL ELEMENTS

25 Tag	26 Description of the Final Elements	27 Activation Mode	28 Safe State

EXEC.

29 Tag:

30 Description of the Logic Executor:

31 Input Modules:

32 Output Modules:

MANUAL TRIP

33 Tag	34 Description of the Manual Trip	35 Type	36 Location

FUNCTIONAL DESCRIPTION

37 Description of the Logic:

38 Secondary Actions:

39 Description of the Safe State to be Reached or Kept:

40 Hazardous Combination of Final Elements (Y/N):

41 Description:

PETROBRAS

DATA SHEET | No. | REV.

SHEET of

TITLE: **SIF Specification**

ALARMS

42	Pre-trip Alarm (Y/N):	43	Description:	44	Setpoint:
45	Trip Alarm (Y/N):	46	Description:		
47	Deviation Alarm (Y/N):	48	Description:	49	Setpoint:
50	Failure Diagnosis Alarm (Y/N): [ ] Initiating Causes [ ] Actuators [ ] E/S Cards [ ] Others:				
51	Other Alarms:				

IMPLEMENTATION REQUIREMENTS

BY-PASS

52	Maintenance By-pass (Y/N):	53	Description:	54	Timing:
55	Additional Care:				
56	Operation Start By-pass (Y/N):	57	Description:	58	Timing:
59	Additional Care:				

60	Reset Procedure:		
61	Action in the Failure Detection: [ ] Trip [ ] Degraded mode operation	62	Maximum Operation Time in Degraded Mode:
63	Degraded Mode Description:		
64	Legal Requirements Applicable:		

OTHER IPLs NEEDED

65 Independent Layers of Protection Analysis	66 RRF	67 Independent Layers of Protection	68 RRF

REFERENCE DOCUMENTS

69	Engineering Flowchart	70	Cause and Effect Matrix	71	Logic Diagram
72	SIS Technical Specification	73	List of Alarms	74	
75		76		77	

78 Notes and Remarks:

PETROBRAS	DATA SHEET	No.	REV.
		SHEET of	
	TITLE: SIF - Completion Instruction		

The instructions to complete each numbered field in SIF data sheet are given below. Please note that several fields shall be completed with preliminary values during the basic project, and updated during the detailing project, with special care to the fields related to the verification of the SIL and MTTFS obtained.

1 **Tag** – Each SIF must have a single identifier (Tag) consisting of the unit number, followed by a sequence number. Example: SIF-2212001 (unit 2212, sequence number 001).

2 **Risk Analysis Report** – Code of the risk analysis report related to this SIF.

3 **SIF Description** – Brief description of the function, containing deviation and action. Example: the high pressure of fuel gas blocks gas to furnace F-501.

4 **Demand Causes** – Cause of the SIF demand being considered in the risk analysis. Examples: failure in the fuel gas pressure control loop, process unbalance, etc.

5 **Consequences of the Demand Failure** – Possible damage and impacts caused by the hazardous event being considered in the risk analysis. Examples: Flame extinguishing with the formation of an explosive mixture and possibility of combustion chamber explosion, followed by fire, injury/death of up to one person, production loss of US$ 200,000, damage to facilities of US$ 2 million.

6 **Consequences of the Spurious Trip** – Examples: production loss, possibility of tubes coking, damage to refractory materials, etc. This item must be completed by the team performing the risk analysis.

7 **Spurious Trip Cost (US$)** – Spurious Trip Cost (US$): according to 6.5.2 of PETROBRAS N-2595. This item must be completed by the team performing the risk analysis.

8 **Process Safety Time (s)** – See terms and definitions in PETROBRAS N-2595. This item must be determined by the process discipline.

9 **Response Time (s)** – See terms and definitions in PETROBRAS N-2595. It shall be small enough to ensure the achievement of the safe state before the process variable reaches the hazard threshold.

10 **Delay Time (s)** – See terms and definitions in PETROBRAS N-2595. The Delay Time must be completed consistent with the dynamics of each SIF. Is admissible to set a preliminary value to each type of variable (P, T, F, L etc.), followed by a note alerting that this value shall be adjusted during the plant acceptance and commissioning tests phase.

11 **Interval Between Periodical Tests (years)** – Interval between periodical tests adopted for the SIF. See items 8.5 to 8.7 of PETROBRAS N-2595.

12 **MTTR (h)** – Mean time to repair the SIF - complete with the value actually used in the SIL verification calculations.

13 Blank field.

14 **Required RRF** – Risk Reduction Factor required for the SIF.

15 **Required SIL** – Safety Integrity Level required for the SIF.

16 **Acceptable MTTFS (years)** – Minimum acceptable MTTFS (Mean Time to Fail Safe) - see item 6.5 of PETROBRAS N-2595.

17 **RRF Obtained** – Risk Reduction Factor obtained for the SIF - complete with the value resulting from the SIL verification calculations.

18 **SIL Obtained** – Safety Integrity Level obtained for the SIF - complete with the value resulting from the SIL verification calculations.

19 **MTTFS Obtained (years)** – MTTFS (Mean Time to Fail Safe) obtained for the SIF. Complete with the verification calculation result.

20 **Tag (of the initiating causes)** – Initiating cause identifier, as per engineering flowcharts and cause and effect matrix. Examples: PIT-2212001A and PIT-2212001B. The devices that interpose between the sensor and the logic executor must be listed as initiating causes (e.g.: relay, insulators, intrinsic safety barriers).

21 **Initiating Causes Description** – Initiating cause service, as per list of instruments and data sheets. Example: pressure transmitter in the fuel gas header.

22 **Activation Mode (of the initiating cause)** – De-energizes or energizes for the trip, in case of one discrete element. If it is a transmitter, indicate if the trip sensed is 4 mA (de-energizes for the trip) or 20 mA (energizes for the trip).

23 **Detection (HH or LL)** – Indicate if the detection is ascending (HH) or descending (LL) in relation to the process variable.

24 **Trip Value** – Setpoint value used for the trip. Specify the engineering unit.

25 **Tag (of the final element)** – Final element identifier, as per engineering flowcharts and cause and effect matrix. Examples: XV-2212001A, XV-2212001B and XV-2212001C. The devices that interpose between the sensor and the logic executor must be listed as final elements (e.g.: interposing relays, solenoid valves, signal converters).

26 **Final Element Description** – Final elements service, as per list of instruments and data sheets. Examples: valve blocking the fuel gas to the furnace, fuel gas intermediate breathing valve.

27 **Activation Mode (of the final element)** – De-energizes or energizes for the trip.

28 **Safe State** – Safety position of the final element. Examples: closed blocking valve, breathing valve open to a safe place.

29 **Tag (of the logic executor)** – Logic executor identifier. E.g.: CP-2201001.

30 **Logic Executor Description** – Type of executor used to implement the SIF. E.g.: Safety CLP SIL 3; Non-programmable Logic Executor SIL 2.

31 **Input Modules** – Description of the input modules used for this SIF. E.g.: digital input module; analogical input module 4-20 mA. Specify if separate modules must be used for each initiating cause.

32 **Output Modules** – Description of the output modules used for this SIF. E.g.: digital output module; analogical output module 4-20 mA. Specify if separate modules must be used for each final element.

33 **Tag (of the manual trip)** – Identifier of the manual trip activation device. E.g.: HS-2212150.

34 **Manual Trip Description** – Description of the manual trip. E.g.: Blocking of fuel gas valves to the furnace, activated by the SSC CLP. Pump shutdown through the shutdown tripping device directly wiredrawn to the switch in the CCM.

35 **Type (of the manual trip)** – Activator type. E.g.: electromechanical tripping device with double (series) contact normally closed, retainer, pulls to activate, retainer, with protection against undue activation; logical button in the operation screen.

PETROBRAS

DATA SHEET | No. | REV.

SHEET of

TITLE:

SIF - Completion Instruction

36 **Location** – Activator location. E.g.: local panel of F-501, field, control room.

37 **Logic Description** – Description, by means of a text or drawing, of the logic relation between the initiating cause(s) (it may include the manual trip) and the final element(s) composing the SIF and the voting architectures of sensors and final elements. Example: Starting from the normal operation state, if there is lack of flame in more than 50% of the burners, or if there is low fuel gas pressure, the gas admission to the burners must be blocked, and the intermediate breathing to a safe place must be opened.

38 **Secondary Actions** – Actions initiated by the SIF activation not directly related to the attainment or maintenance of the safe state, with the purpose of helping the operation. E.g.: after the furnace trip, the extinguishing vapor admission and the chimney damper opening to facilitate the blowing out of the combustion chamber.

39 **Description of the Safe State to be Reached or Kept** – Characterization of the SIF activation success. E.g.: fuel gas blocked to the furnace and intermediate breathing opened to the safe place.

40 **Hazardous Combination of Final Elements (Y/N)** – In case of more than one final element, if there is any hazardous condition arising from the failure in their joint activation.

41 **Description (of the hazardous combination of final elements)** – Describe the possible combination and the deriving hazard. E.g.: Non-closing of the first blocking (XV-2212001A) when the intermediate breathing is opened (XV-2212001B), causing a fuel gas cloud in the external area close to the furnace. Remember that combined partial activations of secondary actions may also result in hazard, and that the indetermination about this information may hide accidental scenarios not analyzed during the HAZOP and LOPA meetings, having an impact on the plant safety.

42 **Pretrip Alarm (Y/N)** – Indicate if an alarm with a setpoint that allows the anticipated activation of the operator must be set up so as to prevent the trip.

43 **Description (of the pretrip alarm)** – Description of the pretrip alarm, as per list of alarms.

44 **Setpoint (of the pretrip alarm)** – Setpoint of the pretrip alarm.

45 **Trip Alarm (Y/N)** – Indicate if an alarm indicating that there has been a trip by the SIF must be set up.

46 **Description (of the trip alarm)** – Description of the trip alarm, as per list of alarms.

47 **Deviation Alarm (Y/N)** – Indicate if a deviation alarm among the values read by different initiating causes must be set up.

48 **Description (of the deviation alarm)** – Description of the deviation alarm, as per list of alarms.

49 **Setpoint (of the deviation alarm)** – Setpoint of the deviation alarm.

50 **Failure Diagnosis Alarm (Y/N)** – Indicate if failure diagnosis alarms must be set up, marking the devices covered by these diagnoses/alarms.

51 **Other Alarms** – If other alarms related to the SIF must be set up, describe them and record the setpoints.

52 **Maintenance By-pass (Y/N)** – Indicate if a by-pass must be set up for maintenance.

53 **Description (of the maintenance by-pass)** – If the maintenance by-pass is necessary, describe the implementation way

54 **Timing (of the maintenance by-pass)** – Indicate the maximum time for the maintenance by-pass if a threshold is set up for this by-pass.

55 **Additional Care (in the maintenance by-pass)** – Special condition or specific procedure to be observed for the by-pass or during it, if applicable.

56 **Operation Startup By-pass (Y/N)** – Indicate if a by-pass must be set up for the startup (e.g.: interlocking by-pass due to the very low flow rate during the startup interlocking of a pump). If a by-pass is required during the shutdown, it shall also be marked (in such case, specify in the description field).

57 **Description (of the operation startup by-pass)** – If the startup and/or shutdown by-pass is necessary, describe the implementation way.

58 **Timing (of the operation startup by-pass)** – Indicate the time during which the SIF will remain by-passed in the startup and/or shutdown.

59 **Additional Care (in the operation start by-pass)** – Special condition or specific procedure to be observed during the startup and/or shutdown, if applicable.

60 **Reset Procedure** – Describe the SIF reset procedure, indicating local and remote actions, besides the verifications that must be made before the reset.

61 **Action in the Failure Detection** – Mark the action to be taken in case a failure in one of the SIF components is detected: trip or operation in degraded mode. The operation in degraded mode occurs when the SIF is partly or totally inoperative.

62 **Maximum Operation Time in Degraded Mode** – Maximum operation time with the SIF in degraded mode. After this time, the SIF shall act, causing the trip. This time shall not be higher than the MTTR used in the SIL verification calculation.

63 **Degraded Mode Description** – Description of the operation in degraded mode when the failure is detected. E.g.: degradation of the voting scheme from 2oo3 to 1oo2; adoption of a specific operating procedure to reduce the risk.

64 **Legal Requirements Applicable** – If applicable, the impacts on the SIF and/or plant project must be observed, early in the basic project phase. Otherwise, complete with a dash. E.g.: environmental legislation, NR-10, etc.

65 and 67 **Independent Layers of Protection** – Description of the remaining layers of protection required to reduce the risk to a tolerable value.

66 and 68 **RRF** – Risk reduction factor of the remaining layers of protection.

69 to 77 **Reference Documents** – Codes of the reference documents for this SIF.

78 **Notes and Remarks**

INDEX OF REVISIONS

REV. A

Affected Parts	Description of Alteration
1	Revised and renumbered
2	Revised
3	Revised
4 to 4.2.9	Revised and renumbered
4.30	Eliminated
5 to 5.1	Revised and renumbered
5.1.1	Revised and renumbered
5.1.2 to 5.7.3	Included
6 to 6.1.6	Revised and renumbered
6.1.7 to 6.1.11	Included
6.2 to 6.24	Revised and renumbered
6.2.5 to 6.2.6	Eliminated
6.3 to 6.30.10	Revised and renumbered
6.3.11 and 6.3.12	Included
6.4 to 6.4.8	Revised and renumbered
6.4.8.1 to 6.4.8.5	Eliminated
6.4.9 to 6.4.11	Revised and renumbered
6.4.12 and 6.4.13	Included
6.5 to 6.5.12	Revised and renumbered
6.6 to 6.11	Included
7 to 7.1.5	Revised and renumbered
7.1.6	Eliminated
7.2 to 7.2.4	Revised and renumbered
7.2.5 to 7.2.14	Eliminated
7.3 to 7.3.2	Revised and renumbered
7.3.3 to 7.3.15	Eliminated
7.4 to 7.4.4	Revised and renumbered
7.4.5 to 7.9.2	Eliminated

REV. A	
Affected Parts	**Description of Alteration**
8 and 8.1	Revised and renumbered
8.1.1 to 8.1.4	Eliminated
8.2	Revised and renumbered
8.2.1 to 8.2.3	Eliminated
8.3	Revised and renumbered
8.3.1 and 8.3.2	Eliminated
8.4	Revised and renumbered
8.4.1 and 8.4.2	Eliminated
8.5 to 8.5.2	Revised and renumbered
8.5.2.1 to 8.5.2.3	Eliminated
8.5.4 to 8.8	Included
9 to 9.7	Eliminated
Anexo A	Revised
REV. B	
Affected Parts	**Description of Alteration**
5.3	Revised
5.4.5.4	Revised
5.5.1	Revised
5.6.6	Revised
6.5.4	Revised
6.5.5	Revised
6.5.9	Revised
7.4.3	Revised
Anexo A	Revised
REV. C	
Affected Parts	**Description of Alteration**
All	Revised
REV. D	
Affected Parts	**Description of Alteration**
1.2 to 1.5	Renumbered
2	Revised

REV. D	
3.1, 3.3, 3.6, 3.8, 3.9	Revised
3.15, 3.22, 3.33, 3.34	Revised
3.47	Revised
3.50	Included
3.51	Renumbered
3.52	Revised and renumbered
3.53 and 3.54	renumbered
3.55	Revised and renumbered
3.56 to 3.60	Renumbered
3.61	Included
3.62	Renumbered
4	Revised
5.1..1 and 5.2.1	Revised
Figure 1	Revised
5.4.2, 5.4.4 and 5.4.5	Included
5.4.6	Revised and renumbered
5.4.7	Revised
5.4.7.2	Included
6.2.1, 6.2.4 and 6.2.6	Revised
6.2.8	Revised
Table 1	Revised
6.4.3, 6.4.6 and 6.4.9	Revised
6.4.10 and 6.5.2	Revised
6.5.2.1 and 6.5.2.2	Revised
Table 2	Revised
6.5.3 and 6.5.4	Included
6.5.5	Renumbered
7.1.1, 7.1.3 and 7.2.3	Revised
7.5.3, 7.6.2 to 7.6.6	Revised
7.7.2, 7.7.11 and 7.8.2	Revised
7.8.5	Revised and renumbered

REV. D	
7.8.6 to 7.8.10	Renumbered
7.8.11 and 7.8.12	Revised and renumbered
7.8.13 and 7.8.14	Renumbered
7.9.1, 7.9.3 and 7.12.1	Revised
7.12.7	Renumbered
7.14.1 to 7.14.3	Renumbered
7.15, 7.15.1 and 7.15.2	Included
8.2, 8.2.1 and 8.2.2	Included
8.3	Revised
A.1.1	Revised
Table A.1	Revised
B.2.1.4 and B.2.1.5	Revised
B.2.2.2 and B.2.4.3	Revised
B.2.6 and B.2.6.1	Revised
Table B.3	Revised
Table B.8	Revised
B.2.7.1 to B.2.7.4	Revised
B.2.7.4.1	Included
B.2.7.4.2	Revised and renumbered
B.2.7.4.3	Included
B.2.7.5 and B.2.7.6	Revised and renumbered
B.2.7.6.1 to B.2.7.6.4	Included
B.2.7.7 to B.2.7.10	Revised and renumbered
B.3.2.2	Revised
B.3.2.3	Revised and renumbered
B.3.2.4 and B.3.2.5	Renumbered
B.3.3.1 and B.3.3.2	Revised
B.3.3.3	Included
B.4.1.3	Revised
Annex C	Revised
Annex D	Revised

EXAMPLE

— process condition: monitors the process variable value until the end of the operation startup condition;
— time: adjustment for a time period not much higher than the necessary for the normal execution of the startup procedure;
— combination of the above.

7.11.2.3 The by-pass commands for operation start shall be kept deactivated when the plant or equipment subject to the SIS protection are not in startup procedure.

7.11.3 Maintenance By-Pass

7.11.3.1 It is recommended that no more than one SIF, belonging to a same plant or equipment, be by-passed at the same time. **[Recommended Practice]**

7.11.3.2 The duration of the maintenance by-pass shall be the lowest possible. If the by-passed device is not repaired within the MTTR assumed in the reliability calculations, the actions predefined in the specific procedure shall be taken in order to keep the plant or equipment in the safe state. The most common example of procedure is the adoption of a special operational regimen (reduction of the process unit charge, operation in state of alert, etc.), with the possibility of culminating in the manual activation of the safety function.

NOTE 1 It is not recommended initiate a startup of plant or equipment with a SIF in by-pass for maintenance. **[Recommended Practice]**
NOTE 2 The startup of a plant or equipment with a SIF in by-pass for maintenance leads to the immediate execution of the actions defined in the specific procedure.

7.11.3.3 For the SIFs that do not have redundancy on its sensors, the maintenance by-pass shall degrade the respective voting architectures as follows:

a) from 1 out of 2 to 1 out of 1;
b) from 2 out of 2 to 1 out of 1;
c) from 2 out of 3 to 1 out of 2.

NOTE If there is the by-pass of more than one sensor in a same SIF, the specific procedure shall be adopted, as per 7.11.3.2.

7.11.3.4 For the SIFs that do not have redundancy on its sensors, there shall be a maintenance by-pass command only in the SIFs that satisfy both the following requirements:

a) existence of another mean to monitor the process variable concerned;
b) the process dynamics allows the operator to timely activate the manual trip command.

7.11.3.5 The SIF shall be by-passed according to a specific procedure and it shall be developed for this purpose during the SIS detailing design phase. This procedure shall include the control of the by-pass duration (see 13.1.5), and shall comply with the plant or equipment operational standards, subject to the SIS protection.

EXAMPLE

After being authorized, the operator activates a by-pass request command, specific for the respective intended sensor, by means of the BPCS HMI. Then, the maintenance technician shall activate a physical switch in the SIS Logic solver panel, which enables the respective bypass command. While the by-pass is active, an alert may be periodically announced.