

CONTECComissão 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.

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.

"This Standard is exclusive property of Petróleo Brasileiro S. A. - PETROBRAS, internal application and PETROBRAS Subsidiaries and shall be used by its suppliers of goods and services under contracts or similar under the conditions established in Bidding, Contract, Agreement or similar.

The use of this Standard by other companies / organizations / government agencies and individuals is the sole responsibility of the users.."

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

Foreword.....	6
1 Scope.....	6
2 Normative References.....	6
3 Terms and Definitions.....	7
4 Symbols and Abbreviations.....	16
5 Assessment of the SIS Need and Basic Design Structuring.....	17
5.1 Risk Analysis.....	17
5.2 Protection Layers.....	17
5.3 SIS Life Cycle.....	19
5.4 SIS Basic Design Structuring.....	20
6 SIS Basic Design - SIFs Assessment.....	21
6.1 General Considerations.....	21
6.2 SIFs Assessment Team Composition.....	22
6.3 Preparation for SIFs Assessment.....	23
6.4 Assessment of the Safety Integrity Level required for a SIF.....	23
6.5 Assessment of a SIF's Spurious Trips Frequency.....	24
7 SIS Basic Design - Implementation Requirements.....	25
7.1 Segregation between SIS and BPCS.....	25
7.2 Segregation between Different SISs.....	26
7.3 Segregation among Redundant Channels of a SIF.....	26
7.4 Power Supply.....	27
7.5 Communication between the Field Devices and the Logic Solver.....	27
7.6 Sensors.....	28
7.7 Final Elements.....	28
7.8 Logic Solver.....	30
7.9 Manual Trip Command.....	31
7.10 SIF Reset.....	32
7.11 SIF By-Pass.....	32
7.11.1 General Considerations.....	32



7.11.2 Operation Startup By-Pass	32
7.11.3 Maintenance By-Pass	33
7.12 Operator Interface	34
7.13 Maintenance and Engineering Interface	35
7.14 Communication Interface with the BPCS	35
7.15 Response and Delay Times	35
8 SIS Basic Design – Verification of the SIL and MTTFS Required for Each SIF	35
9 SIS Detailing Project.....	37
9.1 General Requirements	37
9.2 Documentation	37
10 Factory Acceptance and Preservation Test	38
10.1 Factory Acceptance Test - FAT	38
10.2 Pre-Requirements to Perform FAT	39
10.4 Preservation	40
11 Installation and Conditioning for SIS Operation Starting.....	41
11.1 Installation	41
11.2 Conditioning	41
12 SIS Pre-Operation and Final Acceptance	42
12.1 Pre-Operation.....	42
12.2 SIS Final Acceptance.....	43
13 Operation, Maintenance, Periodic Tests and Modifications	43
13.1 Operation.....	43
13.2 Maintenance.....	44
13.3 Periodic Tests.....	45
13.4 Changes	47
Annex A - Determination of Required Safety Integrity Level Using Risk Chart Method.....	49
A.1 Introduction	49
A.2 Risk Chart Summary	49
A.3 Documentation Related to Determination of Safety Integrity Level (SIL) Results	50
A.4 Using Risk Chart Related to People Safety	51
A.5 Using Risk Chart for Environmental Consequences.....	53



A.6 Using Risk Chart for Material Consequences	55
A.7 Determination of Integrity Level of Safety Instrument Function When its Failure Causes More than One Type of Consequence	56
Annex B - Layer of Protection Analysis (LOPA).....	57
B.1 Introduction	57
B.2 Procedure.....	57
B.2.1 Selection of Scenarios to be Analyzed	59
B.2.2 Classification of Severity.....	59
B.2.3 Tolerable Frequency (F^{TOL}).....	59
B.2.4 Initiating Cause Frequency (ICF).....	60
B.2.5 Enabling Event (EE)	61
B.2.6 Modifying Factors (MF).....	62
B.2.6.1 Probability of Ignition	62
B.2.6.2 Presence of People	63
B.2.7 Independent Protection Layers (IPL).....	64
B.3 Analysis Conclusion	71
B.3.1 Scenario Residual Risk Not Considering Instrumented Function.....	71
B.3.2 Determination of SIL Required for SIF	71
B.4 Results Management	72
Annex C - LOPA Spreadsheet Model.....	73
Annex D - SIF Data Sheet.....	75

Figures

Figure 1 - Typical Layers of Protection.....	18
Figure 2 - Graphical Representation of the Risk Reduction.....	19
Figure 3 - SIS Life Cycle Model.....	20
Figure A.1 - Risk Chart Related to Personal Safety	51
Figure A.2 - Risk Chart Related to Environmental Safety	54
Figure A.3 - Risk Chart for Material Consequences.....	55
Figure B.1 - LOPA Procedure Flow.....	58
Figure B.2 - Mitigating Protection Layer	70

Tables

Table 1- SIL Scale for SIF in Demand Mode.....	23
Table 2 - Criteria for Determining the Acceptable MTTFS	25
Table A.1 - Description of Parameters of Risk Chart	50
Table A.2 - Description of Parameters Used in Figure A.1	52
Table A.3 - General Environmental Consequences	54
Table A.4 - Classes of Material Consequence	56
Table B.1 - Tolerable Frequency (F^{TOL}).....	59
Table B.2 - Initiating Cause Frequencies	60
Table B.3 - Modifying Factors of Ignition Probability According to the Amount of Ignition Sources	63
Table B.4 - Modifying Factors of Ignition Probability According to the Type of Flammable Material.....	63
Table B.5 - Modifying Factors According to the Presence of People.....	63
Table B.6 - Safeguards Generally Not Considered as IPL.....	64
Table B.7 - Passive IPL and Their Typical PFD_{avg}	65
Table B.8 - Active IPL and Their Typical PFD_{avg}	66

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 $\text{Risk} = \text{frequency} \times \text{severity}$.

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).

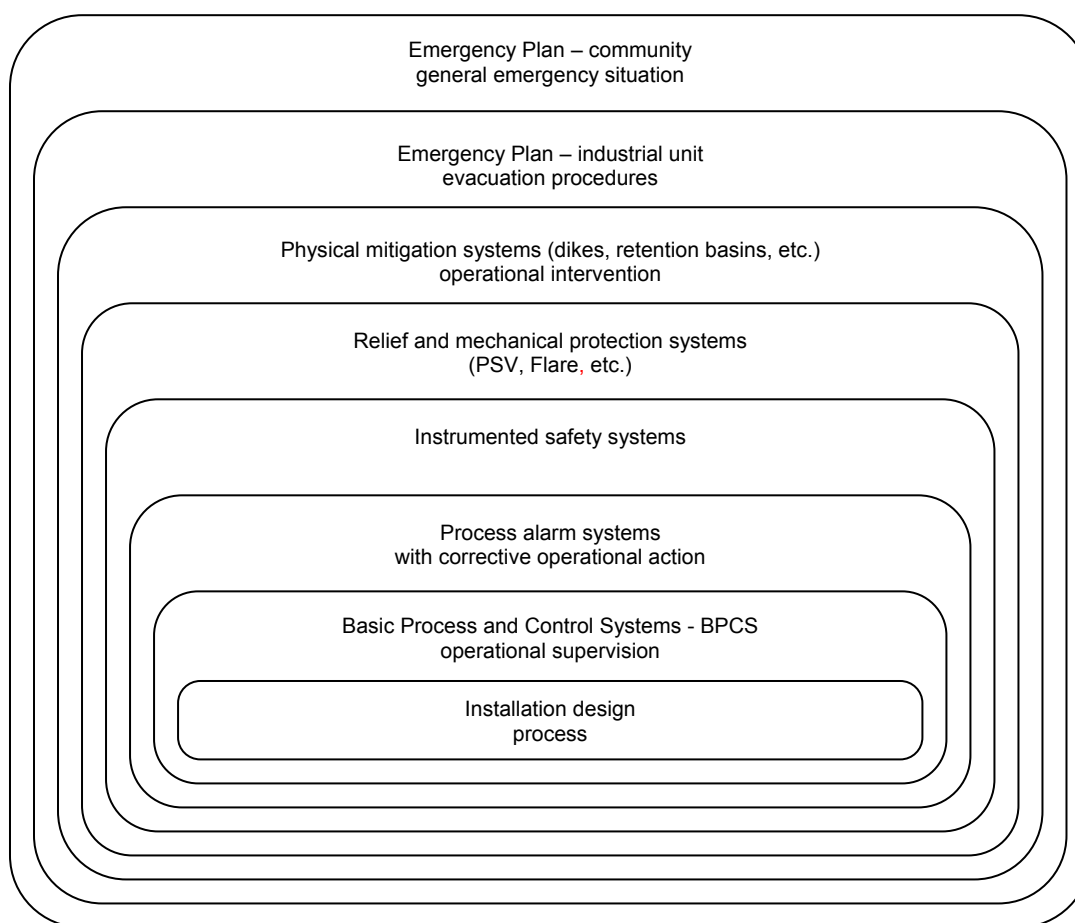


Figure 1 - Typical Layers of Protection

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]

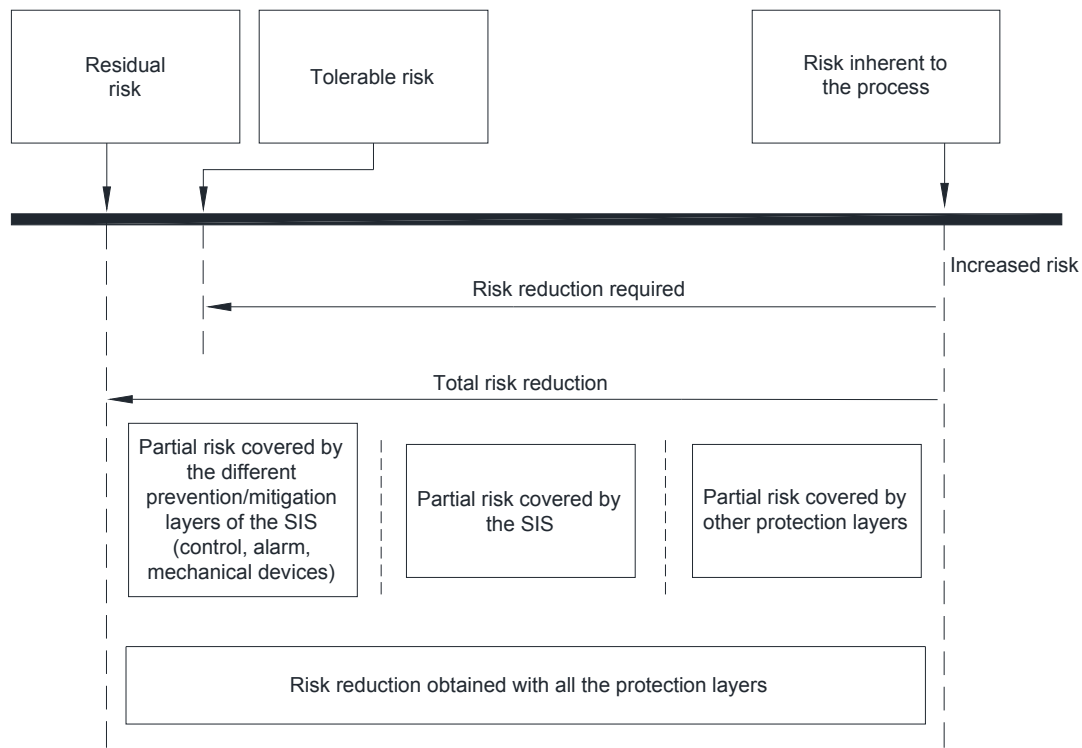
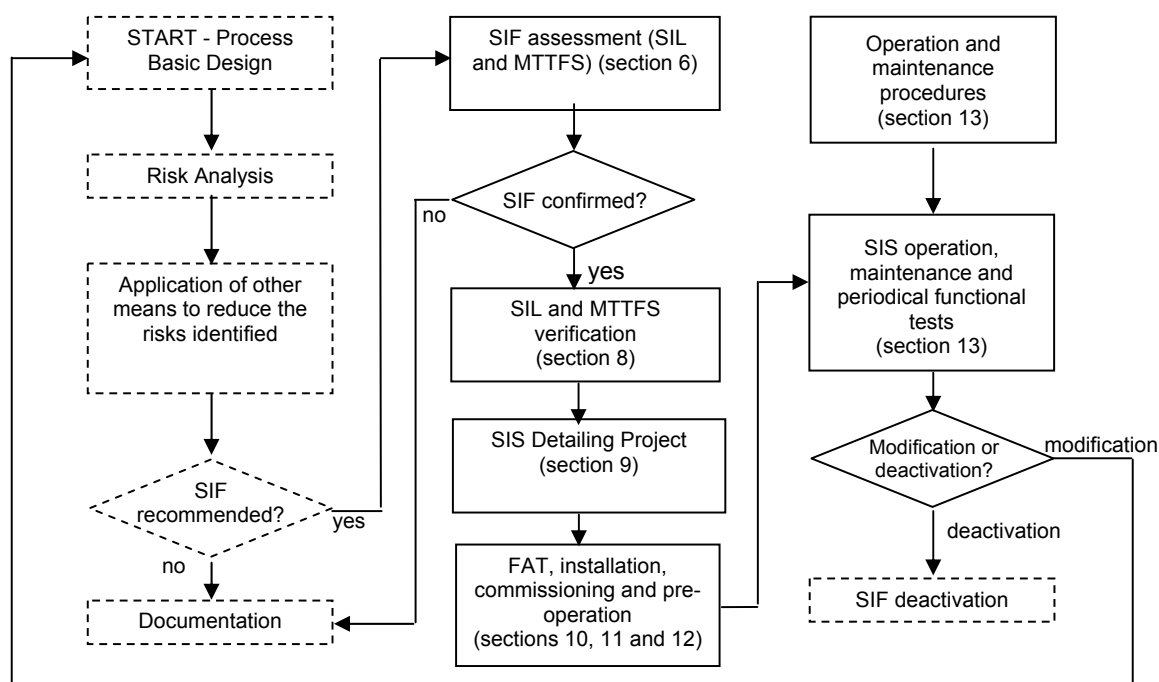


Figure 2 - Graphical Representation of the Risk Reduction

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).



Key: - scope of this Standard

- scope of other standards

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:

- the people and organizations involved in each phase of the life cycle are identified, and their respective responsibilities are assigned;
- the training programs required are applied;
- each phase foreseen is performed and documented;
- the documents generated are distributed, controlled and kept up to date;
- 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	$\geq 10^{-2}$ to $< 10^{-1}$	1
> 100 to ≤ 1,000	$\geq 10^{-3}$ to $< 10^{-2}$	2
> 1,000 to ≤ 10,000	$\geq 10^{-4}$ to $< 10^{-3}$	3
> 10,000 to ≤ 100,000	$\geq 10^{-5}$ 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 MTFS. [Recommended Practice]

Table 2 - Criteria for Determining the Acceptable MTFS

Spurious trip cost (US\$)	Acceptable MTFS (years)
$\leq 10\,000$	Spurious trip tolerance not required
$> 10\,000$ to $\leq 100\,000$	25
$> 100\,000$ to $\leq 1\,000\,000$	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 MTFS 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:

- process taps (see Note 1);
- impulse lines;
- sensors;
- signal wirings;
- junction boxes;
- multicables;
- terminal blocks;
- control and marshalling panels;
- fuses and circuit breakers;
- Logic Solver;
- final elements (see Note 2).