

Alarm Management

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

Industrial Automation and
Instrumentation

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.....	4
1 Scope.....	4
2 Normative References.....	4
3 Terms and Definitions.....	4
4 Symbols and Abbreviations.....	8
5 Alarm Philosophy.....	8
5.1 Objective	8
5.2 Basic Requirements	8
5.3 Alarm Prioritization	8
5.4 Alarm Class.....	11
5.5 Performance Indicators	12
6 Alarm Management Life Cycle	12
6.1 Identification and Rationalization	13
6.2 Detail Design and Implementation	14
6.2.1 Characteristics of an Alarm System.....	14
6.2.2 Implementation of Processing Strategies in the Alarm Systems	15
6.2.3 Alarm System Interface Design Practices.....	19
6.3 Commissioning and Training.....	21
6.4 Operation and Monitoring.....	22
6.5 Management of Change, Maintenance and Audit.....	22
Annex A - Examples of Consequences to the Asset and Operational Continuity.....	23
Annex B - Procedure for Alarms Rationalization.....	24

Figures

Figure 1 - Alarm Deadband	6
Figure 2 - Example of Suppression of Alarms Configured for the Same Variable	16
Figure B.1 - Procedure for Alarms Rationalization	24

Tables

Table 1 - Allowable Response Time.....	9
Table 2 - Determination of Priority by Risk to Assets / Operational Continuity (See Examples - Annex A).....	10
Table 3 - Priority Determination by Risk to the Environment	10
Table 4 - Priority Determination by Risk to Personnel Safety	11
Table 5 - Summary of Recommended Metrics for Alarm Performance	12
Table 6 - Alarms Documentation.....	13

Foreword

This Standard is the English version (issued in 07/2015) of PETROBRAS N-2900 REV. A 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 The purpose of this Standard is to define the alarm management philosophy of PETROBRAS. This Standard may be complemented with a specific philosophy of each business segment of the Company.

1.2 This Standard applies to project, operation and maintenance of alarm systems in PETROBRAS Units.

1.3 This Standard applies to procedures started from the date of its issue.

1.4 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.

PETROBRAS [N-2595](#) - Critérios de Projeto, Operação e Manutenção de Sistemas Instrumentados de Segurança em Unidades Industriais;

PETROBRAS [N-2782](#) - Applicable Techniques to Industrial Risk Analysis;

IEC [62682](#) - Management of Alarm Systems for the Process Industries.

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 alarm

any audible or visual mean that indicates an abnormal condition associated with the process or equipment and that requires an action in a limited time

NOTE The term equipment also applies to systems and instruments.

3.2 deviation alarm

an alarm generated when the difference between two analogical values exceeds a limit (e.g.: deviation between redundant instruments or deviation between the process variable and setpoint)

3.3**discrepancy alarm**

an alarm generated by the error between the comparison of an expected state of the plant or equipment and its real state (e.g.: motor start failure when it is commanded)

3.4**nuisance alarm**

an alarm announcing excessively, unnecessarily, or which does not return to its normal state, even after operator action

3.5**chattering alarm or fleeting alarm**

an alarm that transits between the annunciation condition and the disable condition, in a short period of time

3.6**stale alarm**

an alarm that remains active continuously for long periods of time (usually 24 hours)

3.7**alert**

a signaling less important than the alarm, characterized by operational conditions that require attention, and whose actions shall be taken whenever time allows

3.8**alarm annunciation**

a function of the alarm system to draw the operator's attention on the alarm

3.9**alarm activation**

a state in which the alarm condition is true

3.10**alarm flood**

a condition during which the alarm rate is larger than that which may be effectively managed (e.g.: more than 10 alarms in 10 minutes interval)

3.11**bad-actors**

the alarms that, during a specified time interval, present a much higher number of annunciations than the others

3.12**alarm deadband**

the range in which the state of the alarm is not altered, regardless of the variation of the signal (Figure 1).

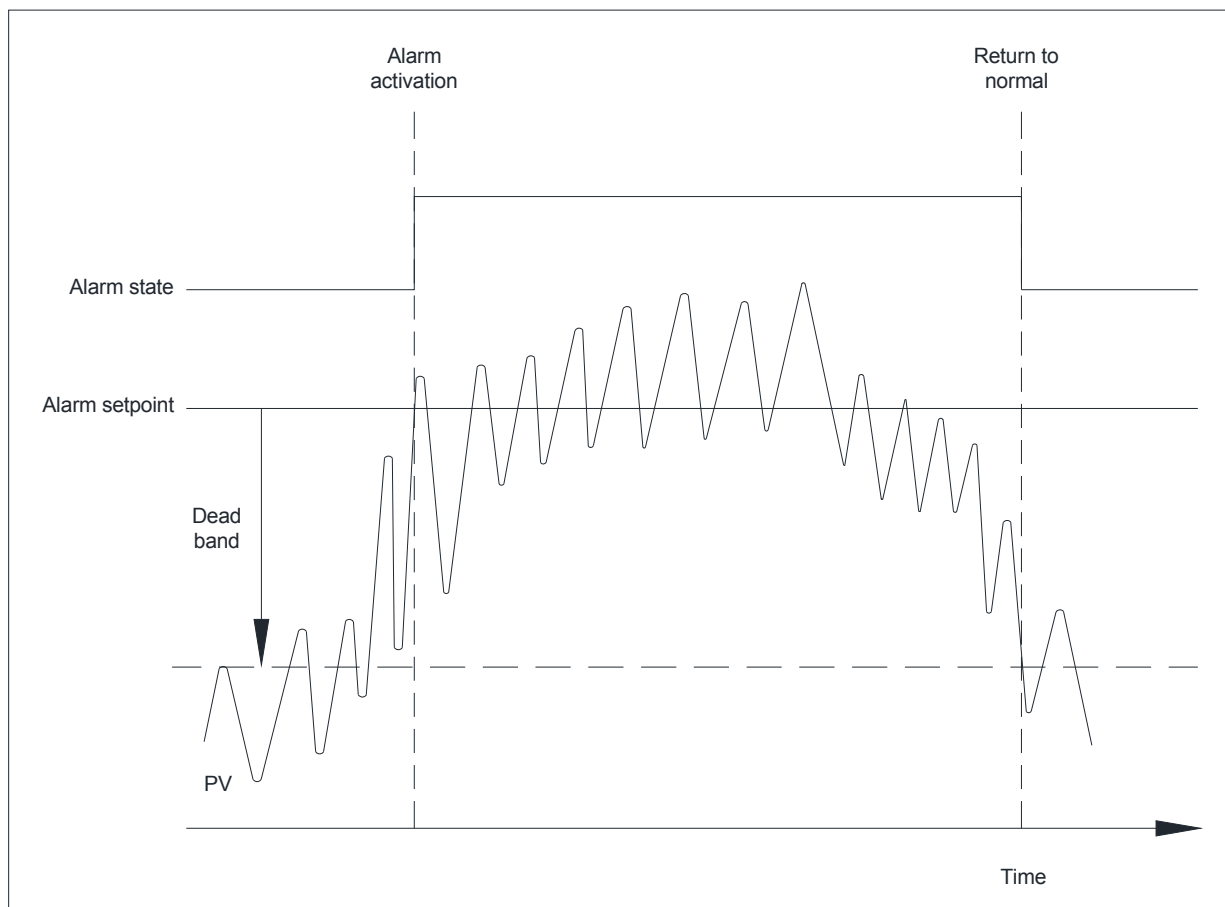


Figure 1- Alarm Deadband

3.13

alarm class

an alarm group with common management requirements as test, training, announcing, audit, etc

3.14

Return to Normal (RTN)

the state in which the condition for alarm announcing has ceased to exist

3.15

event

a change in the conditions of the plant, equipment or a variable

3.16

alarm philosophy

the documentation that establishes the basic definitions, principles and procedures to design, implement and maintain an alarm system

3.17

alarm management

the processes and practices to conceive, design, document, operate, monitor and maintain an alarm system

3.18**alarm group**

a set of alarms, determined by some logical criteria of grouping, such as: physical location, function, system, etc

3.19**alarm priority**

the relative importance attributed to an alarm within an alarm system to indicate the urgency of a response

3.20**rationalization**

the process of alarm analysis to justify and document their conception and/or use based on the alarm philosophy

3.21**acknowledge - ACK**

an action that confirms the acknowledgment of the alarm annunciation

NOTE It does not mean resolution of the alarm reason.

3.22**shelve**

action initiated by the operator to temporarily suppress an alarm, with controlled mechanisms to remove this suppression

3.23**alarm system**

a set of hardware and software that enables the detection of alarm states, annunciation, and also record their changes

3.24**suppression**

any mechanism to prevent the annunciation of the alarm when the abnormal condition is present

3.25**allowable response time**

the maximum time between the alarm annunciation and the beginning of a corrective action on the process, regardless where the action will be executed, to avoid the consequences of the abnormal condition. Reference: Figure 4 of IEC [62682](#)

3.26**alarm timer**

minimum time which the variable must remain continuously beyond its setpoint value, so that the alarm is announced

NOTE This timer may be applied also to remove the alarm annunciation

3.27**alarm setpoint**

a threshold value of a process variable or discrete state that announces the alarm

4 Symbols and Abbreviations

ESD	- Emergency Shutdown;
HAZOP	- Hazard and Operability Study;
HMI	- Human Machine Interface;
IPL	- Independent Protection Layer;
LOPA	- Layers of Protection Analysis;
PV	- Process Variable;
SCADA	- Supervisory Control and Data Acquisition System;
DCS	- Distributed Control System;
SIS	- Safety Instrumented System;
BPCS	- Basic Process Control System;
ART	- Allowable Response Time;
CPU	- Central Processing Unit.

NOTE This document shall use the term BPCS to generally refer to automation architectures adopted in different business segments of the company, replacing terms such as SCADA, DCS and other similar systems.

5 Alarm Philosophy

5.1 Objective

5.1.1 The definition of a philosophy for an alarm system has the following goals:

- to ensure consistency and uniformity of the alarm management for all company plants;
- to ensure alignment with management goals and objectives;
- to provide inputs for the specification, implementation, operation, monitoring and maintenance of a robust and efficient alarm system.

5.1.2 The alarm system does not replace the SIS, but it helps the operator to take actions that will prevent plant shutdown caused by safety instrumented system action, decreasing its demand.

5.2 Basic Requirements

In order to comply with the definition, an alarm shall be designed considering human limitations, and shall have the following features:

- relevance: shall have a defined operational significance; if no response is associated with the signal which generates the alarm, such signal shall not be an alarm;
- singularity: the same information shall not be represented by two different alarms, avoiding duplication of response procedures that can confuse and overload the operator;
- adequate response time: no alarm shall be announced so much before its response or too late for the corrective actions be taken;
- degree of importance: every alarm shall have a priority to facilitate the operator's decision-making;
- clarity: the alarm message shall be easy to understand and focus on the description of the problem.

5.3 Alarm Prioritization

5.3.1 All alarms shall be prioritized so that their interface be properly designed considering the characteristics previously presented.

5.3.2 Alarms shall be prioritized based on the allowable time for the operator's response, and the impacts caused on the plant when no response is taken. These impacts may be related to loss of production and assets, environment damage and personnel safety, considering, within these categories, the alarms defined to comply with local legislation or company's internal policies.

5.3.3 During the assessment of these impacts, the protective layers which are available on the plant at the time of analysis shall be considered for alarms whose operator response has not been classified as IPL. These protective layers may be safety instrumented functions or mechanical protective devices such as safety relief valves.

NOTE 1 The lack of adequate protection layer tends to leave to a high priority alarm. The availability of a well designed SIS, for example, tends to reduce the impact associated with the environment and personnel safety, and to increase the impact associated with production loss, since in the lack of operator response to the alarm will leave the SIS to demand. High priority alarms may indicate an eventual need to revise the upper protection layers. The impact of an alarm status changed to an alert, or an alarm removal, should be verified in other analyzes (e.g.: HAZOP, safety instrumented functions classification).

NOTE 2 The same criterion applies to plants that were not subject to LOPA study.

5.3.4 Alarms whose operator response has been classified as IPL shall be prioritized disregarding the presence of any protective layers.

5.3.5 Criteria for Alarm Prioritization

5.3.5.1 The criteria presented below shall be applied to each alarm. This analysis results in an alarm priority, which can be used to lead the operator to choose which alarm shall be dealt first, when two or more alarms are announced simultaneously.

5.3.5.2 Determination of ART (Allowable Response Time)

5.3.5.2.1 Table 1 shall be used to determine the allowable response time.

Table 1 - Allowable Response Time

ART	Criterion
Long	More than 10 minutes and less than an hour
Medium	Between 3 and 10 minutes
Short	Less than 3 minutes

5.3.5.2.2 For response times longer than one hour, any abnormal signaling shall be considered as an "ALERT".

5.3.5.2.3 For periods of time shorter than 1 minute, it shall be evaluated if the operator's action can be performed accordingly. In case this action is not possible, it shall be foreseen an automatic actuation. For periods of time between 1 and 3 minutes, special alarm annunciation mechanisms and special training for the operation staff shall be considered in order to respond to the abnormal event.