



Document No.	GP 30-47
Applicability	Group
Date	DRAFT 23 February 2010

GP 30-47

Alarm System Design and Management

Group Practice

**BP GROUP
ENGINEERING TECHNICAL PRACTICES**

Foreword

This is the first issue of Engineering Technical Practice (ETP) GP 30-47 Alarm System Design and Management and supersedes the alarm management content within GP 30-45 Guidance on Practice for Human Machine Interface for Process Control, published 31 December 2002.

DRAFT FOR REVIEW

Copyright © 2010 BP International Ltd. All rights reserved.

This document and any data or information generated from its use are classified, as a minimum, BP Internal. Distribution is intended for BP authorized recipients only. The information contained in this document is subject to the terms and conditions of the agreement or contract under which this document was supplied to the recipient's organization. None of the information contained in this document shall be disclosed outside the recipient's own organization, unless the terms of such agreement or contract expressly allow, or unless disclosure is required by law.

In the event of a conflict between this document and a relevant law or regulation, the relevant law or regulation shall be followed. If the document creates a higher obligation, it shall be followed as long as this also achieves full compliance with the law or regulation.

Table of Contents

	Page
Foreword.....	2
1. Scope.....	5
2. Normative References	5
3. Terms and Definitions.....	6
4. Symbols and Abbreviations	11
5. Introduction	12
5.1. Operating Envelopes	12
5.2. Alarm Definition	13
5.3. Safety Categorisation	13
5.4. Alarm Sources	14
5.5. Alarm Classes	14
5.6. Alarm Types	14
5.7. Other Notification Types	15
6. People.....	15
6.1. Major Projects Organisational Capability and Accountabilities.....	15
6.2. Operational Organisational Capability and Accountabilities	16
6.3. Training and Competency Assessment.....	17
7. Alarm Philosophy Document	17
8. Alarm System Design	18
8.1. Overall Requirements.....	18
8.2. Alarm Design Fundamentals	19
8.3. Alarm Response Manual (ARM).....	19
8.4. Storage of Real Time Alarm Data.....	25
8.5. Alarm Logical Processing	25
8.6. HMI Requirements.....	28
8.7. Audible Annunciation.....	30
8.8. Annunciator Panels	30
9. Project Delivery Requirements	30
9.1. General.....	30
9.2. Factory and Site Acceptance Testing.....	30
9.3. Alarm System Design / Modification Performance Assessment and Validation	31
9.4. Handover to Operations	31
10. Operational Responsibilities	31
10.1. Managing Risks	31
10.2. Management of Change	32
10.3. Static Alarm Metrics, Analysis and Targets	33
10.4. Dynamic Alarm Metrics, Analysis and Targets	33
10.5. Continuous Improvement	36

10.6. Auditing and Assurance.....	39
10.7. Alarm Enforcement.....	39
11. Alarm Management Lifecycle	39
Bibliography	40

List of Tables

Table 1 – Minimum Required and Recommended Alarm Philosophy Content.....	18
Table 2 - Alarm Consequence Rating.....	21
Table 3 - Urgency Categorisation	22
Table 4 - Alarm Distribution across a Three Priority Alarm System.....	22
Table 5 - Alarm Distribution across a Four Priority Alarm System.....	22
Table 6 - Alarm Priority Table for a Three Priority System	23
Table 7 - Alarm Priority Table for a Four Priority System.....	23
Table 8 - Alarm Modification MOC Requirements	32
Table 9 - Alarm Totals Metrics (EEMUA 191 Rev2, Table 25)	33
Table 10 - Alarm Performance Metrics and Levels.....	35

List of Figures

Figure 1 Operating Envelopes	13
Figure 2 Alarm Continuous Improvement Process	37

1. Scope

- a. This ETP provides alarm system design and management requirements associated with an automation system.
- b. Specifically, this ETP:
 1. Defines accountabilities and organisational capability requirements to specify, design, implement and operate an effective alarm system.
 2. Defines a set of minimum requirements for alarm handling and performance measurement.
 3. Details project delivery and operational requirements to achieve continuous improvement.
- c. Each BP entity shall detail within its Alarm Philosophy document (see section 7) how it meets these requirements.
- d. Where legacy systems, that predate the release of this GP, can not meet the functional requirements of this GP, each functional gap shall be documented within the alarm philosophy document (see section 7).
- e. This ETP is applicable to wholly owned BP facilities and/or BP operated facilities and is highly recommended for joint venture (JV) facilities.

2. Normative References

The following referenced documents may, to the extent specified in subsequent clauses and normative annexes, be required for full compliance with this GP:

- For dated references, only the edition cited applies.
- For undated references, the latest edition (including any amendments) applies.

BP

GDP 5.0-0001	Integrity Management.
GFD 0.0-0002	OMS Elements of Operating Including Group Essentials
EP SRP 5.0-0001	Engineering Management
GP 48-03	Layer of Protection Analysis (LOPA).
EP GP 30-43-1	Automation Blueprint (E&P).
GP 30-45	Human Machine Interface for Process Control.
GP 30-60	Automation Systems Digital Security and Integrity
GP 30-80	Safety Instrumented Systems (SIS) - Specification and Implementation.
GP 30-81	Safety Instrumented Systems (SIS) - Operations and Maintenance.
GN 35-050	Work Management Data Standards.

The Engineering Equipment and Materials Users' Association (EEMUA)

Pub. No 191 Edition 2 Alarm Systems - A Guide to Design, Management and Procurement.

Abnormal Situation Management (ASM®) Consortium

Guideline v.5.01 Effective Alarm Management Practices.

The International Society for Automation (ISA)

ISA-SP18.02	Management of Alarm Systems for the Process Industries.
ANSI/ISA-5.1-2009	Instrumentation Symbols and Identification

Interessengemeinschaft Automatisierungstechnik der Prozessindustrie (NAMUR)

NAMUR NA102	Alarm Management.
-------------	-------------------

The Alarm Management Handbook, A Comprehensive Guide, Hollifield and Habibi, 2006.**3. Terms and Definitions**

For the purposes of this GP, the following terms and definitions apply:

Abnormal Operation

Abnormal Operation is a deviation from normal operating conditions, but still within the allowable safe design limits. The process is moving towards a state which may cause automatic action by the Safety Instrumented System (SIS), a mechanical trip, pressure relief, etc. if not returned to the normal operating range by the automation system or operator action.

Abnormal Situation Management (ASM)[®]

Abnormal Situation Management and ASM[®] are U.S. trademarks of Honeywell International. The term refers to methods and tools by which abnormal situations can be prevented, mitigated and addressed during plant operations.

Accepted (Acknowledged)

An alarm is accepted when the operator has indicated awareness of its presence (usually by push button or mouse click). It is unaccepted until this has been done.

Active Alarm

An alarm condition which is on (i.e. limit has been exceeded and condition continues to exist or limit is no longer exceeded and alarm has been configured to latch). It may be accepted or unaccepted.

Alarm Attributes

The alarm parameters configured within the automation system (e.g., alarm setting, alarm priority).

Alarm Deadband

The range between which the alarm is raised and then cleared.

Alarm Enforcement

The manual or automatic process by which alarm attributes in the automation system are over written by a master database, located hierarchically above the automation system.

Alarm Flood; Alarm Overload

The situation where more alarms are received than can be processed by a single console operator.

Alarm Grouping

Grouping of alarms, to, for example, produce a single grouped alarm, whose resultant operator action is the same for the respective abnormal condition.

Alarm Handling

Alarm handling describes the actions, procedures and processes involved in managing an alarm by the automation system and by the operator.

Alarm Limit; Alarm Setpoint; Alarm Trip Point; Alarm Set Point, Alarm Setting

The threshold value or discrete state of a process variable that triggers the alarm.

Alarm Log

The historical record of all alarms generated by an automation system.

Alarm Management

The processes and practices for determining, documenting, designing, monitoring, and maintaining alarm systems.

Alarm Masking (Dynamic Suppression)

A method using logical processing to reduce the number of alarms generated during an abnormal situation. Alarms are said to be masked if they are inhibited from triggering whilst a defined condition or conditions persist.

Alarm Message

Text information presented to the operator that describes the alarm condition.

Alarm Off-Delay Timer (Debounce Timer)

The time a process measurement remains in the normal state before the alarm is cleared.

Alarm On-Delay Timer

The time a process measurement remains in the alarm state before the alarm is annunciated.

Alarm Priority

The relative importance assigned to an alarm within the alarm system to indicate the urgency of response (i.e. a function of seriousness of consequence and allowable response time).

Alarm Processor

Part of the automation system for processing and displaying alarms.

Alarm Response Manual

A database containing all pertinent information, including details of the associated operator response, relating to each alarm configured on the automation system.

Alarm System

The complete system for generating and handling alarms including field equipment, signal conditioning and transmission, alarm processing, alarm display and supporting information (e.g. alarm response procedures, management controls, etc).

Alarm State

The status of an alarm (cleared, acknowledged, unacknowledged etc) at any one time.

Alert (Message)

An alert or message is a notification to the operator that he or she should be aware of something e.g. a laboratory result has just been received, and there is no serious consequence if ignored or missed. An alert or message is not an alarm. An alarm has an accompanying action to prevent or address an abnormal situation, an alert or message does not and as such is risk-ranked lower than "alarms".

Automatic Shelving

A facility within an automation system to automatically shelve and un-shelve alarms (See EEMUA 191 Rev 2 Appendix 9.10).

Automation System

The collective term for equipment and legacy equipment types (integrated control and safety system [ICSS], supervisory control and data acquisition [SCADA], distributed control system [DCS], process automation system [PAS], process control system [PCS], process shutdown [PSD], emergency shutdown system [ESD], safety instrumented system [SIS], fire and gas [F&G], panel mounted controls and alarms, etc.) that perform safety, control, and/or monitoring functions on process facilities and may reside on or across process control networks (PCNs), process information networks (PINs), or similar systems below and segregated from business IT systems. Automation systems encompass all functional types, for example, process, drilling, marine, subsea, packaged control and safety systems etc.

Bad Actors (Nuisance Alarms)

Nuisance alarms, which have not been designed correctly such that they fall into one or more of the following categories:

- Quickly repeating alarms (i.e. chattering alarms)
- Too-long-lasting alarms (i.e. stale alarms)
- Multiple alarms produced by a common cause and requiring the same operator action (i.e. duplicated alarms)
- Incorrectly configured alarms (e.g. an alarm with incorrectly defined setting)
- Alarms requiring no operator action

Cleared

Alarm state: an alarm is cleared when the condition has returned to normal.

Consequential Alarm

A consequential alarm is one that will activate as a direct consequence of the process or equipment conditions that caused a previous alarm. Consequential alarms can be inhibited through appropriate alarm masking.

Console

The interface for a single operator to monitor the process.

Disable

An alarm is disabled when the system is configured to stop an alarm activating.

Event Log

An automation system resident log that contains time stamped records of actions or status changes, made, for example, by operators or batch control software.

Fleeting (Chattering) Alarm

An alarm that fluctuates above and below its setting, e.g. because of process noise. Also known as “Repeating” alarm within EEMUA 191.

Hazard and Operability Studies (HAZOP)

A structured analysis technique to assess the hazards and operability of a process design.

Human Machine Interface

Means of interfacing the automation system with the user, usually via a keyboard, mouse, and display screen.

Inhibit

To manually suppress the annunciation of an alarm.

Initiating event

A failure or other condition that may result in an alarm.

Latched alarm

An alarm that remains in alarm state after the process has returned to normal and requires an operator reset before it will clear.

Management of Change (MOC)

The formal process/system used to authorise/record changes to the plant or infrastructure that supports that plant. With regard to alarms, MOC is to be defined in the alarm philosophy of a BP entity.

Manual Shelving

The manual act of temporarily suppressing (inhibiting) an alarm e.g. because it is deemed to be a nuisance. A shelved alarm will be removed from the alarm display list (but will still be logged) and will not re-annunciate until un-shelved (See EEMUA 191 Rev 2 Appendix 9.8).

Normal Operating Limit (NOL)

The point at which a process variable enters an alarm zone and operator action is expected to bring the process back within the NOL.

Operating Mode

The different operating states that the process can be in e.g. shutdown, start-up, standby, duty, etc.

Operating Procedure

A set of explicit guidelines and instructions to be followed by the operator.

Operations

The period and people associated with the Operate phase of the BP entity.

Operator

A person, who through the use of automation system, is responsible for the real-time operation of the BP entity or part of the BP entity.

Operator Response Time (ORT)

The total time required, following the annunciation of the alarm, for the operator to correctly analyse, through the respective automation system HMI, the current associated process conditions, identify the initiating cause, ascertain the potential consequences and take all necessary actions to avoid escalation of the abnormal situation and prevent the consequences of the event related to the alarm.

Permanent Alarm Change

Any alarm change that is recorded under MOC. Thus the implementation of dynamic alarm shelving, for example, is a permanent change, as is the change to an alarm setting, or the intentional disabling of an alarm, for a period of a few days/weeks until a repair can be carried out.

Proof Test Interval

Periodic function testing to verify the operation of an alarm. The interval selected is dependant on the criticality of the alarm in question and the statistical likelihood of the alarm failing.

Prioritisation

The process of assigning a priority to an alarm.

Raised

An alarm is raised or initiated when the condition creating the alarm has occurred.

Rationalisation

The process by which alarms are reviewed and modified in a consistent manner across the BP entity by a multi-disciplined team, using the principles and targets set within the Alarm Philosophy document.

Remote Alarm

An alarm from a remotely operated facility.

Release ('One-Shot') Shelving

Similar to manual shelving. The manual act of releasing a standing alarm, thereby removing it from the alarm list. The operator does not know when the alarm clears but when the alarm triggers again it appears on the alarm list in the normal way (See EEMUA 191 Rev 2 Appendix 9.9).

Safe Operating Envelope

The boundaries described by the upper and lower safe operating limits.

Safe Design Limit

The limits above (or below) which it is considered unknown or unsafe to operate. Outside these limits, unpredictable behaviour may occur including catastrophic loss of containment.

Safe Operating Limit

Limits above (or below) which immediate action is required to prevent the process from reaching the safe design limit. Typically automatic trips, mechanical pressure reliefs, or safety related alarms will be set at this limit.

Stale Alarm

An alarm which remains in the alarm state for an extended period of time. See standing alarm.

Standing (Stale) Alarm

An alarm is standing whilst the condition persists (stale and standing are often used interchangeably).

Suppress

To suppress, by means of configured logic, the operation of an alarm function.

System Prompt

A request from the automation system that the operator performs an action that the system cannot perform or that requires operator authority to perform.

Temporary Alarm Change

A manually-initiated change requiring no MOC, applied through no more than operator-level access/authority, affecting the display/annunciation of alarm(s) and whose effects are reversed/removed either after a set time period (e.g. 2 hours) or at a set time (e.g. nominal shift change time) or by a pre-determined event (e.g. feed flow rate greater than threshold). A change that is not

retriggered after a period of time or a pre-determined event is a permanent change and should be formally recorded under MOC.

Time to Event (TTE)

The time between the alarm initiating and the event reaching a critical stage, after which any corrective action will not avoid the consequence.

Unaccepted (Unacknowledged)

An alarm is accepted when the operator has indicated awareness of its presence (usually by push button or mouse click). It is unaccepted until this has been done.

Urgency

The time the operator has before taking action in response to an alarm to avoid the consequence.

Workstation

The interface for a single operator to monitor the process or an engineer to modify the configuration of the automation system.

4. Symbols and Abbreviations

For the purpose of this ETP, the following symbols and abbreviations apply:

ASM®	Abnormal Situation Management.
ARM	Alarm Response Manual.
C&E	Cause and Effect.
C&I	Control and Instrumentation.
COTS	Commercially off the shelf.
DCS	Distributed Control System.
ESD	Emergency Shutdown System
FAT	Factory Acceptance Test.
FDS	Functional Design Specification
FEED	Front End Engineering Design.
F&G	Fire and Gas.
HAZID	Hazard Identification
HMI	Human Machine Interface.
I/O	Input / Output.
ICSS	Integrated Control & Safety System
IT&S	Information Technology and Services
KPI	Key Performance Indicator.

LOPA	Layers of Protection Analysis
MAC	Main Automation Contractor.
MMS	Maintenance Management System.
OEM	Original Equipment Manufacturer
OTS	Operator Training Simulator
P&ID	Piping (or Process) and Instrumentation Diagram.
P&PS	Process and Process Safety
PFD	Process Flow Diagram
PFDavg	Average Probability of Failure (to perform its design function) on Demand.
SAT	Site Acceptance Test
SETA	Segment Engineering Technical Authority.
SIF	Safety Instrumented Function
SME	Subject Matter Expert
SORA	SIS Override Risk Assessment
SPA	Single Point of Accountability.
SPU	Strategic Performance Unit.
SRA	Safety Related Alarm.
SRS	Safety Requirements Specification
TA	Technical Authority.
TMEL	Target Mitigated Event Likelihood.
UPS	Uninterruptible Power Supply.

5. Introduction

5.1. Operating Envelopes

- a. For the purposes of this ETP, the description of the operating envelopes described in section 5.3 of EP SRP 5.0-0001 Segment Recommended Practice for Engineering Management, and depicted in Figure 1, shall apply.