

DEP SPECIFICATION

ALARM MANAGEMENT

DEP 32.80.10.14-Gen.

February 2014

ECCN EAR99

DESIGN AND ENGINEERING PRACTICE

DEM1



© 2014 Shell Group of companies
All rights reserved. No part of this document may be reproduced, stored in a retrieval system, published or transmitted, in any form or by any means, without the prior written permission of the copyright owner or Shell Global Solutions International BV.

This document contains information that is classified as EAR99 and, as a consequence, can neither be exported nor re-exported to any country which is under an embargo of the U.S. government pursuant to Part 746 of the Export Administration Regulations (15 C.F.R. Part 746) nor can be made available to any national of such country. In addition, the information in this document cannot be exported nor re-exported to an end-user or for an end-use that is prohibited by Part 744 of the Export Administration Regulations (15 C.F.R. Part 744).

PREFACE

DEP (Design and Engineering Practice) publications reflect the views, at the time of publication, of Shell Global Solutions International B.V. (Shell GSI) and, in some cases, of other Shell Companies.

These views are based on the experience acquired during involvement with the design, construction, operation and maintenance of processing units and facilities. Where deemed appropriate DEPs are based on, or reference international, regional, national and industry standards.

The objective is to set the standard for good design and engineering practice to be applied by Shell companies in oil and gas production, oil refining, gas handling, gasification, chemical processing, or any other such facility, and thereby to help achieve maximum technical and economic benefit from standardization.

The information set forth in these publications is provided to Shell companies for their consideration and decision to implement. This is of particular importance where DEPs may not cover every requirement or diversity of condition at each locality. The system of DEPs is expected to be sufficiently flexible to allow individual Operating Units to adapt the information set forth in DEPs to their own environment and requirements.

When Contractors or Manufacturers/Suppliers use DEPs, they shall be solely responsible for such use, including the quality of their work and the attainment of the required design and engineering standards. In particular, for those requirements not specifically covered, the Principal will typically expect them to follow those design and engineering practices that will achieve at least the same level of integrity as reflected in the DEPs. If in doubt, the Contractor or Manufacturer/Supplier shall, without detracting from his own responsibility, consult the Principal.

The right to obtain and to use DEPs is restricted, and is typically granted by Shell GSI (and in some cases by other Shell Companies) under a Service Agreement or a License Agreement. This right is granted primarily to Shell companies and other companies receiving technical advice and services from Shell GSI or another Shell Company. Consequently, three categories of users of DEPs can be distinguished:

- 1) Operating Units having a Service Agreement with Shell GSI or another Shell Company. The use of DEPs by these Operating Units is subject in all respects to the terms and conditions of the relevant Service Agreement.
- 2) Other parties who are authorised to use DEPs subject to appropriate contractual arrangements (whether as part of a Service Agreement or otherwise).
- 3) Contractors/subcontractors and Manufacturers/Suppliers under a contract with users referred to under 1) or 2) which requires that tenders for projects, materials supplied or - generally - work performed on behalf of the said users comply with the relevant standards.

Subject to any particular terms and conditions as may be set forth in specific agreements with users, Shell GSI disclaims any liability of whatsoever nature for any damage (including injury or death) suffered by any company or person whomsoever as a result of or in connection with the use, application or implementation of any DEP, combination of DEPs or any part thereof, even if it is wholly or partly caused by negligence on the part of Shell GSI or other Shell Company. The benefit of this disclaimer shall inure in all respects to Shell GSI and/or any Shell Company, or companies affiliated to these companies, that may issue DEPs or advise or require the use of DEPs.

Without prejudice to any specific terms in respect of confidentiality under relevant contractual arrangements, DEPs shall not, without the prior written consent of Shell GSI, be disclosed by users to any company or person whomsoever and the DEPs shall be used exclusively for the purpose for which they have been provided to the user. They shall be returned after use, including any copies which shall only be made by users with the express prior written consent of Shell GSI. The copyright of DEPs vests in Shell Group of companies. Users shall arrange for DEPs to be held in safe custody and Shell GSI may at any time require information satisfactory to them in order to ascertain how users implement this requirement.

All administrative queries should be directed to the DEP Administrator in Shell GSI.

TABLE OF CONTENTS

1.	INTRODUCTION	5
1.1	SCOPE.....	5
1.2	DISTRIBUTION, INTENDED USE AND REGULATORY CONSIDERATIONS	5
1.3	DEFINITIONS	5
1.4	CROSS-REFERENCES	12
1.5	SUMMARY OF MAIN CHANGES.....	12
1.6	COMMENTS ON THIS DEP	13
1.7	DUAL UNITS.....	13
1.8	NON NORMATIVE TEXT (COMMENTARY).....	13
2.	ALARM SYSTEM PHILOSOPHY.....	14
2.1	GENERAL	14
2.2	ALARMS AND ALERTS - BACKGROUND	14
2.3	OPERATING CONSTRAINTS, LIMITS, SETTINGS, AND NOTIFICATIONS	14
2.4	OPERATING LIMIT DEFINITION	15
2.5	MANAGING ALARM RATES.....	15
2.6	MANAGING STANDING ALARMS.....	16
2.7	MANAGING THE INTEGRITY OF ALARM SETTINGS	16
3.	ALARM SYSTEM LIFECYCLE	16
3.1	GENERAL	16
3.2	SITE ALARM PHILOSOPHY AND PROJECT ALARM SYSTEM REQUIREMENTS SPECIFICATION	16
3.3	NOTIFICATION WORK PROCESS.....	17
3.4	ALARM SYSTEM DESIGN.....	17
3.5	ESTABLISH ALARM SYSTEM PERFORMANCE TARGETS.....	17
3.6	COMMISSIONING AND START-UP	18
3.7	RUN AND MAINTAIN PHASE	18
4.	NOTIFICATION INITIAL SETUP (ISU) WORK PROCESS	19
4.1	GENERAL	19
4.2	THE ISU TEAM	19
4.3	IDENTIFICATION PHASE WORK PROCESS	21
4.4	MASTER ALARM DATABASE OF CONSTRAINTS, LIMITS, NOTIFICATIONS AND VARIABLES (VARIABLE TABLE).....	21
4.5	CONSTRAINTS	22
4.6	LIMITS.....	23
4.7	HIERARCHY OF CONSTRAINTS AND LIMITS.....	25
4.8	SOURCES OF CONSTRAINTS AND LIMITS	25
4.9	VARIABLES	27
4.10	RATIONALIZATION PHASE OF THE INITIAL SETUP WORK PROCESS	27
4.11	LIMIT SETTING	28
4.12	HANDSHAKE FOR CRITICAL INFORMATION TO OTHER PROCESSES	28
4.13	CUSTOMER ACCEPTANCE CHECK	28
4.14	COMPLETION	28
5.	ALARM SYSTEM DESIGN	29
5.1	PROCESS ALARMS.....	29
5.2	FOUNDATION FIELDBUS (FF) PROCESS ALARMS	29
5.3	IPF PRE-ALARMS	29
5.4	IPF ALARMS/NOTIFICATIONS.....	29
5.5	FIRE AND GAS ALARMS.....	30
5.6	DIAGNOSTIC ALARMS.....	30
5.7	MAINTENANCE ALARM SUMMARY	31
5.8	OPERATOR SWITCHES AND CONTROLS	31
5.9	ALARM PRESENTATION.....	31
5.10	COMMON ALARMS	31
5.11	INTERMITTENTLY OPERATED AND SPARED EQUIPMENT	32
5.12	FACILITY ALARMS	32
5.13	SIGNAL FILTERING REQUIREMENTS.....	32

5.14	MASTER ALARM DATABASE (VARIABLE TABLE) INTERFACES.....	33
5.15	BPCS CONFIGURING CAPABILITY – ENFORCING.....	33
5.16	MAINTENANCE.....	33
5.17	ALARM SYSTEM PERFORMANCE MEASUREMENT.....	33
5.18	ALARM MANAGEMENT TOOLS	33
6.	NOTIFICATION SUPPRESSION	35
6.1	GENERAL	35
6.2	ALARM SHELIVING	35
6.3	STATIC ALARM SUPPRESSION.....	35
6.4	DYNAMIC ALARM SUPPRESSION.....	37
6.5	DYNAMIC STATE-BASED ALARM SETTINGS.....	39
7.	REFERENCES	42

APPENDICES

APPENDIX I	NOTIFICATION ANALYSIS CHECKLIST	43
APPENDIX II	REQUIRED FIELDS IN THE VARIABLE TABLE	46

1. INTRODUCTION

1.1 SCOPE

This DEP specifies requirements and gives recommendations for the engineering of notification (alarms and alerts) systems.

The alarm management philosophy in this DEP is based on alarm best practices, such as those defined in EEMUA 191 and ISA 18.2.

This DEP specifies a rigorous work process that is to be applied to identify and document the set of notifications that are included in the alarm system. These notifications are based on plant operating limits obtained from equipment and process constraints, commonly referred to as the plant operating envelope. The DEP also specifies requirements of notification suppression logic, and the design of alarms of safety-critical sub-systems and equipment diagnostic alarms.

This DEP contains mandatory requirements to mitigate process safety risks in accordance with Design Engineering Manual (DEM) 1 – Application of Technical Standards.

This is a revision of the DEP of the same number dated February 2011; see (1.5) regarding the changes.

1.2 DISTRIBUTION, INTENDED USE AND REGULATORY CONSIDERATIONS

Unless otherwise authorised by Shell GSI, the distribution of this DEP is confined to Shell companies and, where necessary, to Contractors and Manufacturers/Suppliers nominated by them. Any authorised access to DEPs does not for that reason constitute an authorization to any documents, data or information to which the DEPs may refer.

This DEP is intended for use in facilities related to oil and gas production, gas handling, oil refining, chemical processing, gasification, distribution and supply/marketing. This DEP may also be applied in other similar facilities.

When DEPs are applied, a Management of Change (MOC) process shall be implemented; this is of particular importance when existing facilities are to be modified.

If national and/or local regulations exist in which some of the requirements could be more stringent than in this DEP, the Contractor shall determine by careful scrutiny which of the requirements are the more stringent and which combination of requirements will be acceptable with regards to the safety, environmental, economic and legal aspects. In all cases the Contractor shall inform the Principal of any deviation from the requirements of this DEP which is considered to be necessary in order to comply with national and/or local regulations. The Principal may then negotiate with the Authorities concerned, the objective being to obtain agreement to follow this DEP as closely as possible.

1.3 DEFINITIONS

1.3.1 General definitions

The **Contractor** is the party that carries out all or part of the design, engineering, procurement, construction, commissioning or management of a project or operation of a facility. The Principal may undertake all or part of the duties of the Contractor.

The **Manufacturer/Supplier** is the party that manufactures or supplies equipment and services to perform the duties specified by the Contractor.

The **Principal** is the party that initiates the project and ultimately pays for it. The Principal may also include an agent or consultant authorised to act for, and on behalf of, the Principal.

The word **should** indicates a recommendation.

The word **shall** indicates a requirement.

The capitalised term **SHALL [PS]** indicates a process safety requirement.

1.3.2 Specific definitions

The definitions below shall not be substituted with site or local terminology.

Term	Definition
Abnormal Situation	The exceedance of any defined <u>critical</u> or <u>standard limit</u> or the condition when the process is not behaving as expected or when other threats have impacted operations.
Alarm	The <u>notification</u> type used to notify operators of the exceedance of a <u>Critical Limit</u> or a <u>Standard Limit</u>. See <u>notification</u>. In this document the word “Alarm” (with a capital A) denotes an alarm as per this definition. When the word “alarm” is used without capital, the generic term is meant. An alarm must result in required alarm action to deal with the exceedance.
Alarm Enforcement	The process whereby a number of key alarm parameters are enforced from a repository that holds the master information to the alarm system. The enforcement may be done manually, fully automatically on a regular basis or semi automatically with manual confirmation.
Alarm Management	Activities related to monitoring, storing, reporting, analyzing and auditing alarm and alert notifications, with the intent to improve the effectiveness and performance of the alarm system.
Alarm Operations	Alarm functions needed in real-time by the console operator, such as alarming, suppression, shelving and proactive monitoring. These functions also typically require high availability and high integrity.
Alarm Processor	The part of the alarm system that processes and displays the alarms. Often this function is carried out by a BPCS and/or hardwired annunciator system.
Alarm System	Complete system for generating and handling <u>notifications</u> including field equipment (instruments), signal conditioning and transmission, alarm processing and alarm display. The alarm system includes hardware, firmware, configuration and supporting information (e.g. alarm response procedures, management controls).
Alert	The <u>notification</u> type used to notify operators and/or operations support personnel of the exceedance of a target limit or other event that is not a critical or standard limit exceedance. See <u>notification</u> .
Allowable Time in Exceedance	The time a <u>standard limit</u> may be exceeded without the onset of potential degradation of equipment integrity. Sites should set a default value and minimize deviations.
Basic Process Control System (BPCS)	A configurable microprocessor-based process control system. The term includes DCS, PLC and SCADA process control systems but excludes the SIS.
Configuration	The combination and the setting of parameters of predefined, application specific library functions and their parameters to implement the <u>alarm system</u> functionality.
Console Operators	The personnel assigned to a single or small number of facilities, utilities or systems responsible for the monitoring and control of the processes via the control system of the facilities, typically reporting to the shift team leader.

Term	Definition
Constraint	An identified restriction on the equipment, such as the design pressure or design temperature of a vessel, a relief valve setting, an IPF setting etc. which limits or restricts the operation of the equipment or process.
Constraint Owner	The person or role that is identified as responsible for maintaining the identified <u>constraint</u> , the <u>constraint</u> value and any supporting documentation of the identified <u>constraint</u> .
Control Room	The section of a control centre containing the essential equipment required to operate the plant optimally and safely.
Critical Limit	The value at which the operator has a last opportunity to timely diagnose a situation and respond in order to correct the process and prevent severe short-term HSE consequences.
Customer Acceptance Check	A step in the initial setup process when operators and other operations personnel are given the opportunity to comment on the variable table work of the initial setup core team: limits, alarm settings, consequences of deviation in the event a limit is exceeded, recommended steps to take to correct the deviation and other information.
Deadband	The difference between the <u>limit</u> and the value of the process parameter at which the <u>notification</u> is de-activated. The <u>notification</u> is de-activated when the process parameter has moved into the safe direction further than the value of the dead band.
Demand	A process or equipment condition or event which requires an Instrumented Protective Function or an operator receiving a notification to take action to prevent a hazardous event.
Demand Rate	The frequency at which a demand occurs, i.e., the number of demands per unit time. Also known as frequency of demand.
Disabled Notification	A notification whose visibility has been removed from the operators but whose activation is still captured in the notification history.
Disabled Notification Log	A record of all notifications that have been disabled, inhibited or re-enabled. The mitigation plan for disabling or inhibiting any notification is also maintained or referred to in this log.
Display	What is seen on a visual display unit.
Distributed Control System (DCS)	A configurable microprocessor-based process control system.
Enforcement	A process by which the master alarm and priority data of the variable table is used to update the control system re-establishing the master alarm values and priorities in the control system, either manually or through the use of a tool.
Enforcer Log	The log produced during the process of enforcement, It includes alarm system deviations from the master alarm data of the variable table and the results of the enforcement.
Enable State	The state of a notification e.g., enabled, disabled or inhibited.
Equipment State Change	The change in equipment status, e.g., a change from on-line to off-line. A controller changing from auto to cascade.
Exceedance	When a process variable's value goes beyond a <u>limit</u> . That is when the variable's value goes above a high <u>limit</u> or goes below a low <u>limit</u> .
Exception Reporting Log	The log produced during the process of comparing the master variable table with the data in the alarm system when reporting deviations.

Term	Definition
Faceplate	A display pre-configured in the DCS that resembles the display and controls of the equivalent conventional panel instrument. It could be a controller faceplate (allowing SP output and controller mode changes), an indicator faceplate, a switch faceplate (status and output changes), etc.
Facility	The group of physical equipment that functions together, as a single unit, to perform a specific operation such as crude oil/gas production well, refining or chemical process, storage, transfer, (un)loading stations, treating or any other operations involved in the production, manufacturing and handling of crude oil, gas, oil products and/or chemicals, including but not limited to, process units (operating and idle), utilities, water and effluent treating units, tank farms and other storage, pipelines, pumping, compression, loading and unloading stations.
Facility Subject Matter Expert	A person with expertise of the facility sufficient for independent decision making on the effects of changes to the process variables on the safety, operability and reliability of the process and equipment. E.g. operations specialist, process specialist, production specialist, shift controller, but personnel in other functional departments may meet the above requirements as well.
Hazardous Situation	A situation with the potential to cause harm, including ill health and injury, damage to property, products or the environment, production losses or increased liabilities.
Human-Machine Interface (HMI)	All the areas where people interact with the system. In this DEP, it mostly refers to the DCS operator workstation but it may also refer to the engineering workstation.
Idle Process Unit	Process units which are not in operation (processing feed stocks or producing products) but contain hazardous products, such as hydrocarbons, catalysts, lubricants, and similar materials posing a hazard or present a source of stored energy, such as flammable liquids and gases, pressure from fuel gas, nitrogen or inert gas blanketing, stored liquids, or having an open (not spaded or blinded) connection to an operating process unit.
Inhibited Notification	A notification whose function has been disabled and removed from the visibility of the operators and whose activation is not captured in the notification history.
Initial Setup (ISU)	The process by which <u>constraints</u> , <u>limits</u> , <u>settings</u> , consequences of deviation in the event a <u>limit</u> is exceeded, recommended steps to take to correct the deviation, and other information are collected for entry into the Master Alarm Database (variable table).
Instrumented Protective Function (IPF)	A function comprising one or more sensors, a Logic Solver function and one or more Final Elements, for the purpose of preventing or mitigating Hazardous Situations.
Instrumented Protective System (IPS)	The electromechanical, electronic and/or programmable electronic Logic Solver component of the Instrumented Protective Function, complete with input and output equipment.
Limit	The critical, standard or target <u>limit(s)</u> of a <u>variable</u> .

Term	Definition
Management of Change	A method of reviewing proposed changes and includes a review process by appropriate personnel and obtaining concurrence before the change is implemented. Examples of Management of Change methods include the Management of Change process or a site-specific change process.
Master Alarm Database	A database under Management of Change that contains all facility constraints, critical, standard and target limits, alarms, alerts, consequences of exceeding critical, standard and target limits, suggested operator responses and other related information.
Normal Operating State	The condition when a process is within all defined limits and behaving as expected.
Notification	Alarms and alerts, used to inform appropriate personnel of limit exceedances or the occurrence of events.
Notification System	See alarm system.
Operator Console	A group of equipment comprising VDU screens, keyboards, pointing devices and switches which are allocated to a defined part of the plant (e.g. "console for hydrogen units").
Operator Response Time	Time taken by the operator to diagnose and take mitigating or corrective actions following notification.
Points And Tags	The instrument, numeric, timer, flag, Boolean, or logical entities within the DCS. Both words are used interchangeably, with "points" often being used to refer to calculated or inner variables of the DCS. "Tags" generally refer to data coming from wired or data inputs to the DCS.
Pre-Trip Alarm	An alarm that, if not responded to, may result in a demand on an IPF
Proactive	Acting in advance in a prescribed and planned manner.
Process Response Time	Time from completion of operator action to reversal of process direction.
Process Safety Time	Period of time in which the process can be operated without protection and with a demand present without entering a dangerous condition. The Process Safety Time determines the dynamic response requirements of an IPF.
Process Unit	See facility.
Risk Based Inspection (RBI)	The risk based development of inspection requirements for prioritising and managing inspection programs for new or existing Facilities based upon the identification of expected degradation mechanisms and a quantitative/qualitative analysis of failure probabilities, consequences and likelihood of detection.
Safety Critical Alarm (SCA)	Alarm defined as part of a process safety review that falls into RAM Red and Yellow 5A and 5B categories. Having "critical" in the term does not mean that it will require a Critical alarm.
Setting	The value as set in the device (e.g., a switch) to generate the <u>notification</u> at the desired <u>limit</u> .

Term	Definition
Shelving	Shelving describes a practice/ability provided to the operator to temporarily remove an alarm from the system in order to keep nuisance alarms from interfering with the overall effectiveness of the alarm system. Examples might be shelving an alarm during maintenance on the alarm or when the alarm triggering device is in override from operations.
Situational Awareness	Knowing the current conditions and activities occurring in and around the facility with respect to the process, equipment and other activities.
Standard Limit	The <u>limit</u> , when exceeded for longer than the <u>allowable time in exceedance</u> , where sustained or recurring short-term operations will begin to cause cumulative degradation of equipment integrity or reliability, or other cumulative effects that could lead to any of the consequences as listed in Table 2.
Standard Limit Exceedance	The exceedance of a <u>standard limit</u> for longer than the <u>allowable time in exceedance</u> .
Standing Alarm	An alarm that is in the alarm state for a long time (in excess of the <u>allowable time in exceedance</u> for standard alarms or more than 12 hours for critical alarms). An alarm may be standing during maintenance, when it is spurious, i.e., not representing a genuine hazardous situation, or when the hazardous situation actually exists but has not been dealt with.
State-based (Mode Dependent) Alarming	The technique that automatically or manually triggers the alteration of the <u>setting(s)</u> for one or more notifications where the constraints and normal operating values differ for various states (modes) of operation so that no setting can be found that satisfies all operating states. State-based (mode dependent) alarming requires either manual or automatic state detection that triggers the setting alteration.
Suppression-Static	<u>Operator-initiated suppression</u> of specific <u>notifications</u> that are associated with a facility or piece of equipment that is out of service. The out of service status of the unit/equipment makes associated <u>notifications</u> redundant if no hazardous situation could possibly arise from the <u>limit</u> being exceeded.
Suppression-Dynamic	Automatic suppression of specific <u>notifications</u> resulting from an event (such as a facility trip) for a defined period of time if the operating circumstances following the event make it impossible for a hazardous situation to arise from the associated <u>limits</u> being exceeded. Dynamic suppression does not change alarm parameter settings; it only suppresses the notification.
System Access	The way into the various parts of the alarm system.
System Security	Safeguards within the monitoring and control systems to prevent the occurrence of conditions which might compromise the integrity of the system.
Target	A value at which the variable is controlled to optimise performance. See also <u>alert</u> .
Target Limit	The limits of the range that business and operating targets may be set within, due to reliability, stability or operability constraints.
Time In Exceedance	See Allowable Time in Exceedance

Term	Definition
Top Event	The undesired effect that results from one or more failure scenarios. Each scenario consists of an initiating event and one or more preventive protection layers that are designed and maintained to prevent the top event.
Variable	Property or condition which may be measured (instrumented or not). A variable may also be calculated from measured variables.
Variable Table	See Master Alarm Database. This is an alternative name.
Variable Table Owner	The person who is responsible for maintaining the information in the variable table.
Workstation	User's workplace with an HMI within the control room. A console typically consists of several workstations.

1.3.3 Abbreviations

Term	Definition
ALARP	As Low As Reasonably Practicable
BPCS	Basic Process Control System
DCF	Diagnostic Coverage Factor
DCS	Distributed control system
DEP	Design and Engineering Practice
DP	Differential pressure
EEMUA	Engineering Equipment and Materials Users' Association
ESD	Emergency shutdown
F&G	Fire and Gas
FAT	Factory Acceptance Test
HAZOP	Hazards and Operability study
HEMP	Hazards and Effects Management Process
HMI	Human–Machine Interface
HSE	Health, Safety and Environmental
IPF	Instrumented Protective Function
IPS	Instrumented Protective System
ISA	International Society of Automation
ISU	Initial Setup
KPI	Key Performance Indicator
LOPA	Layer of Protection Analysis
MOC	Management of Change
MOS	Maintenance Override Switch (bypass switch)
MVC	Measurement Validation and Comparison
OOS	Operational Override Switch
P&ID	Process and Instrumentation Diagram (see PEFS)
PEFS	Process Engineering Flow Scheme (see P&ID)

Term	Definition
PFD	Probability of Failure on Demand
PHA	Process Hazards Analysis
PLC	Programmable Logic Controller
PRV	Pressure Relief Valve
PV	Process Variable
RAM	Risk Assessment Matrix
RBI	Risk-Based Inspection
RCM	Reliability-Centered Maintenance
SCA	Safety Critical Alarm
SCADA	Supervisory Control and Data Acquisition
SIL	Safety integrity level
SIS	Safety Instrumented System, the collection of IPFs that together protects a facility, unit or equipment.
SME	Subject Matter Expert
S-RCM	Shell Reliability Centered Maintenance

1.4 CROSS-REFERENCES

Where cross-references to other parts of this DEP are made, the referenced section or clause number is shown in brackets (). Other documents referenced by this DEP are listed in (7).

1.5 SUMMARY OF MAIN CHANGES

This DEP is a full revision of the DEP of the same number dated February 2011. The following are the main, non-editorial changes.

Section/Clause	Change
1.3.2	Added definitions and discussion about Alarm Operations versus Alarm Management tools. Also deleted some unneeded definitions.
many	Changed mode and mode dependent to state and state-based to better match ISA 18.2 terminology
many	Moved some text from Spec to Informative where not needed by a contractor
2.7, 6.2	Added some discussion on alarm shelving
3.2, others	Changed Alarm Requirement Specification to Alarm System Requirements Specification to better match terminology being used in ISA 18.2 and company alarm practices
3.6	Added some requirements related to Commissioning and Start-up of the alarm system
5.12	New section for facility alarms. Renumbered lower sections
5.4.2	Change to alarming strategy for transmitters in a 2oo3 scheme
5.6	Added differentiation of system and process diagnostics
5.15	Changed section covering alarm system design for Maintenance. Previous version did not clearly explain anything.

Section/Clause	Change
5.17	Added to section on alarm management tools
6.6	New section for Alarm Suppression in Batch Operations
Appendix I	Added new steps to reference notifications that have been identified in external processes (e.g., IPF) prior to ESP alarm rationalization

1.6 COMMENTS ON THIS DEP

Comments on this DEP may be submitted to the Administrator using one of the following options:

Shell DEPs Online (Users with access to Shell DEPs Online)	Enter the Shell DEPs Online system at https://www.shelldeps.com Select a DEP and then go to the details screen for that DEP. Click on the "Give feedback" link, fill in the online form and submit.
DEP Feedback System (Users with access to Shell Wide Web)	Enter comments directly in the DEP Feedback System which is accessible from the Technical Standards Portal http://www.shell.com/standards . Select "Submit DEP Feedback", fill in the online form and submit.
DEP Standard Form (Other users)	Use DEP Standard Form 00.00.05.80-Gen. to record feedback and email the form to the Administrator at standards@shell.com .

Feedback that has been registered in the DEP Feedback System by using one of the above options will be reviewed by the DEP Custodian for potential improvements to the DEP.

1.7 DUAL UNITS

This DEP contains both the International System (SI) units, as well as the corresponding US Customary (USC) units, which are given following the SI units in brackets. When agreed by the Principal, the indicated USC values/units may be used.

1.8 NON NORMATIVE TEXT (COMMENTARY)

Text shown in italic style in this DEP indicates text that is non-normative and is provided as explanation or background information only.

Non-normative text is normally indented slightly to the right of the relevant DEP clause.

2. ALARM SYSTEM PHILOSOPHY

2.1 GENERAL

1. This section specifies the Principal's requirements for managing alarms. Understanding of these requirements is essential to correctly apply this DEP.

2.2 ALARMS AND ALERTS - BACKGROUND

1. Alarms are used to annunciate Critical and Standard limit exceedances or high priority events (digital tags) requiring action. Alarms can be included in HSE barrier counting to manage risk to ALARP (As Low As Reasonably Practicable) if the following are true:
 - the alarm sensors are independent of the IPF and other barriers
 - there are effective action(s) that operator can perform
 - there is enough time for operator to respond
 - they are auditable
2. Alerts are used to notify operators and/or Operations support personnel of target limit exceedances or low priority event messages. Events (e.g., system diagnostics) which are classified as Standard or Critical would still require an alarm.
3. Alarms and Alerts are collectively called notifications. They are designed for each operating location based on the business type, the Hazards and Effects particular to the process, the operating philosophy (e.g., continuously manned, partially manned or unmanned), the automation systems deployed (e.g., DCS or SCADA), and the associated alarm philosophy.

2.3 OPERATING CONSTRAINTS, LIMITS, SETTINGS, AND NOTIFICATIONS

1. Before defining any notifications (i.e., alarms and alerts), it is necessary to determine the limits upon which these will be based. This DEP adopts a simple, straightforward work process to define operating limits with a strict nomenclature to achieve a standard approach to Alarm Management.

a. Constraint

An identified restriction on the equipment, materials of construction, or operating point, such as design pressure or design temperature of a vessel, a relief valve setting, an IPF setting, etc., which limit or restrict the operation of the equipment or process. There are usually several constraints. A constraint shall have a limit associated with it unless it can be proven that there is no limit within the ability of equipment operation (i.e., a constraint has a limit of 900 °C, but the heating equipment and reaction of process can only raise the temperature to 700 °C).

b. Limits

The critical, standard or target limit of a variable (pressure, temperature, pH, etc.) associated with an instrument, equipment, facility or site. If the variable exceeds the limit a notification is generated. A limit is expressed in the same engineering units as the process variable.

c. Settings

The limit is used to calculate the setting of a device that generates the notification. The setting may be in the engineering units of the device (e.g., mA) or in the engineering unit of the process variable (e.g., the alarm setting of a variable in the DCS).

d. Notifications

Alarms and alerts used to inform appropriate personnel of an exceedance of limits or the occurrence of events. Notifications can be:

- i. An Alarm
 - A critical Alarm when a critical limit is exceeded (or critical event has been detected) or,
 - A standard Alarm when a standard limit is exceeded (or standard event has been detected).
 - ii. An Alert
 - A target alarm when a target limit is exceeded (or target event has been detected) or,
 - An event message (e.g., the auto start of a standby pump).
2. Critical and standard limits and any associated alarm attributes (e.g., priorities, actions, etc.) shall be modified under a Management of Change process. Target limits and event messages can be changed without using MOC as long as standard processes exist.
3. In the case of a discrete notification of an abnormal situation (e.g., the running pump changed from running to stopped, valve failed to trip), there shall be an identified state rather than a setting in engineering units that is defined for a variable limit.

2.4 OPERATING LIMIT DEFINITION

1. The following limits shall be defined within the engineering constraints of the equipment:

Critical limit	Immediate action required to prevent severe short-term consequences
Standard limit	Action required as quickly as possible to mitigate slow, cumulative degradation
Target limits	related to optimisation

2. It is imperative that all limits and constraints are identified for valid operating conditions such as start-up, shutdown and normal operations.
3. Limits may be from mechanical, process, utility, quality, performance optimization or operational constraints. This requires a multidisciplinary approach.
4. A standard limit usually comes with a critical limit unless it can be demonstrated that there is no critical limit that can be exceeded.
5. Many critical limits, however, do not have associated standard limits.

2.5 MANAGING ALARM RATES

1. Excessive alarm rates result in a loss of situational awareness due to operator cognitive overload. In normal operation, the alarm rates are managed by eliminating notifications that do not have an assigned action or important awareness function (i.e., should not have been alarms in the first place), and through proactive monitoring and control activities that keep the process within the safe, stable and profitable region.
2. Alarm suppression techniques may be employed to reduce alarms from normal production events and also in upset conditions, to further reduce alarm rates and alarm floods.
3. To help manage alarm rates, only alarms from unexpected, abnormal situations shall be sent to the operator.
4. The rate at which a well-trained operator can handle this work process has been established as follows: