

DEP SPECIFICATION

PROCESS CONTROL DOMAIN - ENTERPRISE INDUSTRIAL AUTOMATION INFORMATION TECHNOLOGY AND SECURITY

DEP 32.01.20.12-Gen.

February 2012

DESIGN AND ENGINEERING PRACTICE



© 2012 Shell Group of companies
All rights reserved. No part of this publication 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.

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 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	4
1.1	SCOPE.....	4
1.2	DISTRIBUTION, INTENDED USE AND REGULATORY CONSIDERATIONS	5
1.3	DEFINITIONS	5
1.4	CROSS-REFERENCES	7
1.5	COMMENTS ON THIS DEP	7
2.	SECURITY FRAMEWORK.....	8
2.1	PRINCIPLES.....	8
2.2	REQUIREMENTS	8
2.3	COMPETENCY AND TRAINING	9
3.	PCD PROJECT EXECUTION	10
4.	PROCEDURES.....	12
4.1	GENERAL	12
4.2	INCIDENT AND EVENT MANAGEMENT	12
4.3	CHANGE MANAGEMENT	12
4.4	USER AND SYSTEM ACCESS.....	13
4.5	BACK-UP AND RESTORE	14
4.6	GENERAL REQUIREMENTS.....	14
5.	ASSURANCE AND RISK BASED CONTROLS.....	15
5.1	ASSURANCE.....	15
5.2	RISK CONTROLS.....	15
6.	SYSTEM SECURITY AND TECHNICAL CONTROLS.....	16
6.1	OPERATING SYSTEM REQUIREMENTS	16
6.2	CRITICALITY ASSESSMENT	16
6.3	PATCH MANAGEMENT	16
6.4	VIRUS MANAGEMENT	17
6.5	SAFETY SYSTEM INTERCONNECTION	17
6.6	EXPLICIT ACCESS	17
6.7	AUTHENTICATION AND AUTHORIZATION	18
6.8	SECURITY ADMINISTRATION	18
6.9	CONFIGURATION MANAGEMENT	19
7.	PCD TECHNICAL ARCHITECTURE	20
7.1	APPLICATION ARCHITECTURE	20
7.2	PHYSICAL ARCHITECTURE	21
7.3	TECHNICAL REQUIREMENTS.....	22
8	LIFECYCLE MANAGEMENT	23
9.	REFERENCES	24

APPENDICES

APPENDIX 1	SHELL PCD TECHNICAL REFERENCE MODEL	25
APPENDIX 2	SHELL PCD LEVEL REFERENCE MODEL	26
APPENDIX 3	SKILLS, RESOURCES, COMPETENCY AND TRAINING DETAILS.....	27

1. INTRODUCTION

1.1 SCOPE

This new DEP specifies requirements and gives recommendations for Process Control Domain (PCD) security of control and automation systems.

This DEP is applicable to all disciplines having systems installed in the PCD. The DEP contains requirements for the entire PCD lifecycle from design to final equipment turnover to the Operating Site.

This DEP is closely related to DEP 32.01.23.17-Gen. and DEP 32.80.10.10-Gen. and shall always be read in conjunction with these two DEPs. Both DEPs are included in DEM1.

The following series of DACA DEPs have been withdrawn and are now superseded by this DEP:

32.01.20.10-Gen.	Data acquisition and control architecture (DACA)
32.01.21.10-Gen.	Data acquisition & control architecture (DACA) – Roles and responsibilities
32.01.22.10-Gen.	Data acquisition & control architecture (DACA) - Procedural controls - Configuration management
32.01.22.11-Gen.	Data acquisition & control architecture (DACA) - Procedural controls - Backup and restore
32.01.22.12-Gen.	Data acquisition & control architecture (DACA) - Procedural controls - Incident management
32.01.22.13-Gen.	Data acquisition & control architecture (DACA) - Procedural controls - Disconnection procedure
32.01.23.10-Gen.	Data acquisition & control architecture (DACA) - Technical controls - Security administration
32.01.23.11-Gen.	Data acquisition & control architecture (DACA) - Technical controls - Infrastructure architecture
32.01.23.12-Gen.	Data acquisition & control architecture (DACA) - Technical controls - Remote user access
32.01.23.13-Gen.	Data acquisition & control architecture (DACA) - Technical controls - Wireless security
32.01.23.14-Gen.	Data acquisition & control architecture (DACA) - Technical controls - Minimal access
32.01.23.15-Gen.	Data acquisition & control architecture (DACA) - Technical controls - Authentication and authorisation
32.01.23.18-Gen.	Data acquisition & control architecture (DACA) - Technical controls - PCD network drawings
32.01.23.19-Gen.	Data acquisition & control architecture (DACA) - Technical controls - Architectural requirements for applications utilising production data
32.01.25.10-Gen.	Data acquisition and control architecture (DACA) - System security - Virus management
32.01.25.11-Gen.	Data acquisition & control architecture (DACA) - System security - Patch management
32.01.26.11-Gen.	Data acquisition & control architecture (DACA) - Assurance - Risk assessment

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 authorisation 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 **shall** indicates a requirement.

The word **should** indicates a recommendation.

1.3.2 Specific definitions

Term	Definition
Deviation	An authorised variance or exemption from the site identified Process Control Domain Security requirement, authorised by the site or asset accountable.
Instrumented Protective Function	A function comprising one or more sensors, a Logic Solver and one or more Final Elements whose purpose is to prevent or mitigate hazardous situations and that have SIL 1, SIL 2, SIL 3 or SIL 4. An IPF is intended to achieve or maintain a safe state for the process, in respect of a specific hazardous event. In IEC 61508 and IEC 61511, an IPF is referred to as a Safety Instrumented Function (SIF).
Instrumented Protective System	The electromechanical, electronic and/or programmable electronic Logic Solver component of the Instrumented Protective Function, complete with input and output equipment. In IEC 61508 and IEC 61511 an IPS is referred to as a 'Logic Solver'.
IPSec	IPsec is a protocol used for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet being communicated.

Term	Definition
IT Security	In this DEP, IT security is equivalent to process control system cyber security, and process control system cyber security controls.
LIS	A LIS is a Logical Isolated Segment, a secure sub-domain (cell) protected by a firewall (L2/L3 Firewall).
Network Device	Electronic equipment that connects or manages network traffic; e.g., switches, routers, and firewalls.
PCD Security Compatible	When a Manufacturer/Supplier's solution complies with the requirements in this DEP, the solution is considered by the Principal to be <i>PCD Security Compatible</i> .
Process Control Access Domain (PCAD)	The Process Control Access Domain is independent from the PCD and separates the PCD from other domains. It contains all devices and applications that are required to provide controlled, secure and reliable user-to-system and system-to-system connectivity between systems within the PCD and other domains.
Process Control Domain (PCD)	The PCD directly monitors, controls, and provides safeguarding of production and manufacturing facilities. The PCD consists of Levels 1, 2, 3 as per (Appendix 1, 2) and the hosting DMZ of the PCAD (also called Level 3.5). Examples of systems in the PCD are: Distributed Control Systems (DCS), Supervisory Control and Data Acquisition (SCADA), Programmable Logic Controllers (PLC), Instrumented Protected Systems (IPS), fire and gas detection systems, fiscal flow metering systems, Electrical Network Management Control Systems (ENMCS), Human Machine Interfaces, Human Machine Interfaces in CCRs, and data historians.
Process Control Network (PCN)	The PCN is the network infrastructure (i.e., cables, fibre, switches, firewalls, and routers) that is used to connect all of the Level 3 PCD systems.
Process Safety	The management of hazards that can give rise to major accidents involving, personnel safety, the release of potentially dangerous materials, and release of energy (such as fire or explosion) or both.
Project	Any minor or major system or network modification activity or Greenfield project that includes (network connected) systems to be installed
Recovery Point Objective (RPO)	The recovery point objective is the point in time to which the system must recover data after a system failure. It defines what the site determines as an "acceptable loss" of data in a disaster situation.
Remote User Access	The words 'remote user access' in this document are considered to be a user coming from a Level 4 or Level 5 network that has user access to the PCD via the PCAD.
System	A combination of hardware and software components, which together provides a function or service.
Third party	Anybody accessing the Shell network from outside the Shell network e.g. the internet not using Mobile Office Private or Business (MOP/MOB)
Two-Factor Authentication	Two-factor authentication is the term used to describe any authentication mechanism where more than one item is required to authenticate a user. The components of two-factor authentication can be something you know (e.g., a username and/or password) and something you have (e.g., a smart card).

1.3.3 Specific abbreviations

Term	Definition
ALARP	As Low As Reasonably Practical
CCR	Centralised Control Room
CS-IT	Control Systems Information Technologist – reports to the site/asset EM/OM/TM.
CS-E	Control Systems Engineer
DCS	Distributed Control System
DH	Data Historian
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
EM	Engineering Manager
FAT	Factory Acceptance Test
GPS	Global Positioning System
IPF	Instrumented Protective Function
IPS	Instrumented Protective System
IRM	Information Risk Management
NTP	Network Time Protocol
OD	Office Domain
OM	Operations Manager
PACO	Process Automation, Control, and Optimization
PCAD	Process Control Access Domain
PCD	Process Control Domain
RMP	Run and Maintain Practice
SAT	Site Acceptance Test
SCADA	Supervisory Control and Data Acquisition
SME	Subject Matter Expert
TE	Technical Expert
TM	Technology Manager
TPA	Third Party Access (for Global Infrastructure of the Principal)

1.4 CROSS-REFERENCES

Where cross-references to other parts of this DEP are made, the referenced section number is shown in brackets (). Other documents referenced by this DEP are listed in (9).

1.5 COMMENTS ON THIS DEP

Comments on this DEP may be sent to the Administrator at standards@shell.com, using the DEP Feedback Form. The DEP Feedback Form can be found on the main page of “DEPs on the Web”, available through the Global Technical Standards web portal <http://www.shell.com/standards> and on the main page of the DEPs DVD-ROM.

2. SECURITY FRAMEWORK

2.1 PRINCIPLES

- a) The information security of the PCD is complementary to the information security requirements of the Principal (in Shell, as defined for the Shell Group).
- b) The requirements outlined in this DEP shall be consistent with internationally recognized information security standards for PCD as published under IEC 62443 (all published sections).
- c) Compliance with applicable country laws and regulations shall be required. Country laws and regulatory requirements that conflict with or are more stringent than the requirements established in this DEP shall be followed.
- d) The requirements in this DEP cannot interfere with operations ability to safely monitor and control the facility.

2.2 REQUIREMENTS

- a) For each PCD, a security framework shall be created or adopted by the project. The security framework shall be compatible with any existing framework(s) used by the site and developed in consultation with the site CS-IT.

NOTE: Each project shall implement and maintain the security framework during the execute phase in preparation for equipment turnover to Operations. Starting with the FAT and continuing with the SAT, system commissioning periods, and other activities prior to turnover to Shell, the system security framework shall be maintained as equivalent to in the care and custody of Shell. This approach allows for smooth transition from Projects to Operations. Refer to (3) for additional details.

Each project shall implement and maintain the security framework during the execute phase in preparation for equipment turnover to Operations. Starting with the FAT and continuing with the SAT, system commissioning periods, and other activities prior to turnover to Shell, the system security framework shall be maintained as equivalent to in the care and custody of Shell. This approach allows for smooth transition from Projects to Operations.

This framework shall be based on the most recent PCD security standard of the Principal (Shell Group).

As a minimum the framework shall consist of:

- i. PCD security policy
 - ii. PCD security assurance methodology and plan
 - iii. PCD security risk based management dashboard to be updated during project and operations phase at least quarterly
 - iv. Formalized PCD security deviations against this DEP
 - v. Competency development and sustainability plan
 - vi. System and applications obsolescence plan
 - vii. Definition of PCD ownership and responsibilities
- b) PCD security roles and responsibilities shall be assigned, and as a minimum comply with the responsibilities as listed in various chapters of this DEP.

As a minimum the following roles and associated responsibilities shall be defined and assigned:

- i. Accountable OM, TM or EM

The Principal shall engage Site Operations to ensure that each site assigns accountability for defining PCD security roles and responsibilities to the Operations Manager (OM), Technology Manager (TM) or Engineering Manager (EM).

- ii. PCD Security focal point at TA/3 level (in Shell)
- iii. PCD Control Systems Information Technology professional (CS-IT), responsible for the integrity, availability and security of the PCD.

NOTE: The PCD Admin role, present at some sites, is being combined into the CS-IT role.

- iv. PCD Control Systems Engineer (CS-E), responsible for integrity, availability and security of a specific control system.

The Operations personnel shall then be engaged by the Principal in the delivery of the security framework during the project activities as defined above. This DEP

- c) All PCD related disciplines such as PACO, Electrical, Rotating shall be included in the definition of security roles and responsibilities.

NOTE: Any discipline that has equipment installed in the PCD can be considered as a PCD related discipline.

- d) The security framework shall be signed off by the site General Manager or Asset Manager.
- e) The assigned PCD security management team member (OM, TM or EM) shall be held accountable for ensuring that site security experts have adequate time to perform their duties.
- f) The security framework shall include a process that address future emerging threat developments and the need to modify the security framework to address these threats within time limits (as determined by the CS-IT) appropriate for the risk associated with the threat.

NOTE: It is difficult to predict future threats that may arise. However, the process requires the flexibility to respond to any threats as they arise in a timely manner – regardless of the requirements presently stated in this DEP.

- g) It is the site CS-IT's responsibility to sustain an "ALARP" level of security relative to current security threats.
- h) Segregation of duties shall exist between those who initiate, approve and implement changes.
- i) The controls employed by sites to comply with the security requirements stated in this DEP shall not inhibit the site's ability to control the assets within the PCD.
- j) Evidence shall be collected and retained of all security incidents. However, where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be presented to conform to the rules for evidence laid down in the relevant local jurisdictions.

NOTE: A framework shall be prepared for each site or asset. However sites and assets shall customize it to local needs and circumstances. This DEP describes the most obvious framework elements but does not dictate the content. Content shall be based on identified risks and local situation.

2.3 COMPETENCY AND TRAINING

Projects shall engage the PCD security SME to identify and develop security competency profiles and design competency development (Appendix 3) and any required training plans. Engagement shall include both project and handover to operations phase.