

DEP SPECIFICATION

PROCESS CONTROL DOMAIN - SECURITY REQUIREMENTS FOR SUPPLIERS

DEP 32.01.23.17-Gen.

February 2011

DESIGN AND ENGINEERING PRACTICE

DEM1



© 2011 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 recommended 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	4
1.1	SCOPE.....	4
1.2	DISTRIBUTION, INTENDED USE AND REGULATORY CONSIDERATIONS	4
1.3	DEFINITIONS	4
1.4	CROSS-REFERENCES	6
1.5	SUMMARY OF MAIN CHANGES.....	6
1.6	COMMENTS ON THIS DEP	6
2.	GENERAL SECURITY POLICY	7
2.1	DEMONSTRATING COMPATIBILITY VIA INDEPENDENT CERTIFICATION	7
2.2	SECURITY APPLICATION	7
3.	PROCESS CONTROL SECURITY FOCAL POINT	8
4.	CONTROLS AGAINST MALICIOUS CODE	9
5.	SOFTWARE PATCH MANAGEMENT	10
6.	SYSTEM HARDENING	11
7.	PROTECTION OF PCD DOCUMENTATION	12
8.	ACCOUNT MANAGEMENT	13
9.	BACKUP, RESTORE AND DISASTER RECOVERY	15
10.	REMOTE ACCESS AND TRANSFER OF DATA FILES	16
11.	WIRELESS CONNECTIVITY	17
12.	SECURE CONNECTIONS TO INSTRUMENTED PROTECTIVE SYSTEMS	19
13.	STANDARDS AND CERTIFICATION	20
14.	SECURITY MONITORING	21
15.	PROCESS CONTROL DOMAIN NETWORK ARCHITECTURE	22
16.	HANDLING OF REMOTE AND ADVISORY SETPOINTS	23
17.	DATA HISTORIANS	24
18.	COMMISSIONING AND MAINTENANCE	25
19.	REFERENCES	26

APPENDICES

APPENDIX 1	ARCHITECTURE LEVELS IN ISA-99.00.01, PART 1	27
APPENDIX 2	DATA ACQUISITION AND CONTROL ARCHITECTURE	28

1. INTRODUCTION

1.1 SCOPE

This DEP specifies requirements for PCD IT security of control & automation systems to be supplied for use in Shell-owned Process Control Domains (PCDs), and is applicable to suppliers supplying such systems or services on such systems.

This DEP covers both:

- Policy; addressing the Supplier's organization, IT security processes, technological solutions and governance of IT security
- Commissioning and maintenance of PCD systems

Supplementing this DEP, a suite of PCD Security (DACA) Design and Engineering Practice (DEP) specifications and guidelines provide guidance on how to produce a PCD Security Compatible solution.

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 March 2010; 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 should 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 capitalised term **SHALL [PS]** indicates a process safety requirement.

The word **should** indicates a recommendation.

1.3.2 Specific definitions

term	definition
PCD Security Compatible	When a Supplier's solution complies with the requirements in this DEP, the solution is considered by Shell to be <i>PCD Security Compatible</i> .
Network device	Electronic equipment that connects or manages network traffic; e.g. switches, routers and firewalls.
Compatible Supplier	A supplier is compatible with the Principal's security policy and standards when the supplier is compliant with this DEP. The Supplier cannot be compliant with the Principal's policy and security standards because part of it should be accomplished by the Principal
system	a combination of hardware and software components, which together provides a function or service. Where ' its systems ' is used in this DEP, this refers to all systems supplied and supported by the Supplier over the systems lifecycle.
Derogation	an authorised variance or exemption from a Process Safety requirement, with specified conditions.
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.
IT security	The equivalent to Process Control System Cyber Security, and Process Control System Cyber Security Controls.

1.3.2 Specific definitions

Term	Definition
ACL	Access Control List
APC	Achilles Practice Certification
AES	Advanced Encryption Standard
AV	Anti-Virus (Appendix 2)
CCR	Centralised Control Room (Appendix 2)
DACA	Data Acquisition and Control Architecture (Appendix 2)
DCS	Distributed Control System
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
EWS	Engineering Work Station
HIDS	Host-based Intrusion Detection System
HMI	Human to Machine Interface
ICMP	Internet Control Message Protocol
IPF	Instrumented Protective Function; All instruments and systems required to safeguard the process, including the hook-up of the instruments (initiators and end-elements) and wetted parts of the system.
IPS	Instrumented Protective System; equivalent to Safety Instrumented System (SIS)
IT security	In this DEP, IT security is equivalent to process control system cyber security, and process control system cyber security controls
L1	Network Level 1 – Basic Process Control (Appendix 1)

Term	Definition
L2	Network Level 2 – Area Supervisory Control (Appendix 1)
L3	Network Level 3 – Site Manufacturing Operations (Appendix 1). Equivalent to the Process Control Network (PCN)
L4	Network Level 4 – Site Business Planning (Appendix 1). Equivalent to the Office Domain (OD)
L5	Network Level 5 – Enterprise (Appendix 1)
MIB	Management Information Base
OD	Office Domain
OPC	OLE for Process Control
PAS	Process Automation System
PCAD	Process Control Access Domain
PCD	Process Control Domain
PCN	Process Control Network. This is equivalent to Network Level 3(L3)
PLC	Programmable Logic Controller
RDP	Remote Desktop Protocol (used by Microsoft Terminal Services)
SIS	Safety Instrumented System; equivalent to Instrumented Protective System (IPS)
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
TCP/IP	Transmission Control Protocol/Internet Protocol
TPA	Third Party Access (for Shell Global Infrastructure)
WMI	Windows Management Instrumentation

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 (19).

1.5 SUMMARY OF MAIN CHANGES

This DEP is a revision of the DEP of the same number dated March 2010. The following are the main, non-editorial changes.

Old section	New section	Change
		The old document has been split into 2 new documents, i.e. DEP Standard and DEP informative. The DEP standard only contains the mandatory requirements.
		After the split the document was sent on global comment round and its agreed changes are included in this version

1.6 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://swwww.shell.com/standards> and on the main page of the DEPs DVD-ROM.

2. GENERAL SECURITY POLICY

2.1 DEMONSTRATING COMPATIBILITY VIA INDEPENDENT CERTIFICATION

Suppliers shall demonstrate PCD Security Compatibility to the Principal by achieving certification by independent parties that have been approved by the Principal. The requirements in this DEP are aligned with WIB Report M 2784 X10 version 2, October 2010 and Wurldtech's Achilles Practices Certification (APC) level silver.

2.2 SECURITY APPLICATION

- 2.2.1 The Supplier shall, within their own organization, practice and maintain policies, standards and procedures that are compliant with the requirements specified in this DEP.
- 2.2.2 The Supplier shall conduct security-related background checks on personnel before they are assigned to the Principal's projects; e.g. identity verification and criminal record check. The Supplier shall ensure, based upon the results of the security-related checks that personnel assigned to activities on the Principal's PCD will not pose a security risk.
- 2.2.3 The Supplier shall ensure that for each project a security lead with sufficient IT security competency is assigned to Principal's projects. The security lead shall instruct Supplier's assigned personnel about the content of this document, prior to being authorized access to the Principal's PCD.
- 2.2.4 Confidentiality agreements and user agreements to follow applicable standards and procedures shall be signed by all persons having access to the Principal's PCD.
- 2.2.5 Unless stated otherwise, the requirements in this DEP shall be applied independent of the type of operating system software (e.g. Microsoft Windows or Unix-like operating system) supplied by the Supplier.
- 2.2.6 The Supplier shall have a policy and procedures for security testing, approval and maintenance of their system, with all integrated third party software installed on the Supplier's system.

3. PROCESS CONTROL SECURITY FOCAL POINT

The Supplier shall nominate a Process Control Security Focal Point in its organization, who is responsible for the following:

- 3.1 Shall act as liaison with the Principal about compliance of the Supplier's system with this DEP.
- 3.2 Shall ensure that tenders to as required by the Principal are in compliance with this DEP and communicate requested deviations from this DEP
- 3.3 Shall provide the Principal with timely information about cyber security vulnerabilities in the supplier's supplied systems and services.
- 3.4 Shall provide timely support and advice to the Principal and SME in the event of cyber security incidents involving the Supplier's systems and services.
- 3.5 Shall provide information to the Principal SME on the Supplier's views and implementation on process control security.

4. CONTROLS AGAINST MALICIOUS CODE

The Supplier shall protect its system against malicious code without this protection affecting the system's normal functionality, as follows:

- 4.1. Each system in the PCD shall have virus detection software installed. Where the installation of antivirus software is not technically possible, a listing of all computers where antivirus software cannot be installed shall be maintained, and other mitigating factors shall be in place to reduce the risk of infection.
- 4.2. New technology to replace the need for virus detection software (e.g. White listing) shall only be allowed to be applied when Supplier has demonstrated to the Principal that the new solution is equal or better than the existing virus detection software. The Principal shall provide written approval that the new technology has demonstrated improvement in functionality, integrity, and availability of the Supplier's system before the new technology can be implemented.
- 4.3. The Supplier shall provide documentation describing how approval of virus definition files shall be communicated to the Principal.
- 4.4. The Supplier shall provide documentation describing how the approved virus definition files shall be installed on the system. New virus definition files shall be distributed to systems in the PCD via the PCAD.
- 4.5. The Supplier shall provide evidence that the configured equipment has been checked to be free of malicious code prior to shipment to the Principal.
- 4.6. The Supplier shall provide documented instructions for ensuring the proper installation, configuration and update of anti-virus software.
- 4.7. The Supplier's system shall support use of antivirus software that has been approved by Shell. However, alternative solutions, as recommended by the system Supplier, may be used with approval by the Principal.
- 4.8. The Supplier shall document a procedure for its staff stating that portable media (e.g. laptops and USB storage) used by the Supplier for commissioning and maintenance of equipment or devices in the PCD shall only be used for this purpose. The procedure shall also include instructions for ensuring that the portable media is free of malicious code.
- 4.9. The Supplier shall ensure use of correctly installed, configured and up-to-date anti-virus software during all phases of the project until successful handover and acceptance by the Principal. Virus definition files shall be 'released for installation' by the Supplier as soon as possible, within a maximum of 30 days after initial release.
- 4.10. The Supplier shall provide evidence, acceptable to the Principal, during the project acceptance testing that malicious code can be detected and correctly handled by the anti-virus software.