

DEP SPECIFICATION

**PROCESS CONTROL DOMAIN - ENTERPRISE
INDUSTRIAL AUTOMATION INFORMATION
TECHNOLOGY AND SECURITY**

DEP 32.01.20.12-Gen.

February 2017

ECCN EAR99

DESIGN AND ENGINEERING PRACTICE

DEM1



© 2017 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).

This document has been supplied under license by Shell to:
UOP Honeywell ted.fuger@honeywell.com 19/01/2018 08:49:45

AVA Documents
Document Sharing Hub

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	4
1.1	SCOPE	4
1.2	DISTRIBUTION, INTENDED USE AND REGULATORY CONSIDERATIONS	4
1.3	DEFINITIONS	5
1.4	CROSS-REFERENCES	12
1.5	SUMMARY OF MAIN CHANGES.....	12
1.6	COMMENTS ON THIS DEP	12
1.7	DUAL UNITS.....	13
1.8	NON NORMATIVE TEXT (COMMENTARY).....	13
1.9	CROSS REFERENCE TO IT CONTROL FRAMEWORK PCD RISK PROFILE	13
2.	SECURITY FRAMEWORK	14
2.1	GENERAL	14
2.2	GOVERNANCE	15
2.3	ASSET INVENTORY	16
2.4	ACCESS CONTROL.....	17
2.5	PORTABLE MEDIA AND COMPUTERS.....	22
2.6	OPERATING SYSTEM SECURITY PATCHES	23
2.7	EVENT LOG MANAGEMENT	24
2.8	ANTI-VIRUS.....	25
2.9	NETWORK ARCHITECTURE	26
2.10	INCIDENT RESPONSE	29
2.11	BACKUP AND RESTORE	29
	REFERENCES	31

APPENDICES

APPENDIX A	SHELL PCD SECURITY ZONE MODEL	32
APPENDIX B	REFERENCE MODEL FOR ISA99 STANDARDS	33
APPENDIX C	SHELL GROUP RISK ASSESSMENT MATRIX (RAM)	34

1. INTRODUCTION

1.1 SCOPE

This 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 project lifecycle from design to final equipment turnover to the Operating Site.

Efforts have been made with various stakeholders in Shell (IRM, TaCIT, PACO) to ensure alignment between this DEP and the IT Control Framework PCD Risk Profile used to measure operations. As this DEP describes PCD IT Security practices that is supposed to deliver a result that is compliant to security requirements in run and maintain with no or minimal regret cost, the requirements in the IT Control Framework PCD Risk Profile have been included in this DEP; see (1.4).

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

The following DEP has been withdrawn (as of February 2015) and is superseded by this DEP:

DEP 32.01.23.17-Gen.	Process Control Domain – Security Requirements for Suppliers
----------------------	---

This is a revision of the DEP of the same number dated February 2015; 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 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 capitalised term **SHALL [PS]** indicates a process safety requirement.

The word **should** indicates a recommendation.

The word **may** indicates a permitted option.

1.3.2 Specific definitions

Term	Definition
Custodian	Person responsible for a PCD IT Component. <i>The purpose of having a custodian assigned to a name is to be able to seek information or inform this person in case of a security incident or potential threat that affects the PCD IT Component.</i>
Exposure Level	Exposure level defines the potential for a PCD IT Component to be affected by threats associated with the transfer of data from a foreign domain, either via network or portable media. The potential is affected by both the likelihood and the impact of a threat. The following exposure levels are defined: Low All PCD IT Components not classified as High or Medium. Medium At a minimum, this includes systems designed to use portable media and/or network file transfer from/to external networks (non-PCD) during their normal course of operation. High At a minimum, this includes all applicable PCD IT Components that are part of the IPF or a Fire & Gas Detection System, or capable of changing operating parameters of an IPF or Fire & Gas Detection System.
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. In IEC 61511-1, an IPF is referred to as a Safety Instrumented Function (SIF). <i>An IPF is intended to achieve or maintain a safe state for the process, in respect of a specific hazardous event.</i>

Term	Definition
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 61511-1, an IPS is referred to as a 'safety instrumented system'. Synonymous with SSDS and SIS.
Internal Remote Access	Any network connection INITIATED from a PCD IT Component and terminated on another PCD IT Component within the SAME PCD. A remote desktop protocol (RDP) connection from a workstation on Level 3 within the PCD to a terminal server on Level 2 within the same PCD is an example of an internal user-to-system connection.
IT Component	See PCD IT Component. Unless specifically mentioned, all IT components referred to in this document are considered part of the process control domain.
IT Security	In this DEP, IT security is equivalent to process control system cyber security, and process control system cyber security controls.
Main Automation Contractor	Responsible for the delivery, physical and functional integration of various control and automation systems in the PCD. <i>MAC Vendors use specially developed standards and guidelines (approved by Shell), whereby a known quality can be realised. This MAC-Vendor standards package is called The MAC Toolkit. The MAC-Vendor will keep the MAC Toolkit up to date and will ask approval to Shell to make changes to the kit.</i>
MAC toolkit	The MAC toolkit is a set of templates and guidance documents (including reference architectures) for implementing MAC supplied solutions in the Shell environment. The MAC toolkits are available from the respective MAC Vendor.
Mobile Office Business	Virtual Private Network connection for remotely connected GI Desktops into the Shell network.
Mobile Office Private	Server Based Computing facility providing Shell contractors and staff access to Shell Office Domain applications such as mail and intranet access.
Network Device	Electronic equipment that connects or manages network traffic; e.g., switches, routers, and firewalls.
Network Security Barrier	A network device that implements access controls and/or network security policy between two or more network security zones.
Operating System	For the purpose of this DEP, Operating System refers to general purpose computer operating systems such as Microsoft™ Windows® or Unix variants. This does not include embedded operating systems running on appliance type devices such as routers, switches and firewalls.

Term	Definition
PCD IT Security Accountable Manager	This role is responsible for ensuring the project has qualified resources assigned to the project from PACO, TaCIT, and IT/IM to fulfil roles required by this DEP and is accountable for ensuring the project is compliant with this DEP.
PCD IT Security Incident	Any event that disrupts the expected standard operation of any PCD service, facility or component and causes disruption of, or denial of operation, or inappropriate access to or use of data or systems. An incident can also be caused by system failure or human error.
PCD IT Security Project Focal Point	This role is assigned directly to the project for the duration of the project and is responsible for the creation of all PCD IT Security related deliverables. On a small project, this could be a single resource. On a large project, this could be a team leader with one or more team members. Different terms might be used to describe this role, like CS-IT for example in Upstream.
PCD IT Support	This role, assigned by the run and maintain organization, will liaise between the project and the run and maintain organization that will operate the facility upon handover.
PCD Incident Owner	This role will ensure a documented process is followed to manage all reported PCD IT Security related incidents. Example: the project may leverage an existing run and maintain organization process or document a project specific process.
Policy	Principles, rules and guidelines formulated in writing to achieve long-term (PCD IT Security) goals, endorsed by an accountable person and available to those that are affected by the scope of the document. Preferably, the policy links the specifics for the organization in scope (e.g. project) to the overarching (Shell) standards and business principles.
Project Delivery Framework (PDF)	The Project Delivery Framework (PDF) is a framework that defines standards for Project Delivery within Shell and can be adapted for all IT projects.
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. Two approved solutions for a Process Control Access Domain exist in Shell at the time of publication of this DEP: SecurePlant and PCAD. Alternative solutions can also be used, but their compliance needs to be assessed prior to use.

Term	Definition
Process Control Domain (PCD)	The PCD is a collection of PCD IT Components, networks and instruments, unique to a facility under common operational governance, used to directly control, monitor, or safeguard the physical production or manufacturing processes of the same facility and are located in Levels 0, 1, 2 or 3 of the Reference Model (see Appendix A and B). A Process Control Access Domain can support one or more PCDs. The network demarcation of a PCD is characterized by a unique tunneling protocol connection (i.e., GRE or IPsec) between a Process Control Access Domain and a local facility network device. 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 (HMIs), and data historians.
Process Control Network	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 functions.
Remote Access	See Internal Remote Access and External Remote Access.
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 function that has user access to the PCD IT Components via the Process Control Access Domain or a user accessing a PCD IT Component in a PCD from a different PCD. Also see External Access.
Remote Setpoint	Change of a desired or target value for an essential variable of a control system, often used to describe a standard configuration or norm (e.g. high and low maximum values) for a control system via external remote access.
System	A combination of hardware and software components, which together provides a function or service.
Safety Instrumented System	See Instrumented Protective System.
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).

Term	Definition
VLAN	A virtual local area network (VLAN) is functionally the same as an IP network. VLANs allow the implementation of different IP networks on the same physical Ethernet switch. Similar to IP networks, computers on different VLANs cannot communicate without the assistance of a router as they are logically separated from each other. While this provides security benefit, it must be understood that these VLANs share the same physical network layer, inclusive of its bandwidth characteristics.
External Remote Access	Any network connection initiated from outside the PCD and terminated on a PCD IT Component. These connections are typically user-to-system, but also include any system-to-system connection originating outside the PCD. External Remote User Access would be an example of user-to-system connection. External Remote Network Management Access would be an example of system-to-system connection.
IP Network	A unique IP network is defined by the network prefix portion of an IP network address. An IP network address is composed of the network prefix number and the IP host number. The IP network mask specifies what part of the IP network address is the network prefix vs. the network host number. Hosts on different IP networks require the assistance of a router or network layer (layer 3) function to communicate.
Network	See IP Network. The unqualified use of the term Network will mean IP Network throughout this document.
PCD IT Component	A combination of hardware and software components, which together provides a function or service and is part of the process control domain. Examples of PCD IT Components are: computers, network switches, firewalls, programmable logic controllers (PLCs) and Human Machine Interfaces (HMIs).
Recovery Point Objective (RPO)	The RPO defines the maximum tolerable data loss (expressed in time) related to a system or business process after a failure without significant impact on the organization. RPO drives data backup strategies.
Recovery Time Objective (RTO)	The RTO defines the maximum tolerable period of outage of a system or business process after a failure without significant impact on the organization. RTO drives system hardware/software recovery strategies.

1.3.3 Abbreviations

Term	Definition
IPF	Instrumented Protective Function, now known as SIF (Safety Instrumented Function)
DCS	Distributed Control System. Also referred to as BPCS (Basic Process Control System)
FAT	Factory Acceptance Test
GI	Global Infrastructure
IP	Internet Protocol
MAC	Main Automation Contractor
OLE	Object Linking and Embedding
PCAD	Process Control Access Domain
RTU	Remote Terminal Unit
SIL	Safety Integrity Level
SIS	Safety Instrumented System
HMI	Human-Machine Interface
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
IPS	Instrumented Protective System, now known as SIS (Safety Instrumented System)
SAT	Site Acceptance Test
GPS	Global Positioning System
PAS	Process Automation System
IEC	International Electrotechnical Commission
DHCP	Domain Host Configuration Protocol
IRM	Information Risk Management
WAN	Wide Area Network
CIFS	Common Internet File System
CS-IT	Control Systems IT

Term	Definition
DMZ	Demilitarized Zone is used within Information Technology to identify a location in the network where a computer is configured outside the inner-firewall but inside the outer-firewall.
ENMCS	Electrical Network Monitoring & Control System
IP	IP Security
IM	Information Management
MOB	Mobile Office Business
MOP	Mobile Office Private
NIST	National Institute of Standards and Technology
OLM	Operational Landscape Management
OM	Operations Manager
OPC(-DA)	OLE for Process Control (Direct Access)
PCDP	Process Control Domain Portal
PCN	Process Control Network
PDF	Project Delivery Framework
RPC	Remote Procedure Call
RPO	Restore Point Objective
RTO	Restore Time Objective
SMB	Server Message Block
TACIT	Technical and Competitive IT
ACL	Access Control List
GRE	Generic Routing Encapsulation
IT	Information Technology
NAT	Network Address Translation
NSB	Network Security Barrier
NTP	Network Time Protocol
PCD	Process Control Domain
RDP	Remote Desktop Protocol
VLAN	Virtual Local Area Network