

MANUAL

DATA ACQUISITION & CONTROL ARCHITECTURE (DACA) – PROCEDURAL CONTROLS – CONFIGURATION MANAGEMENT

DEP 32.01.22.10-Gen.

June 2007

DESIGN AND ENGINEERING PRACTICE



This document is restricted. Neither the whole nor any part of this document may be disclosed to any third party without the prior written consent of Shell Global Solutions International B.V., The Netherlands. The copyright of this document is vested in this company. All rights reserved. Neither the whole nor any part of this document may be reproduced, stored in any retrieval system or transmitted in any form or by any means (electronic, mechanical, reprographic, recording or otherwise) without the prior written consent of the copyright owner.

PREFACE

DEPs (Design and Engineering Practice) publications reflect the views, at the time of publication, of:

Shell Global Solutions International B.V. (Shell GSI)

and/or

Shell International Exploration and Production B.V. (SIEP)

and/or

other Shell Service Companies.

They are based on the experience acquired during their involvement with the design, construction, operation and maintenance of processing units and facilities, and they are supplemented with the experience of Shell Operating Units. Where appropriate they are based on, or reference is made to, international, regional, national and industry standards.

The objective is to set the recommended standard for good design and engineering practice applied by Shell companies operating an oil refinery, gas handling installation, chemical plant, oil and gas production facility, or any other such facility, and thereby to 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 the quality of work and the attainment of the required design and engineering standards. In particular, for those requirements not specifically covered, the Principal will expect them to follow those design and engineering practices which will achieve 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 or its technical advisor.

The right to use DEPs is granted by Shell GSI, in most cases under Service Agreements primarily with Shell companies and other companies receiving technical advice and services from Shell GSI or another Shell Service Company. Consequently, three categories of users of DEPs can be distinguished:

- 1) Operating Units having a Service Agreement with Shell GSI or other Shell Service 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 authorized 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 Service Company. The benefit of this disclaimer shall inure in all respects to Shell GSI and/or any Shell Service Company, or companies affiliated to these companies, that may issue DEPs 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 GSI. 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	ABBREVIATIONS	5
1.5	CROSS-REFERENCES	5
1.6	COMMENTS ON THIS DEP	5
2.	GENERAL PRINCIPLES OF CONFIGURATION MANAGEMENT	6
2.1	OBJECTIVES.....	6
2.2	OVERVIEW	6
2.3	REPORTING.....	7
2.4	TECHNOLOGY	7
3.	CONFIGURATION MANAGEMENT CYCLE	8
3.1	GENERAL	8
3.2	PLAN / UPDATE	8
3.3	CONTROL.....	10
3.4	VERIFY / REPORT	11
4.	DATA RECORDS IN ASSET REGISTER	12
4.1	SCOPE.....	12
4.2	GENERAL RECORDS.....	12
4.3	USER COMMUNITY RECORD	12
4.4	NETWORK RECORD	13
4.5	ACCESS POINTS TO THE PCD	13
4.6	INFRASTRUCTURE DEVICE RECORDS	13
4.7	THIRD PARTY RECORD	14
4.8	APPLICATION RECORD.....	15
4.9	INFORMATION REPOSITORY RECORD	15
4.10	CONTRACT RECORD	16
4.11	CONNECTION RECORD	16
4.12	FILE LOCATION RECORD	16
5.	REFERENCES	17

1. INTRODUCTION

1.1 SCOPE

This new DEP specifies requirements and gives recommendations on how to develop a Configuration Management Database (CMDB), making use of Information Technology Infrastructure Library (ITIL) and specific aspects of the Opportunity and Project Management Guide (OPMG).

This DEP supports ITCI 117.

This DEP is intended for:

- PCAD administrators;
- PCD administrators;
- OU C&A Discipline Head;
- C&A Maintenance personnel;
- C&A Project Engineers;
- Vendors;
- Application Specialists.

Where specific roles and responsibilities have been described in this DEP they have been based on DEP 32.01.21.10-Gen. In case of conflicts, this DEP shall prevail.

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.

This DEP is intended for use in major development projects and existing producing assets in exploration and production. However, it may be applied to other Business Groups at the discretion of the Principal.

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 may 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/Vendor** 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 its design and construction. The Principal will generally specify the technical requirements. 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

Availability	The property of data or resources that are accessible and usable on demand by an authorized entity.
Confidentiality	The property that indicates the extent to which data have not been made available or disclosed to unauthorized individuals, processes, or other entities.
Configuration Management	Establishing and maintaining the integrity and control of software and hardware products (e.g. servers, source code, patches, documents, CPUs etc.) throughout a project's life cycle.
Data integrity	The property of data whose accuracy and consistency are preserved regardless of external changes and upsets. The property of data that has not been altered or destroyed in an unauthorized manner.
System integrity	The quality of a data processing system that fulfils its operational purpose while preventing unauthorized users from making modifications to or using resources and preventing authorized users from improperly modifying or using resources.

1.4 ABBREVIATIONS

C&A	Control and Automation
CCR	Central Control Room
CI	Configuration Items (defined in ITIL)
CMDB	Configuration Management Database
DACA	Data Acquisition & Control Architecture
GITI	Global IT infrastructure – the global IT service provision within Shell
IP	Internet Protocol
ITIL	Information Technology Infrastructure Library. See BS 15000-2.
OD	Office Domain
PAS	Process Automation System
PCAD	Process Control Access Domain
PCD	Process Control Domain
PLC	Programmable Logic Controller
RFC	Request For Change
TPA	Third party Access – a service for secure access by third parties via the OD

1.5 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 (5).

1.6 COMMENTS ON THIS DEP

Comments on this DEP may be sent to the DEP Administrator at standards@shell.com. Shell staff may also post comments on this DEP on the Surface Global Network (SGN) under the Standards folder.

2. GENERAL PRINCIPLES OF CONFIGURATION MANAGEMENT

2.1 OBJECTIVES

The high-level objective of Configuration Management is control of changes that are made to the hardware, software, firmware, and documentation throughout the system lifecycle. This shall include keeping accurate records of all changes and versions of software, firmware, etc. with appropriate measures for system restoration.

Implementing Configuration Management is essential for meeting ITCI 117 Section 3.2.1, which states:

An asset register of all key components relevant to security within the PCD and PCAD shall be maintained. This asset register shall include the following as a minimum:

- *All nodes in the PCD & PCAD with an network address and associated peripherals*
- *Network addresses*
- *All Windows, Unix & Linux software, relevant to the nodes above and used within the PCD & PCAD, including revision levels*

2.2 OVERVIEW

2.2.1 General

Configuration Management is a term taken from the ITIL methodology. It describes a process that tracks all the individual Configuration Items (CIs) in a system. A system may be as simple as a single server, or as complex as an entire Operating Unit. Configuration Management includes:

- Creating a parts list of every CI (hardware or software) in the system.
- Defining the relationship of CIs in the system.
- Tracking the status of each CI, both its current status and its history.
- Tracking all Requests For Change to the system.
- Verifying and ensuring that the CI parts list is complete and correct.

There are five basic activities of Configuration Management:

- Planning
- Identification
- Control
- Status Accounting
- Verification and Audit

2.2.2 Planning

The Configuration Management plan covers the coming three to six months in detail, and the following twelve months in outline. It is reviewed at least twice a year and includes a strategy, policy, scope, objectives, roles and responsibilities, the Configuration Management processes, activities and procedures, the CMDB, relationships with other processes and third parties, as well as tools and other resource requirements.

2.2.3 Identification

The selection, identification and labelling of all CIs. This covers the recording of information about CIs, including ownership, relationships, versions and unique identifiers. CIs should be recorded at a level of detail justified by the business need, typically to the level of "independent change".

All relevant information shall be carefully stored in a dedicated Configuration Management database (CMDB).

Examples of information that should be recorded are serial numbers, version numbers, installation dates, warranty status, actual configuration settings, updates, etc. Also the Configuration Management system shall obtain input data from Vendors, Suppliers etc. relating to any changes to patches, configurations, licences, etc.

2.2.4 Control

This gives the assurance that only authorised and identifiable CIs are accepted and recorded from receipt to disposal. It ensures that no CI is added, modified, replaced or removed without the appropriate controlling documentation such as an approved RFC or updated specification. All CIs shall be under Change Management Control.

2.2.5 Status Accounting

The reporting of all current and historical data relating to each CI throughout its life cycle, including changes to CIs and their various statuses, e.g. ordered, received, under test, live, under repair, withdrawn or for disposal.

2.2.6 Verification and Audit

This is a series of reviews and audits that verifies the physical existence of CIs, and checks that they are correctly recorded in the CMDB. It includes the process of verifying Release and Configuration documentation before changes are made to the live environment.

2.3 REPORTING

A comprehensive reporting and alerting system shall be implemented, utilizing the information in the CMDB, to provide alerting of any necessary configuration changes with due notice so that they can be planned and executed in accordance with the Change Management system.

2.4 TECHNOLOGY

There are a number of software tools on the market to support Configuration Management. Most of these tools support more ITIL processes than Configuration Management alone (e.g. Incident Management and Change Management).

The chosen solution does not necessarily need to cover all CIs, as some of the data that should be stored might already be in existing systems. The possibilities of interfacing with existing systems should be considered.

Automated discovery tools can be very useful to help build a Configuration Database and to audit the quality of CMDB data. However, using them to keep the CMDB up to date introduces the risk of changes bypassing the Change Management process. In all cases, the potential impact of the use of automated tools on the system integrity of the PCD shall be assessed prior to use. The application Vendor shall support the installation of the auto-discovery client on its system.

The CMDB contains confidential and vital information. Appropriate measures shall be taken to ensure Confidentiality, Availability and Integrity.

Minimizing the number of links to other databases will increase Confidentiality, Availability and Integrity. If multiple databases are required (e.g. to a patch management server), the number of custodians should be minimized.

For reporting purposes, it should be possible to pick up the path at any point and follow it forward to the released change and backward to the change request or to a fault report.

For instance, it shall be possible to determine for each change in the database:

- What change request or fault report triggered the change, and
- Which subsequent actions were taken to accomplish the change.

This can be achieved by assigning a unique number (associated to the change request or fault report) to each changed record.

3. CONFIGURATION MANAGEMENT CYCLE

3.1 GENERAL

The EP Business Model describes the management cycle which should be used in all management processes.

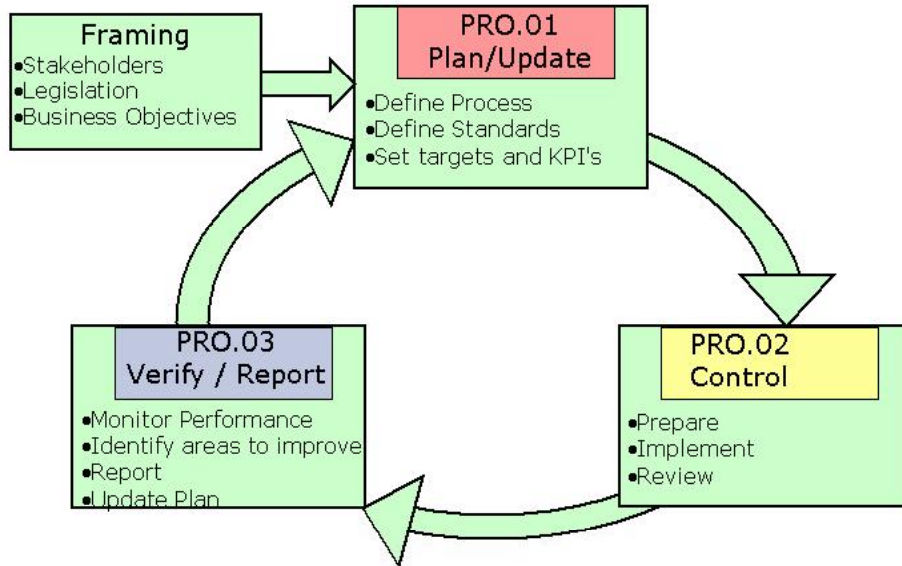


Figure 1 Configuration Management

3.2 PLAN / UPDATE

3.2.1 Scope

A Configuration Management plan shall be developed to implement the Configuration Management process in the Operating Unit.

It shall describe the purpose, scope, policies and processes necessary to implement an effective Configuration Management system.

It shall describe how this management system shall be implemented, taking into account the local situation.

The annual plan is developed within the framework of DACA and other Shell and external standards. It has a five-year perspective, and is based on an annual review of performance and objectives.

It defines resources such as staffing and funding requirements.

It sets "Base" and "Stretch" targets for the next 5 years, intended to challenge the Operating Unit to do better than the minimum acceptance criteria.

The high-level objectives and 'SMART' Key Performance Indicators are expressed in words, but contain clear measures of success/value and timing.

The plan shall refer to the Roles and Responsibilities that apply in that Operating Unit.

Following review on the Regional and Operating Unit level, the agreed plans provide the framework for the activities.

3.2.2 Responsibilities

See DEP 32.01.21.10-Gen.: The Operating Unit's C&A Discipline Head is responsible for Configuration Management and is supported by the PCD Administrator and the PCAD Administrator. The Operating Unit's Engineering Manager is accountable.

In practice, the custodian of the process will generally be the PCD Administrator.

Those responsibilities include but are not limited to:

- Develop the Configuration Management Plan
- Propose KPIs for Configuration Management performance, to be agreed by the Operating Unit's Engineering Manager
- Maintain an integrated audit programme on Configuration Management
- Co-ordinate performance review on a regular basis
- Communicate / Report Performance to the Operating's Unit Engineering Manager

Operating Unit's Engineering Manager's input into the Configuration Management process:

- Identify Asset Business Objectives and how Configuration Management relates to them
- Agree criteria for business risk and criticalities associated with Configuration Management
- Agree KPIs
- Agree control measures and responsibilities associated with Configuration Management
- Ensure adequate resources and skills

3.2.3 Configuration Management performance targets

The Configuration Management KPIs are chosen because they are:

- Specific
- Relevant to Business
- Measurable

Examples of Configuration Management KPIs are:

- (%) Completeness of overview of all or part of the Process Control Domain infrastructure
- (#) Number of CIs fully registered
- (%) Changes failed due to incorrect information in CMDB
- (%) Growth of Process Control Domain infrastructure
- (%) Delayed resolution of incidents due to incorrect information in CMDB
- (%) Missing CIs (and value)
- (USD) Value of installed base
- (USD) Annual license cost
- (%) Unlicensed software

KPIs can depend on the CI's security classification. KPIs that can be controlled by the process owner shall be measured separately from those that are determined by third parties. The latter shall be managed through Service Level Agreements with third parties.

3.3 CONTROL

3.3.1 CMDB in the business

Changes to the CMDB can only be originated from the PCD Change Management process.

Groups feeding into that process are PCAD administrators, Vendors, Contractors, C&A maintainers, application specialists and others.

Processes that use the data from the CMDB include but are not limited to:

- Back-up and restore (periodic, based on criticality)
- Virus management (ad-hoc, as and when released and advised by Vendor)
- Patch management (monthly, as and when released and advised by Vendor)
- Incident management (as and when they occur)
- Change management
- Audits

These activities may require an update to the CMDB, upon completion, using change control.

If information which is required to be stored in the CMDB cannot be stored there for business reasons, a step-out is required.

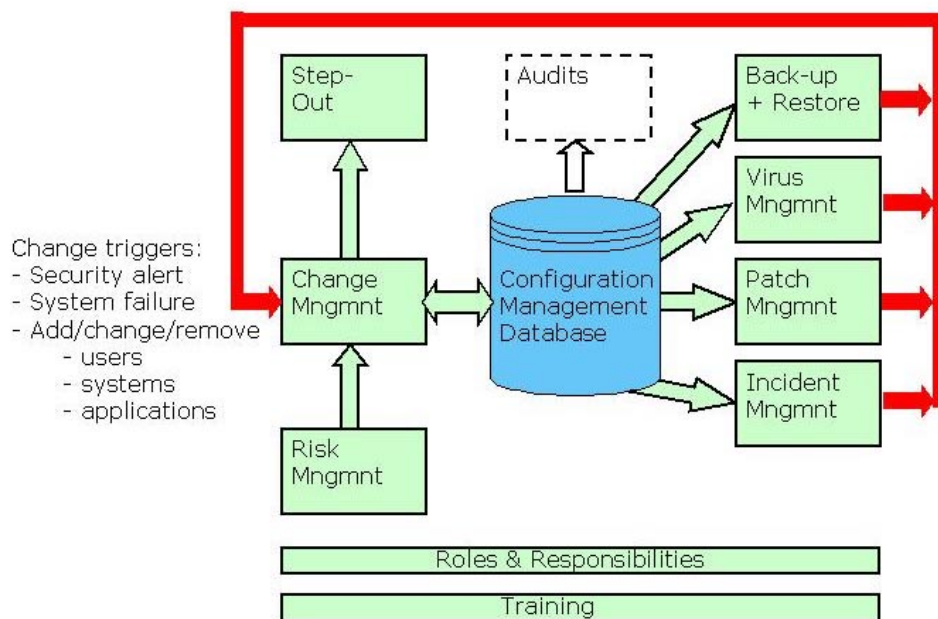


Figure 2 CMDB maintenance plan

Before participating in the Configuration Management process, staff shall receive the required training.

3.4 VERIFY / REPORT

3.4.1 Scope

Key activities in this part of the process are:

- Monitor Performance
- Identify Areas to Improve
- Update Plan

3.4.2 Monitor / Analyse CMDB process performance

- Determine frequency of process monitoring.

Initially this should be done at quarterly intervals, as in the early stages of implementation the rate of change will be rather high. After the CMDB has "matured" a bi-annual or annual interval may be applied.

- Monitor the performance of the process.

The effort associated with this activity mainly depends on how "automated" the data gathering is. Initially, this will be time consuming but it is expected to reduce to an acceptable level once the appropriate tools have been developed.

- Analyse performance against company and process forecasts and targets, highlighting any trends and deviations.
- Prepare and submit compilation reports, as agreed for internal or external review purposes.
- Benchmark the process against "best in class/industry" as appropriate.

Benchmarking achieves two objectives. First of all it will allow a comparison of the performance of the different Operating Units. Secondly, useful tools, best practices and additional KPIs can be shared amongst the Operating Units participating in the benchmarking.

3.4.3 Identify Areas for improvement

- Identify areas for improvement based upon an analysis of business performance and opportunities available (e.g. through new technology).
- Prepare terms of reference to action the improvement including cost, time and resources required, and identify the perceived benefits.

3.4.4 Update plan

- Optimise/ prioritise improvements and develop/update a business-driven plan for targeted performance improvement.
- Review as appropriate

Progress should be reported quarterly, with the management plans reviewed and updated annually. Changes to plans, objectives and budgets can be proposed at any time throughout the year in response to evolving business opportunities, but shall be approved by the appropriate delegated authority.

Monitoring of performance against plans and objectives is carried out at an Operating Unit basis, on an annual basis and through regular meetings as appropriate.

Performance measurement takes place on various levels such as company, department, asset/team and function as appropriate.

4. DATA RECORDS IN ASSET REGISTER

4.1 SCOPE

A wide variety of information is required to assist in configuration management. This is done using a Configuration Management Data Base (CMDB). This database consists of tables, subdivided in records which are subdivided in fields. These tables may be linked to avoid duplication and aid in database management.

Any record in the CMDB that needs to be managed in order to deliver a security or maintenance service is seen as a Configuration Item (CI). CIs are under the control of Change Management. CIs typically include hardware, software, buildings, people, and formal documentation such as process documentation and agreements.

The tables given in (4.2) to (4.12) are not necessarily complete and may be supplemented with Operating Unit specific fields. They should be used for guidance purposes and are not intended to be used as the actual tables in the database. Additional tables will be required to create relationships between these tables, e.g. to identify which users are allowed to access a specific application. These linking tables are not considered to be CIs but they may still need to be managed.

The three elements of system security are: Confidentiality, Integrity and Availability (CIA), see (1.3.2). The following records should have a CIA ranking: Network (4.4), Access Point (4.5), Infrastructure Device (4.6), Application (4.8), Information Repository (4.9) and Connection (4.11).

4.2 GENERAL RECORDS

General Record - Information Field:
Custodian
Responsibility for Operation – Organization charged with administering security on the device (according to requirements of DACA-responsible organization).
Location information (incl. Site ID)

4.3 USER COMMUNITY RECORD

User Community Record - Information Field:
Individual's Name – Name of the user
Reference Indicator
Network Access – Does the user have authorisation to access local network resources?
Performed Training – Has user undergone general DACA awareness training?
Guest (TP) – Is the user a member of a Third Party (if yes, specify Third Party)
Organisational information (Business Unit, Organisation, Line Manager, Community name, etc.)

4.4 NETWORK RECORD

Network Record - Information Field:
IP Range – IP range in the standard format nnn.nnn.nnn.nnn/nn (e.g. 10.1.1.0/24), where the numbers following the “/” indicate the significant bits of the applicable sub-net mask.
Network ID – Selected name, providing information about the nature of the systems hosted within the range (e.g. “PAS”, “CCR”, “Process Control” etc.).
Location of network – Inside PCAD (what PCAD segment?), in PCD (what segment?)
CIA information
Change window

NOTE: ALL networks inside the PCD perimeter for organization shall be listed in the above table (incl. networks in PCAD that are in DACA scope).

4.5 ACCESS POINTS TO THE PCD

This record shall provide the following information about the access points that connect all networks in the PCD to other networks (internal or external):

Access Points to the PCD Record - Information Field:
(External) Boundary – Device ID of Network Access Control Device
Connected to Which Remote Network
Remote Network Outside DACA Perimeter (Y, N)
CIA information
Change window

4.6 INFRASTRUCTURE DEVICE RECORDS

This record contains the necessary fields records of all IP-enabled devices on the ‘open’ Process Control Network that shall be maintained for inventory/scoping purposes.

Device Record - Information Field:
IP Address – IP address of the device.
Device ID – Host name or other unique identifying name of the device.
Device Type –e.g. Linux workstation, this can be free text.
Device operating system
Vendor / Brand of device
System custodian
Device patch/revision level (update)
CIA information
Change window

The device ID shall use a coding system which achieves a character string that is (at least) unique to the Operating Unit. This shall be a combination of a simple (three letter) code designating the area, a code designating the serial number of that device and, if needed, a simple code designating the type of device. The latter can be clarified in more detail using the field Device Type.

The PCD Administrator is responsible for developing a transparent coding system and applying it to all devices. It should relate to the facility or asset at which it is in use. This could use the three-letter codes, specific to a certain facility, similar to those used on PEFS drawings and cabinets, for instance. The PCD Administrator is also responsible for issuing blocks of codes to, for instance, a project team working on extensions.

Notes and Further Clarification:

All devices with an IP connection, inside the Process Control Domain, shall be listed and identified.

Non-DACA-compliant systems, such as “unpatched” engineering workstations, shall be listed in a separately maintained table, including System ID and user/owner information; the following is an example:

Device ID	Device Type	Owner	Site ID	Justification for “unpatched”	Approved by	Last Validated
PCN1-F123-HMI	HMI Yokogawa	A. Smith, SIEP-EPT SD	F123 CCR	Node not networked	B. Jones (Mgr. EPT-D)	20/12/04
PCN1-F123-APP	Application node	B. Smits, SIEP-EPT SD	F123 CCR	Legacy system not supported by Vendor	B. Jones (Mgr. EPT-D)	20/12/04

4.7 THIRD PARTY RECORD

Third Party Record - Information Field:
Third Party – Name of organization and individual
Via OD-TPA Service? (Y, N) – Is the connection provided via the standard OD TPA services.
Devices Accessible by Third Party – Device IDs to which access is enabled for this Third Party [applicable to Remote Third Party Access (RTPA) connections only]
Sponsoring Business Group/Person – Name of Business/Person working with (sponsoring) the TP
Contract Holder – Name of responsible function or individual in sponsoring Shell Business
Number of TP Users with Network Access – Number of TP users who have authorisation to access local or Group network resources
Audit date / Date validity check

4.8 APPLICATION RECORD

Application Record - Information Field:
Application name
Application Custodian - Name of individual or function and business unit that owns the application (e.g. pays for the application maintenance, etc.)
Responsible (e.g. service provider) - Name of individual or function and business unit that on a daily basis is responsible for the application (e.g. undertakes management, maintenance, etc.)
Device(s) name – Device name that the application resides on
IP address(s) or Standalone - IP address or network status of devices the application resides on
Logical Location (Internet facing/sitting) - On Group TCP IP network, Externally facing (Internet or to non-Group company) or on local network only
Operating System (the originally installed version, but not the patch level)
DACA Compliance - Is the application compliant or not, and with which technical specification (i.e. document version number)
Regulatory Compliance – Is the application subject to any legislative regulations
Third Party Access (including Service Providers) - Do third parties access the application for maintenance or use
BCP/DR Status - Is the application covered in a BCP/DR plan
CIA information
Change window
Obsolescence Date – Obsolescence date of the application (mm/yy)
Application Type/Function - Description of what the application does
Version/ Level – Application version level (see device for OS version)
Local Custodian – Business and Department
Dependant on Application/Middleware - Name
Operational Date
Required Completion Date
Vendor / Brand of device
Last Backup Date

4.9 INFORMATION REPOSITORY RECORD

Information Repository Record - Information Field:
Name - Name of the information repository
CIA information
Dependent on server – Name of server the information repository resides on
Dependent on Software (name) – Name of any software the information repository requires
Type – Type of information repository

e.g. Security Bulletins; operating system update info, critical security update info

4.10 CONTRACT RECORD

Contract Record - Information Field:
Contract party
Service Description - support hours, method, call-to-fix time / response time, support method
Support information - support codes, telephone number, etc.
Contract end date
Contract Owner
Contract Location

4.11 CONNECTION RECORD

Only connections with a source and/or destination inside the PCD require a description in the CMDB. All other connections are outside the scope of this document.

Connection Record - Information Field:
Source (Application / Device)
Destination (Application / Device)
Risk analysis (e.g. connection through PCAD?)
Technical details (e.g. Communication protocol, port numbers, wireless, etc.)
CIA information
Block Manager level

4.12 FILE LOCATION RECORD

File Location Record - Information Field:
File Type e.g. update, upgrade, virus patch, backup.
Application Name (match application above)
File Name Support information - support codes, telephone number, etc.
Version number
Installed or not Y/N
Justification for not installing
Date installed
File location
Application backup file location/file name

5. REFERENCES

In this DEP, reference is made to the following publications:

- NOTES:
1. Unless specifically designated by date, the latest edition of each publication shall be used, together with any amendments/supplements/revisions thereto.
 2. The DEPs and most referenced external standards are available to Shell staff on the SWW (Shell Wide Web) at <http://sww05.europe.shell.com/standards/>.

SHELL STANDARDS

Data Acquisition and Control Architecture (DACA) - Roles and Responsibilities DEP 32.01.21.10-Gen.

Information Security Standard for PCADs and PCDs ITCI 117

BRITISH STANDARDS

IT service management - Part 2: Code of practice for service management BS 15000-2

Issued by:
British Standards Institution
389 Chiswick High Road
London W4 4AL
UK

IT Infrastructure Library

ITIL

Issued by:
Office of Government Commerce
Rosebery Court
St Andrew's Business Park
Norwich, Norfolk
NR7 0HS
UK