

MANUAL

DATA ACQUISITION & CONTROL ARCHITECTURE (DACA) – PROCEDURAL CONTROLS – BACKUP AND RESTORE

DEP 32.01.22.11-Gen.

January 2008
(DEP Circular 10/08 has been incorporated)

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	6
1.6	COMMENTS ON THIS DEP	6
2.	GENERAL PRINCIPLES	7
2.1	OBJECTIVES.....	7
2.2	FRAMEWORK	7
2.3	OTHER REQUIREMENTS	10
3.	BACKUP STRATEGIES	12
3.1	OVERVIEW.....	12
3.2	STRATEGY SELECTION	12
3.3	BACKUP TRIGGERS	13
4.	BACKUP SCOPE	15
4.1	TYPES OF SYSTEMS IN SCOPE.....	15
4.2	TYPES OF DATA TO BE BACKED UP	16
4.3	BACKUP TYPES	17
5.	BACKUP ARCHITECTURE	19
5.1	BACKGROUND	19
5.2	LOCATION OF THE BACKUP SERVER.....	19
5.3	PROPRIETARY BACKUP ARCHITECTURE	20
5.4	SINGLE SYSTEM BACKUP ARCHITECTURE	20
5.5	DISTRIBUTED BACKUP ARCHITECTURE.....	21
5.6	CENTRALIZED BACKUP ARCHITECTURE	22
5.7	INFRASTRUCTURE DESIGN	23
6.	RESTORING	24
6.1	METHODS	24
6.2	RE-INSTALLATION	24
6.3	INSTALLING A SYSTEM IMAGE	24
6.4	USING A CENTRAL BACKUP TOOL.....	24
6.5	SINGLE FILE RESTORE.....	25
6.6	TESTING OF THE RESTORE PROCESS	25
6.7	SOFTWARE LICENSES	25
7.	BACKUP APPLICATION	27
7.1	SELECTION.....	27
7.2	GENERAL CONSIDERATIONS	27
7.3	BACKUP SCRIPTS AND AGENTS	28
7.4	ENCRYPTION.....	28
8.	REMOVABLE BACKUP MEDIA	30
8.1	STORAGE.....	30
8.2	VERIFICATION OF REMOVABLE BACKUP MEDIA	32
8.3	REMOVABLE BACKUP MEDIA REFRESHMENT RATES.....	32
9.	TESTING AND TRAINING	33
9.1	TESTING.....	33
9.2	TRAINING	33
10.	REFERENCES	35

1. INTRODUCTION

1.1 SCOPE

This new DEP specifies requirements and gives recommendations for backup and restore of electronic data files that exist on computer-based nodes located in the Process Control Domain (PCD).

The purpose of this document is to provide guidance on implementing a backup and restore process based on an appropriate strategy and methods, which satisfies ITCI-117 security requirements.

This DEP is intended for:

- PCD Administrators;
- PCAD Administrators;
- C&A Project Engineers;
- C&A Maintenance Personnel;
- PCD System Vendors;
- Backup and Restore Technology Providers.

The GI-H (Global Infrastructure – Hosting) servers installed in the PCAD are outside the scope of this DEP; those systems shall follow the Trust Domain rules.

1.2 DISTRIBUTION, INTENDED USE AND REGULATORY CONSIDERATIONS

Unless otherwise authorized by Shell GSI, the distribution of this DEP is confined to Shell companies and, where necessary, to Contractors and Manufacturers/Suppliers nominated by them.

Amended per Circular 10/08

This DEP is intended primarily for use in exploration and production facilities but it may also be applied to other facilities 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 regard 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 its design and construction. The Principal will generally specify the technical requirements. The Principal may also include an agent or consultant authorized 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
backup	In information technology, backup refers to making copies of data so that these additional copies may be used to restore the original functionality after a data loss event. These additional copies are typically called "backups." Backups are useful primarily for two purposes: 1) To restore a computer to an operational state following a failure (called disaster recovery) and 2) To restore small numbers of files after they have been accidentally deleted or corrupted.
restore	The process of copying data from a backup to make it available again after a failure. See also (2.2.5).
criticality	Impact or severity of a failure mode that would demand it to be addressed and mitigated. Expressed as C0 (least critical) to C5 (most critical). Refer to the Shell Risk Assessment matrix for a description of the severity classes.
PCD system	The system definition includes servers, workstations, network communication equipment and any other networked device. This definition may not be clear enough, in my view we should consider including all items covered by this DEP into the CMDB.
PCD node	A device that is connected as part of a computer network. For example, a node may be a computer, a router, switch, or hub.
PCD device	A piece of computer hardware such as a workstation or a server but also peripheral devices such as I/O cards, network interface cards, mass storage devices, printers etc. (Keyboards, monitors, and mice are not considered to be peripheral devices.)
PCD field devices	Transmitters, valves, PLCs, flow computers

1.4 ABBREVIATIONS

C&A	Control & Automation engineering discipline
DRP	Disaster Recovery Plan
DACA	Data Acquisition & Control Architecture
PAS	Process Automation System
EWS	Engineering Work Station
HMI	Human Machine Interface
IPS	Instrumented Protective System
PCAD	Process Control Access Domain
PCD	Process Control Domain
PCN	Process Control Network

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 (9).

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

2.1 OBJECTIVES

From ITCI-117 Section 3.3.1: *There shall be a managed process for developing and maintaining continuity within the PCD/PCAD. It shall bring together the following key elements:*

- *Each system/configuration/data in the PCD/PCAD shall be assigned a criticality level;*
- *Each system/configuration/data should be backed-up and restored in accordance with its criticality;*
- *Of each system/configuration/data a formulated and documented backup and restore plan should exist in accordance with its criticality;*
- *The backup plan should be tested regularly.*

NOTE: Wherever this DEP mentions a backup service or activity, it automatically implies an associated restore service or activity.

A backup and restore service should be part of an overall Disaster Recovery Plan (DRP) for the asset. The DRP is part of a larger process known as a Business Continuity Plan. Disaster recovery is the process of regaining access to data, hardware and software necessary to resume business operations after a security incident, hardware failure or disaster. The need for inclusion of the DRP in the asset risk register and risk management plan should be assessed.

The availability of systems can be affected by hard- or software malfunctions, malware attacks, or application changes. This applies not only to hard disk-based computers but also transmitters, valves, PLCs, flow computers, network equipment and other configurable electronic devices.

When planning for disaster recovery, Single Points of Failure require detailed attention.

The scope of this DEP covers PCD computer based nodes only; other devices in the PCD shall be managed in accordance with the operational availability/maintenance plan.

It is essential that information security services such as backup and restore are defined in an early phase of project implementation. The strategy selected for the backup and restore service may impact significantly on the required data processing and bandwidth requirements. Deciding this in the later phases of a project may limit the freedom of choices.

2.2 FRAMEWORK

2.2.1 Business continuity plan

A Business Continuity Plan is defining the steps required to restore business processes following a disruption. The plan identifies the triggers for invocation, people to be involved, communications etc. The objectives of a Business Continuity Plan include:

- Ensuring the continuous performance of an Operating Unit's essential functions/operations during an incident or emergency;
- Protecting essential facilities, equipment, records, and other assets;
- Preventing or mitigating disruptions to operations and further escalation;
- Reducing loss of life, minimizing damage and losses; and,
- Achieving a timely and orderly recovery from an emergency and resumption of full service to system users.

2.2.2 Disaster recovery plan

A DRP shall be developed and documented that, when implemented, will provide for continued performance of essential business functions under all circumstances. As a minimum, the plan should:

- Define essential business functions and activities;
- Outline a decision process for determining appropriate actions in implementing the DRP;
- Establish a roster of trained personnel with the authority to perform essential functions and activities;
- Include procedures for employee advisories, alerts, and DRP activation, with instructions for relocation to pre-designated facilities, with or without warning, during both duty and non-duty hours;
- Provide for personnel accountability throughout the duration of the recovery;
- Provide for attaining operational capability within a defined period; and,
- Develop a backup plan.

2.2.3 Backup and restore plan

A good backup and restore plan will involve the architecture of the systems in the planning process. Procedures and tools needed for the restore as well as standards for performing the backup and restore should be included. The Configuration Management Data Base (CMDB) should form the basis for this backup plan (see DEP 32.01.22.10-Gen.).

The steps required to develop such a backup plan are:

- Identify all PCD systems (both network-connected & standalone) in use by the Operating Unit (part of Configuration Management);
- Determine the criticality C0 to C5 of these systems (see Table 1);
- Determine overall strategy to provide backup and restore services to each system;
- Determine types of files and directories to be backed up
- Determine the scheduling (day of the week, time of the day) for the services;
- Determine staffing and resources requirements needed to perform these services;
- Verify that the existing network infrastructure is able to support the services (where required);
- Integrate supporting activities to ensure that the recovery can be achieved in accordance with the criticality and that the agreed service levels can be met.

2.2.4 Criticality classification

Criticality classification is a structured process that can be used to assess and quantify information security threats associated to processes, services and systems in the PCD. It is intended to:

- Identify business functions performed by these processes, services and systems,
- Assess the economic value of these business functions, in USD/d,
- Identify and quantify the information security threats (availability, integrity and confidentiality) associated with each function, in USD per event,
- Classify the criticality of each business function by determining the severity of an information security incident on each of these functions, C0 to C5,
- Apply measures to satisfy the criticality requirements associated to these threats that are based on the criticality of that business function.

In terms of the backup and restore service this means that for each PCD system and node a criticality shall be determined which should be included in the Configuration Management Database. This classification shall determine the service levels through the Backup and Restore Plan.

It should be noted that the criticality class could change over time. Verification of the criticality shall be included in the change management process.

2.2.5 Recovery

The Information Technology Infrastructure Library (ITIL) used by many IT people defines 'recovery' as returning a system or a service to a working state.

Within the PCD, a different meaning of that word applies, as indicated in Figure 1 below. Recovery means the sum of all phases between an incident happening and the return of the production facility to its normal state.

One of the objectives of the backup and restore process is to minimize the duration of the recovery from an incident. Minimizing the duration of the data restoration process is not the only action required to minimize the recovery time.

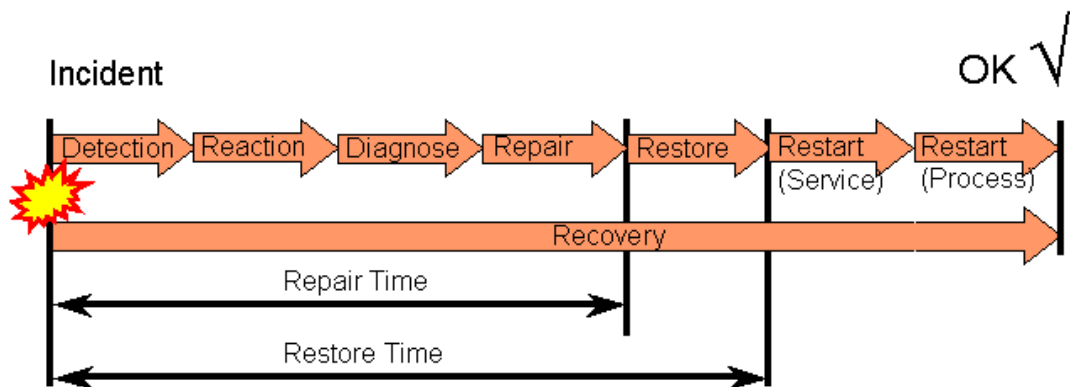


Figure 1 Expanded incident lifecycle in the PCD

Table 1 Table of criticalities

RAM severity	Criticality	Value to business indicator	Response
			Time frame and response actions in case of sudden outage
C0	C0	None	No action required
C1	C1	Overhead	Schedule repairs at next scheduled maintenance interval
C2	C2	Supporting	Schedule repairs at shortest notice
C3	C3	Contributing	Immediate repairs
C4	C4	Critical	Immediate repairs. Entire Operating Unit personnel required
C5	C5	Strategic	Immediate repairs. Entire Operating Unit personnel required and calling in additional resources

2.3 OTHER REQUIREMENTS

2.3.1 Legal

Where applicable, all relevant legal requirements shall be adhered to.

- Check for legal requirements on records retention and subsequent destruction as input into the backup and restore plan.
- Where legal requirements exist, ensure that backups are adequate to demonstrate compliance.
- It may be necessary to retain (e.g. fiscal) data for a number of years or archive copies to be retained permanently.
- Software licensing may require that all backup copies shall be destroyed after a certain period or at the end of a contract.
- Consider separation of backup data from fiscal metering data to ensure separate data storage requirements for custody transfer data can be assured. (I.e. to prevent early accidental erasure of metering data).

2.3.2 Records management

Records management is the systematic control of records throughout their lifecycle.

Records are all information which is required for legal, tax, regulatory, or accounting purposes, or which is of importance to the Operating Units business or corporate memory.

Within Shell, since 2005 records management is standardized in the Group Records Management approach.

Ineffective Records Management creates significant business risks that may have negative financial, competitive, business integrity, reputation, regulatory and compliance consequences. Compliance with the Group Records Management Standard and Guidelines shall be demonstrated and will help protect the Group and its employees from risks, such as:

- Fines or sanctions from courts and regulators;
- Additional tax liability;
- Competitive disadvantage or loss of license to operate;
- Cost to the Group through unnecessarily lengthy searches for Records;
- Inability to defend litigation properly;
- Loss of valuable corporate memory;
- Making poor decisions based on incomplete or out-of-date information; and

- Damage to Group reputation, e.g. as a result of inability to demonstrate compliance with specific Sarbanes-Oxley Act/Legal/Tax documentation and evidence requirements.

Examples of records from within the PCD that should be retained: (remove codes)

- Log files, specific attention should be given to these files since they may contain evidence that may be required for security incident investigations,
- Configuration changes made, to document what the original situation and the situation after the change were,
- Security incidents, to document how security incidents propagated,
- Quality testing and monitoring, measurements in terms of quality and quantity of emissions and spills into water and soil as well as flaring and venting data.
- Measurement and control, tracking and monitoring of crude, natural gas, LNG and products through pipelines and stations.

In general, records retention shall be handled by the IT Preservation Focal Point in the OD and not in the PCD.

Global Process 18 - Information Management and the Group Records Retention Schedule, dictates this process.

3. BACKUP STRATEGIES

3.1 OVERVIEW

A backup strategy is the organization's procedures and rules for ensuring that adequate amounts and types of backups are made, including suitably frequent testing of the process for restoring the original system from the backup copies.

Two different objectives are possible:

- Recovery Point Objective (RPO): The maximum **amount of data** that may be lost when Service is restored after an interruption. Recovery Point Objective is expressed as a length of time before the Failure. For example, a Recovery Point Objective of one day may be supported by daily Backups, and up to 24 hours of data may be lost.
- Recovery Time Objective (RTO): The maximum **time** allowed for recovery of an IT Service following an interruption.

These objectives have some conflicting requirements but in most cases, the latter objective will prevail in the PCD.

Wherever possible, the backup strategy shall comply with the vendor recommendations for backup. Furthermore, vendor recommendations regarding system management actions should be considered as input to the strategy. For example, regular database cleaning on certain DCS systems can have a significant impact on the reliability and completeness of the actual backup.

The Operating Unit C&A Discipline Head and the PCD Administrator are responsible for developing a backup strategy for all systems in the PCD.

Such a strategy shall cover the following aspects as a minimum:

What:	What systems and data shall be subjected to backups, what kind of backups shall be made
How:	What type of architecture and which applications shall be used to perform the backup
When:	How often and on which events shall the backups be performed
Where:	Where will the backups be stored
How long:	For which period shall the backup be retained and when shall it be deleted

3.2 STRATEGY SELECTION

A strategy for the selection of the backup process is required to properly balance costs and business value.

The backup strategy may depend on the following characteristics and limitations:

- Vendor recommendations for backup and storage,
- Type of system (operating system, size, location, function),
- Criticality of the system,
- Possibilities to make the systems more robust (redundancy, mirroring),
- Backup requirements (whether or not a system must be taken offline to make a backup or whether a re-boot will be needed),
- Possibilities to combine backup with archiving
- Frequency of changes to the configuration of the system,
- Network infrastructure
- Availability and knowledge level of the personnel to perform the backups,

- Mean Time To Repair
- Cost effectiveness

3.3 BACKUP TRIGGERS

There are a number of reasons that may trigger a backup being made:

- Time passed: Expiration of a certain interval since the last backup was made. The main purpose of time-based backups is to ensure that at all times a restore can be done without significant data loss or re-entry of changes.
- Events: Certain situations or activities may require a backup to be made. Certain security incidents may also require a backup to be made, which should be retained for a certain period, determined by contractual or legal requirements.

3.3.1 Time-based triggers

For each Configuration Item a certain backup interval is determined, based on the criticality of that item and dependent on how often that item changes, in combination with the backup effort required. This can for instance be daily, once a week, once a month or even never. There may be a number of ways in which a schedule for these activities can be handled:

- Manually maintained lists and activity rosters (this can be sufficient for small plants with low criticalities).
- Scheduled activities that are generated by an ERP system such as SAP. Due to the often large numbers of systems this may be less practical for daily backups.
- A dedicated backup server, which includes a scheduler. This automates a large amount of the work associated to making backups.

The backups that are made this way are normally following a removable media rotation schedule whereby media can only be used after a certain minimum time has expired, for instance six months.

3.3.2 Event-based triggers

There are a number of events in the operational life of a facility that may require detailed documentation and archiving of its state at that moment in time:

- At Ready for First Start-Up
- At Handover to Operations
- Before each subsequent start-up
- After each trip or major upset
- Before each subsequent planned shutdown

Contracts and/or legislation may require these backups to be retained for a certain minimum period.

Other event-based triggers are:

- After security incidents, for instance based on a PCAD disconnect level or other meaningful parameter.
- Before and after each engineering change made to the hardware or software. These may include:
 - o Installing an operating system patch or upgrade,
 - o Hardware modifications,
 - o Before a change is made for which no roll back is possible,
 - o After modifications to the system (scheduling changes, authorization and authentication changes, trip or alarm level changes or application changes),
 - o Uploading of new virus definition files.

Changes as listed above should be included in the Management of Change process and be covered by a suitable Permit-to-Work. Detailed Control Procedures and Job Hazard Analysis sheets need to be available for most of the regular changes, which include information on when and what kind of backups need to be made, how they need to be retained and if and when reboots are necessary. Also whether the restore functionality should be tested. These control measures shall be risk-based.

It should be noted that for a number of small changes no Management of Change may be required and as such, no backups are made as part of change management. This is at the discretion of the local operational procedures.

Examples of changes that can be made by the operator are:

- Changes in controller set points and control modes
- Changes in the configuration of local trends

Examples of small engineering changes are:

- Minor changes to graphics, reports and trends
- Changes to PID controller settings

These changes should be documented in logbooks and they will accumulate until the next scheduled backup is made.

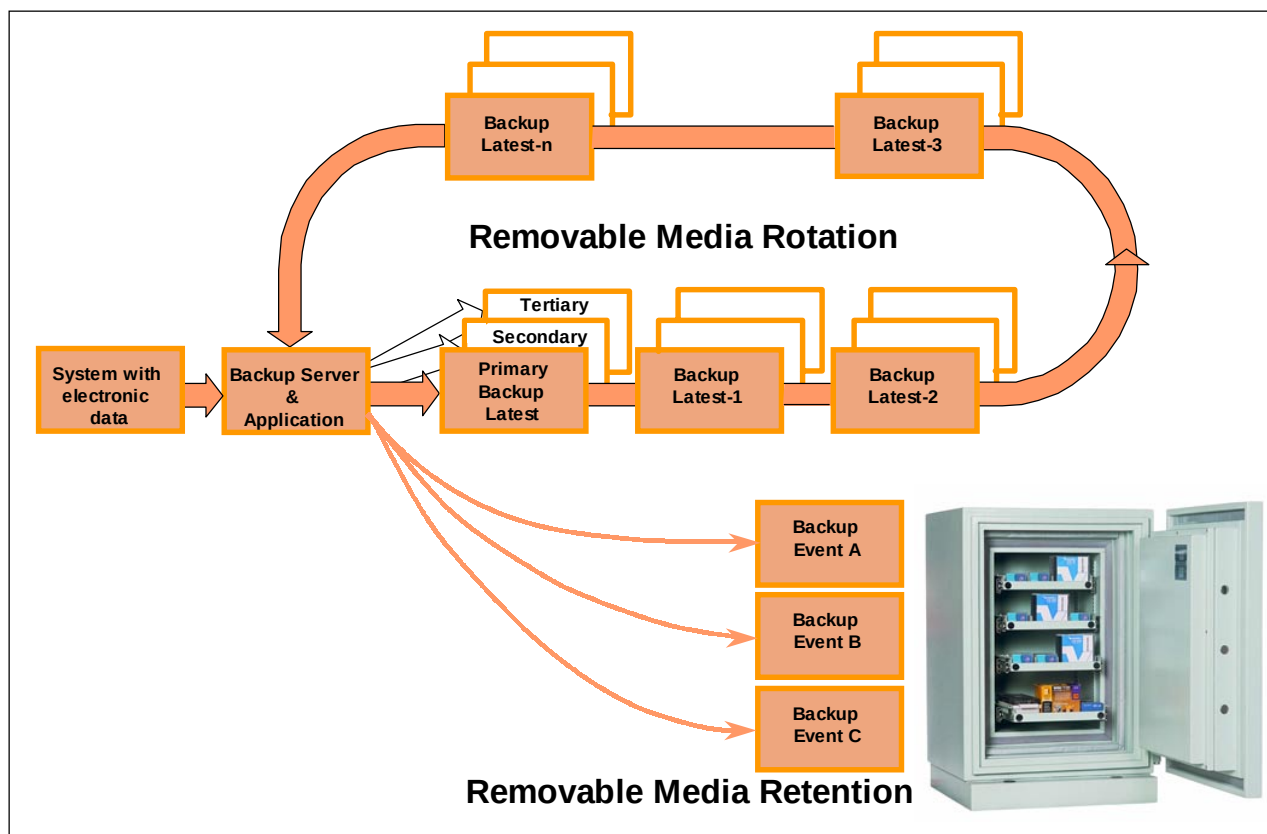


Figure 2 Media rotation and retention

4. BACKUP SCOPE

4.1 TYPES OF SYSTEMS IN SCOPE

4.1.1 General

The systems in (4.1.2) through 4.1.7) require backup services. By default, all computerized systems, programmable systems, and systems, which utilize microprocessors and store configuration data in the PCD, shall be evaluated.

NOTE: In the PCD there will be exceptions to the standard backup methods. These exceptions are specific for a real time environment and reflect the low rate of change found on these systems.

4.1.2 Default computer systems

Computers in this category have the following characteristics:

- The system runs on Windows, Unix, Linux or other "standard" operating system (this could be a server or workstation type of installation);
- The system will have a Network Interface Card connected to the PCN;
- The system is constantly switched on (24 x 7);
- The vendor must actively support the hardware and operating system software.

These types of system include the PI Historian(s) in the PCD.

Outside the backup scope is the data on the PCD PI Historian that has not yet been forwarded to the OD PI Historian. The reason for this is that a restore of the historic data may take some time and adds only little value to the applications using that historic data in the PCD. All other files on the PCD PI Historian such as the configuration of the historian shall be included in the backup scope.

4.1.3 IPS workstations

Workstations of IPS systems are not allowed to be connected to the PCN (see DEP 32.80.10.30-Gen) and therefore a centralized backup method is not possible for this equipment.

Every system has specific requirements and restrictions. Using these, one should be able to select the best backup strategy from the previous section.

The backup strategy shall always be in accordance with the vendor recommendation.

Typically, the IPS workstation will not require a regular time-based backup schedule, as the data does not regularly change (unless Sequence of Event data is collected). This kind of data shall be managed as part of the Records Management scheme, which will specify regular updates and retention.

4.1.4 Controllers in PAS systems

The PAS workstation generally contains a database of all these configuration parameters, and the PAS vendor supplies a process to ensure the backup of controller configuration is included into the overall PAS backup.

In all cases, the backup strategy recommended by the vendor shall be used.

4.1.5 Embedded systems

Embedded systems like flow computers will generally require backups, dependent on their system design. The parameters that are configured into the flowcomputers shall be available at site on paper (usually as a print-out from the supervisory computer) and shall always be kept as built. Checking the correctness of these paper prints shall be included in the periodic validation of the metering station.

4.1.6 Field equipment

The configuration settings of field equipment like transmitters, sensors, variable speed drives, motor control centres and valves require also backups. A centralized Asset

Management System (AMS) will provide an on-line asset register, which is included in the backup, and restore process. It is recognized that other databases such as SAP-PM and In-Tools also provide the capability to store configuration and other data about field equipment; however, these are off-line databases and rely on change management processes instead of on automated configuration capturing.

4.1.7 Network equipment, including telecoms

Network equipment, such as managed switches and routers, also require backups. The configuration of the network equipment should be stored in a centralized system.

4.2 TYPES OF DATA TO BE BACKED UP

4.2.1 General

The above-mentioned systems in the PCD contain different types of data. Each of these files will have its own characteristics. It is important to know these characteristics before backup techniques are chosen.

4.2.2 Operating system files

The operating systems files may be changed by normal computer use and maintenance.

- Regular changes of users and passwords;
- Regular installations of operating system patches;
- Regular installation of anti-virus definition files.

However, it may be acceptable to only maintain the media used for the original installation of the operating system and re-build the computer upon recovery. This would be a more time-consuming approach, but would reduce the backup overhead and may be an acceptable strategy for non-critical, non-networked nodes, such as engineering workstations.

4.2.3 Applications

The application (including middleware such OPC tunnelers) installed on a node to provide the core functionality of the system will not typically require regular backup, and will often be restored from the media used for the original installation.

4.2.4 Configuration data

Configuration data in a node consists of a number of different types of information. Some examples are:

- Files that describe how the different components of the node are identified and how they are connected to other systems;
- Files that describe how the inputs and outputs of the system are identified. This includes tag names, signal ranges etc;
- Files that describe how the different inputs and outputs are connected to the different controllers and how these controllers are programmed (for instance controller PID settings).

Small changes to controller settings (e.g. set points, modes, tuning parameters) are made continuously. If it is considered essential to restore these settings as well in case of a failure, a backup should be made more often. These types of settings may not always fall under change management.

4.2.5 Database files

Many types of databases are used in the PCD for storing historical data, event logs and alarm logs. These databases may need to be stopped when performing a backup since it is generally impossible to backup open files (cold back-up of database).

Databases may require special backup tools. Database records must be in the correct status before a backup can be made. This can be done by stopping the database engine in a controlled way or by using online backup tools, or by exporting the database to flat files.

Selection of the appropriate backup strategy will typically depend upon the following:

- Is the database operational continuously?
- What is the brand of the database engine?
- What is the size of the database?
- Are regular changes made to the content of the database?

4.2.6 Log files

Log files typically change regularly (due to the addition of fresh events) and are often required to facilitate post-incident investigation or audits.

Consequently, log files should be backed up in accordance with their importance, rate of change and data type.

4.2.7 Unconventional file types

There are certain types of files that cannot be backed-up in a traditional way.

Table 2 Unconventional file types

Type of file	Backup method
Network equipment settings	A specific tool should be used to make backup of network equipment.
PAS controller settings (tuning parameters, manual, auto, set points, alarm levels)	The standard backup tools of the PAS vendor shall be used.
Field instrumentation parameters	For non-hard disk based systems (HART transmitters, valves, network equipment) an inventory shall be made detailing how to make backups of these systems. In general, the backup of field instrumentation shall be managed using SAP. Where possible, online asset management tools should be used to backup all device parameters.
Active Directory	(Some DCS vendors use AD)

4.3 BACKUP TYPES

4.3.1 General

A number of types of backup methods are listed in (4.3.2) through (4.3.6) for information. Different methods may be used in an asset's backup strategy to ensure adequate implementation of the strategy.

4.3.2 Imaging

Imaging is a technology that makes a copy of an entire hard disk or disk partition. This image can be restored such that a computer can be brought back on line from a hardware failure, application crash, operating system failure, or virus within a very short period of time, back to its last known good running state. Imaging works well when capturing a static 'picture' of a computer periodically for later restoration, but does not suit well in capturing more dynamic disk changes, such as database file changes, user access, controller settings etc. It also tends to take longer, and as such is not performed with short intervals.

4.3.3 Full backup

This is a procedure for backing up all the files on a hard disk by copying them to a tape or another storage medium. Software is available that allows backups of open file systems or databases.

4.3.4 Differential or incremental backup

This type makes a backup of only those files that have been changed or added since the last full backup was made. Older versions of these files will be replaced by the more recent ones in a differential backup. The restore process is complex and may require more time, however more regular backups can be taken which means the restored system will be closer to the actual system prior to failure.

4.3.5 Individual file backup

A method suited for ensuring the most recent changes to individual and frequently changing files are captured such that these files can be restored to a particular point-in-time. File backup is the preferred method for capturing changes to database files and other application specific files that change frequently. Architectures and tools are available to make frequent differential backups (of only those files that have changed since the last backup) and less frequently a full backup (only when the file has changed). This is possible over a large range of systems in a centralized manner with limited human intervention.

4.3.6 Database backup

A database backup is a backup method to guarantee the backup of all changes to a database until a specific moment in time. Several options are possible and together with the vendor of the application or system, the most appropriate method should be chosen.

5. BACKUP ARCHITECTURE

5.1 BACKGROUND

The backup process is one of the most demanding tasks in terms of CPU load, memory access, network use, disk-access and storage. It requires careful planning together with other security services that demand network resources. Good housekeeping and reporting is needed to prevent overloading of systems or networks.

Installing extra hardware or an upgrade of hardware (CPU or memory) may be required to minimize the backup time or to lower the required system resources during the backup process.

DEP 32.01.23.11-Gen. offers four different architectures to make backups, each with its own specific requirements in terms of hardware, software and networking:

- Proprietary backup architecture
- Single system backup architecture
- Distributed backup architecture
- Centralized backup architecture

The primary objectives of choosing the backup architecture are:

- Minimizing the number of backup tapes
- Installing the backup tape drives in a well conditioned environment
- To have the backup tape drive on a physical location which is different from that of the clients (different room or a different platform).
- Minimizing the time it takes to physically back up the necessary data
- Minimizing the time it takes to restore all necessary data when required
- Minimizing the impact from the system being backed up on other operating systems
- Maximizing the integrity of the data being backed up.

5.2 LOCATION OF THE BACKUP SERVER

In case centralized or distributed backup servers are used, they shall be located inside the PCD for a number of reasons:

- Independence of PCAD availability. The restore processes in the PCD shall not be dependent on the availability of the PCAD or the OD. Disconnecting the PCD from the OD could be one of the first mitigation actions in case of an incident. In those situations restores in the PCD will not be possible anymore.
- Network security. A network backup requires a number of network services like authentication, remote execution of applications, disk sharing, DNS, etcetera. When the PCD backup server is not located in the PCD the PCAD firewall must allow many network ports to be opened. This will seriously compromise the DACA security.
- Network capacity. Backup software is the most infrastructure demanding software. The network must be capable of handling large amounts of data. Placing the PCD backup server outside the PCD will stress the PCAD Firewall and PCAD routers to a maximum and normal operations or maintenance can be affected easily.
- Software revision levels. When the PCD backup server is not located in the PCD, there can be a difference between the revision level of the backup application and backup agent software. Synchronizing of revision levels between the PCD and OD can be a difficult task.
- Authorization. Backup/restore software is very powerful software. When a restore is being initiated, PCD systems can be stopped or corrupted and thus affect the availability of the plant. The use of the backup software shall be covered by a Permit-

to-Work and executed by staff that are explicitly qualified and authorized by the PCD administrator.

5.3 PROPRIETARY BACKUP ARCHITECTURE

Wherever possible, the vendor's recommended backup process shall be used. The vendor is in the best position to assess the most practical, reliable and complete method of ensuring backups is available when required.

Lack of vendor support during the development and implementation of the backup process may result in the following:

- Incorrect state of data (open files) prior to backup can result in incomplete backup sets
- Missed data in the backup process
- Lack of, or limited, vendor support in the event of failed backups.

5.4 SINGLE SYSTEM BACKUP ARCHITECTURE

When using the single system backup architecture, a tape drive or DVD writer (or other removable backup media with the right capacity) and the appropriate backup software is included on each computer or sub-system that requires a backup service.

The picture shows a number of components that are not relevant in the context of the backup service. However, for clarity these have been retained in the picture below.

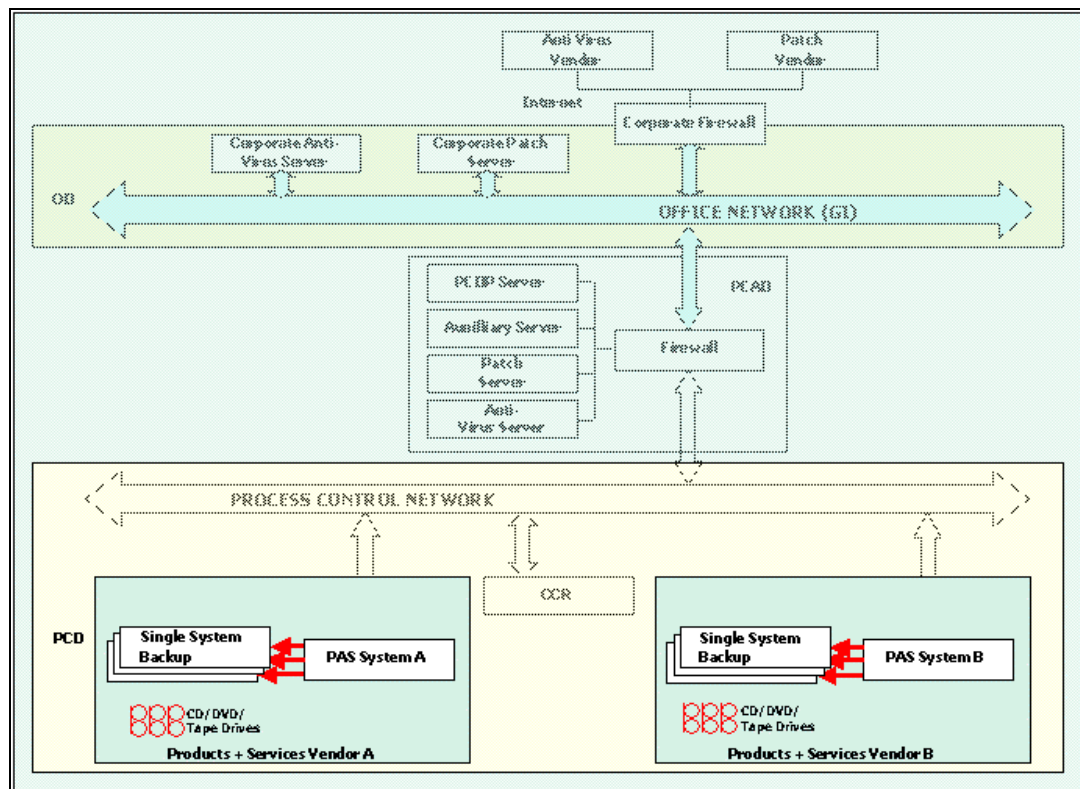


Figure 3 Single system backup architecture

The advantages of this architecture include:

- Clear delineation of vendor responsibilities
- Direct support by the vendor
- Easy to implement
- No impact on network performance

- The disadvantages may include: Performing backups and testing the restores may take additional time
- Higher cost & complexity for removable backup media handling (transport);
- The use of removable backup media may require additional device drivers to be enabled on the systems, allowing inappropriate use of those drives.

5.5 DISTRIBUTED BACKUP ARCHITECTURE

When using the distributed backup architecture, use is made of larger tape drives and backup software per location or per system vendor.

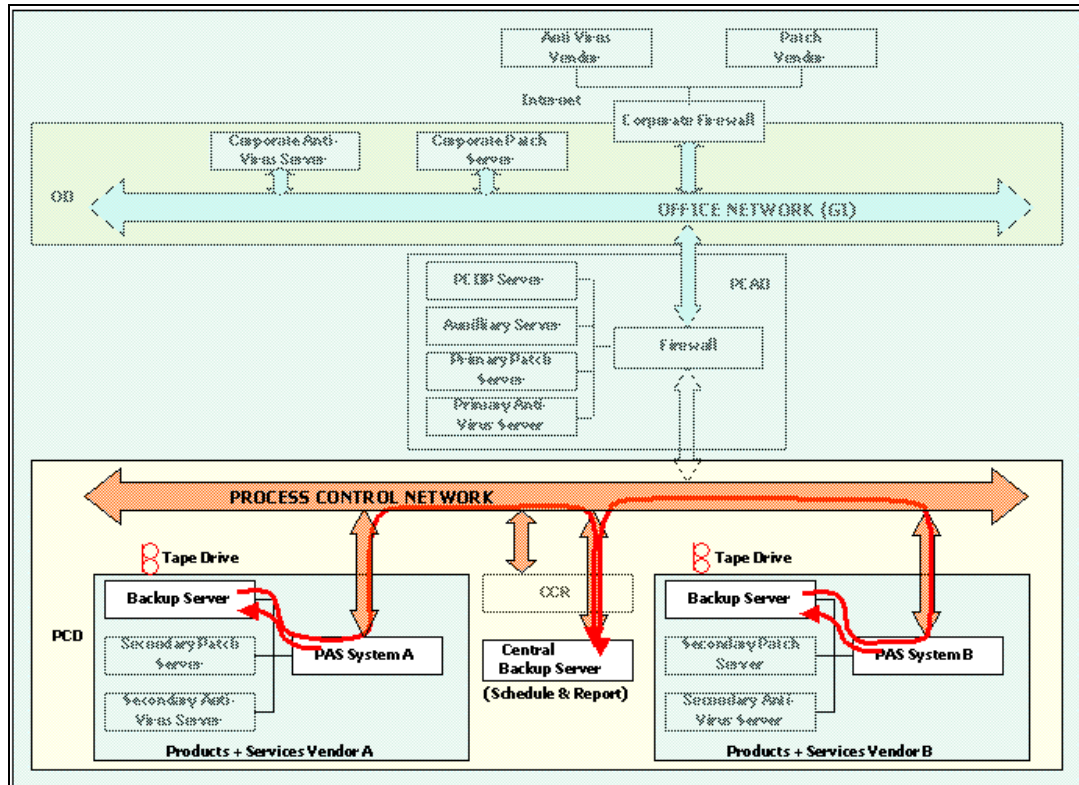


Figure 4 Distributed backup architecture

The advantages of this architecture include:

- The backup process is managed from a central location, for instance a Local Control Room, and no site visits of support staff are required for initiating and managing backups;
- Individual vendor strategies are supported

There are also some disadvantages:

- Support of the PAS vendor is needed in order to qualify and support backup agents installed on the systems.
- Slow PCN links to remote locations may be incapable of supporting the additional data load for backups.
- The write speed of tape drives is often ten times higher than the read speed of the hard disks of the systems that are being backed-up. This requires either multi-streaming or multiplexing of data streams in order to get sufficient dataflow and keep the tapes 'streaming'.
- Need for clear communication between the activity executor and the operator in the field.

5.6 CENTRALIZED BACKUP ARCHITECTURE

This architecture uses a centralized backup server with a large tape/disc robot. This system should be located near the Central Control Room or at the PCD support base. A backup server can typically handle up to 100–200 systems. This architecture is the most advanced, but the network infrastructure may require modifications to support the data load.

The most common issue for centralized backups is not having enough bandwidth on the network, so careful planning and sizing is needed (the bandwidth requirements could also be needed for remote access, patch and virus management, central control rooms, historical databases and advanced control or measurement techniques).

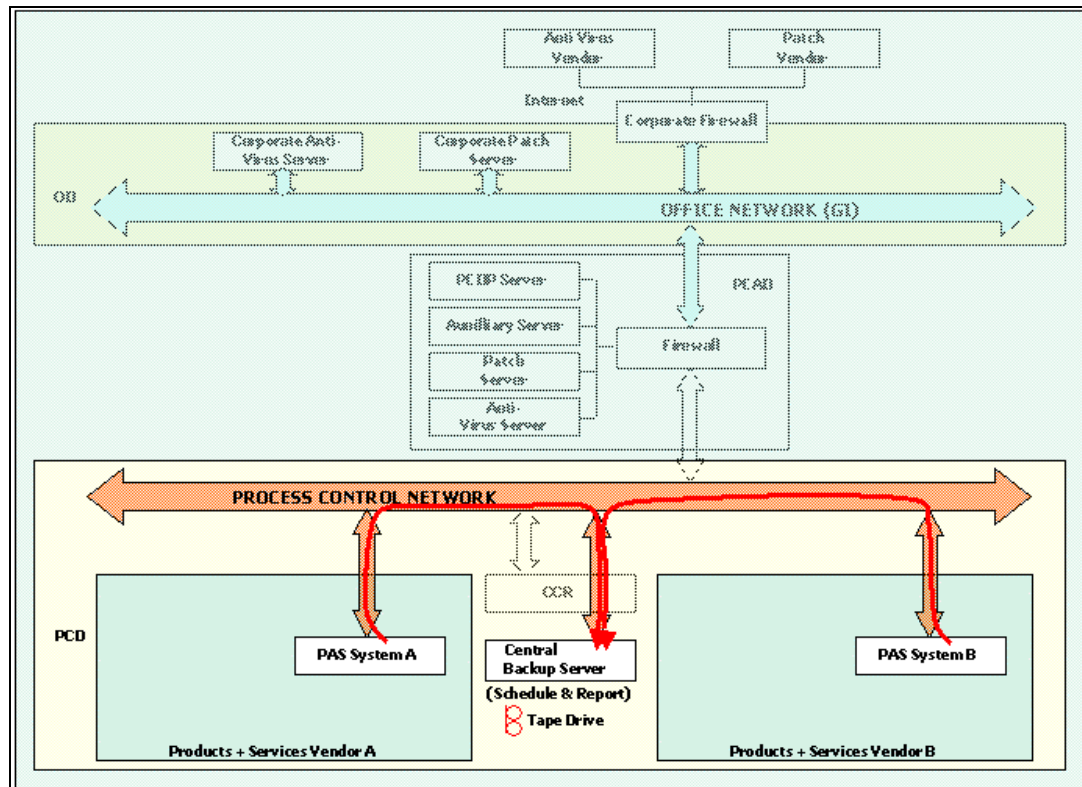


Figure 5 Centralized backup architecture

The advantages of this architecture are:

- There is no need for tape handling on remote places;
- Use can be made of centralized backup tools, performing scheduling and reporting tasks;
- There is an automated cleaning process of tapes and tape heads;
- The backup interval can be daily, no additional manpower required;
- Automatic restore of some type of servers may be possible;
- Standardization of backup methods, used software and procedures.
- Long distance between equipment and tapes are possible.

There are also some disadvantages:

- The backup is not immediately available at the remote location, which may lengthen a restore process (resulting in longer repair and recovery times)
- The network should be able to handle large amounts of data; a separate network or an upgrade of the existing network may be required;

- The network load during the backup process should not affect the operation of the system or network. The backup process involves a large number of variables which will ultimately determine the backup speed, system and network loading;
- Careful backup strategy planning is required;
- Network-based software can have problems when used with firewalls;
- The PAS vendor should support the configuration and allow the installation of the agent of the backup software;
- The correct multi-vendor backup software is not always available.

5.7 INFRASTRUCTURE DESIGN

5.7.1 General

An infrastructure design shall be made for the backup service. This design shall cover the following aspects:

- The selected backup strategy, scope and type
- Impact of that selection on the network infrastructure (bandwidth, locations)
- The equipment and utilities required for the backup service
- Availability of backups for PAS vendors for engineering
- Environmental requirements such as dust, humidity and UV light will decrease the lifetime / quality of the tapes, the environmental requirements for tape drives are high compared with the rest of the computer system.
- Storage requirements of removable backup media.

For transmitters and other configurable equipment a backup strategy shall also be developed. Storing the configuration files on a field engineer's laptop does not guarantee that the correct configuration file will be used in case of a restore.

5.7.2 Network upgrade

In case of constraints on the existing network infrastructure an upgrade of the network is preferred over the provision of a separate backup network for the following reasons:

- Cost, an upgrade is usually cheaper,
- DNS, a separate naming system is required,
- Time synchronization between the networks is required,
- Separate authentication and authorization is required,
- Require separate IP addressing range for backup network.

6. RESTORING

6.1 METHODS

Restoring data to a working system is a complex process. There are four restore methods for systems:

- Re-installation
- Installing an image
- Using a backup tool
- Single file restore

6.2 RE-INSTALLATION

Reinstallation of a system can be a lengthy process. The following steps should be taken to restore a system:

- Repair of the hardware (if required);
- Installation of the operating system + related reboots;
- Installation of the latest patches + related reboots;
- Assigning user names and security levels (where required);
- Installation of antivirus software + configuration;
- Installation / configuration of remote access tools;
- Installation of monitoring software and other utilities;
- Installation of the application + basis configuration settings;
- Installation of the configuration files;
- Testing of the application.

Generally, system specialists and/or application specialists are required to restore the system. All the steps in this process shall be clearly documented and tested in preparation for an eventual restore.

In all cases, the option to restore by reinstallation shall be available.

6.3 INSTALLING A SYSTEM IMAGE

In general, images of a system are often only made immediately after the original installation of the system.

System imaging will avoid a number of the re-installation steps but installing and testing of patches, security settings changes and any application/configuration modifications that have been applied after the image has been created must still be performed.

The time to restore would be shorter than for a complete re-installation, but system specialists are usually required.

6.4 USING A CENTRAL BACKUP TOOL

This method achieves the shortest restore time, especially when a backup is made regularly (e.g. once per day), dependent upon the rate-of-change of data on the system. The restore process can be similar for all the systems in the PCD.

Modern central backup tools also allow using other hardware than the hardware that has been used for the backup. This makes it easier to test the restore process.

However, generally the backup tools available are not directly compatible with non-Windows systems.

6.5 SINGLE FILE RESTORE

Restoring may not require a complete re-build, but a re-installation of certain components of the system. Consideration should be given to ensuring capability to quickly restore certain components of the system (e.g. individual data files, re-loading an application or service, etc).

6.6 TESTING OF THE RESTORE PROCESS

There are a number of occasions that would require testing of the restore process:

- After starting the backup service, for all individual systems,
- Whenever a new version of the backup agent is used,
- Whenever the backup policy has been changed,
- Whenever hardware such as disks, CPUs, Network Interface Cards, memory etc. has been replaced,
- After each major system upgrade or changes.

Furthermore, it is recommended to test the restore process during each planned shutdown when sufficient time is available to resolve problems identified.

Regular analysis of log files will also indicate if the backup process is being performed as planned.

The actual restore test may be done in a number of different ways:

- Installing an empty hard disk in the system and restore the software so the system will function identically. One complication of this is that the network IP address is normally stored on the hard disk. To resolve that it may be required to insert a bootable CD or USB to identify the system IP address and then initialize the restore to the hard disk.
- Do the restore on an empty system or on a test bed. Obviously this test does not cover all functionality of the software because the network environment of the test system will be totally different from the one for which the restore is tested.

6.7 SOFTWARE LICENSES

Most of the software used in the PCD is covered by licenses, which specify the permissions and restrictions that are related to that software. The license permits the licensee to use the software in line with the specific terms of the license. Use of software without such a license may be a violation of copyright or patent law and allow the owner of the software to sue the infringer.

Software licenses can be implemented in a number of different ways:

- A special file on the computer with a unique key (this file could get lost or damaged)
- The hardware MAC address is used to create a unique key (this could cause a problem when hardware is replaced)
- A key based on the CPU number of the 1st CPU (this could cause a problem when hardware is replaced)
- A specially programmed dongle on a parallel port or USB (the dongle could get lost or could be damaged),
- The hostname of the machine is used (this could mean that a restore cannot be tested in a test environment using a different logical location),
- One of the IP addresses of the server is used (this could mean that a restore cannot be tested in a test environment using a different logical location),
- A combination of hardware serial numbers (used in Windows XP and Vista),

- There may be a need for remote authentication with the software vendor, through the Internet,
- A separate license server could be used
- A unique code or number may need to be typed in
- It is also possible that licensed software can be used without any particular protection.

It is essential to know what licensing method has been used and how a restore of a system can be done successfully. It is equally important that details of licenses, numbers and locations are recorded.

The number of licenses required for a particular application could be based on the number of concurrent users, the number of control loops, number of tag names, data points and so on.

7. BACKUP APPLICATION

7.1 SELECTION

Often the backup devices such as tape decks are provided with basic backup application in the form of a stripped-down version of commercial packages. Features that are required may not be available. It is recommended that the PCD System Vendor or Backup and Restore Technology Provider supply the application to execute the backup plan and the services under guarantees covered by SLAs, KPIs and Leading Indicators. The PCD administrator should evaluate the effectiveness of the backup plan and manage the associated services and contracts.

Evaluation of the considered application may cover:

- Standards compatibility / compliance as mentioned in the Records Management
- PCD Vendor compatibility/compliance/certification of the application and agents required
- Device support
- Operating system support (Windows, Unix, Linux)
- Software compatibility (Versions of Windows, Unix)
- Multitasking capabilities
- Backup type selection
- Restore functionality
- Disaster recovery capability
- Scheduled and automatic operation
- Backup verification
- Compression
- Removable backup media append and override
- Tape tools
- Security (Encryption possibilities)
- Backup configuration profiles
- Quality criteria.
- Costs of the backup tools
- Familiarity and knowledge of staff

7.2 GENERAL CONSIDERATIONS

Various backup applications are available and could offer effective solutions for restoring a computer system after a hardware or software failure. It is recommended to keep the backup process in the PCD as simple as possible, in particular for legacy systems, as specialised sophisticated tools may become the source of system unavailability if not properly used or supported.

Some general comments about backups:

- The easiest way to restore a computer is making use of full backups – only one tape is needed and the restore process is relatively simple. Most systems in the production environment are small so a number of subsequent backups will fit on a single tape.

- Do not make the backup process complex – a full backup every day is simple and an incremental backup is complex. In cases where the capacity of the network is limited, changes of infrastructure are preferred to incremental backups.
- Challenge the need for exceptions for each system – each exception will require a tailor-made documented backup procedure.
- Automate the process as much as possible – a complete backup process will need many man-hours if manual labour is required.
- Never rely upon specific individuals to be available in the event that a system restore is required. Instead, ensure that appropriate training is provided to a number of staff and that the procedural coverage is sufficient.
- Implement routines for checking of log files to ensure that the backup process has performed as prescribed and that all necessary files have been backed up.

7.3 BACKUP SCRIPTS AND AGENTS

7.3.1 Scripts

In most cases, scripts need to be installed on client systems that are included in the backup scope. The purpose of these is to specify which files and directories are to be backed up and to where.

Scripts are small programs which contain instructions on the files that need to be backed up. They are easy and cheap to write. Disadvantages are that they may need maintenance each time the system is updated and thus need to be carefully documented by the user. They cannot do a restore – files are transferred one-by-one and they usually do not include error management.

7.3.2 Agents

Agents are normally associated to the backup application and provide a much more flexible backup solution. They are able to interact with databases so backups can be made of those files as well. Multistreaming and multiplexing are usually possible. They can be adjusted to restrict the bandwidth used for the service. They include error management and handling possibilities and can also enable a restore process.

A disadvantage is that they need to be bought with the backup application and licenses are required. Also, PCD System Vendors need to test and qualify these agents before they can be applied.

7.4 ENCRYPTION

With respect to the backup and restore service there are two aspects of encryption:

- Making backups of encrypted files,
- Encryption of backups (en-route or on removable backup media)

Depending on their criticality and confidentiality, certain files within the PCD are normally used in an encrypted form. When making a backup of these files two options are possible:

- De-encrypt the encrypted files and re-encrypt the backup copy. This requires the backup application to initiate decryption of the encrypted files, which requires access to the encryption key. From a security perspective, this is not recommended, because the information flows un-encrypted through the network. Backup script and agents also need to acquire in a secure way the correct decryption key belonging to specific data.
- Make a normal backup of the encrypted file and ensure that the encryption key is included in a separate file. The file containing the key may be encrypted as a backup. In view of the limited validity of encryption keys it is essential that the keys that were used for the encryption will be available to decrypt in case of a restore. From a security perspective, it is not advisable to have the key on the same media as the encrypted

data. The encryption strength of the backup solution might be different from the necessary encryption strength for that particular kind of data.

Other files that originate from within the PCD may need encryption for a number of reasons:

- The backup data traffic passes through a third party operated network,
- The removable backup media are handled by third parties (such as couriers)
- The source files are not encrypted but the backup copy needs to be encrypted for a particular reason.

In these cases, most backup applications provide an encryption tool, which also handles the encryption keys as part of the service. That way, when encryption keys are rotated it will always be possible to recover the encryption key that was valid at the time that the backup was encrypted.

7.5 PROCEDURAL COVERAGE

For the backup of systems in the PCD, procedures shall be in place. These should be written in conjunction with the PCD System Vendors and should take note of the specific requirements of the systems. These procedures should also include the steps required to restore the system in case of a hardware or software failure.

Backup procedures should be tested regularly and confirmed for coverage and performance. The time it takes to restore a system shall be monitored and compared with the business requirements.

In case of disasters, PCD administrators may not be available. Other administrators and nominated staff who are not familiar with the daily backup routines shall be able to use the procedures to restore the systems effectively.

- The backup procedure shall be completely documented and fully tested.
- Variations on the strategy shall be minimised to simplify the task and to reduce the risk of error.

All backup and restore activities shall be covered by suitable Key Performance Indicators which shall be reviewed regularly.

8. REMOVABLE BACKUP MEDIA

8.1 STORAGE

8.1.1 General

From ITCI-117 Section 3.3.2: *All critical software backups including IPS shall be kept offline and should be kept off-site.*

From ITCI-117 Section 5.1.4: *Equipment or media moved off-site for storage should be secured and protected in a manner equivalent to on-site equipment.*

Any removable backup media used should be rotated either within the site, or in some cases, off-site to ensure the media are available for restoration in the event of catastrophe. If off-site storage and handling of removable backup media is utilized, and a third-party such as a courier is used in handling or storing the removable backup media, the data shall be encrypted.

Removable backup media shall be stored in a data safe, which shall be made of heavy, fire-resistant, tamper-resistant, magnetically inert, materials. Data safes are usually dual controlled, and are designed for the safe keeping of removable media, including original installation media, other critical software, and top security data files. The storage process shall be appropriately administrated.

8.1.2 Multiple backups

In general, multiple copies of the backup should be available:

- A primary copy stored on-site (in a format that is not dependent upon a network for the restore function, e.g. CD-ROM)
- A secondary copy stored off-site, or in a geographically separate location (e.g. outside of the blast zone, in a different building, and not impacted by the same weather events, flooding, etc)
- Possibly a tertiary copy on the OD network (e.g. Livelink)

In all cases, the primary copy should be available within minutes of being required, whilst the secondary copy may be up to a few hours away if physical transport of the backup media is required.

Providing a copy on the OD network will make the backup independent upon failure of the removable backup media, and offers the advantage of enabling the backup to be available to support staff for activities such as reviewing logics, etc (dependent upon the backup file type). However, care should be taken to protect confidential data such as passwords.

There are two ways to obtain multiple backups:

- Repeat the complete backup process on a different removable backup media. The disadvantage of this is that the network and processor loading is repeated for each copy of the backup. However, this is the most reliable form of obtaining multiple copies.
- Use the primary copy as the source for the secondary and tertiary backups. This is not recommended if the primary copy is a tape but it is acceptable if the primary copy is another hard disk.

8.1.3 Removable backup media protection

Procedures and controls shall be in place to restrict access to removable backup media to approved personnel.

The removable backup media shall be removed from the writing device and where feasible write-protected after the backup process is completed to prevent accidental overwriting or modification of the backup copy.

8.1.4 Version control

Care shall be taken to ensure that expired backup versions are either destroyed or clearly marked as such. It is recommended that a minimum of three previous version shall be kept to ensure recovery to a last-known good operating state is available in the event of certain failure modes of the system (e.g. corruption of a configuration file after the implementation of a change).

8.1.5 Removable backup media lifetime

All removable backup media are susceptible to ageing and increased failure rates over time. Subsequently, consideration shall be given to ensuring stored removable backup media are in optimum condition when required. Note that the lifetime of most removable backup media is also dependent on environmental conditions, and the handling recommendation of the removable media vendor should be adhered to. The handling recommendation from the vendor of the removable media should be adhered to. In general, removable media should be kept in cool, dark and dry environments. Removable media should never be exposed to direct sunlight.

8.1.6 Removable backup media labelling

An appropriate labelling method should be used to ensure that each removable backup media is clearly identifiable. The following information should, as a minimum, be contained on the label:

- System name and physical location
- Backup version and copy number
- Backup date
- Person who performed the backup
- Reason for the backup; routine, planned change etc.
- Type of back-up (i.e. full, incremental, partial)
- Security classification (i.e. if tape contains critical or confidential data)
- Back-up retention date and tape expiry date
- Type and version number of the backup software used
- Type and version number of the antivirus software used for scanning the files

NOTE: When making use of barcode labels with a centralised or distributed backup solution this data will be covered inside the backup application.

8.1.7 Removable backup media rotation

The following guidelines are provided on the handling of tapes. Tapes are a relatively volatile media and generally require special handling to ensure correct operation. In all cases, the tape media vendor's instructions should be adhered to.

The best way to maintain proper, reliable removable media condition is to keep the environment clean and well maintained, and to handle all systems and removable media with care. It is recommended to regularly refresh the removable media, use fresh removable media in a timely manner.

- Consider cross-site backups, tape rotation and other methods of maximising backup availability and to minimize the transport of sensitive tapes.
- Tape drives and CD/DVD writers shall operate in a dust free environment.
- Removable backup media must be stored in a fire protected and lockable cabinet. These requirements are independent of the data criticality. All removable media that is needed to rebuild a computer system shall be stored off-line in a data safe certified for protection against fire for at least two hours.

- The removable media should be transported in certified lockable cases (shock protection, environmental protected, magnetically protected).

There shall be a register with the location of all the removable media. This register shall be kept up to date. Barcode registration can simplify this process.

From ITCI-117 Section 5.1.3: *Equipment and media containing confidential and/or most confidential information shall be destroyed at the end of its functional life in accordance with a documented process.*

- An expiry date for removable media must be indicated on the media
- A qualified company must be assigned for the destruction of removable media (CDs, hard disk, USB sticks)

In case a qualified company is not available, special destruction equipment shall be purchased to destroy the removable media safely and effectively.

8.2 VERIFICATION OF REMOVABLE BACKUP MEDIA

Any backup software option to automatically verify the backup should be set to 'on'. Alternatively, the backup software shall allow the backup to be verified after the data is written.

Removable media should be refreshed in a timely manner. No removable media should contain more than one version of software to eliminate the risk of wrongly loading software.

The backups should be audited annually for completeness and fit-for-restore purposes.

8.3 REMOVABLE BACKUP MEDIA REFRESHMENT RATES

There is considerable disagreement among experts about how long a given medium can be expected to last, and experience seems to imply that the answers can be quite different, depending on storage, environmental and handling conditions.

Two years of refreshment of removable media should be a reasonable period. When testing the restore capabilities this period can be refined.

Depending on the criticality of PCD systems, the removable media should be frequently refreshed and be stored for the operational lifetime of the systems. Some automated backup solutions have built-in facilities for drive cleaning and tape refreshment.

9. TESTING AND TRAINING

9.1 TESTING

9.1.1 General

Regularly testing of the backup process and backup software is needed to guarantee the availability of systems in the PCD. Testing will not only provide confidence in that the business interests are properly protected, it will also provide metrics to track as a Key Performance Indicator (KPI).

9.1.2 Test of backup software in a testing environment

Periodic testing of the backup software is recommended. Initial tests should be performed during the acceptance of the systems. These tests should be repeated when the infrastructure or functional requirements are changed or new versions of backup software and when new applications are installed. This can be included in a vendor scope of work.

The tests should also be repeated at regular intervals to prove that the backup method is still working properly. The following aspects require attention, some of which can be tracked as a KPI:

- CPU, memory and disk usage during the backup process. The backup is a resource demanding process so this parameter should be monitored to prevent loss of performance;
- Test the restore of the backup not only for functionality but also for the time it takes to restore. Measure also the time it takes to bring the tapes to the location, time for the reboots and time it takes to test the functionality of the system after the system is reinstalled.
- Verify that the restore can be done within the required time;
- Test the encryption of the tapes if they are handled by third parties such as couriers;

The test environment can also be used for training purposes for PCD administrators.

Where a spare system is not available, testing backups is not an option. In this case, testing should be limited to the following:

- Review backups to ensure that all backups are present & have coverage of all systems
- Check that the removable backup media is readable
- Confirm nominated staff knowledge of restore processes is still current

9.1.3 System resources

The backup process is one of the most CPU, memory, network and storage demanding tasks. Careful planning with other resource demanding processes (such as virus checking, batch processing; housekeeping or reporting) is required to prevent overloading of systems or networks.

Installing extra hardware or an upgrade of hardware CPU, memory or network capacity may be required to minimize the backup time or to lower the system resource demands during the backup process. In most cases, installing extra (low cost) hardware will also simplify the design of complex backup methods.

9.2 TRAINING

9.2.1 Competencies

Making structured backups requires specific roles, skills and competences. Staff should be nominated for performing these activities and to have the appropriate coverage given a particular system's service level agreement (SLA).

Typical skills are:

- System administration knowledge

- Network knowledge
- PAS and other application knowledge
- Imaging and backup software knowledge
- Specific operational environment knowledge
- Maintenance strategy/execution knowledge

The people that make the regular backups may not be available at the time of the requirement for a backup. The restore procedures shall be simple and shall be able to be executed by other persons (usually production maintenance staff).

Restores require a higher degree of skill and intimacy with the system being restored than that necessary to back it up. For example, configuring an automated backup of an SQL server or Oracle database from cold backup to disk, then on to a tape device across the network, and monitoring to ensure backups can be done is easier than restoring that file. When restoring a database, knowledge of the database's relationship with applications is required, in order to select the right point-in-time to restore from, and to detect when corruption might have occurred to ensure the data that is being restored is accurate, etc.

9.2.2 Training requirements

If a network based backup solution is chosen, training is needed for the design, implementation and maintenance. A centralized backup tool is a complex product, however if the tool is working correctly the benefits are high.

Hands-on training should also be provided for any production maintenance staff that may assist in restoring the system in case of an incident.

10. 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

DACA – Procedural controls – Configuration management	DEP 32.01.22.10-Gen
DACA – Technical controls – Infrastructure architecture	DEP 32.01.23.11-Gen
Instrumented protective systems	DEP 32.80.10.30-Gen
Information security standard for PCADs and PCDs	ITCI-117

BRITISH STANDARDS

Information Technology Infrastructure Library	ITIL V3
---	---------

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