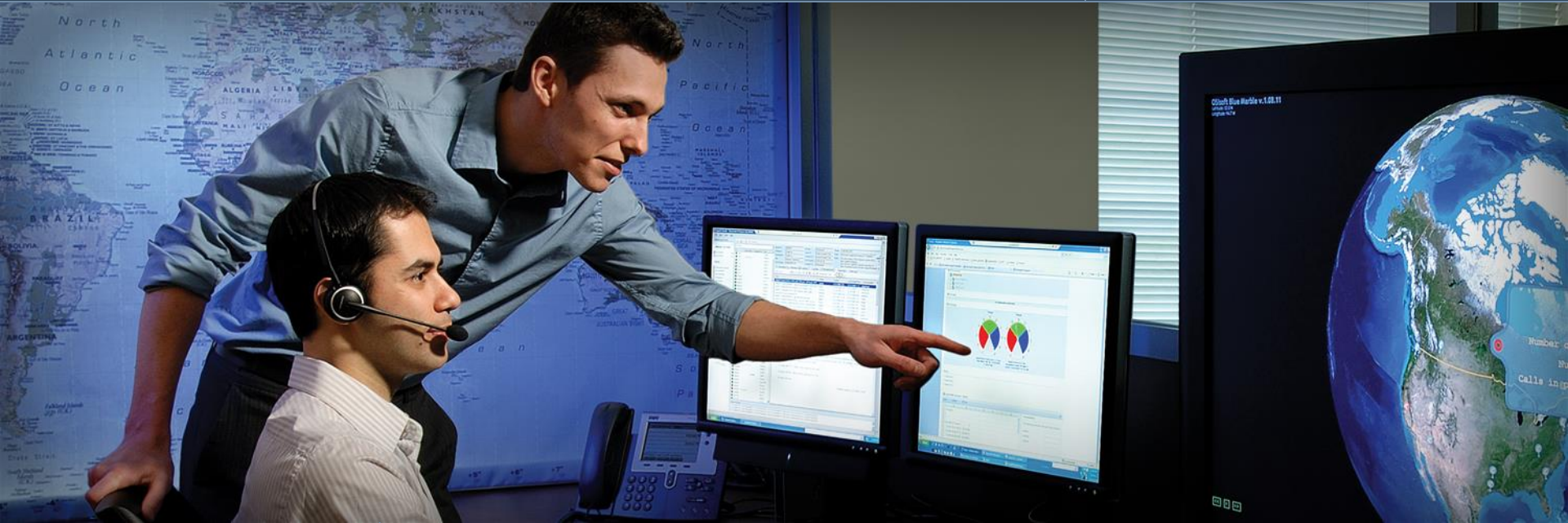# Architecture and Best Practices: Recommendations for PI Systems

Brandon Lake
Sales Support Engineer
OSIsoft, GmbH

Overview

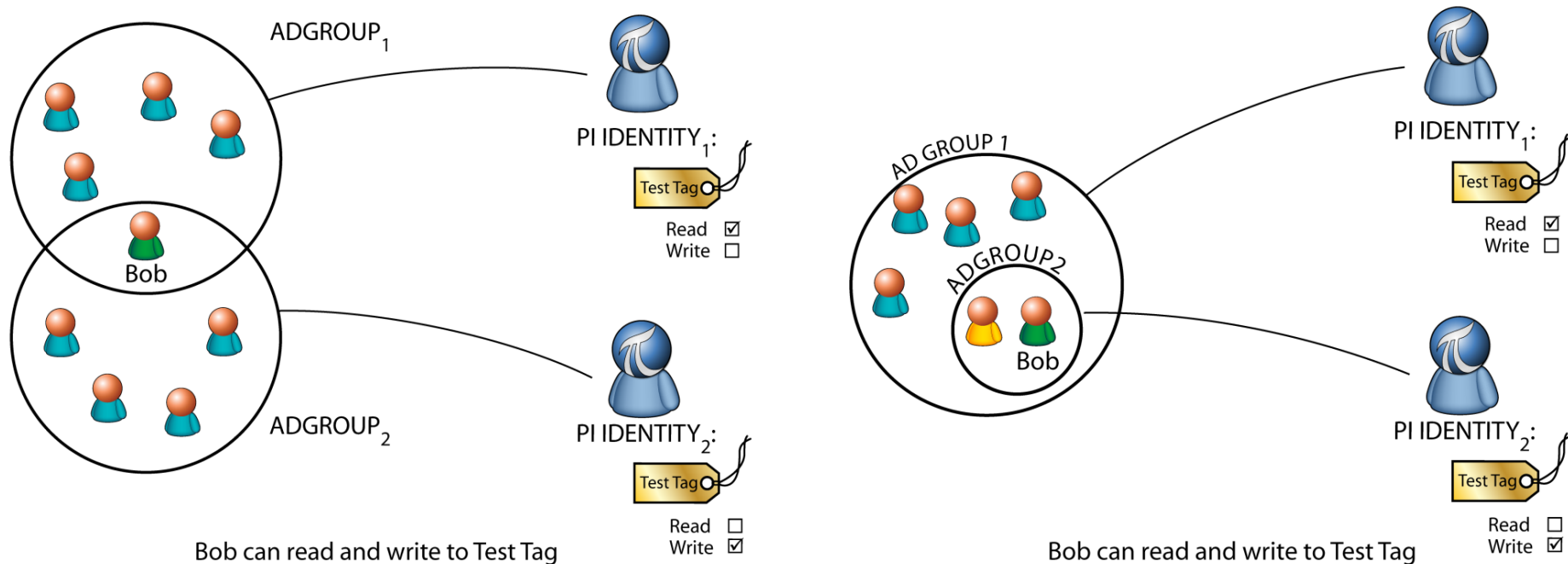- PI Server with Windows Integrated Security (WIS)

- PI High Availability

- PI Interface Failover

- Virtualization and PI

Empowering Business in Real Time.

New PI Security Concepts

Empowering Business in Real Time.

PI Identities, PI Mappings

ADGROUP₁

PI IDENTITY₁:

Test Tag

Read ☑
Write ☐

Bob

ADGROUP₂

PI IDENTITY₂:

Test Tag

Read ☐
Write ☑

Bob can read and write to Test Tag

AD GROUP 1

ADGROUP2

Bob

PI IDENTITY₁:

Test Tag

Read ☑
Write ☐

PI IDENTITY₂:

Test Tag

Read ☐
Write ☑

Bob can read and write to Test Tag

- PI Identities = Security Principals within PI

  - Examples: PIOperators, PIEngineers, and PISupervisors
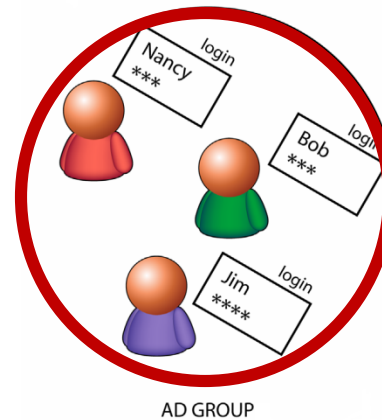
- PI Mappings – link AD Groups to PI Identities

User Identity in the PI Server

Old Model

Windows

Windows login
Nancy
***

Windows login
Bob
***

Windows login
Jim
****

PI Server

PIServer login
PINancy
****

PIServer login
PIBob
*****

PIServer login
PIJim
****

New Model

Windows

Nancy
login
***

Bob
login
***

Jim
login
****

AD GROUP

Mapping

PI Server

PI Identity

☑ **Nancy**
☑ **Bob**
☑ **Jim**

- The security principal is the PI User

- Audit and Change logs reflect the PI User
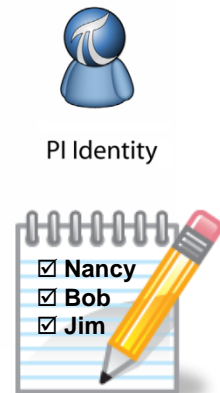
- The security principal is the Windows User, <u>not a PI User</u>

- Audit and Change logs in the PI Server reflect <u>the Windows User</u>

PI Identity vs. PI Groups and Users

Differences between PI Identity and PI Users and Groups

Unlike PI Users, PI identities don't have a password and can't be used for explicit login

Unlike PI Groups, PI Identities can not contain PI Users

Common Properties Shared by PI Identities, Users, and Groups

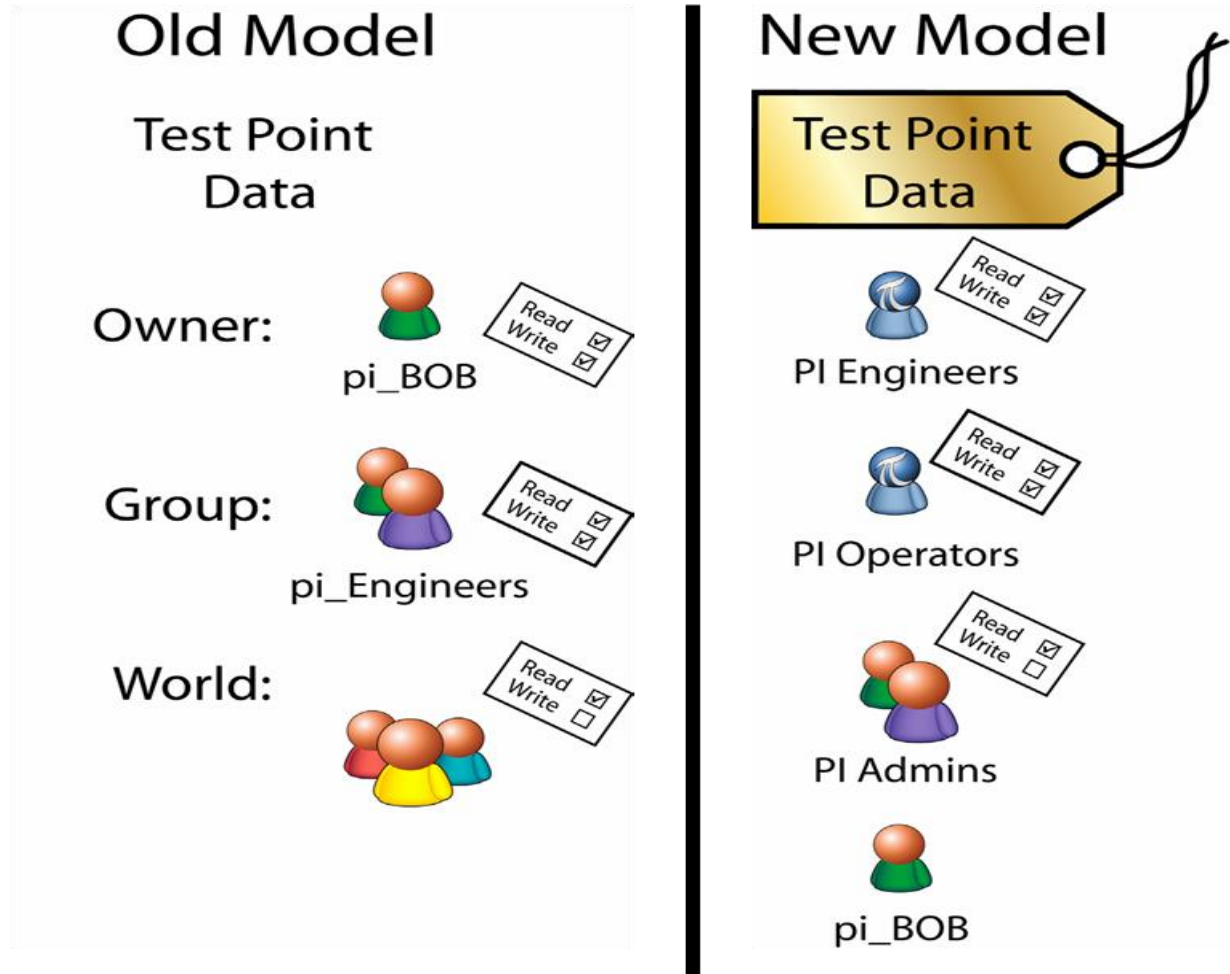Can be used for PI Mappings or PI Trusts (except PIWorld)

Can be used in all Access Control Lists (ACL)

Have the same authentication control flags

Empowering Business in Real Time.

Active Directory Integration

- PI Server must be a member of a domain to leverage Kerberos authentication

- Multiple AD domains must have trusts established or users and groups from other domain cannot be used

  - One-way trusts are supported: the server domain must trust the client domain

- Users in Workgroups can be configured to use Windows Local Groups from the PI Server machine

  - Passwords have to match for NTLM authentication

Empowering Business in Real Time.

Active Directory Integration

- Considerations when Integrating with AD

  - Kerberos authentication can be used without creating domain groups

    - Create a Local Group then add users from AD into those local groups

  - Who will manage the AD Security groups?

    - Will IT allow you to manage them?

    - Do you want to manage them?

  - Design Identity mappings and AD or Local Groups to ensure consistent access management across your PI System(s) with Active Directory

- Develop a PI Identity Scheme for your Organization

  - Use common Identities across PI Systems

    - What will the structure be?

      – Why would you build them that way?

        » Protect data

        » Ease of maintenance

        » Organizational separation

  - Standardize the application of Identities for security in PI Systems

- Use Kerberos authentication either by directly mapping AD Security Principles, or by using Local Groups with AD Security Principles

Empowering Business in Real Time.

Object Level Security Model

Object Level Security - Compatibility

Access permissions are automatically converted

Tag	dataaccess	datagroup	dataowner
sinusoid	o:rw g:rw w:r	pi_users	bob

New single ACL attribute or security descriptor

- `Identity1:A(r,w) | Identity2:A(r,w) | Identity3:A(r)`

Tag	datasecurity
sinusoid	pi_users:A(r,w)	bob:A(r,w)	PIWorld:A(r)

Backwards
Compatible

Same schema for PI Database and Module Database security

Empowering Business in Real Time.

Use PIWorld for generic read access

- Everyone is granted at least PIWorld privileges

- World access is controlled through a PI Identity

- Default setting: read-only access

- You can disable PIWorld

Empowering Business in Real Time.
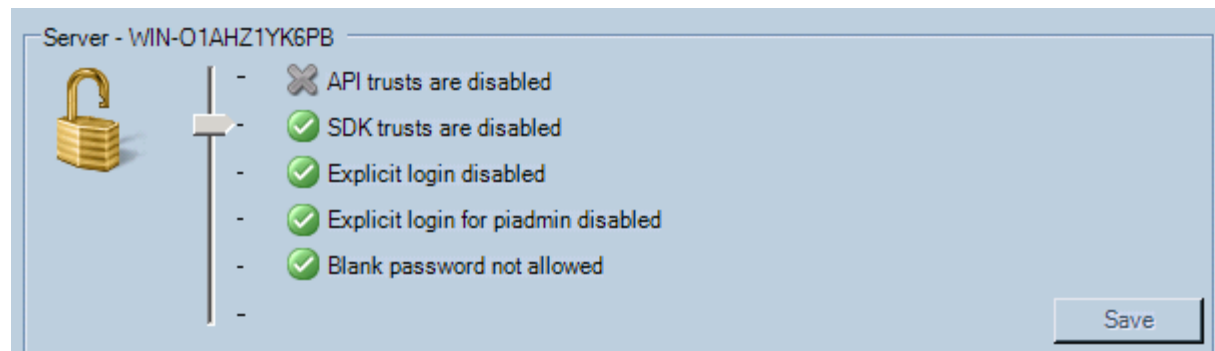
PI Client Considerations

- Clients

  - No more explicit logins

  - Seamless authentication from a Windows session

  - You can revert to the old method (explicit login) by selecting the authentication procedure in the SDK

Empowering Business in Real Time.
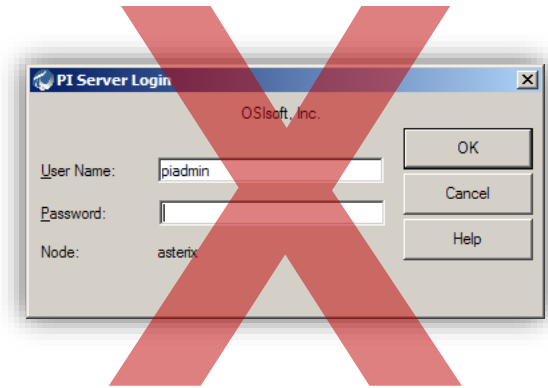
How to Tighten Security

1. Use the new Security Tool to help secure your PI Server

2. Disable or protect the PIADMIN account

3. Disable PI password authentication (Explicit Logins)

4. Secure piconfig by forcing login

5. Retire PI SDK-based Trusts

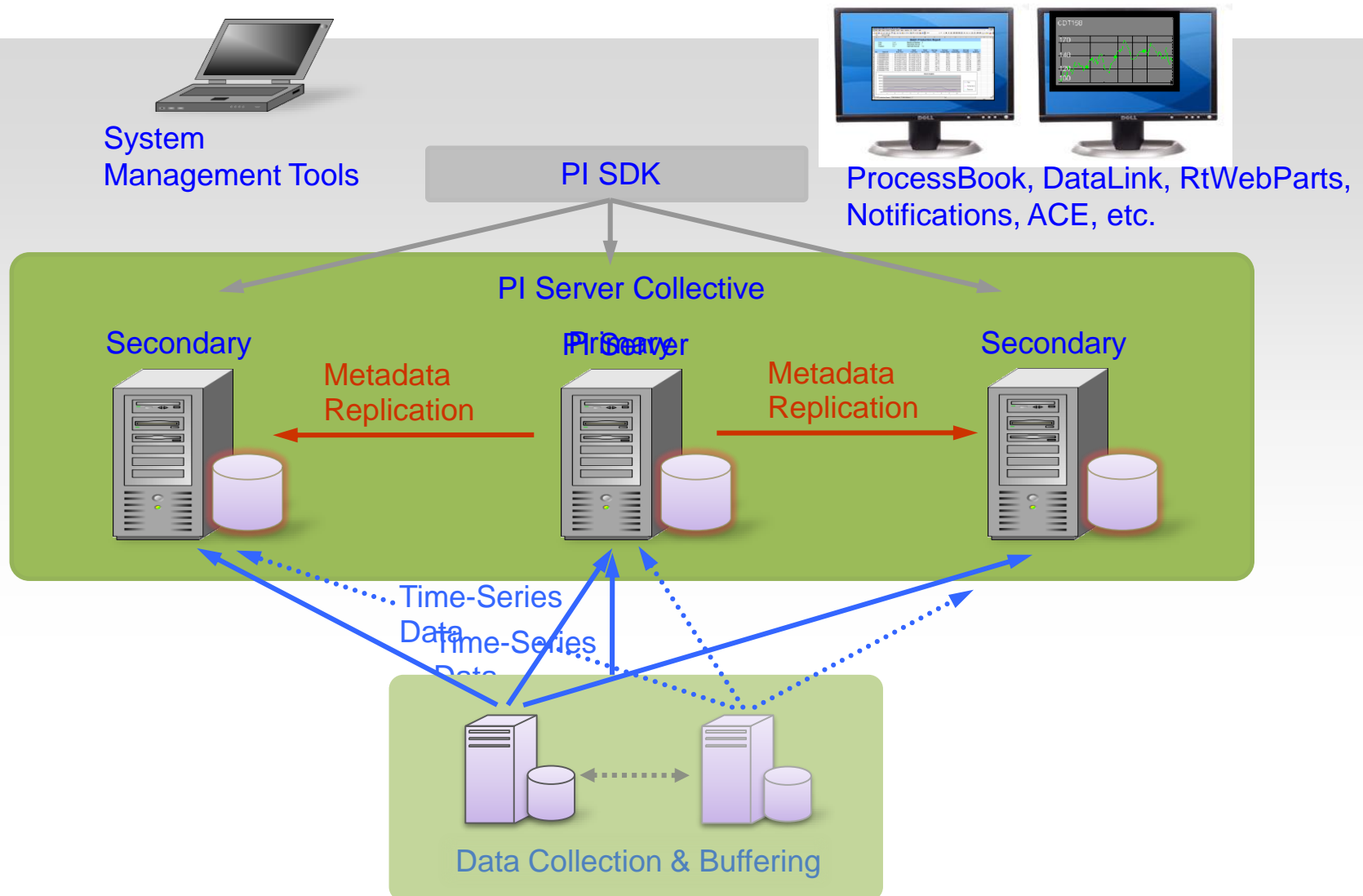6. Configure the PI Server Firewall

7. Disable PIWorld Identity

Server - WIN-O1AHZ1YK6PB
- API trusts are disabled
- SDK trusts are disabled
- Explicit login disabled
- Explicit login for piadmin disabled
- Blank password not allowed

Save

Empowering Business in Real Time.

- Perform impact and risk analysis

- Work with the CoE to update your architecture

- Develop a migration plan with EPM

    1. Identify access roles "read-only" & "read-write"

    2. Create PI Identities

    3. Create AD Groups

    4. Create PI Mappings

    5. Plan for AD Group Maintenance (add/remove users)

PI High Availability (HA)

System Management Tools

PI SDK

ProcessBook, DataLink, RtWebParts, Notifications, ACE, etc.

PI Server Collective

Secondary

PI Server Primary

Secondary

Metadata Replication

Metadata Replication

Time-Series Data

Time-Series Data

Data Collection & Buffering
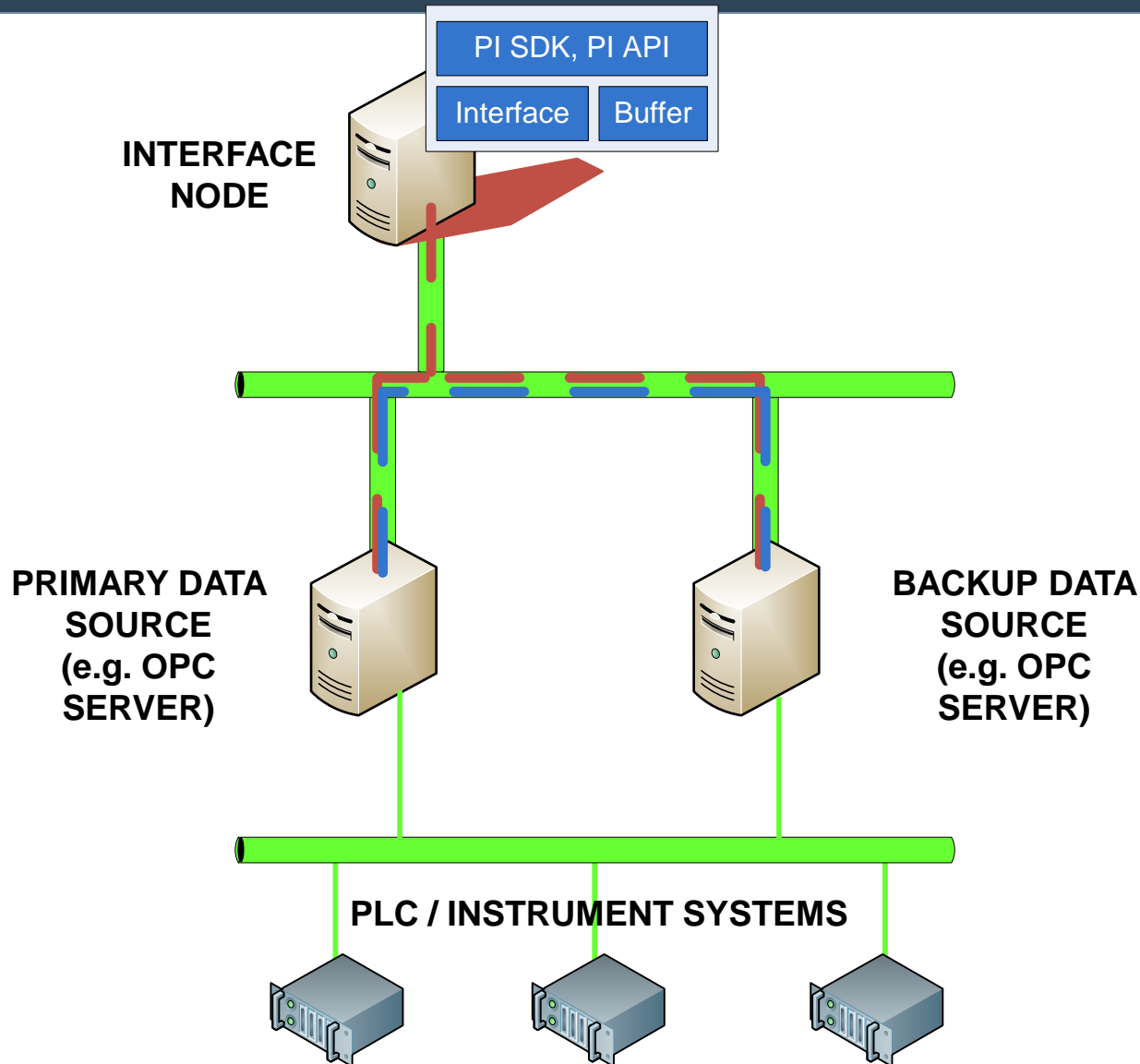
Built-in Benefits of HA PI

- PI is there all the time – users trust it

- No late night heroics to restore a backup or perform routine maintenance

- Removes fear of a bad backup

- Simple design is robust, low bandwidth and supported by WANs

- Geographical independence (replace PI to PI)

- Support more or specialized users

- Facilitates capacity planning

- Complements virtualization strategies:

  - PI is perfect for monitoring a virtualized environment (HyperV performance counters; VMWare SNMP interface)

Customer Examples: HA

- Transmission & Distribution customers cannot lose visibility or the grid can go down (e.g., Cal ISO)

- Customers with dispersed sites can deploy collective members in each location for better client retrieval performance without losing synchronization (International Paper)

- Customers want to balance the load of data retrieval by many users (PJM, Cal ISO)

- Customers need to aggregate data into one large PI system (PSE&G)

- NRC 5-node collective

- Load Balancing and Failover for virtual machines

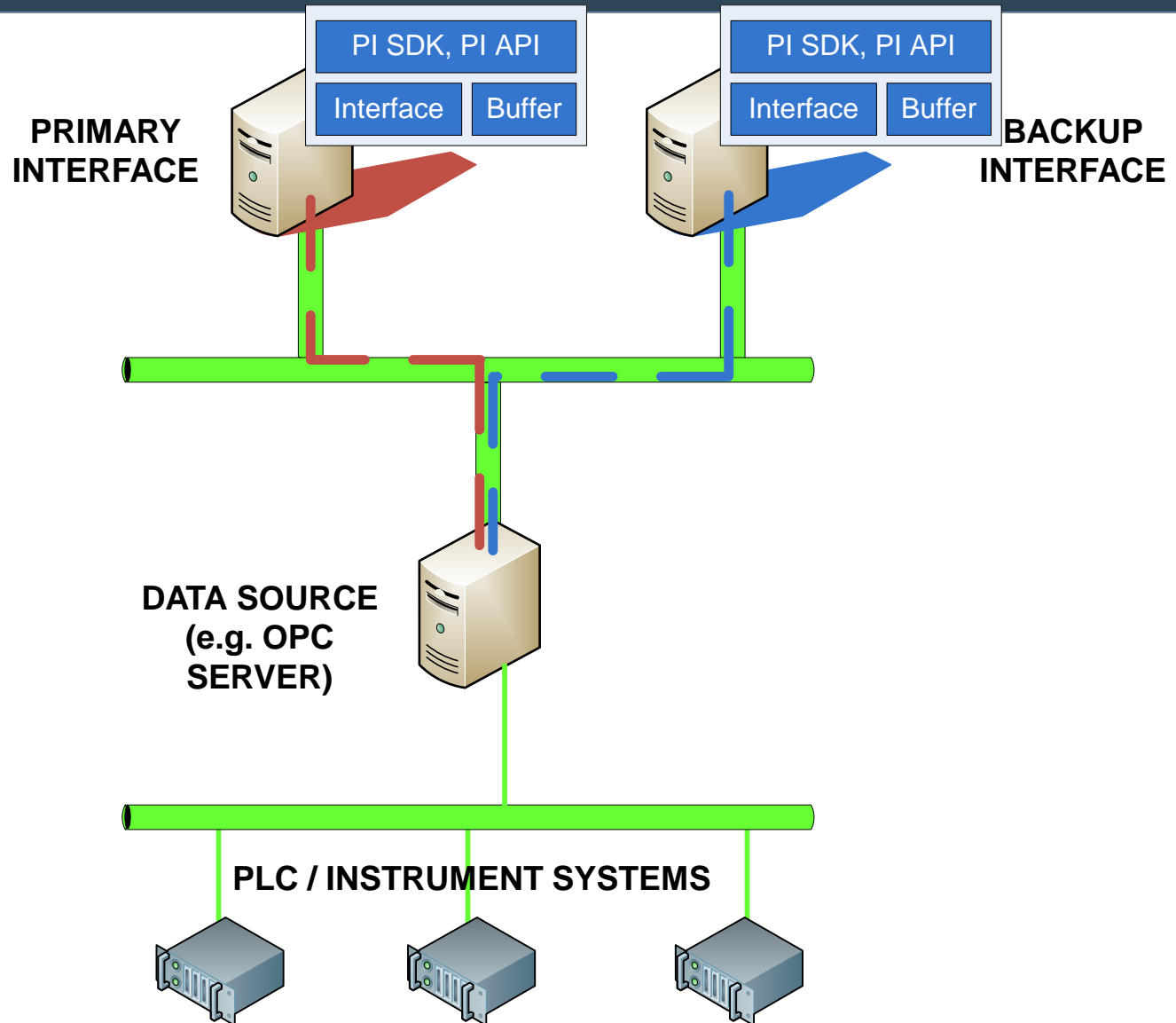- NERC CIP: dedicated PI server inside the security perimeter
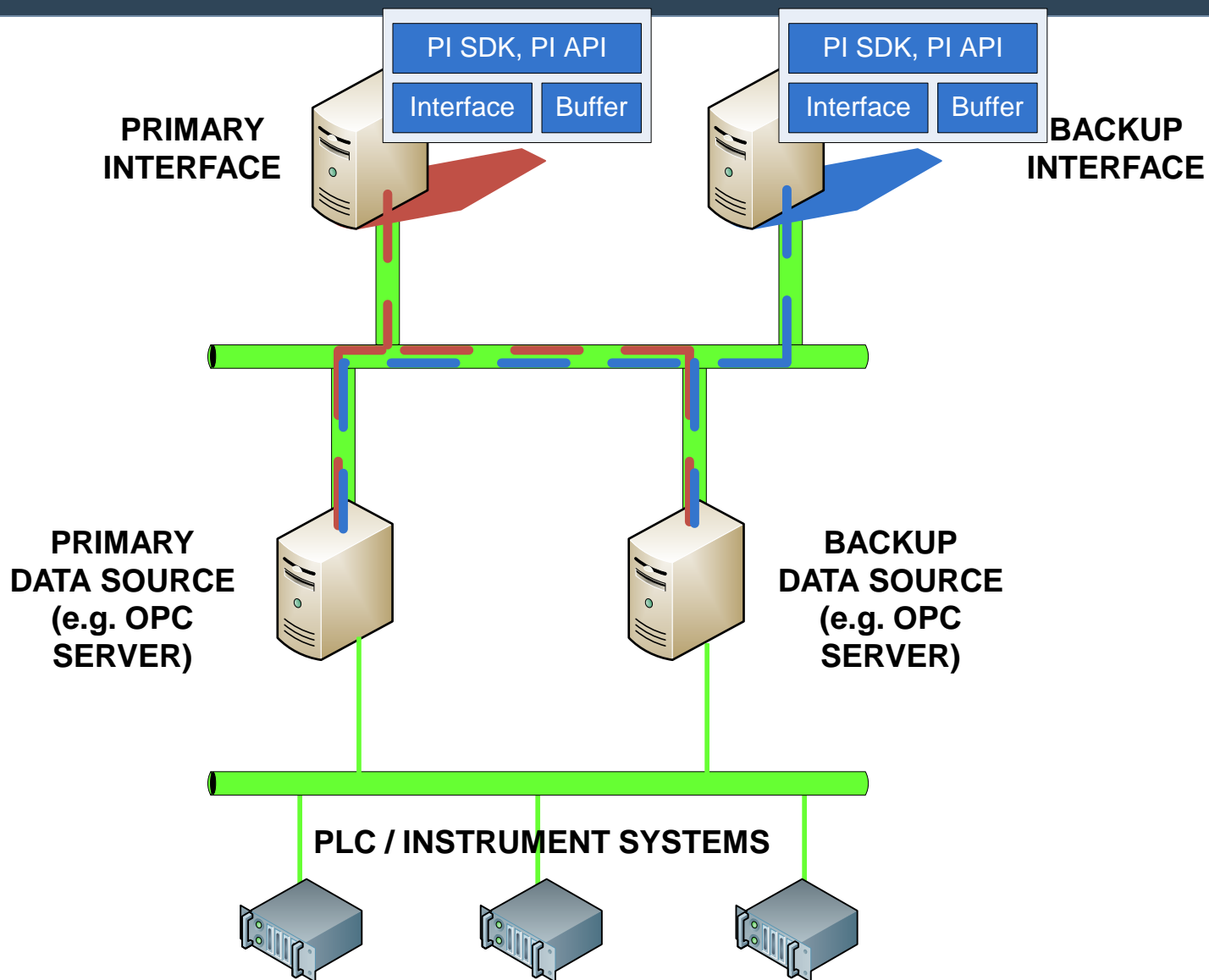
PI Interface Failover

Empowering Business in Real Time.

Native Data Source Failover for Data Collection

Empowering Business in Real Time.

Interface Failover for Data Collection

PRIMARY INTERFACE

BACKUP INTERFACE

PI SDK, PI API

Interface | Buffer

PI SDK, PI API

Interface | Buffer

DATA SOURCE (e.g. OPC SERVER)

PLC / INSTRUMENT SYSTEMS

Combination of native Data Source and Interface Failover

OSIsoft.

| PI SDK, PI API |
| Interface | Buffer |

| PI SDK, PI API |
| Interface | Buffer |

PRIMARY INTERFACE

BACKUP INTERFACE

PRIMARY DATA SOURCE (e.g. OPC SERVER)

BACKUP DATA SOURCE (e.g. OPC SERVER)

PLC / INSTRUMENT SYSTEMS

Empowering Business in Real Time.
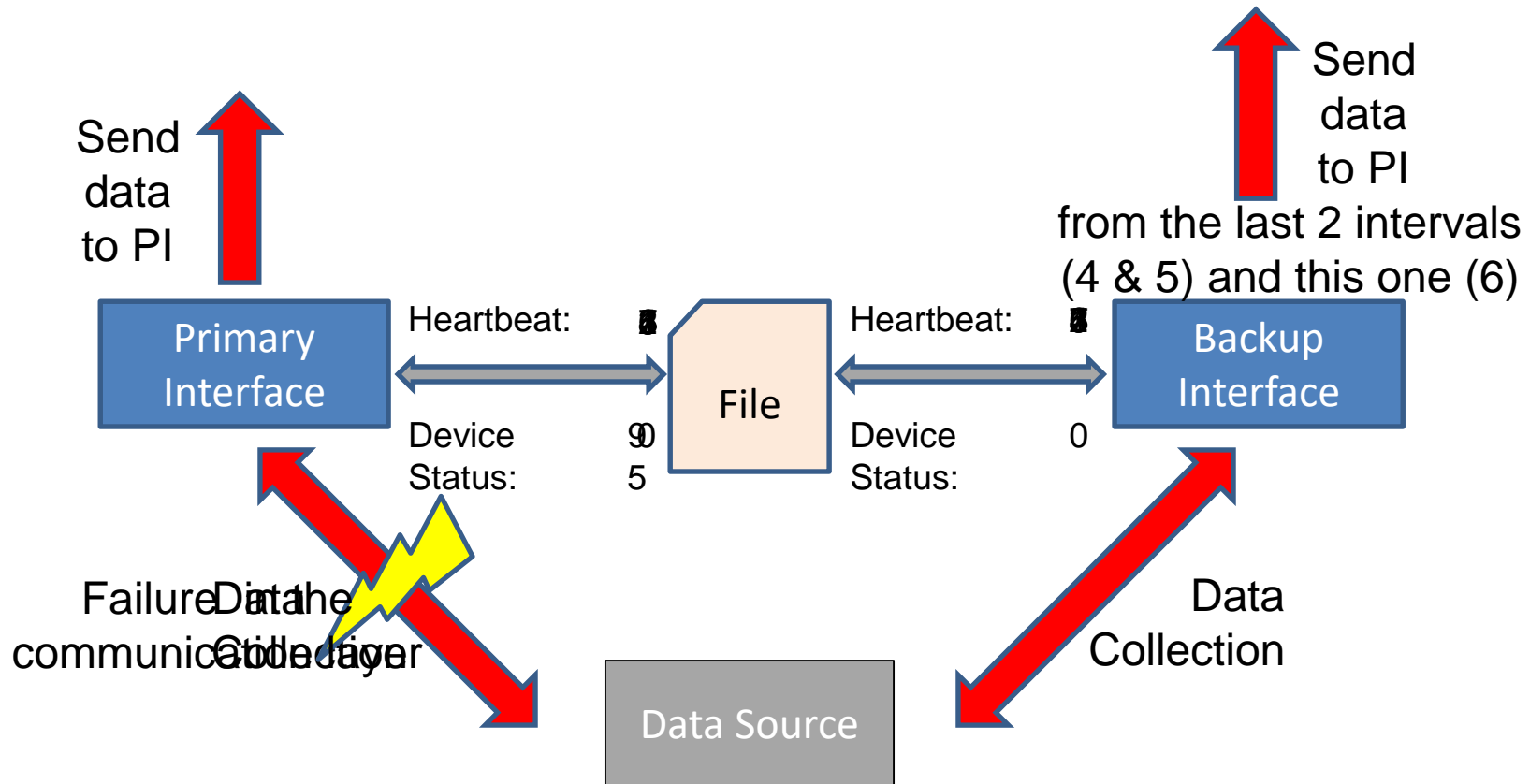
Types of Interface failover

- Phase 1

  - Maintains heartbeat via source data system

  - Only available for selected interfaces

- Phase 2

  - Maintain heartbeat via shared file

  - Many interfaces implement

  - OSIsoft recommended

Empowering Business in Real Time.

- Interface failover provides

  - 2 instances collecting the same data from the data source.

  - Communication mechanism between 2 instances of the interface.

  - Backup interface is sleeping; it means no data is sent to PI.

  - If one fails the other will recognize it, wake up and start sending data to PI.

Send data to PI

Primary Interface

File

Backup Interface

Data Collection

Data Collection

Empowering Business in Real Time.

PI Interface Failover
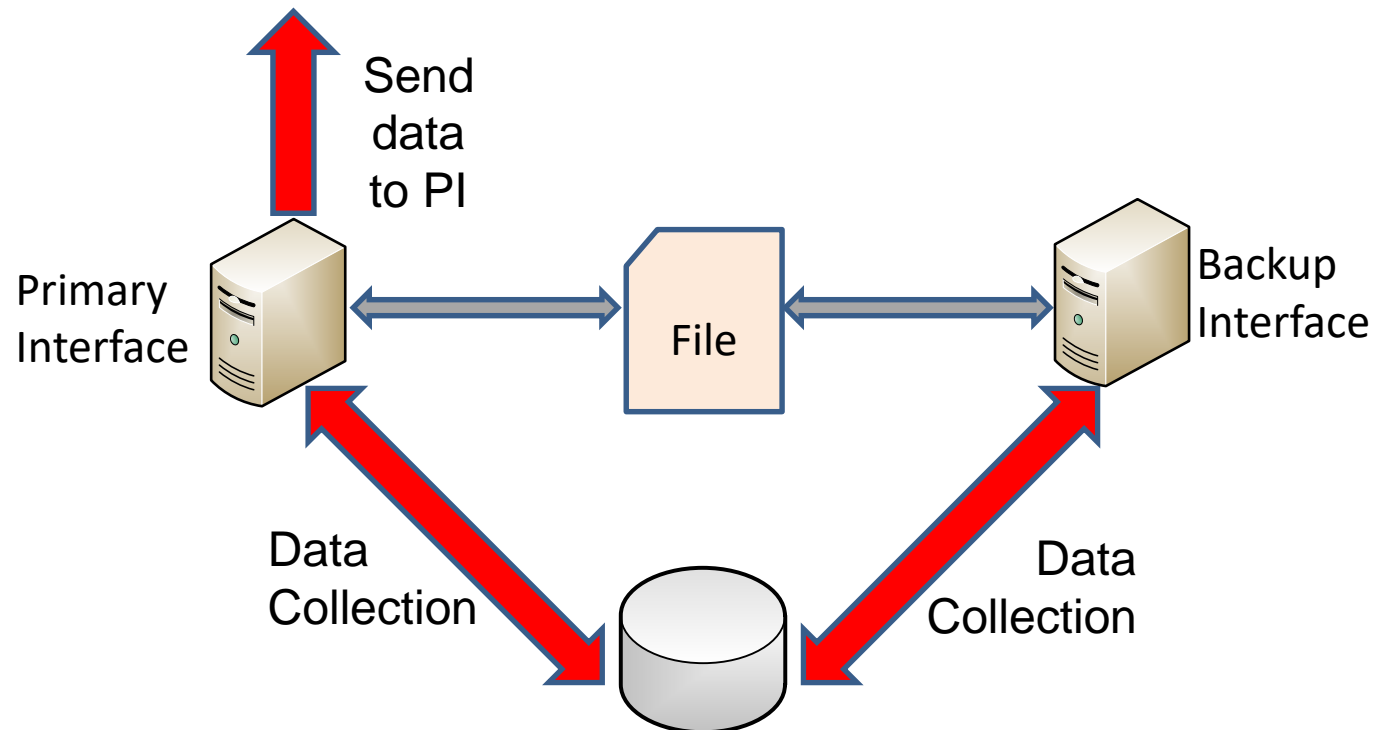
- Signals updated by both nodes at a defined frequency to the shared file and the PI Server:

    - Device Statuses

    - Heartbeats

    - Active ID

- 3 types of failover

    - **Hot** = Primary node sends data, secondary one does not send but has the data. There is no data loss.

    - **Warm** = Secondary node is connected, points are loaded but no collection is performed. Minimal data loss is possible.

    - **Cold** = Secondary node is only connected to the data source but nothing is done. Some data loss is possible.

Hot Failover Example

Send data to PI

Send data to PI from the last 2 intervals (4 & 5) and this one (6)

Primary Interface

Heartbeat:

File

Heartbeat:

Backup Interface

Device Status: 90 5

Device Status: 0

Failure in the communication Code layer

Data Collector

Data Collection

Data Source

Timeline : 3 5 (interval)

Possible overlap of data during intervals 4 and 5

Prerequisites

- Make a plan

  - Verify if the PLC and/or instrument systems can support doubling the requests on the automation network.

  - Determine the heartbeat interval. Need to ensure that it is long enough to prevent false failover.

- Hardware will be needed.

  - Other computers for the file sharing system for heartbeat and the backup interface node.

  - Supplemental networking equipment.

  - 3rd party software and hardware might be required.

  - Licenses may have to be upgrade to manage more than one connection to the data source.

- Security

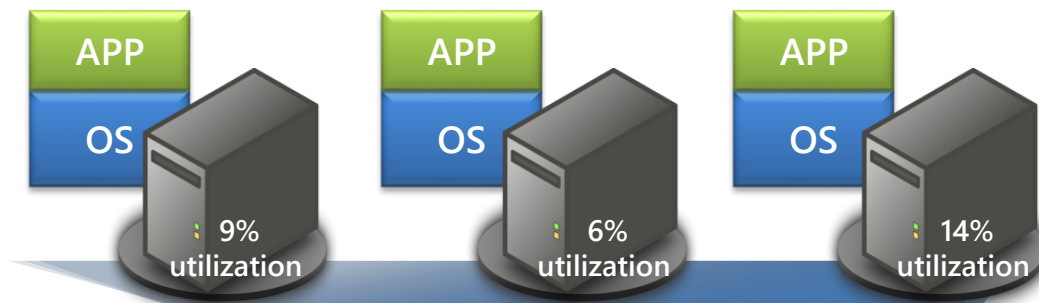 - Manage the security on computer for the file sharing system.

Empowering Business in Real Time.

PI and Virtualization

Empowering Business in Real Time.

Virtualization

- Servers

- Storage

- Applications

Empowering Business in Real Time.

Server Virtualization

- Instead of having physical machines, virtual servers run on a physical host

- Case Study: AtlantiCare

  - Eliminated need to expand or relocate data center

  - Microsoft® Virtual Server 2005 used to consolidate infrastructure and legacy application servers

 - Consolidation ratio achieved of 33:2
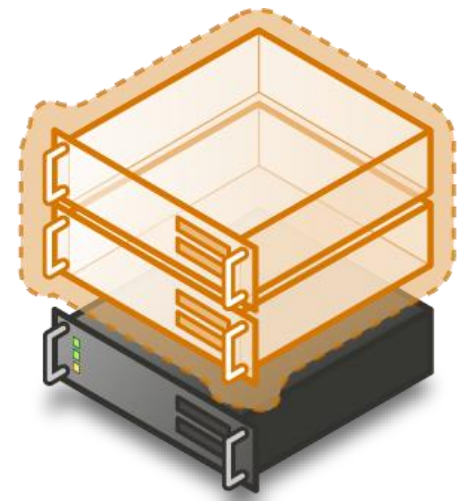
Example: Server Consolidation

APP	APP	APP
OS	OS	OS

9% utilization 6% utilization 14% utilization

APP	APP	APP
OS	OS	OS

30% utilization

Typically server workloads only consume a small fraction of total physical server capacity, wasting hardware, space, and electricity

Through virtualization, these workloads can be consolidated onto fewer physical servers, saving resources and increasing flexibility

Empowering Business in Real Time.
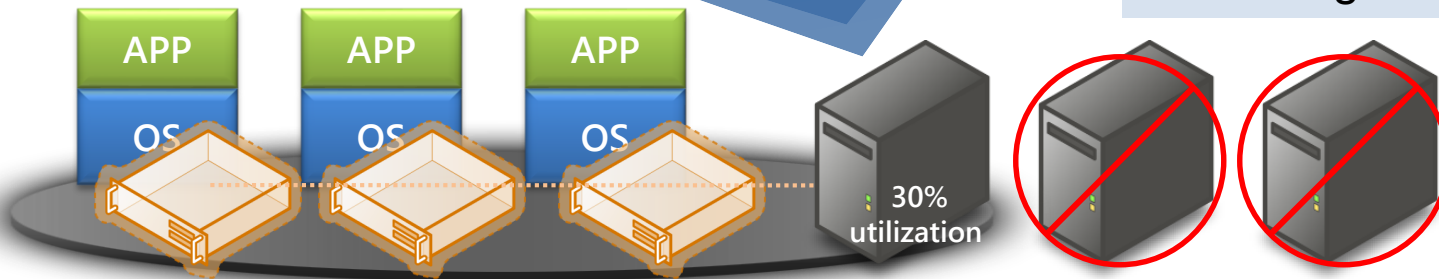
Benefits of Server Virtualization*

- Less hardware required (HP went from 85 data centers to 6)

  - up to 35% reduction of annual server costs per user ($100-$200K per year per server)

- Better utilization of hardware (HP decreased servers by 40%)

- Reduce power consumption (HP reduced energy by 40%)

- Provide higher availability by supporting redundancy

- Rapidly deliver adaptive and reliable IT services

- Tie diverse components together into a single managed entity

- Storage efficiency can lead to higher storage utilization

*Gillen, A., Grieser, T., Perry, R. 2008. Business Value of Virtualization: Realizing the Benefits of Integrated solutions. IDC.

Empowering Business in Real Time.
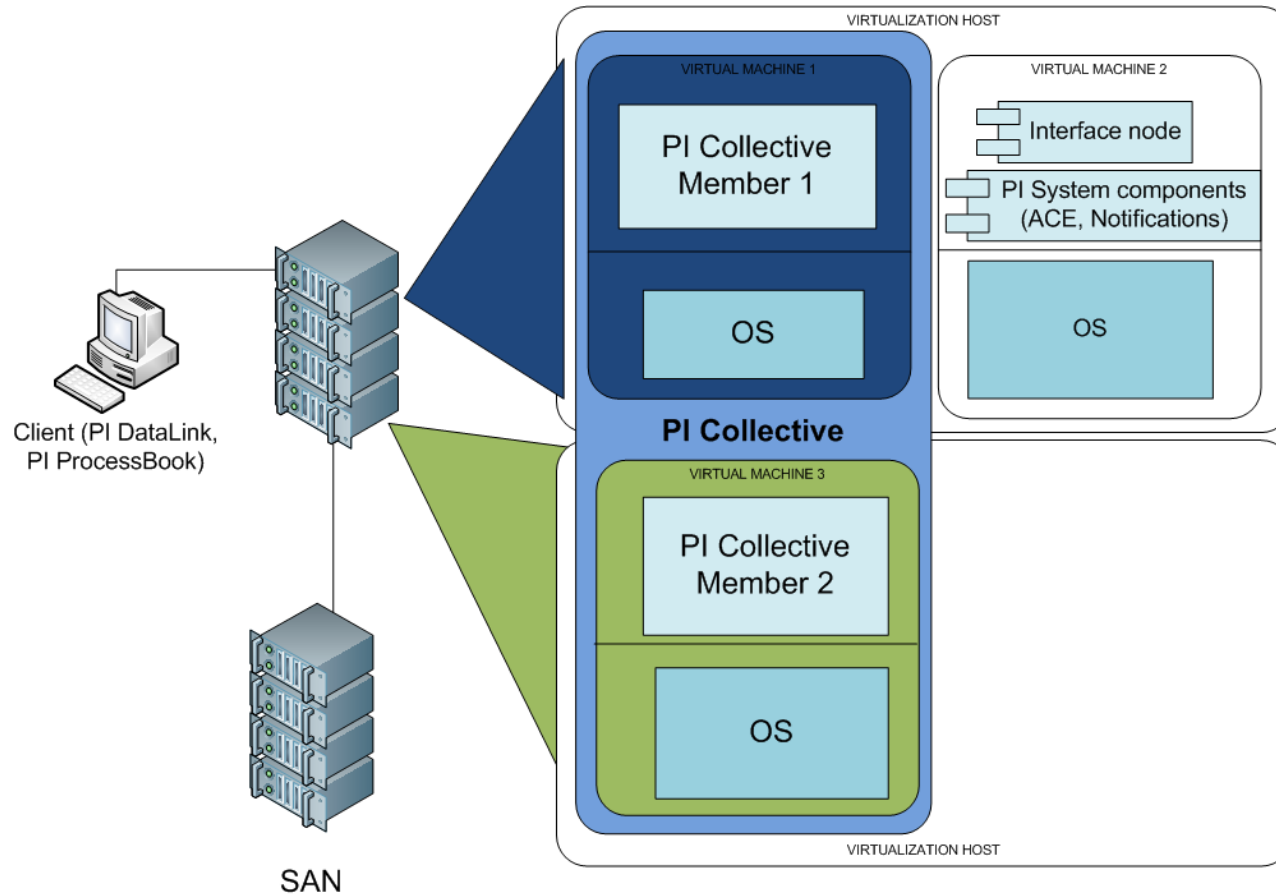
- Multiple hosts (cluster)

- Collective can be split across hosts

- PI Server components can run as separate virtual machines for scalability and performance

- SAN can offload storage

PI and Server Virtualization
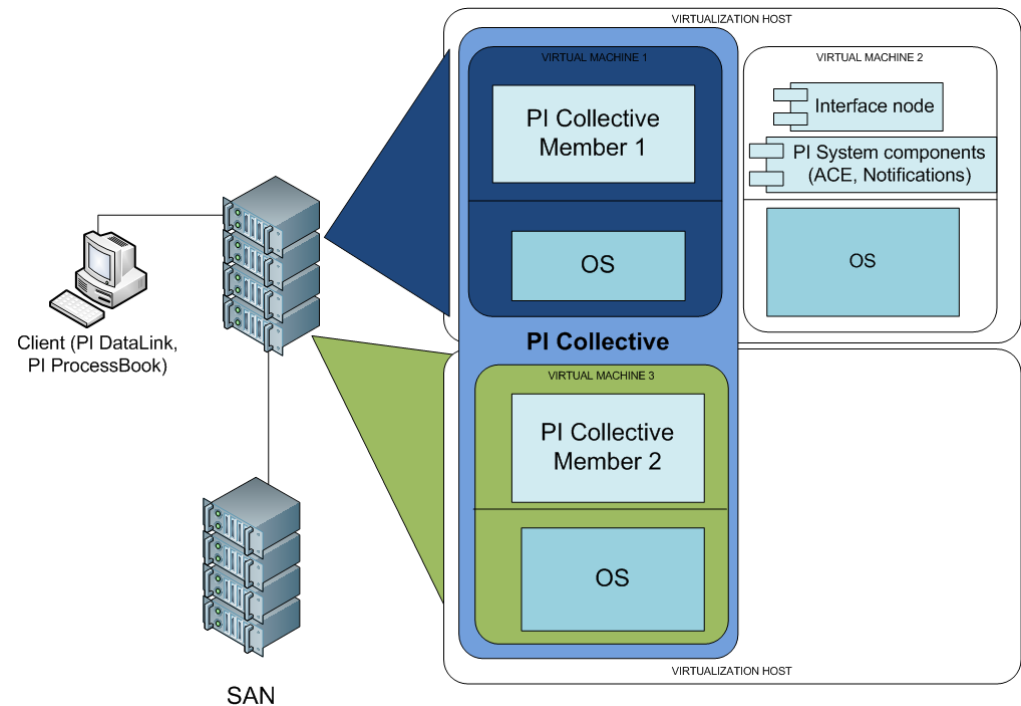
- Validated environments need a test bed (any pharmaceutical company; BMS; Shell)

- Environments that require portability of IT assets (Cargill Deicing Technology – Salt mining)

- Deploying new sites (Rio Tinto)

- Flexibility in assigning resources (OSIsoft NOC for monitoring EA PI Systems)

Empowering Business in Real Time.

Storage Virtualization

- **Challenge**:
  Grow available storage space without disrupting applications and servers

- **Solution**:
  Storage Area Networks (SAN) allow dynamic sizing of available storage

Data Store

Server A

Server B

Empowering Business in Real Time.

Benefits of SAN Technology
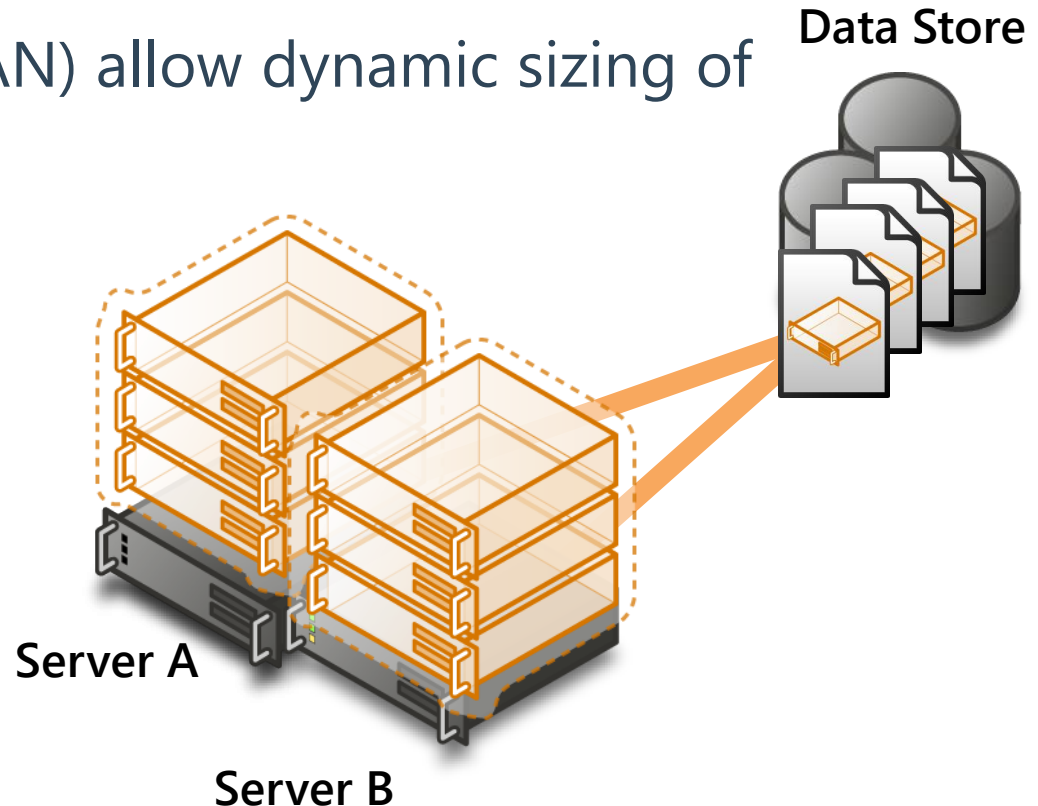
- Additional storage appears to be local to the host so users don't have to know where the files are stored

- Improve the ties between centralized storage and virtual infrastructure

- Provide virtual-machine consistent backups for data stores and the ability to restore virtual machines in a few clicks

- Provide relief from disk subsystem access in virtualized environments (biggest performance hit on virtual host)

- Consolidate disk resources

Empowering Business in Real Time.

PI and Storage Virtualization

- Keep more and higher fidelity data online; add or expand PI archive files

- Support aggregated PI Systems; VSS support enables PI backups

- Store PI Client files centrally

- Backup virtualized application and data servers

- Backup virtualized Terminal Server hosts

- Complete system backup storage

Empowering Business in Real Time.

Empowering Business in Real Time.
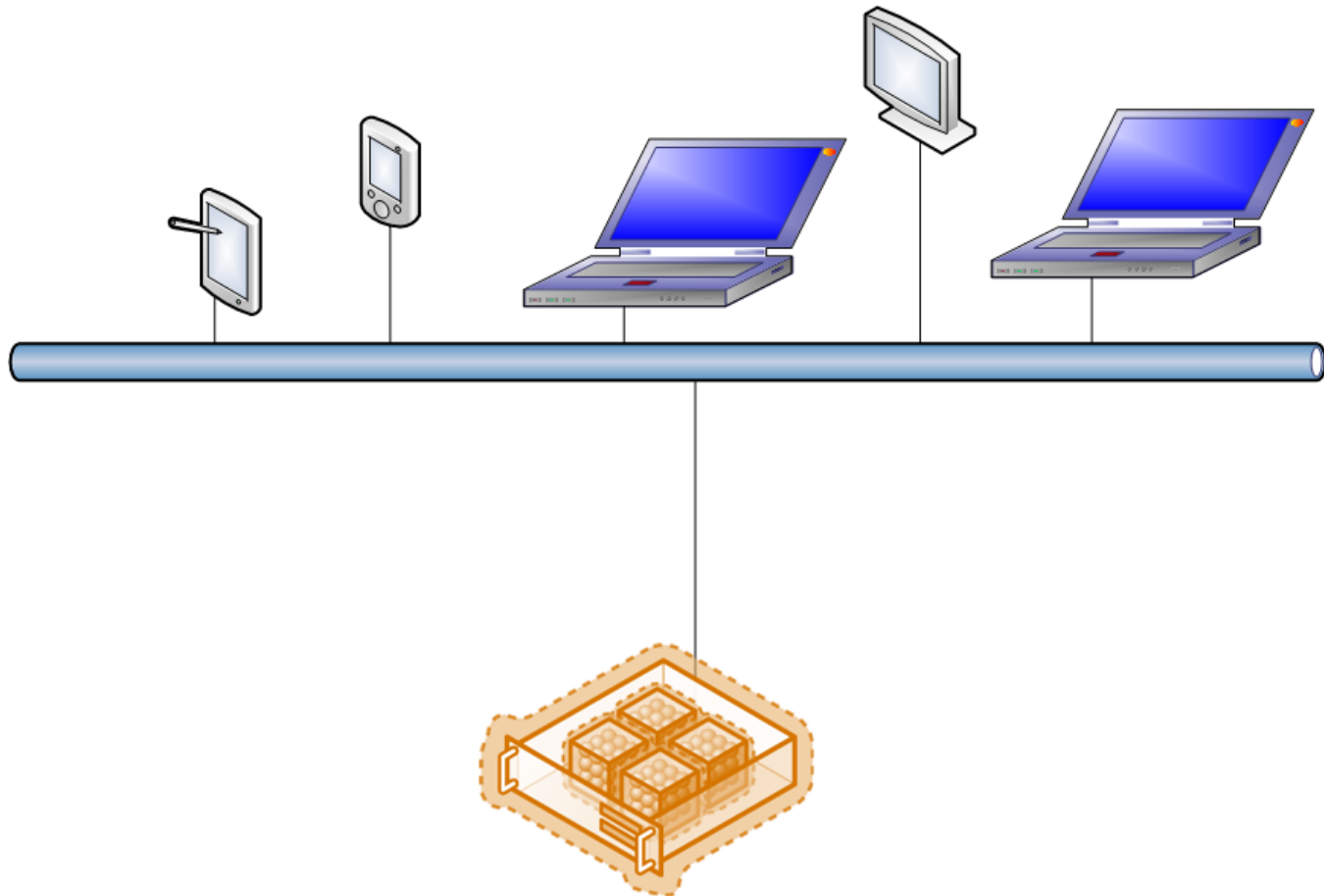
Application Virtualization
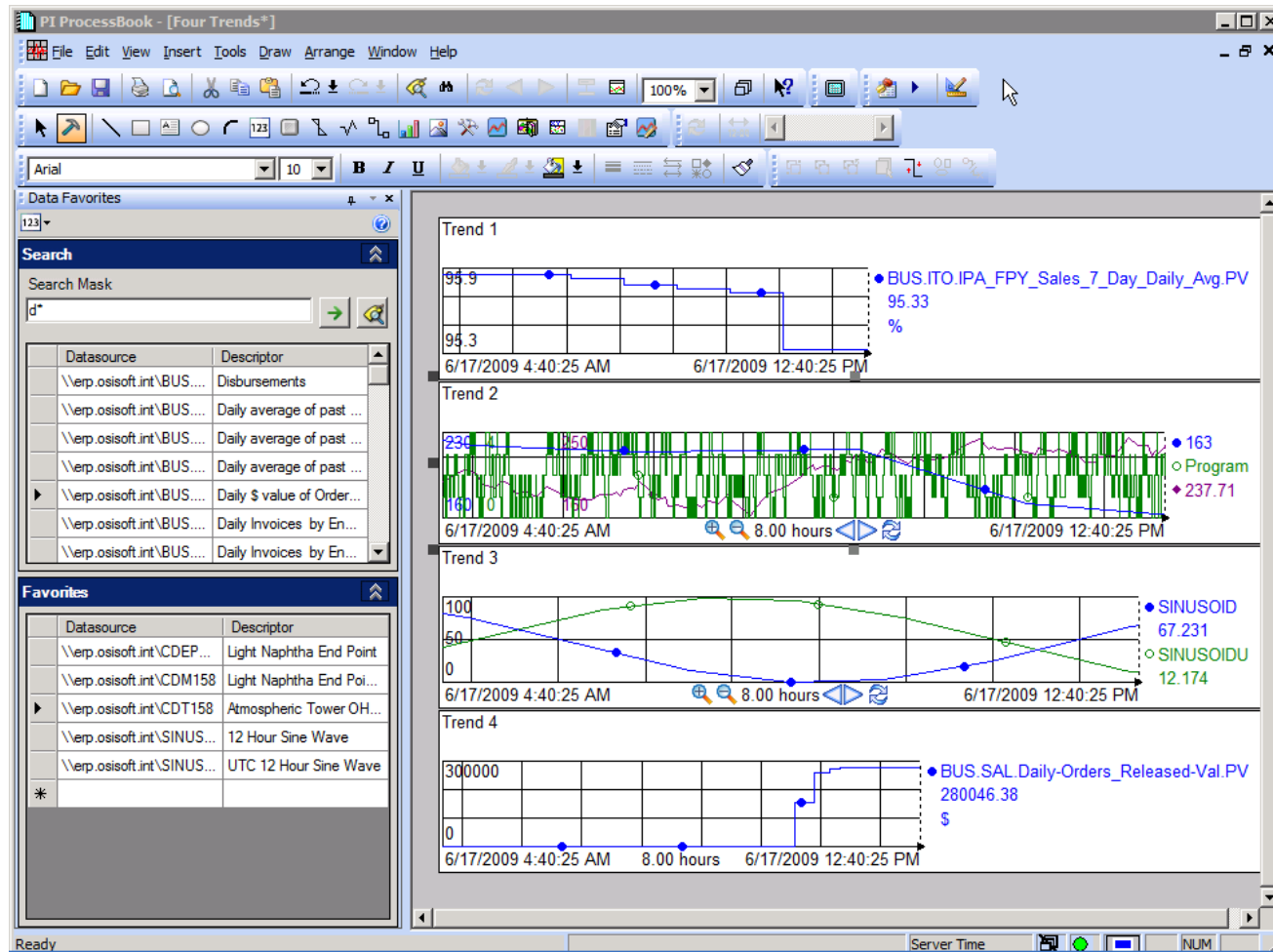
- Customers currently use Citrix or Terminal Server to reduce deployment costs and maintenance for client apps

- Windows 2008 Server offers a service that provides applications over an SSL connection (HTTPS) without client-side deployment (a thin deployment) – Terminal Services Gateway

- Terminal Services Gateway provides URL access to a host (like Remote Desktop connections, without the VPN requirement) or to specific applications on a host (even more secure for those outside the firewall)

Empowering Business in Real Time.

Benefits of Application Virtualization

- One point of installation makes deployment simpler

- Access to applications secured

- All users have the same version of the software; no version or compatibility issues

- Casual users do not need to install anything to get started

- Save money on hardware upgrade investments by deploying client software in one place

PI and Application Virtualization

- Environments with casual client users who need low barrier to entry for system access (Inco Limited)

- Terminal Server users (a partial list)

  - Georgia Pacific, Kellogg, SASO, SAPPI Fine Paper, Wacker Chemie, Alcoa, Eli Lilly, ExxonMobil Upstream, Iberdrola, Progress Energy Services

- Citrix users (a partial list)

  - SDG&E , Water Corporation, Amgen, Bayer Material Science, Genmab, PPG, Vaxgen, Katahdin Paper, Celanese Chemicals, Novo Nordisk, Queensland Alumina, Total

- Windows 2008 Terminal Services Gateway

  - OSIsoft

Empowering Business in Real Time.

Five Principles for Virtualization Success*

- Treat virtual machines as if they were physical machines

- Invest in Enterprise-level hardware and software

- Do not mix virtual and physical on the same host

- Use qualified Virtualization support personnel

- Test on the target platform

*OSIsoft Center of Excellence

Benefits: PI in a Virtualization Project

- PI works as well in a virtual environment as it does on physical hardware

- PI is perfect for monitoring a virtualized environment

- If you are thinking about virtualization, it's a good time to consider the value of HA PI

- If you are thinking about network storage, it's a good time to consider the value of virtualization and PI with SAN support

- If you are thinking about problems with client software deployment, it's a good time to consider the value of Terminal Services Gateway, virtualization and PI

Empowering Business in Real Time.

Benefits of PI in a Virtualization Project

Value of HA PI

| Availability, Quality of Service (QoS) | No data loss | Scaling | Improved IT management |

Value of Virtual Machines and SAN

| Consolidation | Scaling and hardware utilization | Centralized IT management |

Higher Quality of Service for Less Cost

More Information

- Whitepapers and Tech Support bulletins on OSIsoft web site

- Vendor web sites

- OSIsoft internal expertise

- Microsoft representatives for Hyper V and Terminal Server Gateway solutions

Empowering Business in Real Time.

Thank you