Regional Seminar Series

Chicago, IL

Architecture and Best Practices: Recommendations for PI Systems

Ken Marsh
COE Engineer
OSIsoft, LLC

12 October, 2010

Empowering Business in Real-time.

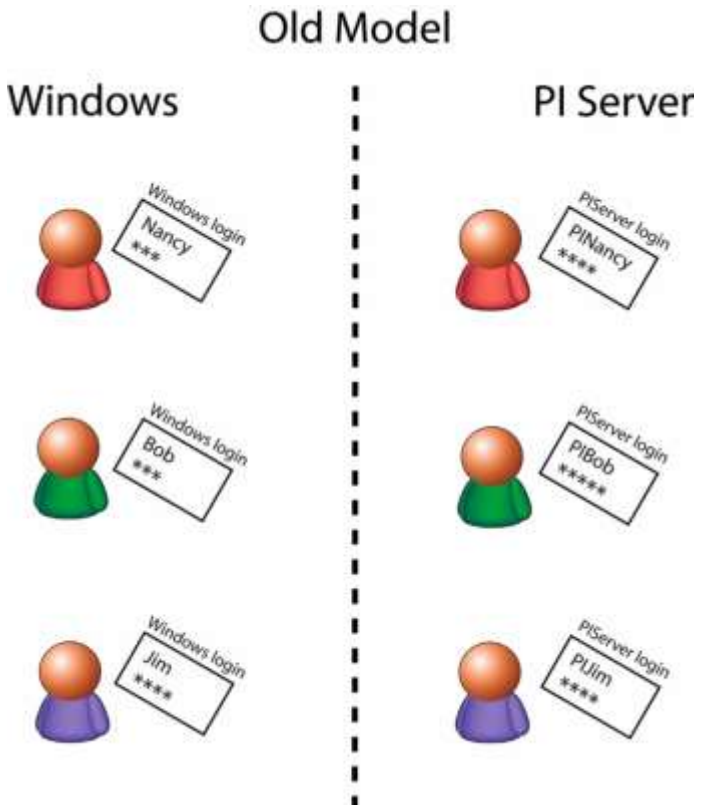
Overview

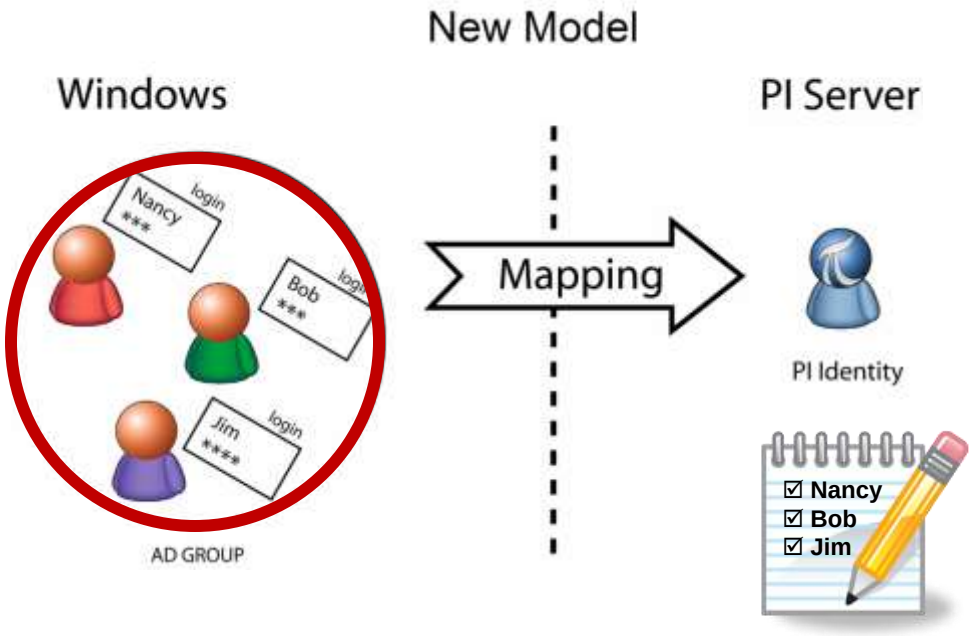
- PI Server with Windows Integrated Security (WIS)
- PI Server High Availability
- PI Interface High Availability
- Virtualization and the PI System

New PI System Security Concepts

Empowering Business in Real-time.

User Identity in the PI Server

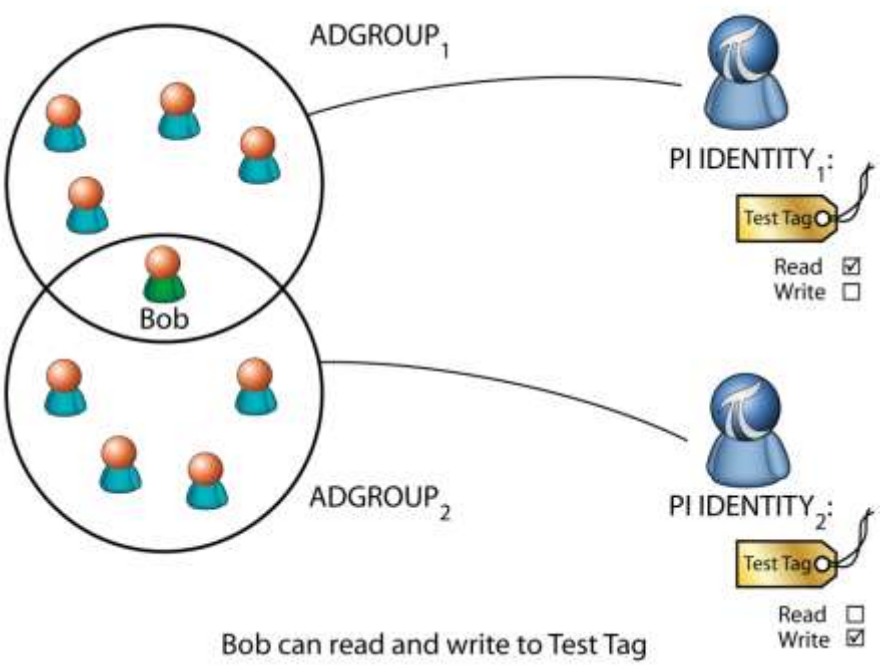


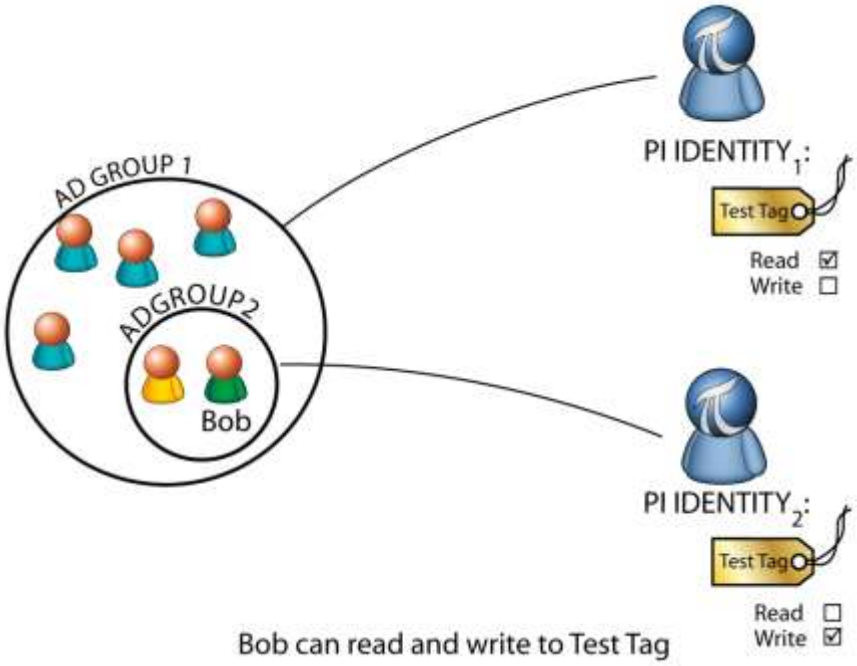


- The security principal is the PI User
- Audit and Change logs reflect the PI User

- The security principal is the Windows User, not a PI User
- Audit and Change logs in the PI Server reflect the Windows User

PI Identities, PI Mappings





- PI Identities = Security Principals within the PI System
  - Examples: PIOperators, PIEngineers, and PISupervisors
- PI Mappings – link AD Groups to PI Identities

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

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
- For non-domain accounts, you can use Windows Local Groups from the PI Server machine
  - Passwords have to match for NTLM authentication

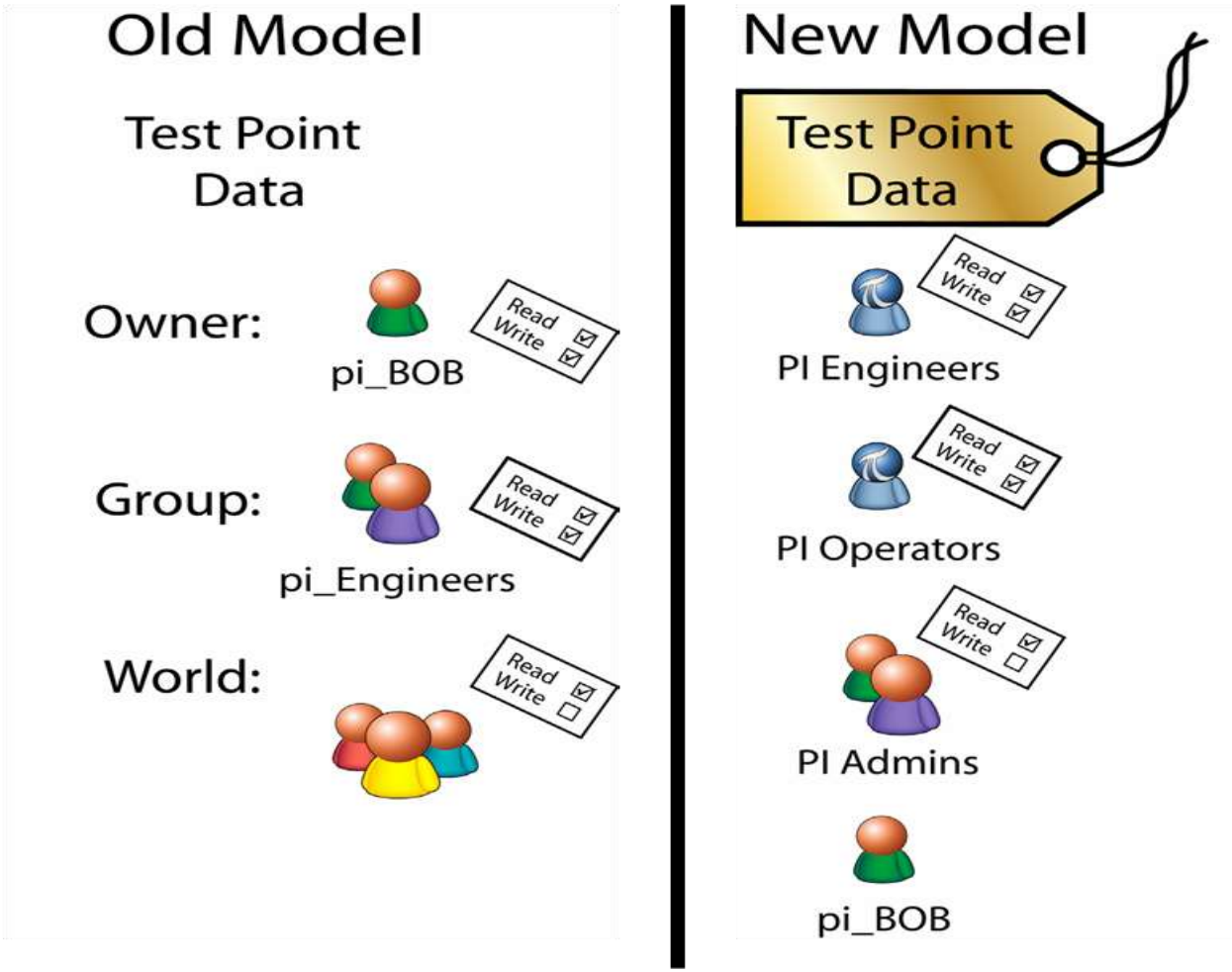
Active Directory Integration

- 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

Identity Planning – Best Practices

- Develop a PI Identity Scheme for your Organization
  - Protect your data
  - Ease of maintenance
  - Organizational separation
  - Standardize
- Consider Kerberos
  - Map AD principals directly
  - Map AD principals to local groups

Object Level Security Model



Empowering Business in Real-time.

Automatic Backward Compatibility

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

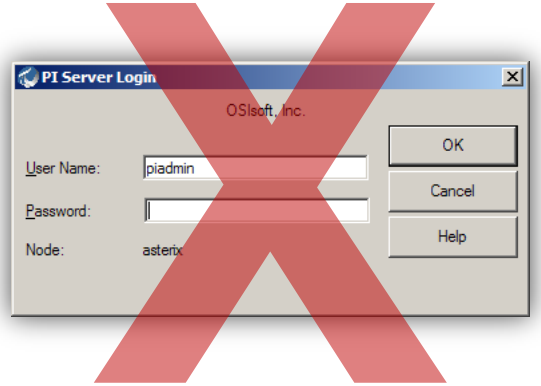
Tag	datasecurity
sinusoid	pi_users:A(r,w) | bob:A(r,w) | PIWorld:A(r)

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

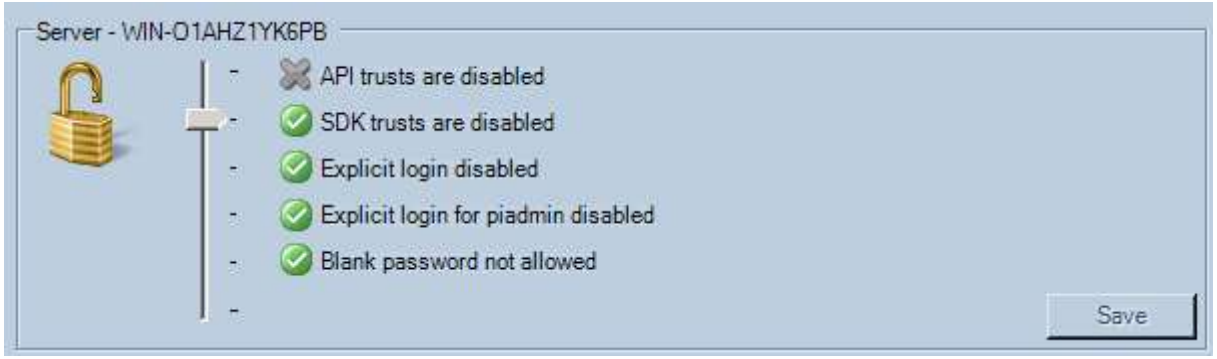
PI Client Considerations

- 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



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



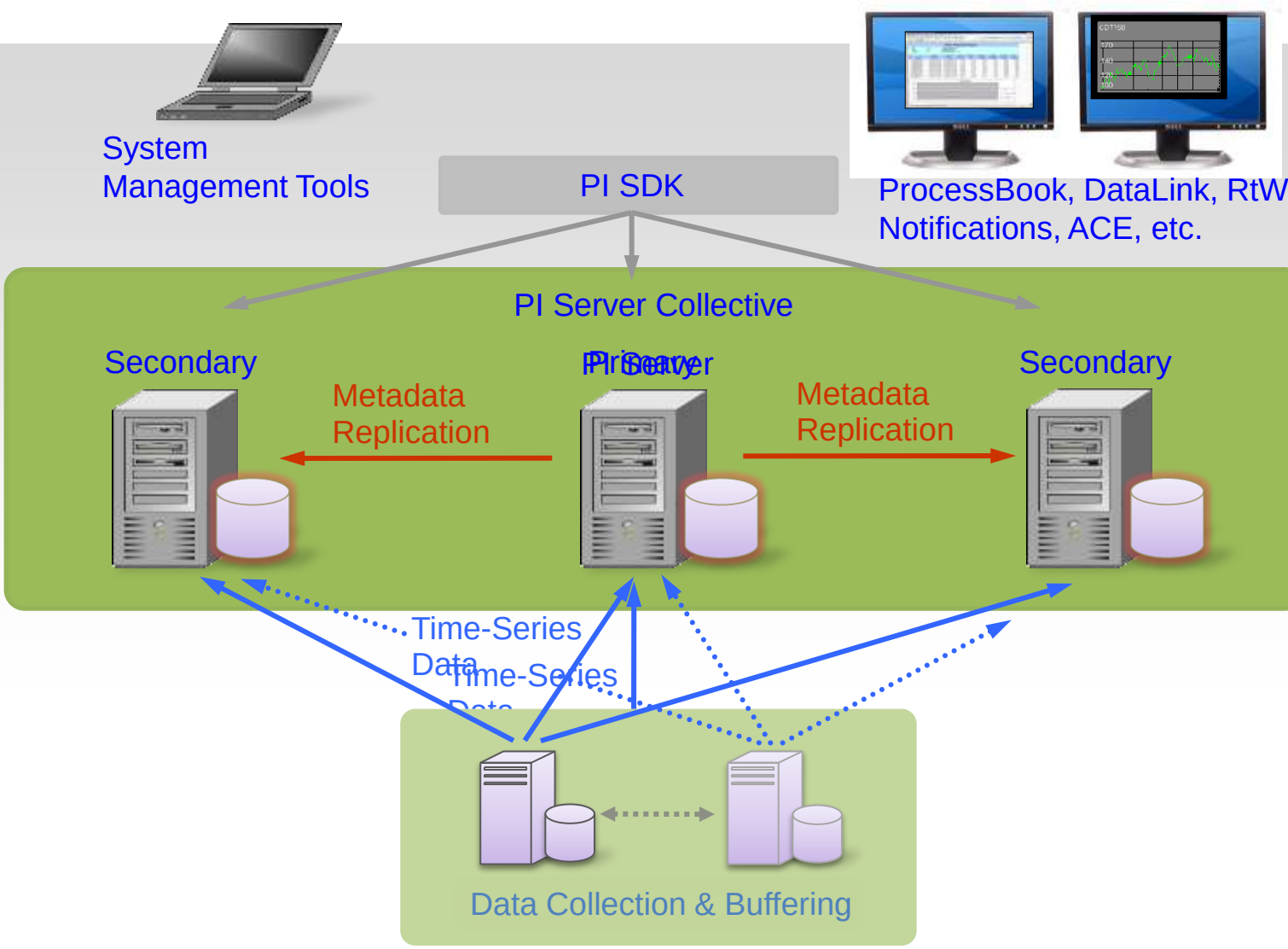
Migration Planning

- 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)

Empowering Business in Real-time.

PI High Availability Architecture



Empowering Business in Real-time.

Built-in Benefits of HA PI

- The PI System is there all the time – users trust it
- No special hardware required
- Routine maintenance less invasive – rolling upgrades
- Simple design is robust, low bandwidth
- Geographical independence
- Complements virtualization strategies:
  - PI can also monitor the virtualized environment (HyperV performance counters; VMWare SNMP interface)

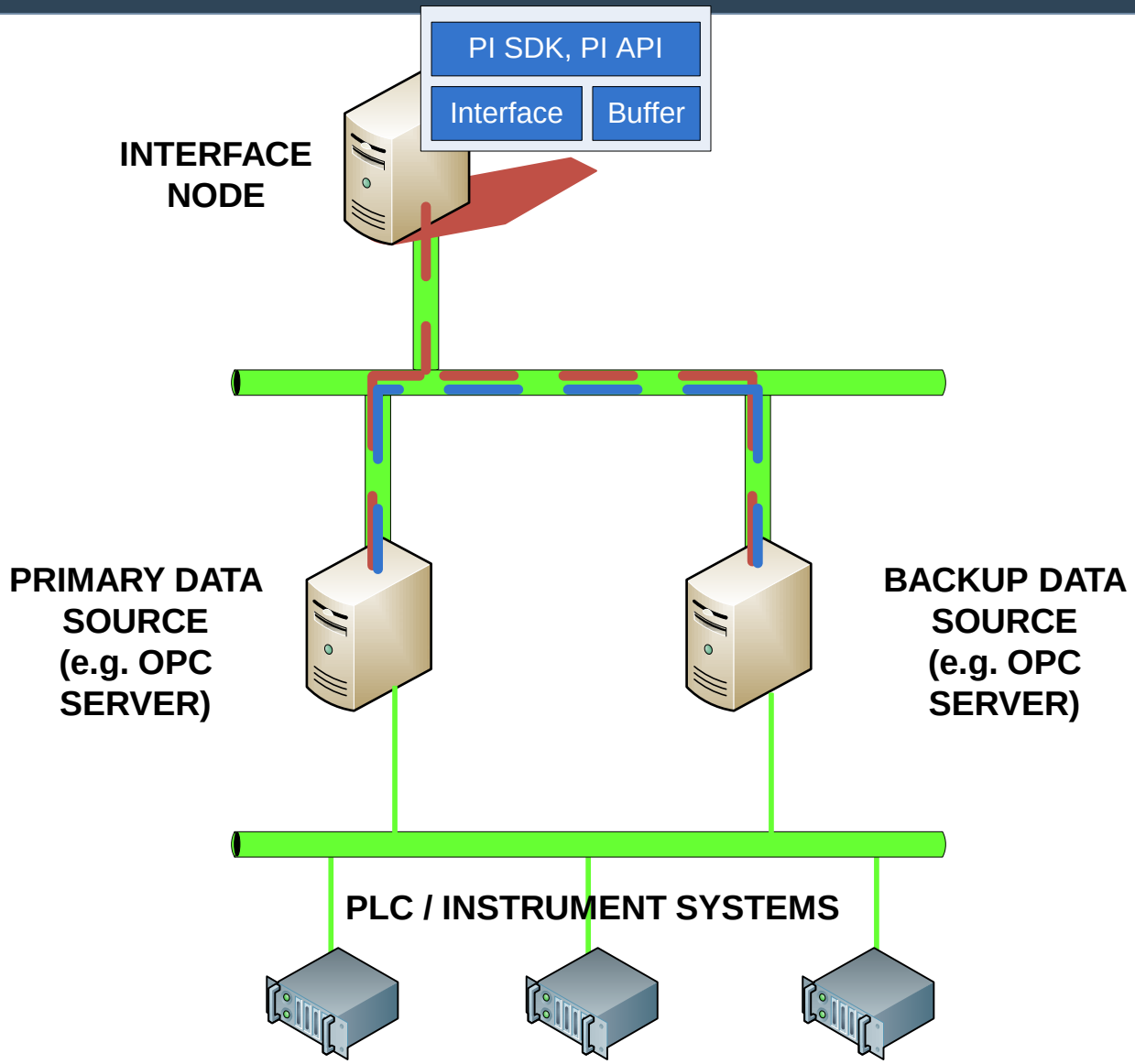
Customer Examples: HA

- Transmission & Distribution – The PI System is mission critical system (e.g., Cal ISO)
- Dispersed sites for better client retrieval performance at all locations (International Paper)
- Load balance the data retrieval by users (PJM, Cal ISO)
- Aggregate data into one large PI System (PSE&G)
- Load Balancing and Failover for virtual machines
- NERC CIP: dedicated PI Server inside the security perimeter

PI Interface High Availability

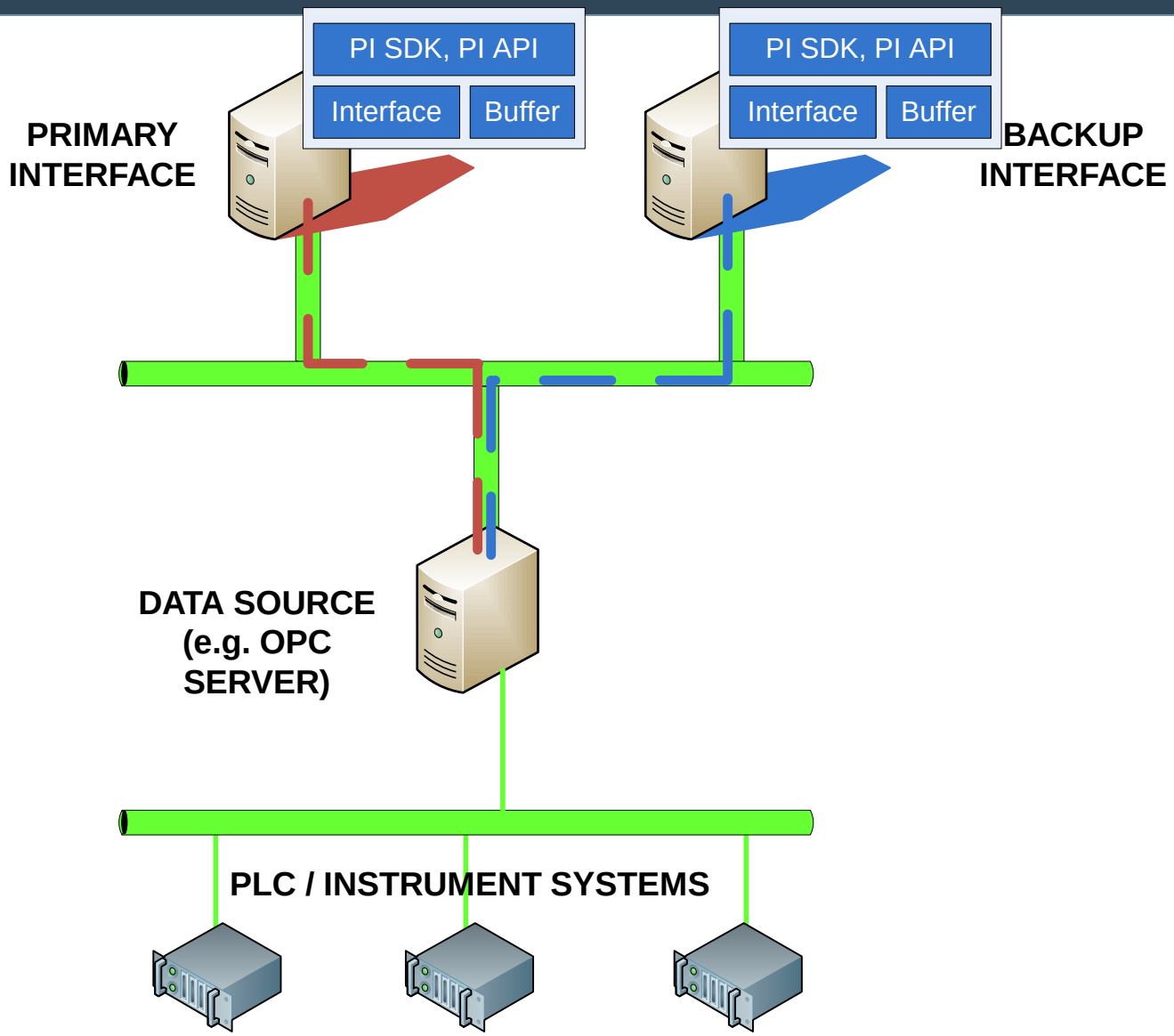
Empowering Business in Real-time.

Native Data Source Failover for Data Collection



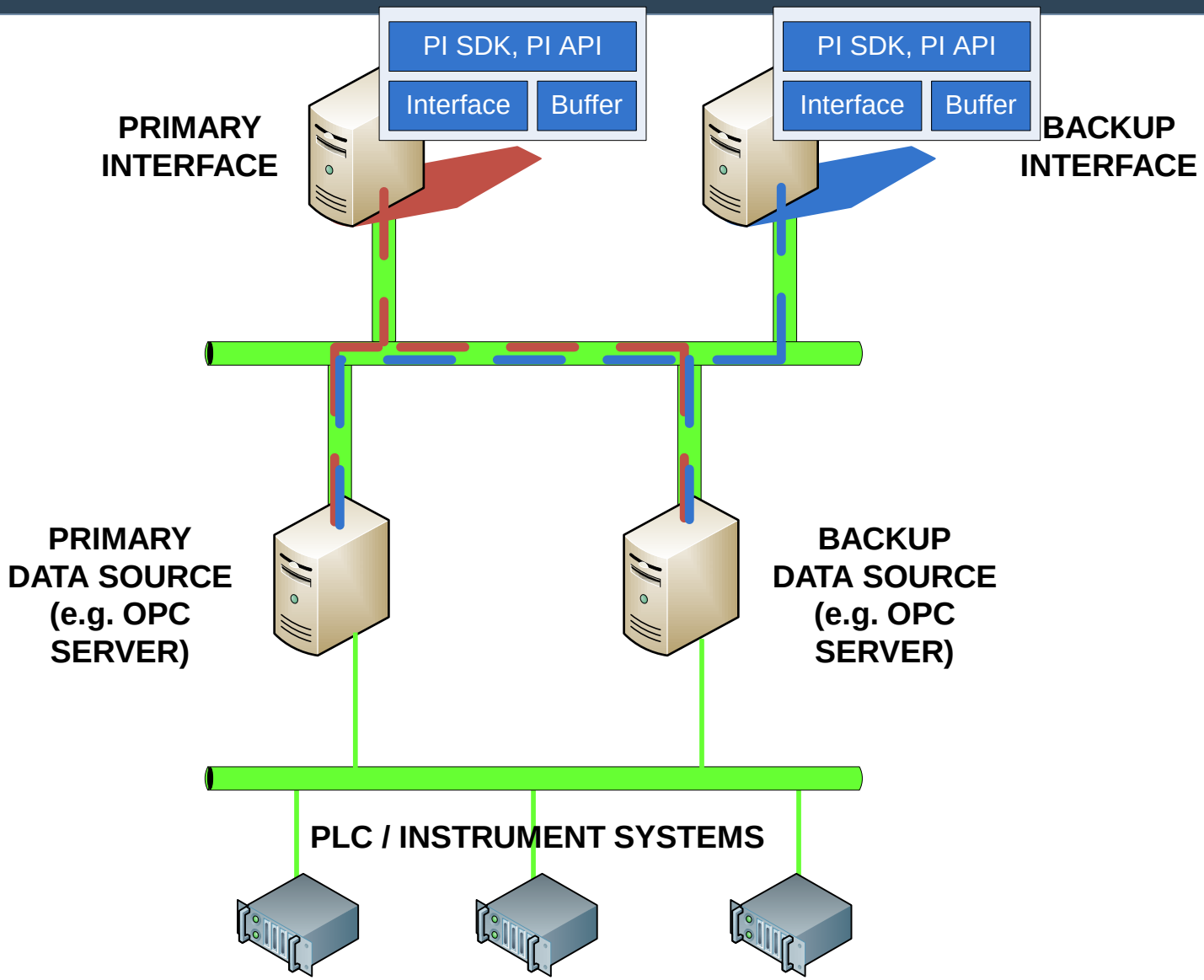
Empowering Business in Real-time.

Interface Failover for Data Collection



Empowering Business in Real-time.

Combination of native Data Source and Interface Failover

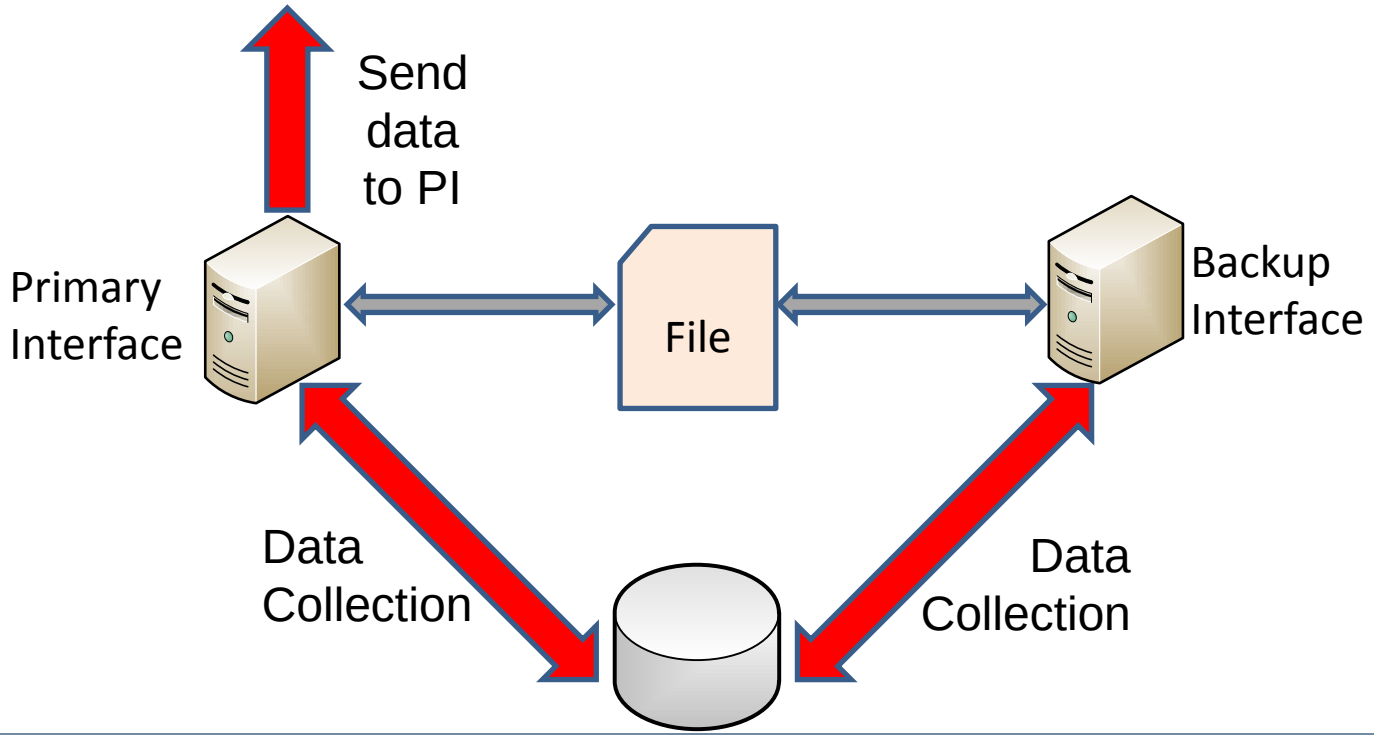


Types of Interface failover

- 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

PI Interface Failover

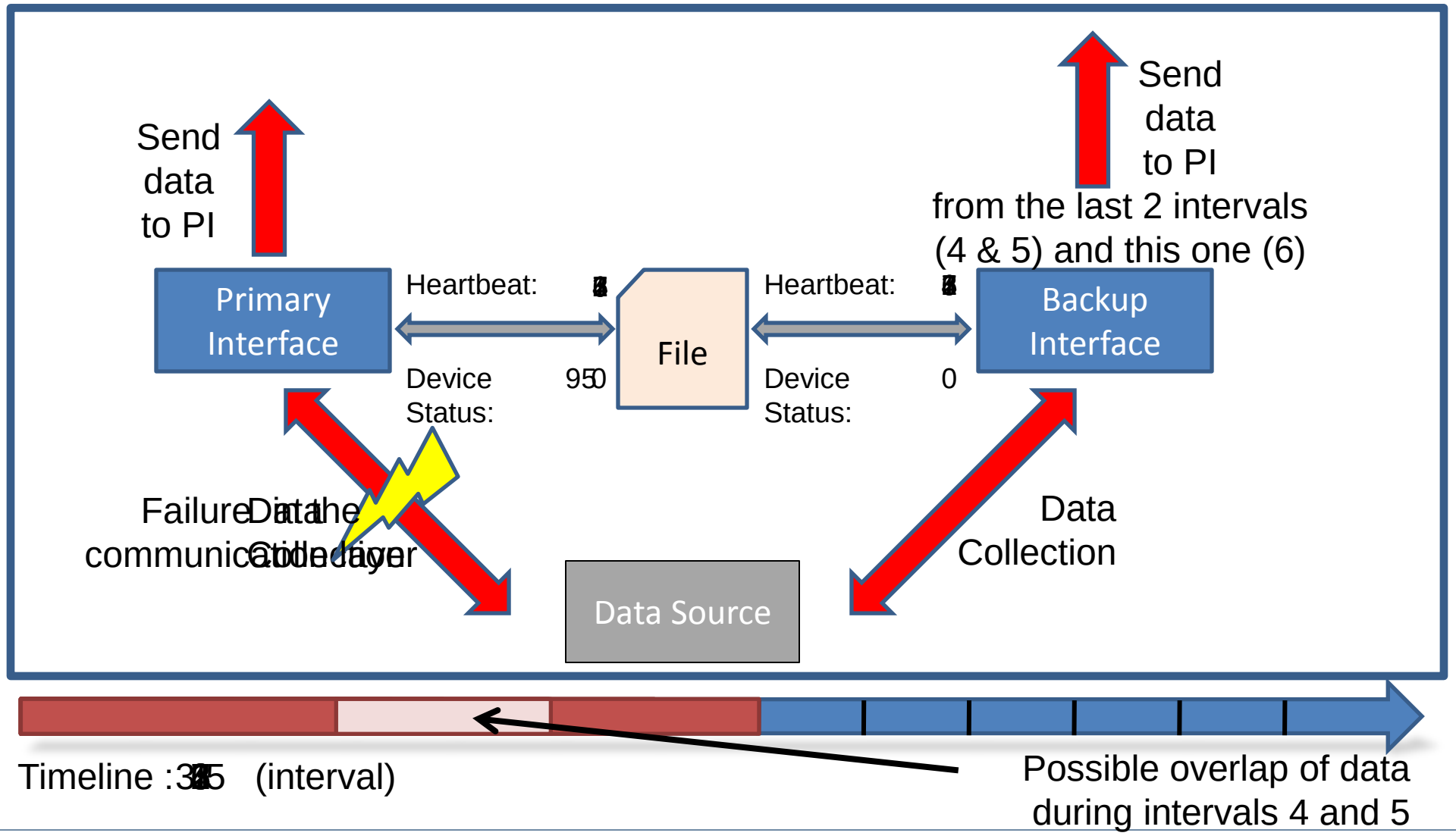
- Interface failover provides
  - 2 instances collecting the same data from the data source.
  - Communication mechanism between 2 instances of the interface.
  - Backup interface is sleeping; it means no data is sent to PI.
  - If one fails the other will recognize it, wake up and start sending data to PI.



PI Interface Failover

- Interfaces “watch” each other’s **Heartbeat** and **Status**
- Failover Types
  - **Hot** = No data loss
  - **Warm** = Maybe data loss
  - **Cold** = Some data lost
    (Hint: minimize data loss by using disconnected startup)

Hot Failover Example



Prerequisites

- Make a plan
  - Verify the PLC and/or instrument systems can support doubling the requests, including license requirements.
  - Determine heartbeat interval. Ensure long enough to prevent false failover.
- Hardware will be needed
  - Computers for file sharing system for heartbeat and the backup interface node.
  - Supplemental networking equipment.
  - 3rd party software and hardware might be required.
- Security
  - Manage the security on computer for the file sharing system.

The PI System and Virtualization

Empowering Business in Real-time.

Virtualization trends in 2010

- Virtualization will affect some part of your PI System if not today then in the near future
  - In 2010 more Operating Systems will be deployed in Virtual Machines than on physical machines – Paul Maritz – CEO VMware
  - Separation between the Hardware, Operating System and Application – In a virtualized environment who controls the Hardware?
  - Virtual Datacenters - Infrastructure as a Service (IaaS)
    - Virtual datacenters are “clouds” of virtual machines that provide computing resources in a utility model
    - Virtual datacenters will be some combination of private clouds and public clouds creating Hybrid clouds

Virtual Machines – Crossing the Performance Barrier

- New Generations of hardware and VM Technology
  - Increasing performance, Decreasing Overhead
    - Most VM's typically between .2-10% overhead
    - Possible to achieve equal performance to physical machines
      - Intel Nehalem processors and AMD-V
  - Find the performance "sweet spot" thru testing
    - Likely between 2-4 vCPU's
    - Storage and its configuration has a high impact on performance
    - Always reserve CPU/RAM for critical applications
    - Don't rely on OS performance statistics use VMKernal level stats
    - Always follow the best practice deployment practices for the application

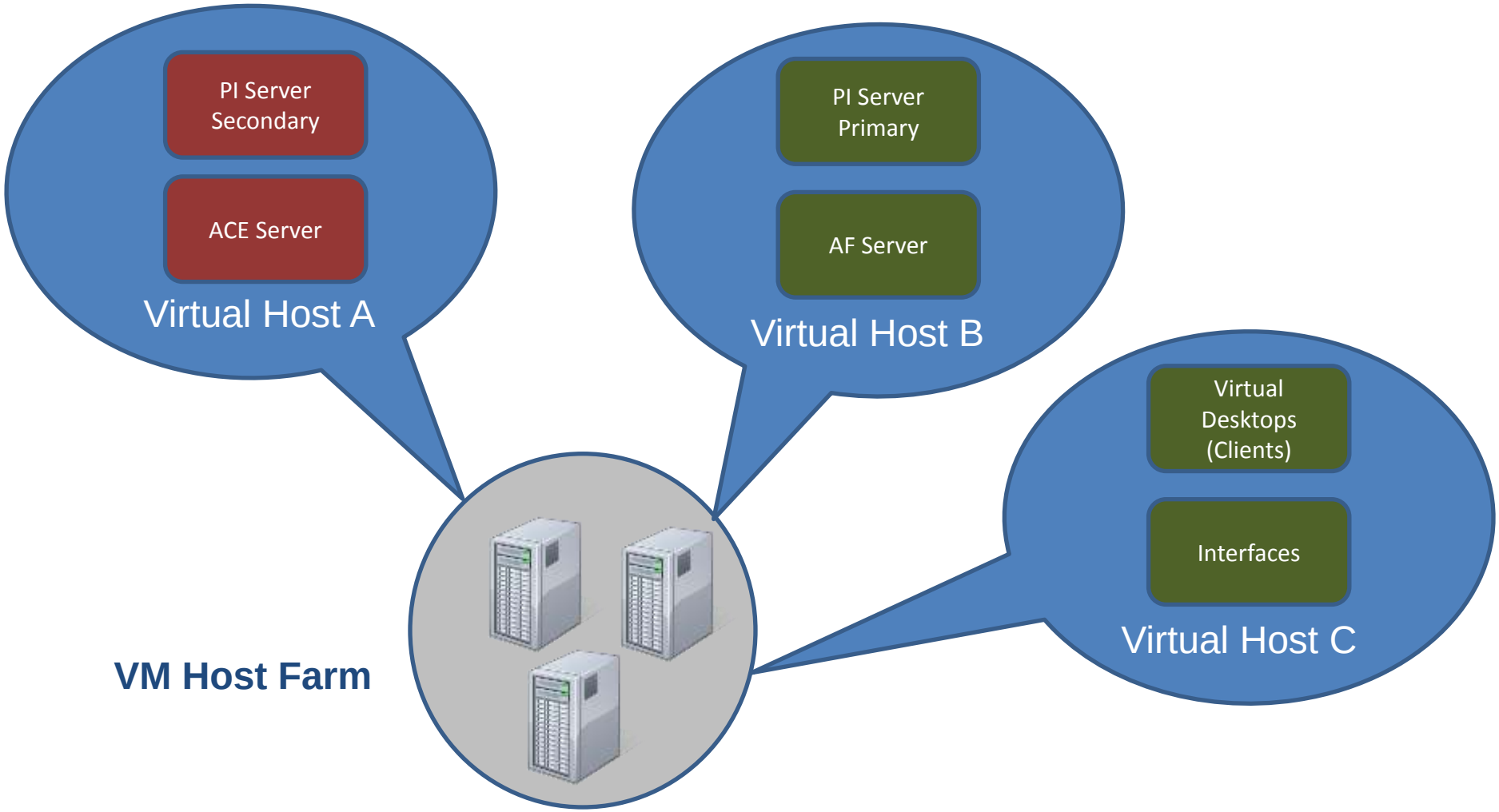
Virtualization Benefits

- Less hardware required
- Better utilization of hardware
- Reduce environmental consumption i.e. power, cooling, rack space
- 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

Benefits of Virtualizing the PI System

- Optimization of resources thru load distribution
- Simplifies the hardware upgrade/maintenance process
  - Ability to add resources such as CPU/Memory on demand
  - Easily move Virtual PI to other Hosts to “upgrade” hardware
- Provides availability in the event of a hardware failure
  - VMotion or Failover to another host
  - Redundant networking thru virtual switches

A Virtualized PI System



Recommendations: Virtualized PI System

- Use Enterprise class hardware and Virtual Host software
  - Microsoft Hyper-V or Vmware Vsphere
- Multiple hosts (cluster)
- Collective should be split across hosts
- PI System components can run as separate virtual machines for scalability and performance
- Optimize storage for virtual machines
- Reserve memory/CPU for PI do not over allocate
- Use resource scheduling to move other guests don't move PI or Interfaces
- Consider PI HA and VMotion and Hyper-V clusters complementary strategies

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

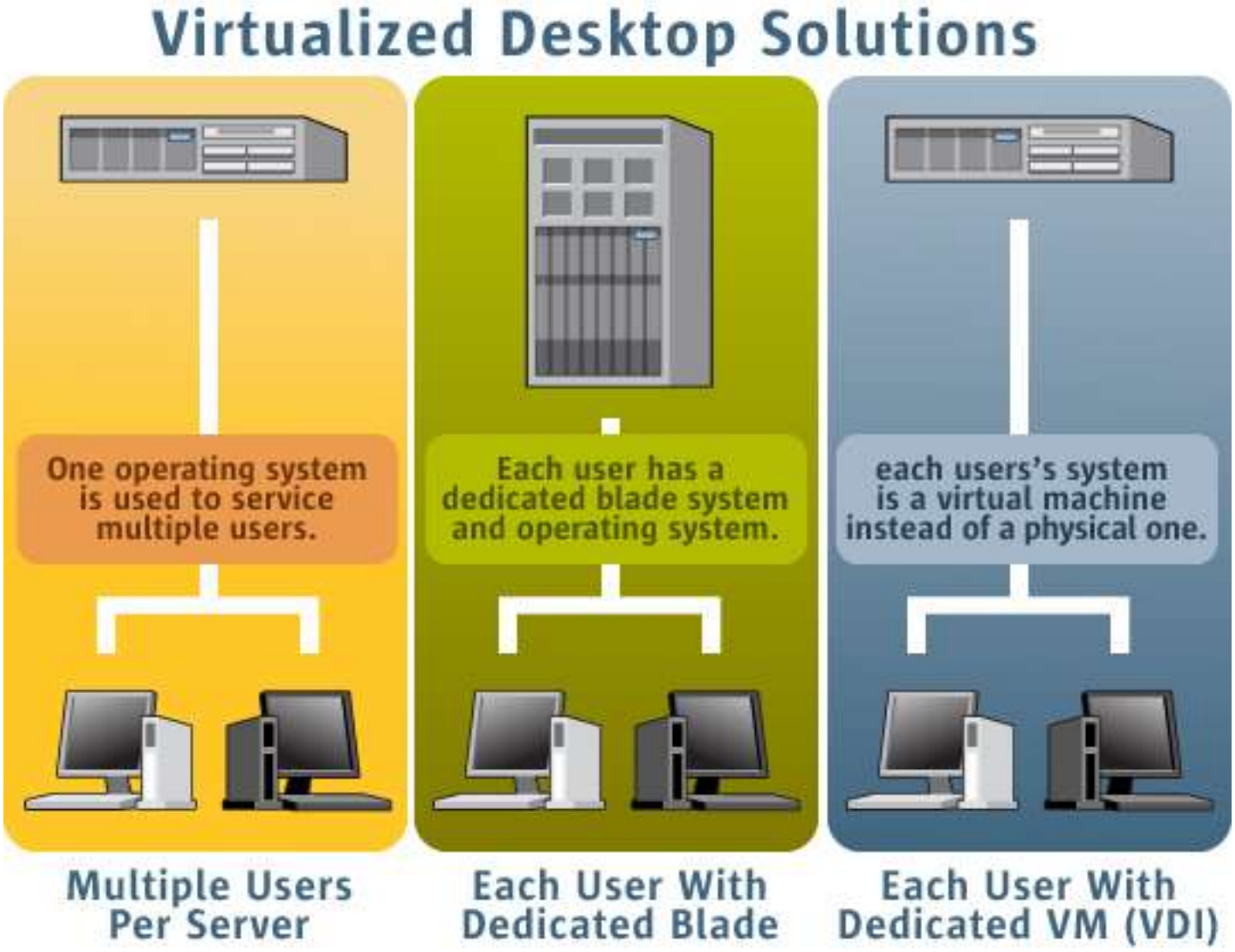
Benefits: PI in a Virtualization Project

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

Desktop Virtualization – Coming to a desktop near you

- Desktop virtualization has become hot in 2010
  - Credit Suisse expects the desktop virtualization market to be at least 1.8 billion by 2012 up from virtually zero. ** Desktop Virtualization comes of age* http://dabcc.com/documents/desktop virtualization_11_26_07.pdf
- A new spin on an old theme
  - Thin clients – Citrix, Terminal Services
- Virtual Desktops take Thin Client computing to the Virtual Datacenter by using some thin clients to connect to virtual machines
  - How do you manage them?
  - How do you maintain them?
  - What is the performance?
  - What is the ROI?
  - What are the licensing implications?

What are Virtualized Desktops?



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

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

Thank you

777 Davis St., Suite 250 San Leandro, CA 94577