OSIsoft.

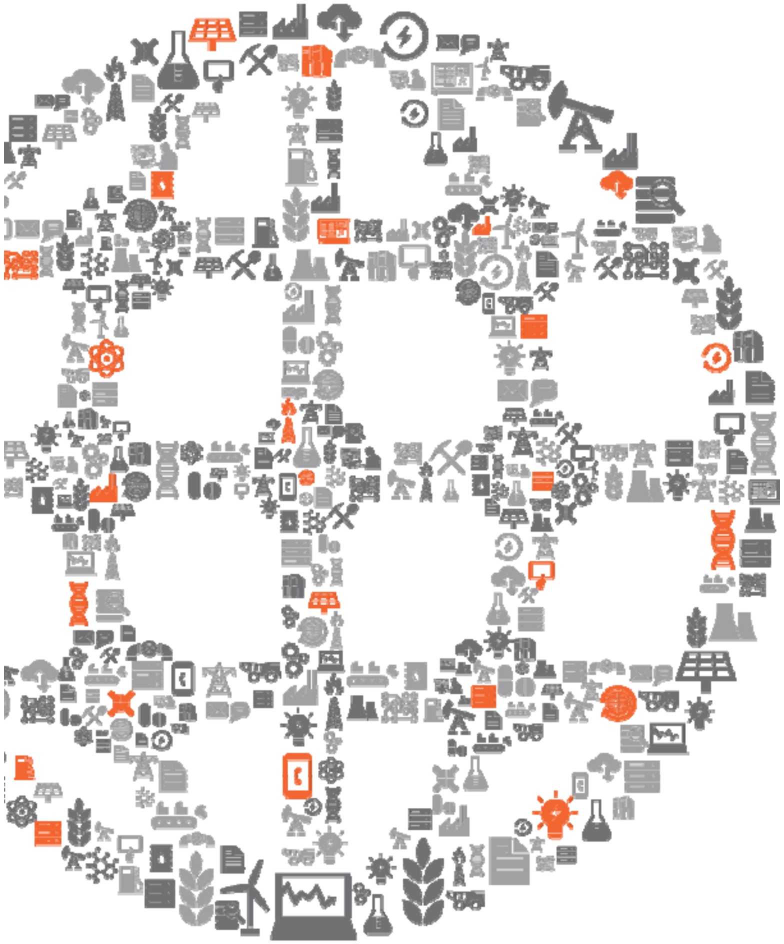
REGIONAL SEMINARS

The Power of Data

THRIVING IN A WORLD OF CHANGE

INDIA

August 22 - 23, 2013
Mumbai, India



Security and Cybersecurity - You Can Still Get to Your Data while Protecting Your Critical Assets!

Presented by **Chris Crosby**

Power Generation Industry Principal

22nd August, 2013

Business – Functional Roles

Enterprise

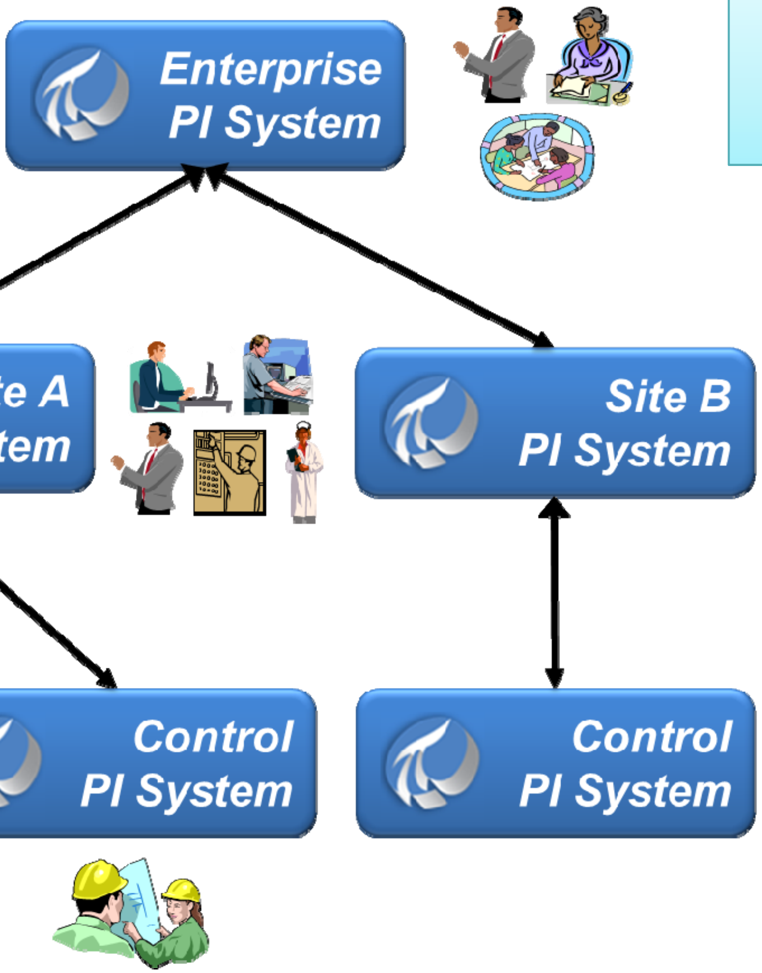
Executive Management
Business Functional Management & Engineers
Business Analysts
Global Subject Matter Experts (SMEs)

Site

Site Management
Process Engineers
Process Managers
Manufacturing
Quality
Maintenance

Control

Operators
Plant Floor
Supervisors



Real-Time Views, Cross Site Comparisons, KPIs, Standardization

Real-Time Views into Process & Historical Data Analysis

Process Execution & Decision Making

Business - PI System Functions

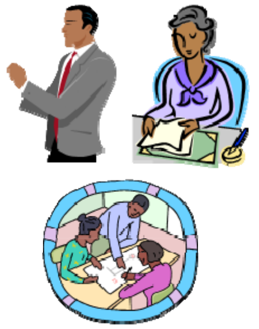
Enterprise PI System

Executive Management

Business Functional Management

Global SMEs

- Enterprise Level aggregation, rollup, reporting, business intelligence, and portal
- Enterprise standard template configuration (PI AF)
- Comparisons across sites



Site PI System

Site Management

Process Manager / Engineer

Quality Maintenance

Manufacturing

- Site Level process data aggregation and visibility
- Site Level rollup, reporting, portal
- Site Level business function support
- Real-time process views & troubleshooting
- Historical data analysis, trending, and process improvement.

Control PI System

Operator

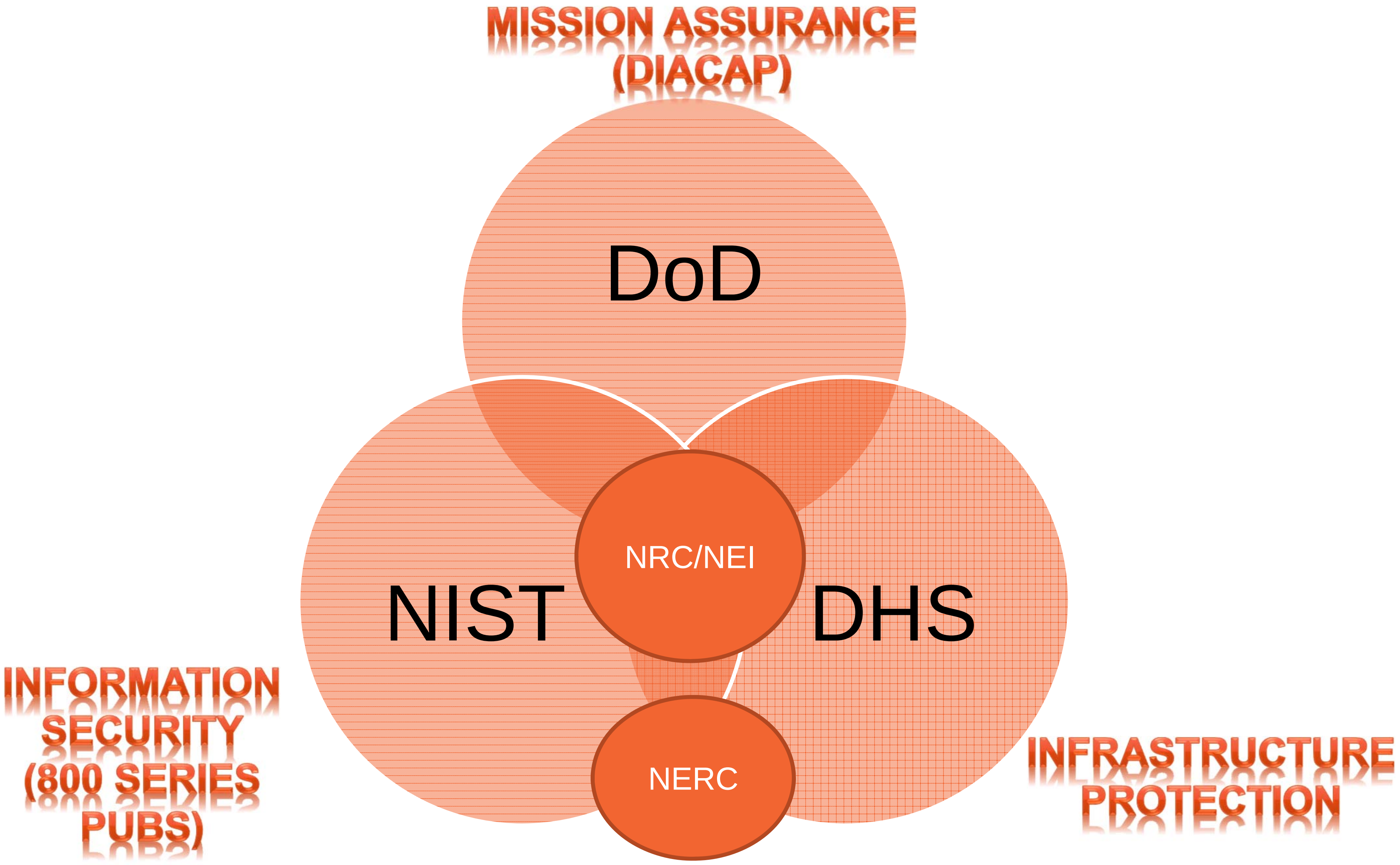
Supervisor

- Real-time process decision support
- Real-time process values and trending
- Real-time process calculations, alarming, and feedback to control

OSIsoft and PI System Security

- OSIsoft “gets” security
  - OSIsoft is **NOT** a compliance consulting or security solutions company, but we do “get” security…
  - *<u>Collaboration</u>* with
    - Homeland Security
    - Department of Energy Labs (INEL)
    - Microsoft (Security Development Lifecycle (SDL) and Security ACE team)
    - Infrastructure partners
    - Many large, experienced customers
- Regulations and standards – ***supports*** compliance (not ***insures*** it)
  - **10CFR73.54** -- “Protection of digital computer and communication systems and networks”
  - **NRC Reg. Guide 5.71** -- “Cyber security programs for nuclear facilities”
  - **NIST 800-53** -- “Recommended security controls for federal information systems”
  - **NIST 800-82** -- “Industrial control system security”
  - **NEI 08-09** -- “Cyber security plan for nuclear power reactors”
  - **DHS Control Systems Security Program** -- “Secure architecture design”

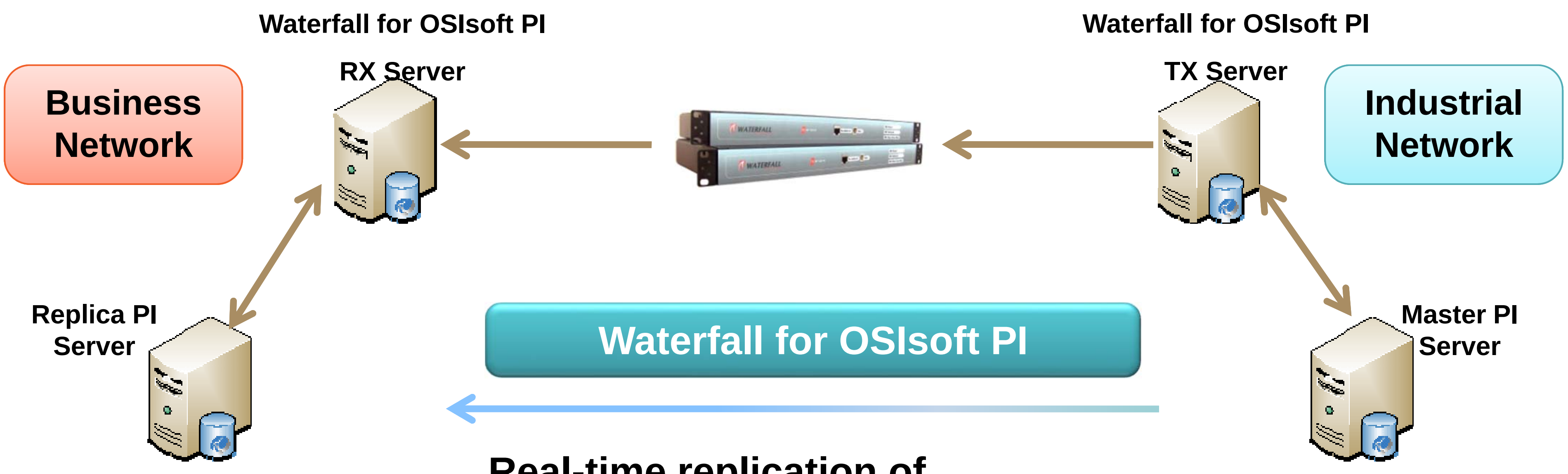
Strategic Security Standards


MISSION ASSURANCE (DIACAP)
DoD
NIST
DHS
NRC/NEI
NERC
INFORMATION SECURITY (800 SERIES PUBS)
INFRASTRUCTURE PROTECTION

OSIsoft Security Partners

- Waterfall for OSIsoft PI
  - Unidirectional Gateways
- Owl for OSIsoft PI
  - Data Diodes
- NitroSecurity (Intel McAfee)
  - Security Information and Event Management (SIEM)
  - Consulting
- Alert Enterprises
  - Software across IT infrastructure
  - Consulting
  - Physical Security Solution

Waterfall for OSIsoft PI© - Typical Topology



Waterfall for OSIsoft PI

RX Server

Waterfall for OSIsoft PI

TX Server

Business Network

Industrial Network

Replica PI Server

Master PI Server

Waterfall for OSIsoft PI

PI Database Subsystem

PI Snapshot Subsystem

PI Database subsystem

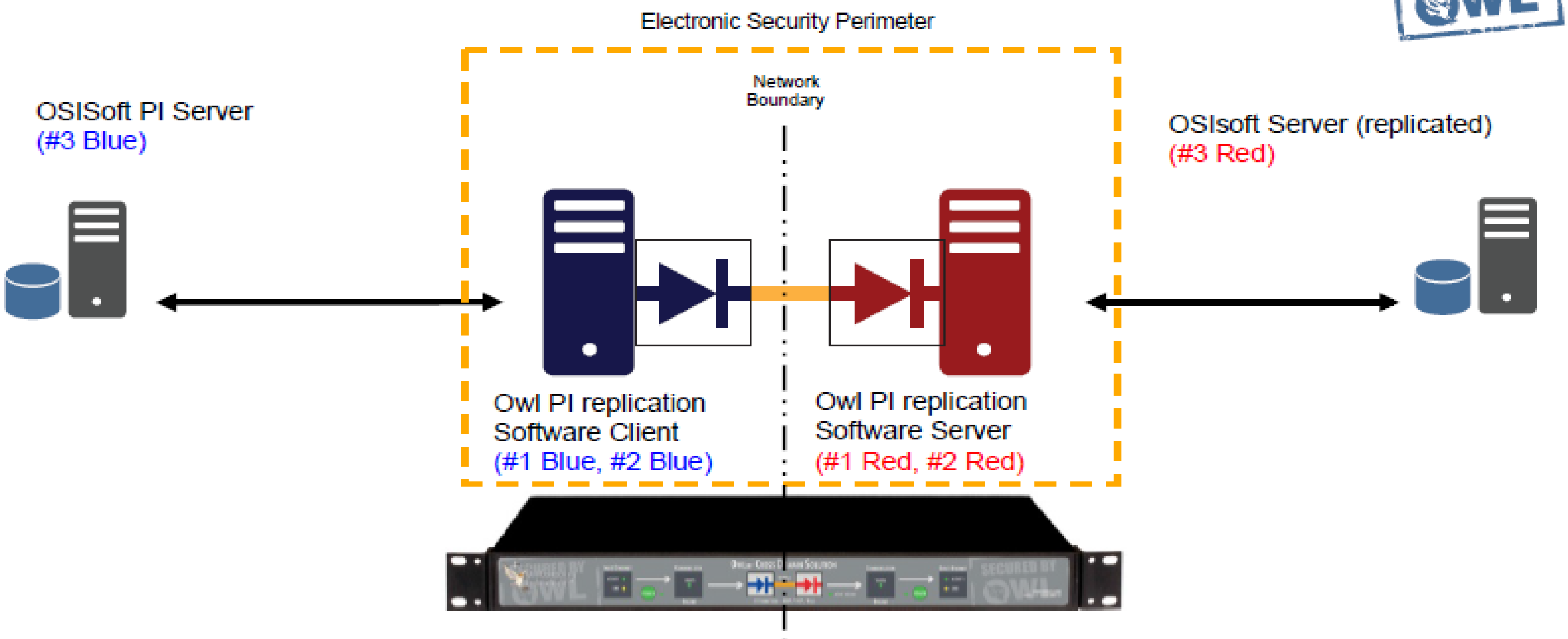
PI Snapshot Subsystem

Real-time replication of

- Tags database changes (APS)
- Tags data (snapshots)
- Additional solution for historical data back-fill

Owl for OSIsoft PI© - Typical Topology

DualDiode® Network Structure utilizing OSIsoft® PI to PI replication



Electronic Security Perimeter

Network Boundary

OSISoft PI Server
(#3 Blue)

Owl PI replication
Software Client
(#1 Blue, #2 Blue)

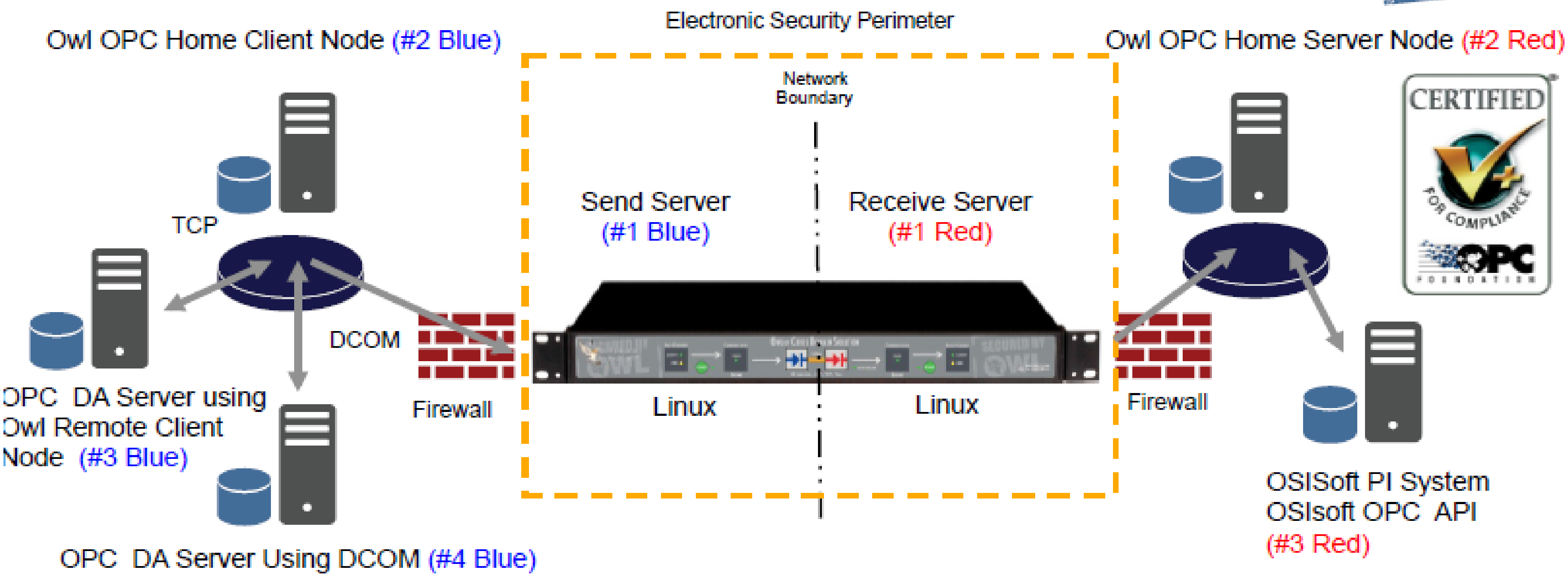
Owl PI replication
Software Server
(#1 Red, #2 Red)

OSIsoft Server (replicated)
(#3 Red)

- Owl DualDiode® running in Windows or Linux servers (#1 Blue) (#1 Red)
- Owl PI replication software (#2 Blue) collects PI data from OSIsoft PI server (#3 Blue),
- PI data sent data across Owl diode to Owl PI replication software in Owl server (#2 Red)
- Owl PI replication software delivers PI data to OSIsoft Server (replicated #3 Red)

Owl for OSIsoft PI© - OPC Topology

DualDiode® Network Structure utilizing OPC to OSIsoft®



Electronic Security Perimeter

Owl OPC Home Client Node (#2 Blue)

Owl OPC Home Server Node (#2 Red)

Network Boundary

TCP

DCOM

Send Server (#1 Blue)

Receive Server (#1 Red)

Firewall

Linux

Linux

Firewall

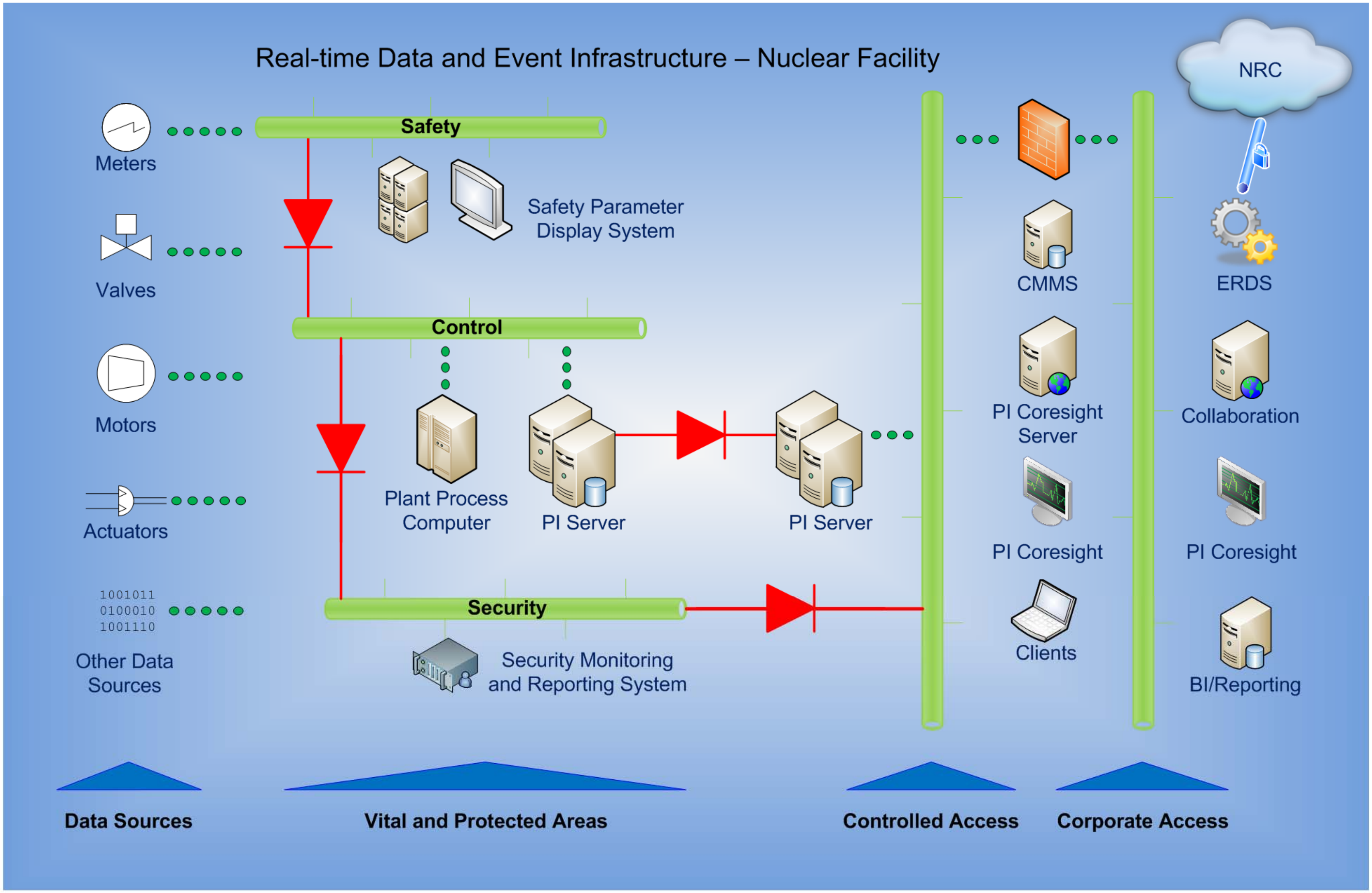
OPC DA Server using Owl Remote Client Node (#3 Blue)

OPC DA Server Using DCOM (#4 Blue)

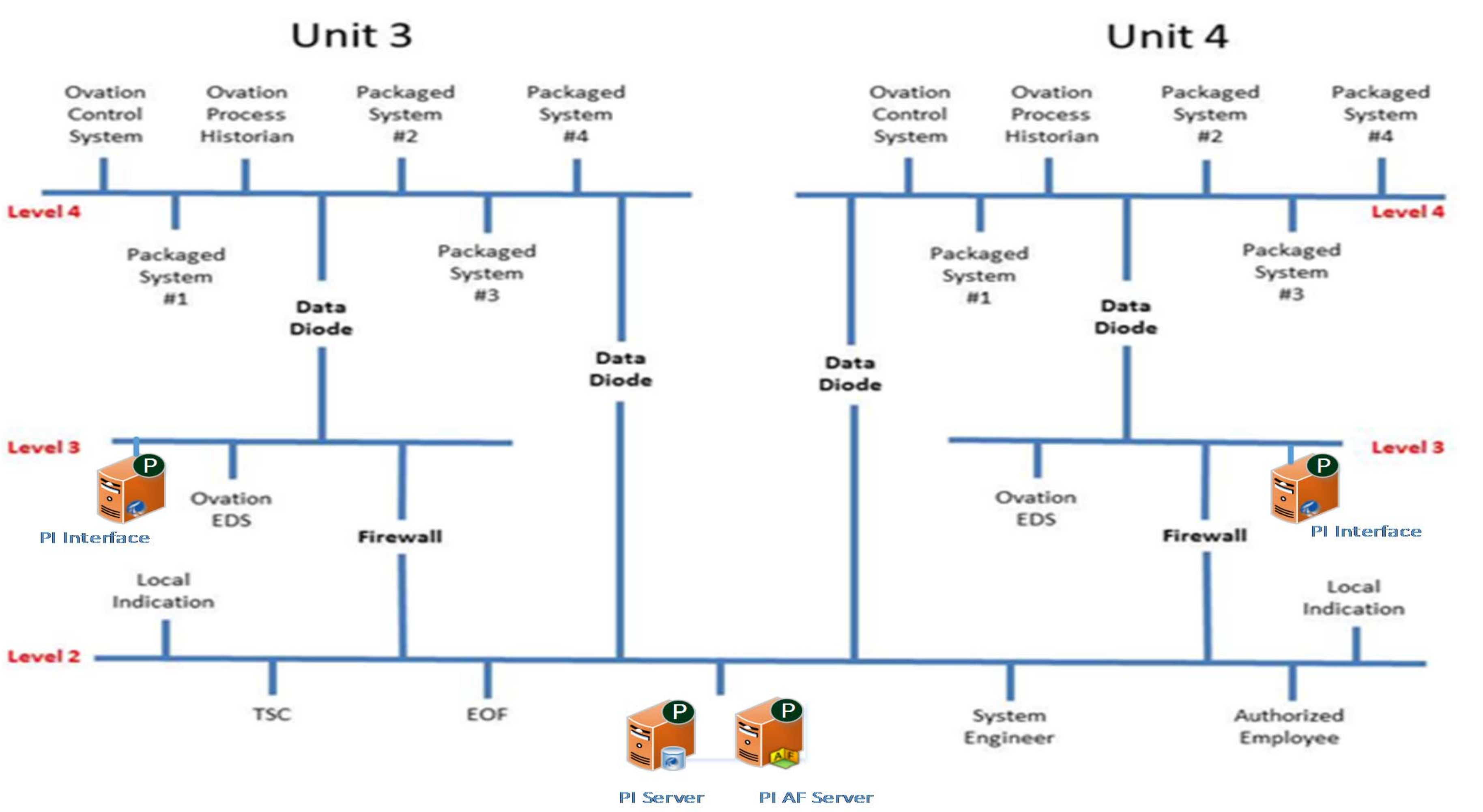
OSISoft PI System
OSIsoft OPC API
(#3 Red)

- Owl DualDiode® running in Owl OPDS Linux servers (#1 Blue) (#1 Red)
- Owl Home Client node (#2 Blue) sends data to Home Sever node (#2 Red) (Windows Servers)
- Owl Remote Client (#3 Blue) or DCOM (#4 Blue) collect OPC data to Owl Client Home node (#2 Blue)
- Owl Home Server (#2 Red) node sends data to OSIsoft OPC API node into OSIsoft PI historian (#3 Red)

PI System Nuclear Reference Architecture



Westinghouse AP1000 Architecture

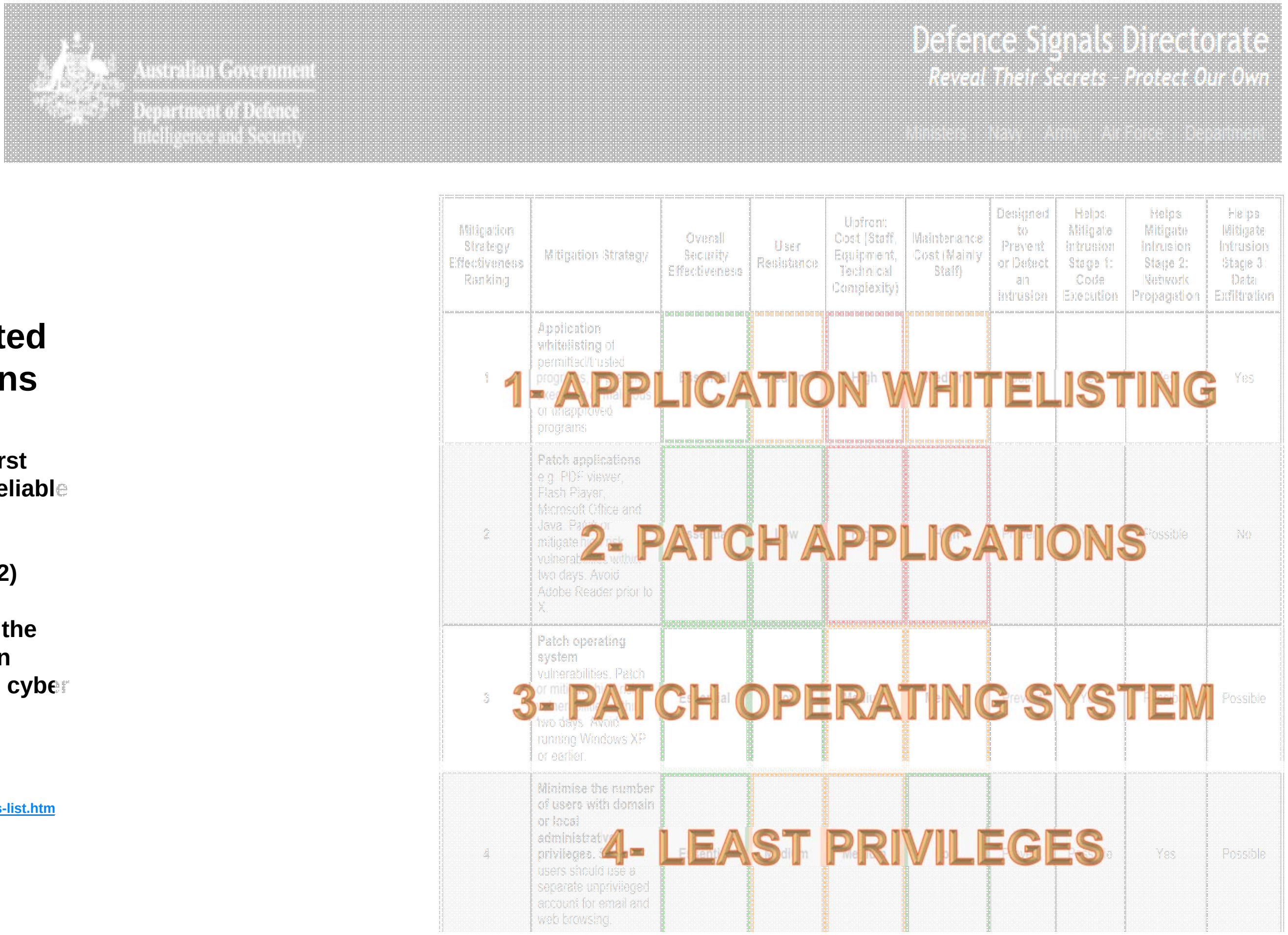


Strategies to Mitigate Targeted Cyber Intrusions

Australia Becomes First Nation To Discover Reliable Method of Stopping Targeted Attacks (October 30 & 31, 2012)

…. implementing just the top four strategies can block 85% of targeted cyber attacks

http://www.dsd.gov.au/infosec/top-mitigations/top35mitigationstrategies-list.htm


Australian Government
Department of Defence
Intelligence and Security
Defence Signals Directorate
Reveal Their Secrets · Protect Our Own
Ministers | Navy | Army | Air Force | Department

Mitigation Strategy Effectiveness Ranking	Mitigation Strategy	Overall Security Effectiveness	User Resistance	Upfront Cost (Staff, Equipment, Technical Complexity)	Maintenance Cost (Mainly Staff)	Designed to Prevent or Detect an Intrusion	Helps Mitigate Intrusion Stage 1: Code Execution	Helps Mitigate Intrusion Stage 2: Network Propagation	Helps Mitigate Intrusion Stage 3: Data Exfiltration
1	Application whitelisting of permitted/trusted programs, [illegible] malicious or unapproved programs.	Essential	Medium	High	Medium	Both	[illegible]	[illegible]	Yes
2	Patch applications e.g. PDF viewer, Flash Player, Microsoft Office and Java. Patch or mitigate high risk vulnerabilities within two days. Avoid Adobe Reader prior to X.	Essential	Low	[illegible]	High	Prevent	Yes	Possible	No
3	Patch operating system vulnerabilities. Patch or mitigate high risk vulnerabilities within two days. Avoid running Windows XP or earlier.	Essential	Low	Medium	Medium	Prevent	Yes	Possible	Possible
4	Minimise the number of users with domain or local administrative privileges. [illegible] users should use a separate unprivileged account for email and web browsing.	Essential	Medium	Medium	[illegible]	Prevent	Possible	Yes	Possible

1- APPLICATION WHITELISTING

2- PATCH APPLICATIONS

3- PATCH OPERATING SYSTEM

4- LEAST PRIVILEGES

Whitelisting

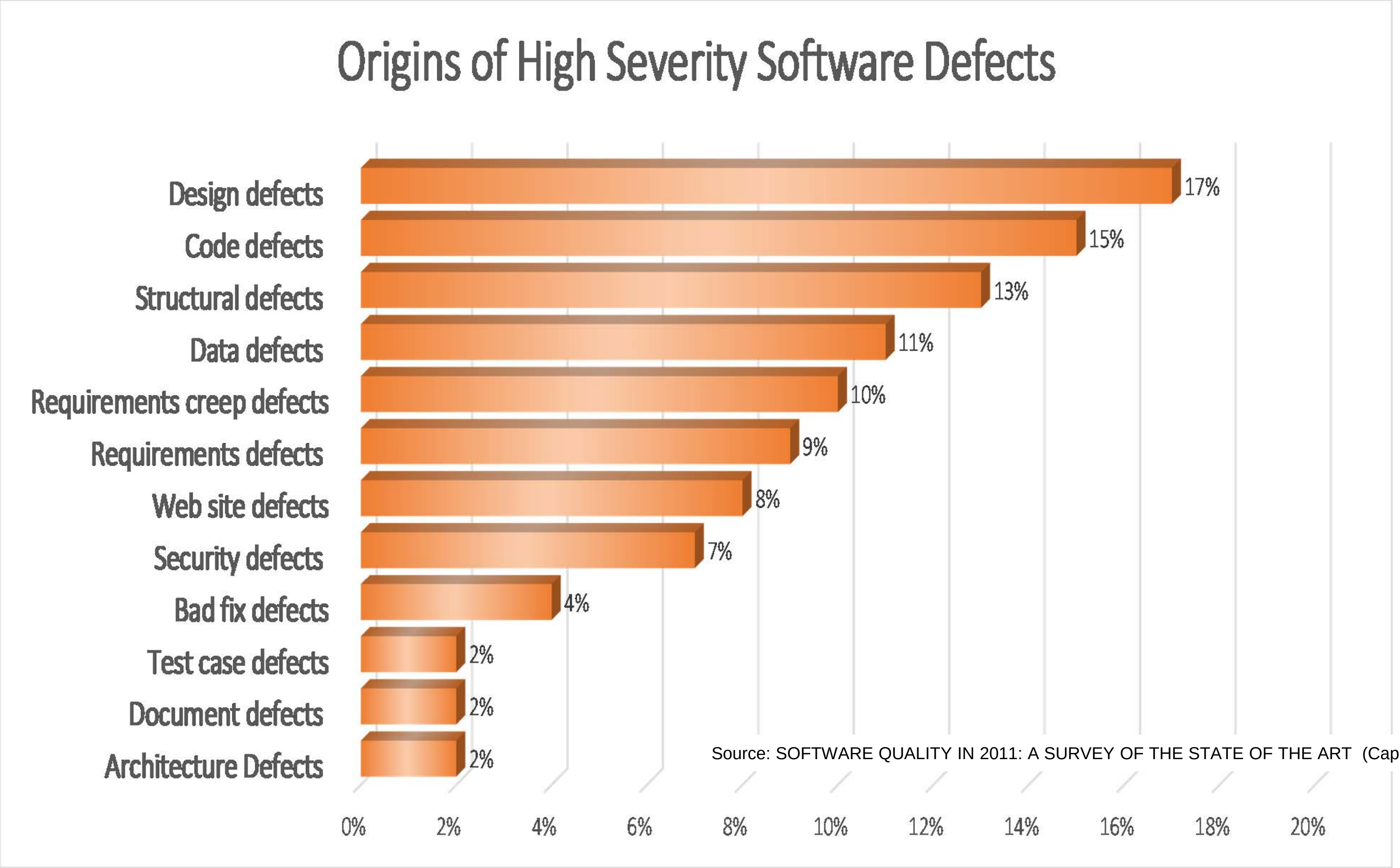
Applications

- Microsoft's Applocker
  - Windows 2008 & 2012
  - Windows 8 Pro

Communications

- Windows Firewall
  - All Current Versions of Windows
  - Enable Output Rules

All Software Has Bugs

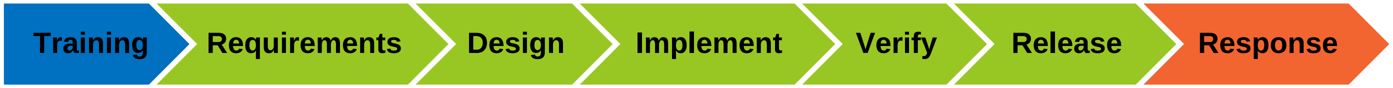


Source: SOFTWARE QUALITY IN 2011: A SURVEY OF THE STATE OF THE ART (Capers Jones)

Security Development Lifecycle

Essential Processes and Practices for:

- Reducing the Number of Vulnerabilities
- Reducing the Severity of Vulnerabilities
- Increasing the Resiliency of the Software
- Increasing the Reliability of the Software



Training

Requirements

Design

Implement

Verify

Release

Response

OSIsoft's Responsibility

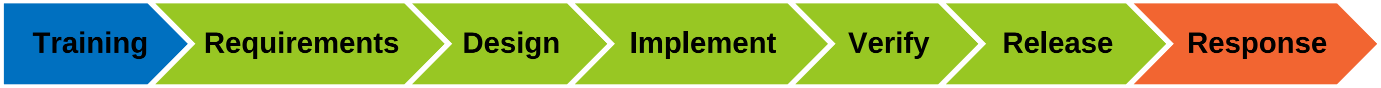
Example: PI Server 2012

19 New Security Bugs Found and Fixed

Reduced exploitability (software resilience)

- Buffer Overrun Detection
- SEH - Safe Exception Handling Protection
- SEHOP – Structured Exception Handling Protection
- DEP/NX – Data Execution Prevention and No eXecute
- **ASLR – Address Space Layout Randomization**
- Heap Metadata Protection

Continuous Improvement



Training → Requirements → Design → Implement → Verify → Release → Response

Patch/Upgrade PI Software

- Each Revision Reduces Bugs
- 64 Bit Versions are more Secure
- PI Server 2012 Certified on Windows Core
- PI AF Server 2012 Tested on Windows Core
- MS SQL Server 2012 Certified on Windows Core

Patch/Upgrade OS

Servers (Running on Windows Core where possible)

- Windows 2012 or
- Windows 2008 R2

Clients

- Windows 8 or
- Windows 7

Windows OS retirement coming

(No further security updates from Microsoft)

- Windows XP support ends in April 2014
- Window Server 2003 support ends in July 2015

Windows Core

- No Graphical User Interface (GUI)
- No Graphic Based Applications
- Smaller Faster Code Base
- More Resources Available
- Fewer Patches Needed
- Less Maintenance
- Lower Total Cost of Ownership

Least Privileges

Do not use piadmin account

Use Windows Integrated Security (WIS)

Enable Windows User Account Control (UAC)

Create Users and Trusts based on Least Privileges

The Top 4

1: Use Whitelisting Techniques

2: Upgrade your PI Software

3: Upgrade your Operating System

Use Windows Server Core for Servers

4: Least Privileges

Additional Information

OSIsoft Links

- Whitelisting guidance
- For the latest in PI security use Search string “PI Security Best Practices” http://techsearch.osisoft.com/Pages/results.aspx?k=pi%20security%20best%20practices
- Product documentation on core
- For Windows Security Requirements look at this technical article: http://techsupport.osisoft.com/Support+Solution/8/KB00354.htm
- OS support

External links

Verizon - 2012 Data Breach Investigations Report: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf?__ct_return=1

Australian Defence Signals Directorate - Strategies to Mitigate Targeted Cyber Intrusions: http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm

Honeywell Whitepaper on Application Whitelisting:

http://www.controleng.com/fileadmin/content_files/ce/honeywell-iits-wp-application-whitelisting.pdf

EA Customers

Contact Your EPM or CoE to Learn More about Best Practice Availability

A1

A2

Slide 23

A1 Need an additional slide here for additional info:

Author, 01-Apr-13

A2 Action Item to Michael Christopher for tech support docs.

Author, 01-Apr-13

THANK YOU

Brought to you by

OSIsoft.