IT Security and OT Security

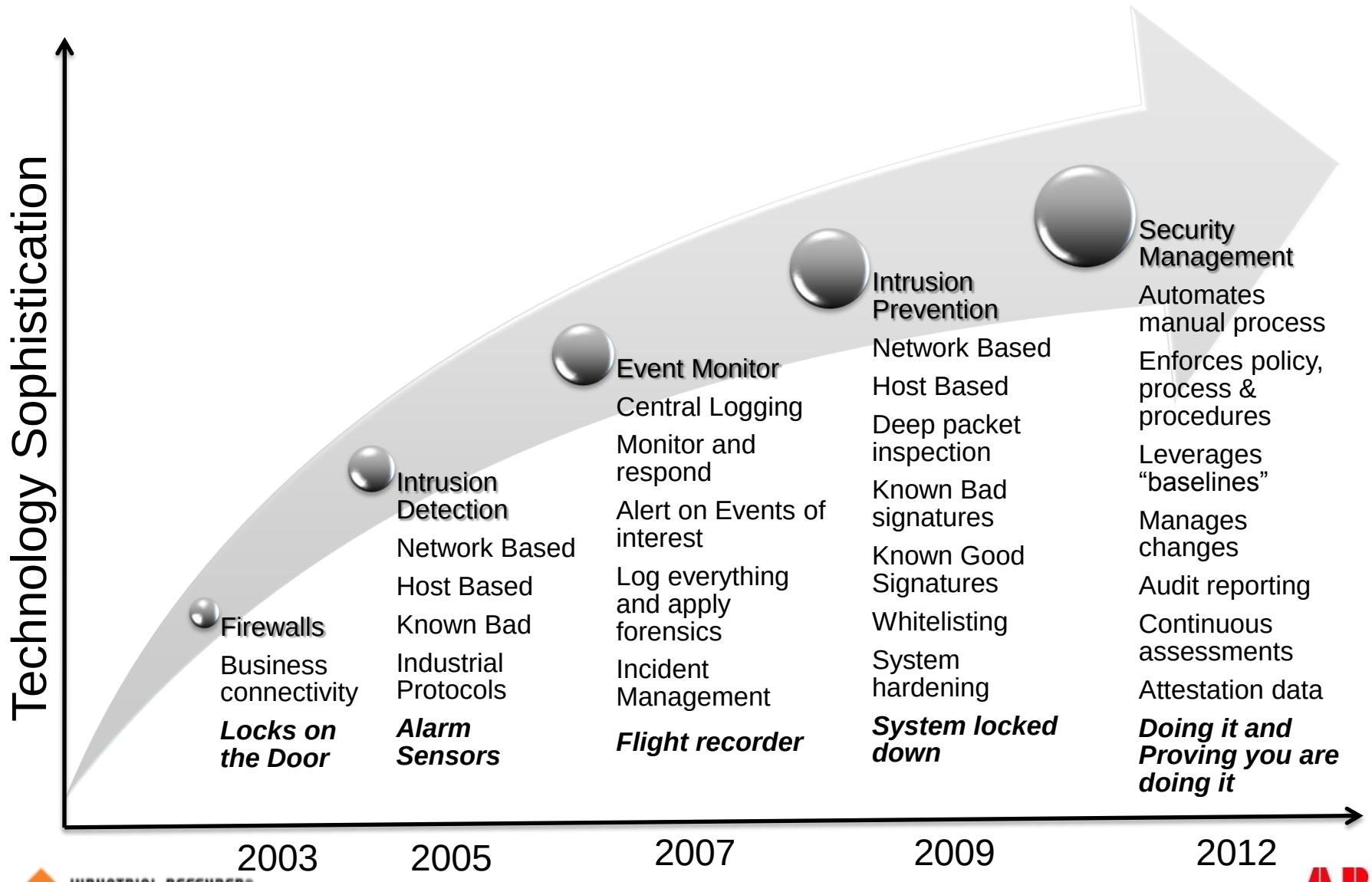
Understanding the Challenges

Security Maturity Evolution in Industrial Control

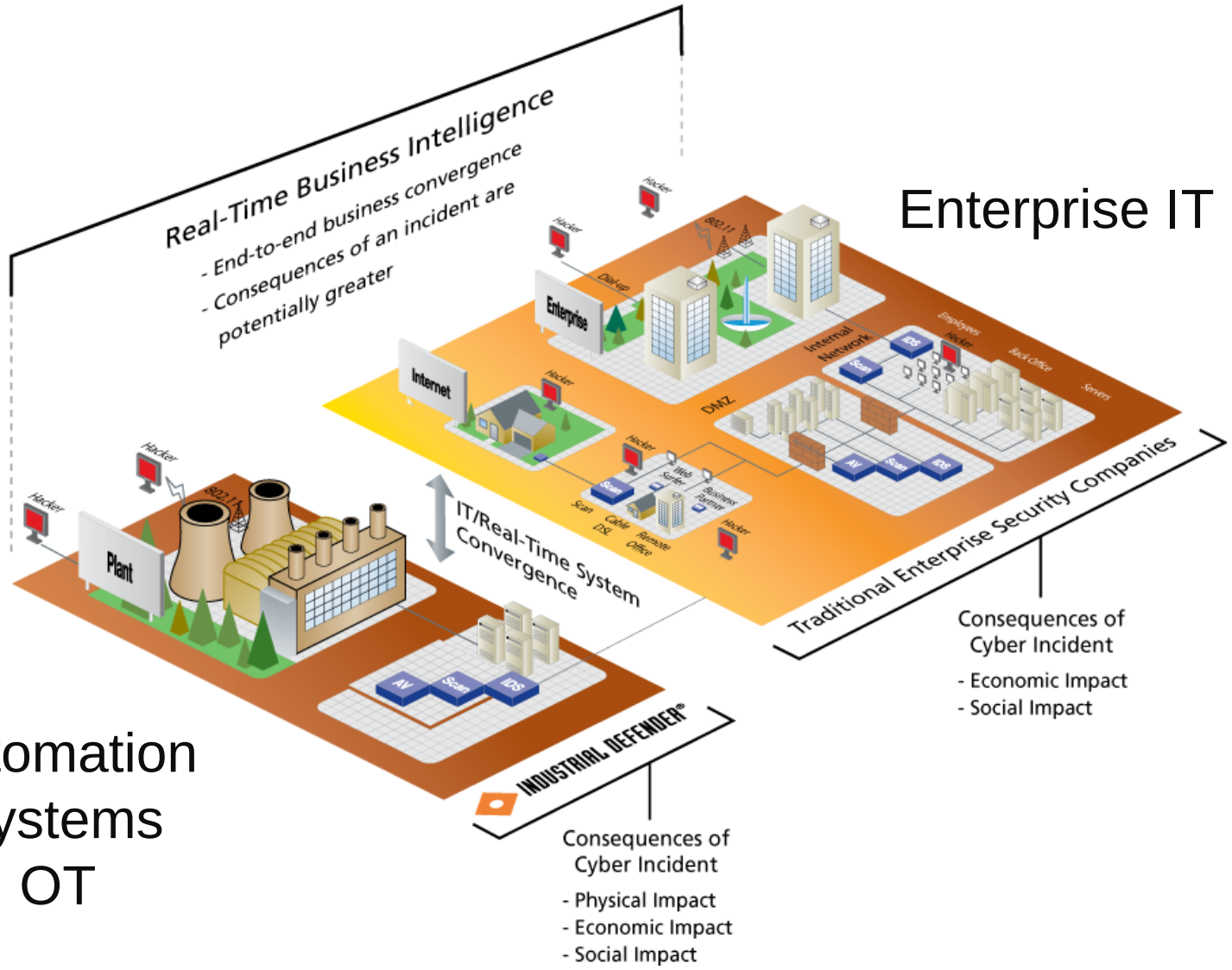
1950s

ABB

Security Maturity Evolution in Industrial Control



IT Drivers vs. OT Drivers



Control Systems Have Unique Architectures

What Needs To Be Protected and Monitored?

- Servers
- HMI's
- Control System Networks
- Network Devices
- PLC's IED's RTU's

Device Interfaces and Communications

- Event / log collection
- IDS / IPS
- Configuration and patch data collection
- Remote access controls

Automation Systems Devices

Servers: PCS, SCADA, …

Work stations

Firewalls

HMI Stations

Hardened networking devices

IEDs, Sensors, Controllers

INDUSTRIAL DEFENDER®

ABB

Automation Systems Security Really Unique?

Corporate IT	Automation Systems IT
Not life threatening	Safety first
Availability important	Non-interruption is critical
Transactional orientation	Real-time focus
IBM, SAP, Oracle, …..	ABB, Emerson, GE, Honeywell, Siemens...
People ~= Devices	Few people; Many, many devices
PCs and Servers	Sensors, Controllers, Servers
Web services model is dominant	Polled automation control model
MS Windows is dominant OS	Vendor-embedded operating systems
Many commercial software products installed on each PC	Purpose-specific devices and application
Protocol is primarily HTTP/HTTPS over TCP/IP -- widely known	Many industrial protocols, some over TCP/IP – vendor and sector-specific
Office environment, plus mobile	Harsh operating plant environments
Cross-industry IT jargon	Industry sector-specific jargon
Cross-industry regulations (mostly)	Industry-specific regulations

IT/Data Center Environment

- Dedicated Specialists
  - Desktop
  - Database
  - Network
  - Security

- Dedicated Tools
  - Desktop Management
  - Database Management
  - Network Management
  - Security Monitoring

Operations Technology(OT) Environment

- OT Specialists
  - Dedicated Applications Specialists
  - Manage Control Network and Control Systems
  - Generalists, Not Specialists
- OT Tools
  - Diagnostic Tools Are Usually Supplied by Control Systems Vendor
  - Control Systems Tools Are Application Centric
  - Network, Security, Database, Desktop Support Tools Not Available or Not Present
  - Learning 4-5 IT Tools To Manage Environment Not Practical

Unique Challenge: 15+ Year Duty Cycle on Control Systems

- Legacy Systems Create Unique Challenges
  - Operating Systems No Longer Supported by Manufacturer
    - Windows NT
    - Older Unix Systems Such as AIX or Solaris
- Limited Network Bandwidth
  - Older Networks Will Be Adversely Affected By Some Standard IT Monitoring Technologies
- Look For:
  - Security Technologies That Support Legacy Systems
  - Technologies That Utilize Limited Network Bandwidth For Reporting/Monitoring

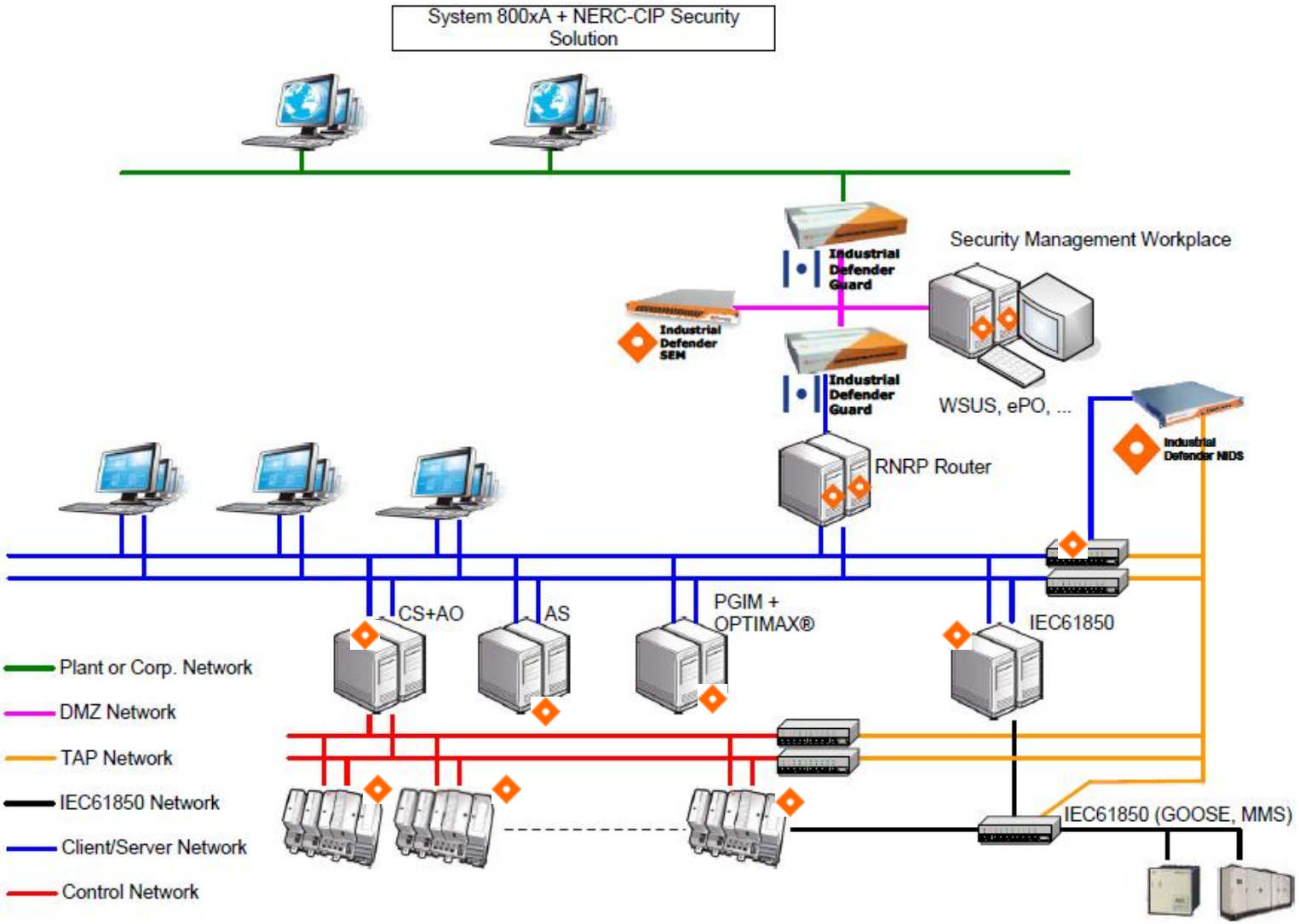
Unique Challenge: Industrial Controls Environment

- Industrial Protocols Within Control System Networks
  - Modbus
  - DNP3
- Industrial End Point Devices
  - Programmable Logic Controllers (PLCs)
  - Intelligent Electronic Devices (IEDs)
  - Remote Terminal Units (RTUs)
- Look For:
  - Technologies that support network monitoring of industrial protocols via purpose built signatures for industrial protocols
  - Technologies that can monitor configurations of industrial end point devices

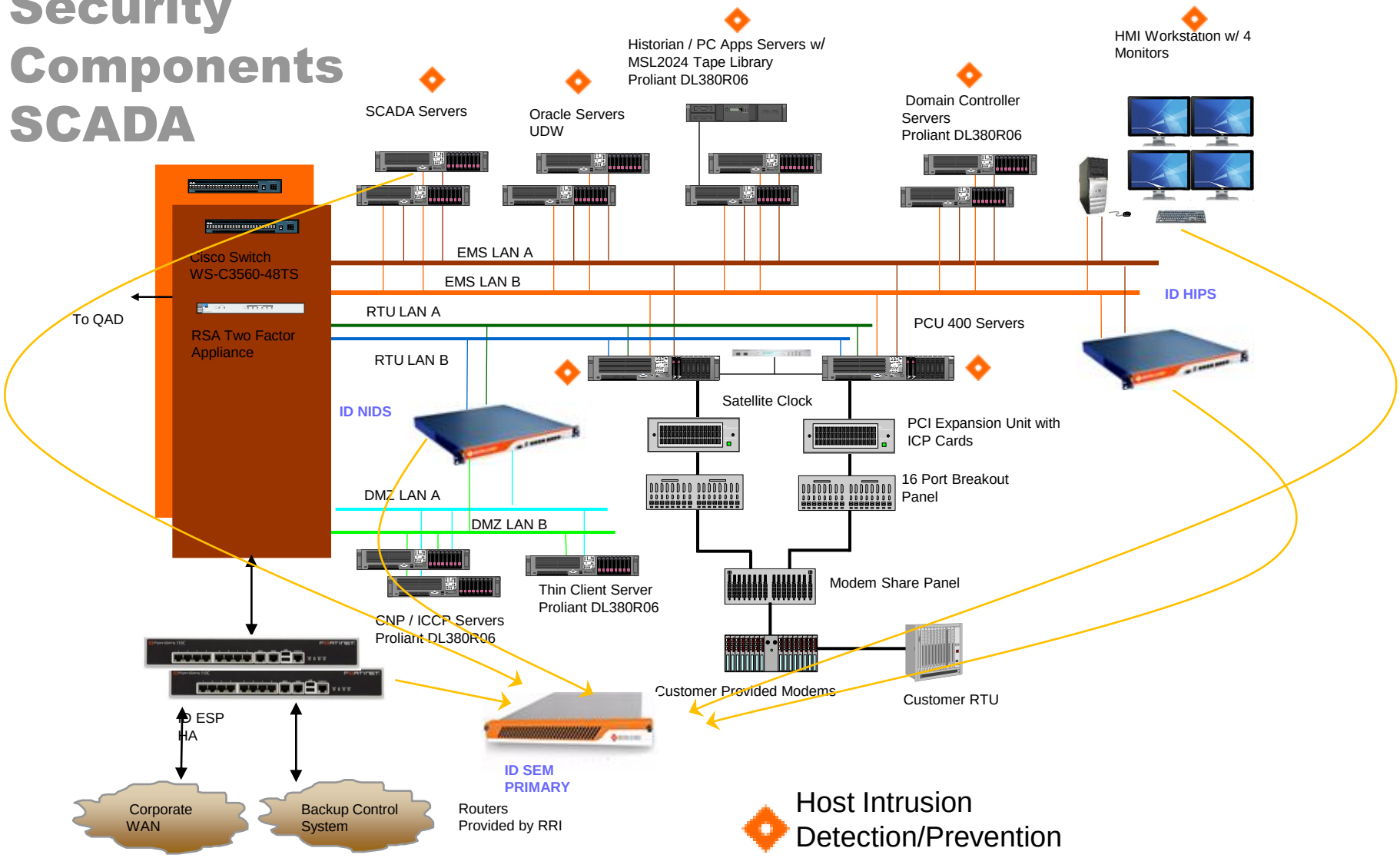
Recommended OT Security Deployment

- Network Segment Monitoring
  - Network Intrusion Monitoring for Including Industrial Protocols
- Monitoring of Servers
  - Syslog
  - Embedded Agents
- Monitoring of Workstations
  - Syslog
  - Embedded Agents
- Perimeter Firewalls
- Anti-Virus Anti Malware
  - Blacklist (signature based)
  - Whitelist (application based)
- Configuration Management
  - Monitoring and Baselines of Configuration Changes

Generation Plant Security Deployment



Security Components SCADA



Example SCADA Management System

Development of Secure Products

- Role-Based Access Control
  - Functions and data
  - Prevent database changes that produce system failures
  - Prevent more than one operator from controlling a single point simultaneously.
- Encryption and Communications
- Audit Trail
  - History of each users access to objects, attributes, data, displays, production areas and controls.
- Vulnerability Testing
  - Independent, un-biased
- Installation Best Practices and Guidelines

Cyber Security Project Execution

Planning
- Functional Design Specification
- Security Policy
- Network Topology Drawings
- Upgrades and Testing

Communicate and agree

Deployment and Commissioning
- Installation and Hardening Guideline
- Remote Access and File Transfer
- Networks and Interfaces
- Group Policy and Organizational Units

Secure the system and make it available

Operation
- Computer and User Administration
- Backup and Recovery
- Patch and Rollup Management

Operation starts on day one

Summary

- OT Has Unique Operating Environments
  - Legacy Systems
  - Industrial Systems And Endpoints
- OT Has Unique Threats
- OT Has Limited Tools and Resources
- Look For:
  - Tools That Are Specialized For OT
  - Tools That Have Been Developed with Security as a Requirement
  - Tools That Have Been Tested By Control System Vendors
  - Are Purpose Built For OT Professionals
  - Proven Methods for Developing and Deploying Secure SCADA Solutions

Power and productivity
for a better world™