TETRA TECH

Common AWIA Assessment Findings and How to Address Them Cybersecurity Focus

David Espy
- CISSP

NATIONAL OPERATIONAL TECHNOLOGY PRACTICE LEADER

PNWS-AWWA
Water 2022
Tacoma, WA • April 27-29

Knowledge Goals:

- Understand the AWIA Cybersecurity RRA Process
- Understand Top 10 AWIA Cybersecurity Findings
- Understand How to Mitigate the Top 10 Findings

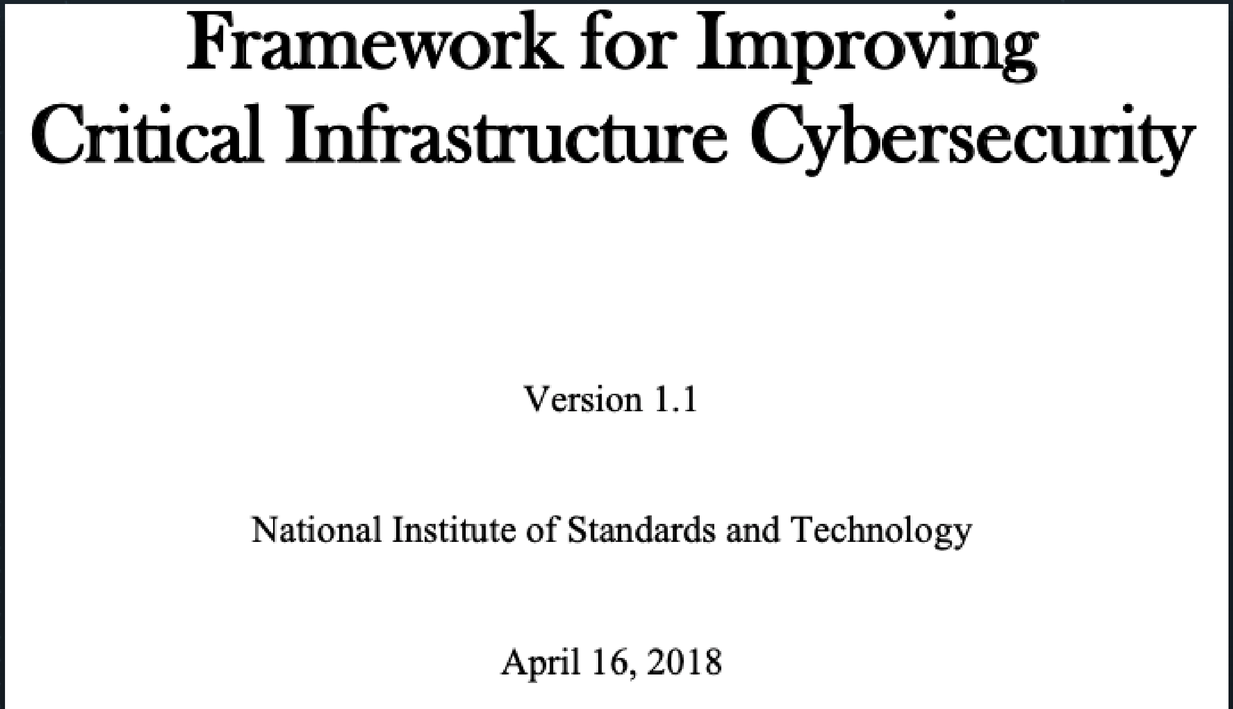
Cybersecurity Critical Assets

Identification

Common Critical Assets Considered in AWIA RRA

Cybersecurity Assets

- ☑ *Network/ Communications Infrastructure*
- ☑ *Firewalls*
- ☑ *Physical Communications Media*
- ☑ *Skilled Staff*
- ☑ *Telemetry Network*
- ☑ *Server Infrastructure*
- ☑ *SCADA –PLC's and HMI Software*
- ☑ *Financial Systems*

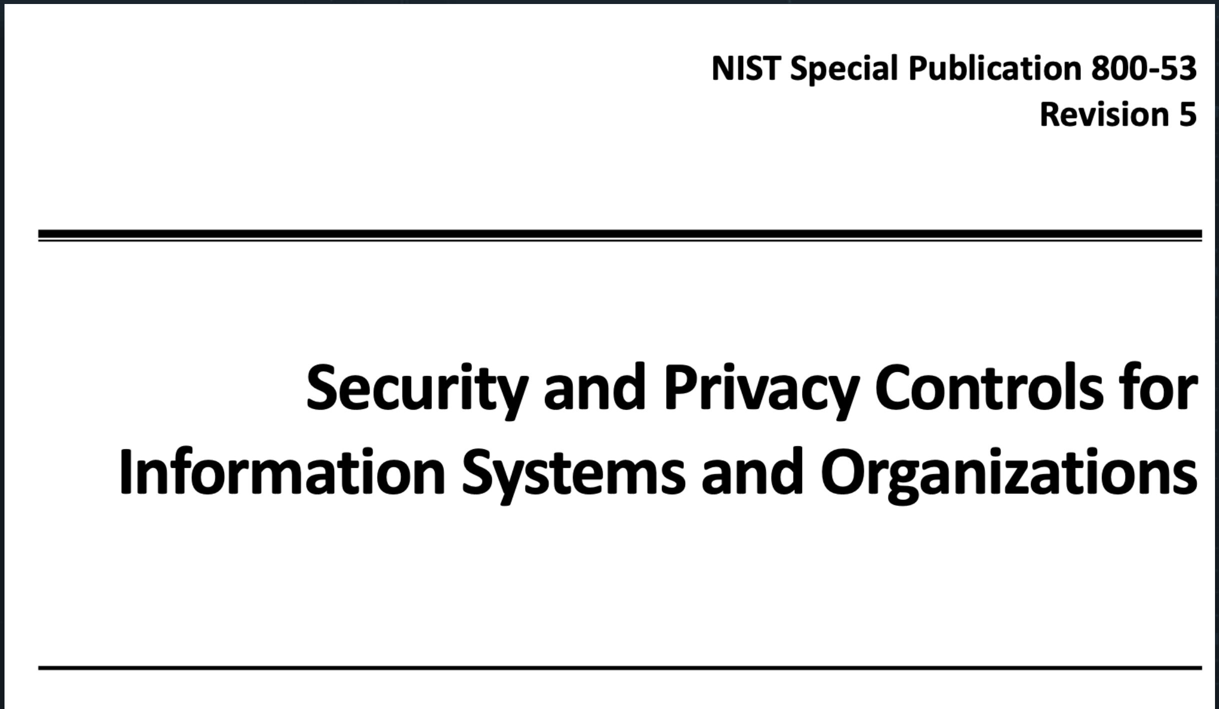


Framework for Improving Critical Infrastructure Cybersecurity

Version 1.1

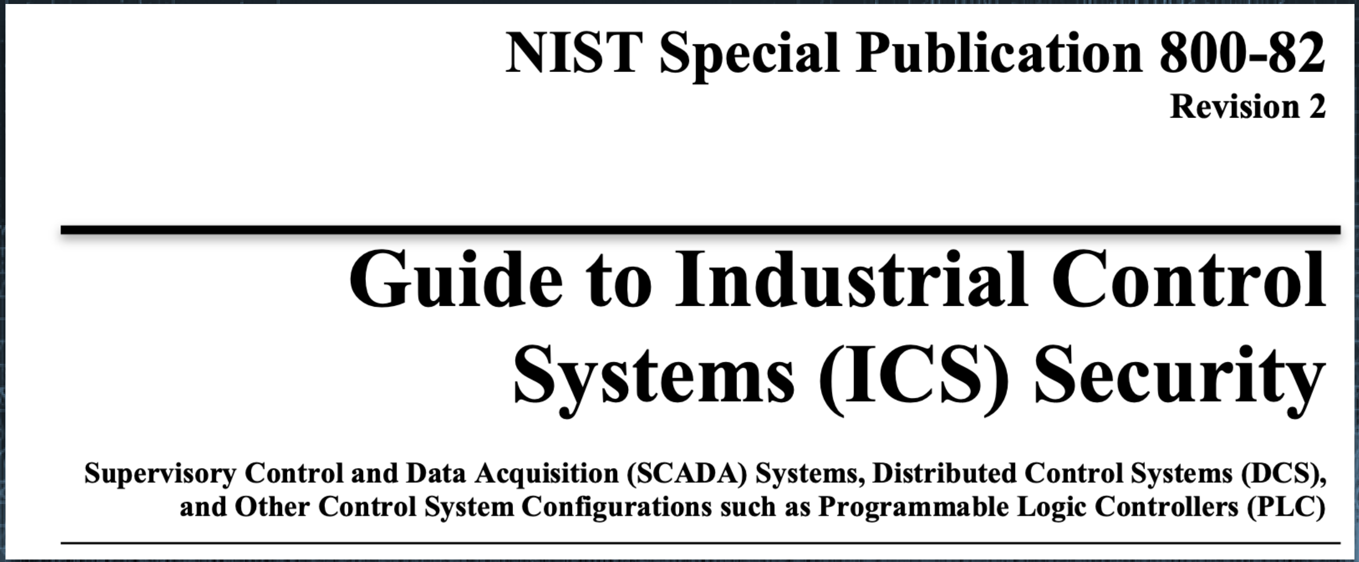
National Institute of Standards and Technology

April 16, 2018



NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations



NIST Special Publication 800-82
Revision 2

Guide to Industrial Control Systems (ICS) Security

Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC)

Cyber Security Evaluation Tool - CSET

- ✓ Standards Based Evaluation Tool
- ✓ Can be Used for Continuous Evaluation
- ✓ Year Over Year Baseline Comparisons
- ✓ Network Diagram Evaluation
- ✓ Continuous Improvements to the Tool

Other Items Considered in AWIA RRA

- Network Architecture
- Documentation
- Age of:
  - *OS*
  - *Hardware*
  - *Software*
- Updates and Patching Status
- Physical Security for OT Components
- Administrative Policies and Procedures

Findings

Natural Disasters Tend to have the Largest Economic Impact, but Extremely Low Probability.

Cyber Attacks can have Large Scale Impacts on Utilities with a Relatively High Probability.

A Widespread Cyber attack can be as Disruptive to Operations as a Regional Storm Event or Natural Disaster.

The Cost-Benefit Ratio for Cyber Improvements is High *(typically 5:1 or higher).*

Top AWIA Findings

10 Most Common AWIA RRA Cybersecurity Findings

Top 10 Most Common Findings

#1 - No ICS Cybersecurity Program

- *No ICS Cybersecurity Policies and Procedures*
- *No Risk Management Program*
- *No Security Framework Identified*
- *No one in charge of ICS Cybersecurity*
- *No Business Continuity Plan*
- *No Incident Response Plan*
- *No Disaster Recovery Plan for OT/SCADA*
- *No personnel screening policies*
- *No termination/departure procedures*

How to Fix It – ICS Cybersecurity Program

(NIST SP 800-82 6.0)

1 *Start with Picking a Framework/Standard*

- *NIST CSF*
- *NIST SP 800-53*
- *NIST SP 800-82*
- *ANSI/ISA 62443*

2 *Start Chipping Away at Policies & Procedures (NIST SP 800-82 Appendix G – ICS Overlay)*

- *Look for templates*
- *Borrow from IT then tweak if needed*
- *Ask Electric Utility*
- *Start with human factors*

How to Fix It – ICS Cybersecurity Program

(NIST SP 800-82 6.0)

3 *Perform Risk Assessment*

(NIST SP 800-82 3.2)

- *Identify critical facilities/equipment*
- *Identify single points of failure*
- *Identify mitigations*

4 *Then Develop the Plans*

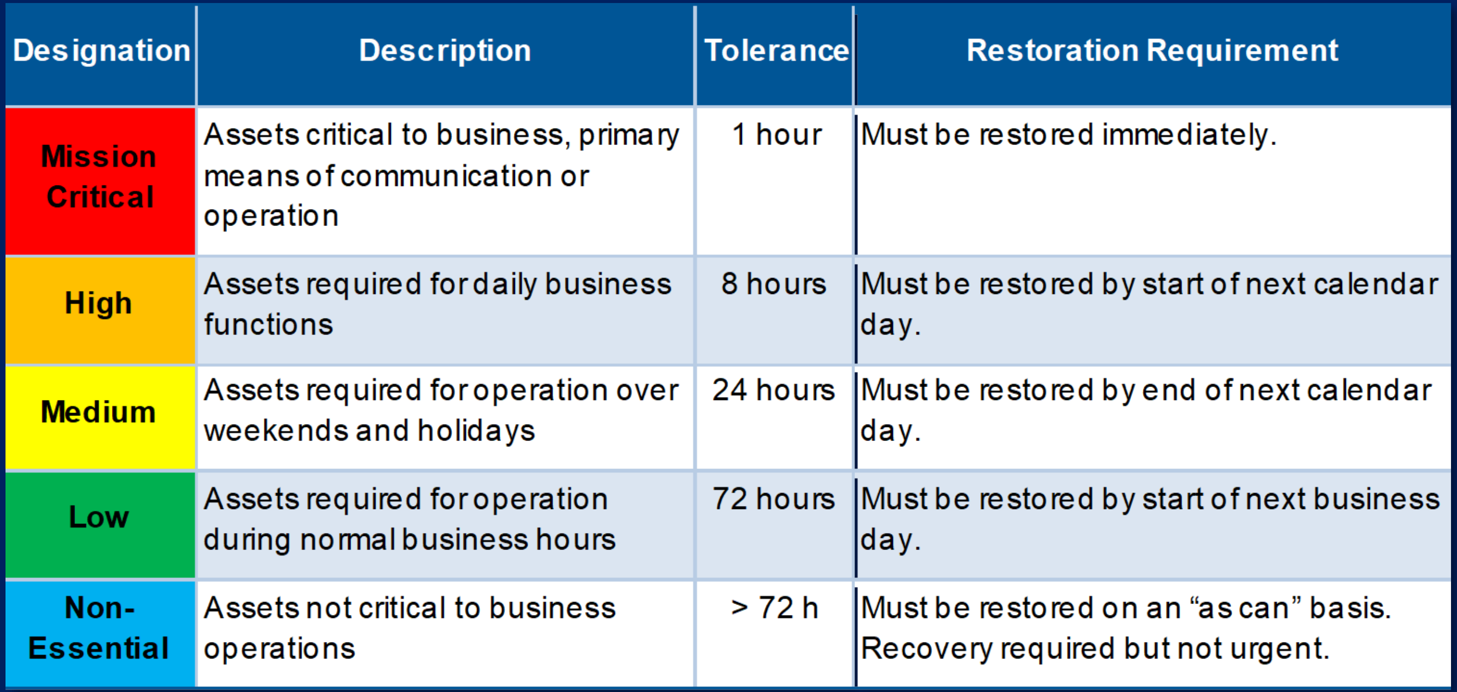
- *Business Continuity*
- *Disaster Recovery*
- *Incident Response*

Risk Assessment - Criticality & Business Impact

Start with an Asset Inventory.

- Hardware
- Software
- Communications
- Data

Identify the Criticality of Each Asset, *then* Determine How to Protect it Appropriately.



Designation	Description	Tolerance	Restoration Requirement
Mission Critical	Assets critical to business, primary means of communication or operation	1 hour	Must be restored immediately.
High	Assets required for daily business functions	8 hours	Must be restored by start of next calendar day.
Medium	Assets required for operation over weekends and holidays	24 hours	Must be restored by end of next calendar day.
Low	Assets required for operation during normal business hours	72 hours	Must be restored by start of next business day.
Non-Essential	Assets not critical to business operations	> 72 h	Must be restored on an “as can” basis. Recovery required but not urgent.

Top 10 Most Common Findings

# 2 - Asset Management Issues

- EOL equipment
- No accurate asset inventory
- No lifecycle plan (OT and SCADA)
- No replacement budget
- No upgrade budget
- No spares or limited spares for critical components
- Unknown devices on the network

How to Fix It – Asset Management

1 *Start with Asset Inventory*

- *Visual Inventory*
- *Electronic Inventory (ICS network monitoring tools can provide this)*
- *Identify EOL status*
- *Identify software/firmware revisions*
- *Account for Spares (ID critical equip and ensure spares)*
- *Add to asset management system*

2 *Develop Lifecycle Plans for Each Component Type*

- *Computers – 5 years max (thin clients can last for 8-10)*
- *Network Equipment – 10 years*
- *PLCs – 10-20 years (depends on when in the manufacturer's lifecycle PLCs are purchased)*
- *Firewalls 3-5 years*

3 *Plan for Lifecycles*

- *Plan CAPEX/OPEX for replacements*
- *Some manufacturers have financing programs that span 5 years and keep costs even*

Top 10 Most Common Findings

#3 - Documentation Gaps

- No IP List
- No connectivity/network drawings
- No SCADA as-builts
- No network inventory
- No document management
- No documentation update procedure

How to Fix It – Documentation

Develop List, Diagrams, & As-Builts

- *The exercise alone will inform you on status of systems*
- *Can help locate single points of failure and critical assets*
- *Will help in long term maintenance and training of new staff*

Top 10 Most Common Findings

#4 - Backups and Disaster Recovery

- No backups
- No testing of backups
- No offsite backups
- No secured backups
- No DR procedure
- No restoration priority/criticality list

How to Fix It – Backups and DR

Follow 3-2-1-1-0 Backup Procedure
(five conditions to be met):

- ***At least 3 copies of your data, including the production copy***
- ***At least 2 different storage media should be used***
- ***At least 1 of the copies should be kept off-site***
- ***At least 1 copy should be kept offline*** *(can use cloud storage if immutable - immutability means that this copy cannot be modified in any way, under any circumstances)*
- ***Your backups should have completed with 0 errors***

How to Fix It – Backups and DR

Verify Backups

- *Ensure restore capabilities*
- *Test regularly*

Develop a DR Procedure

Procedure for complete server room destruction

- *Spare equipment?*
- *Order new equipment?*
- *VMs make recovery easier*
- *Have restore priority list*

Backups / Disaster Recovery

Backups

- HMI backups
- PLC code backups
- Server backups
- Workstation backups
- Offsite storage
- Keep backup data secure
  - From deletion
  - From unauthorized access

Top 10 Most Common Findings

#5 - Change/Configuration Management

- No change management procedure
- No change management board/committee
- No PLC configuration management
- No network configuration management
- No way to track changes
- No policy or procedure to document 3rd party vendor changes

How to Fix It – Change/Configuration Management

1 *Develop Change Management Policy & Procedure*

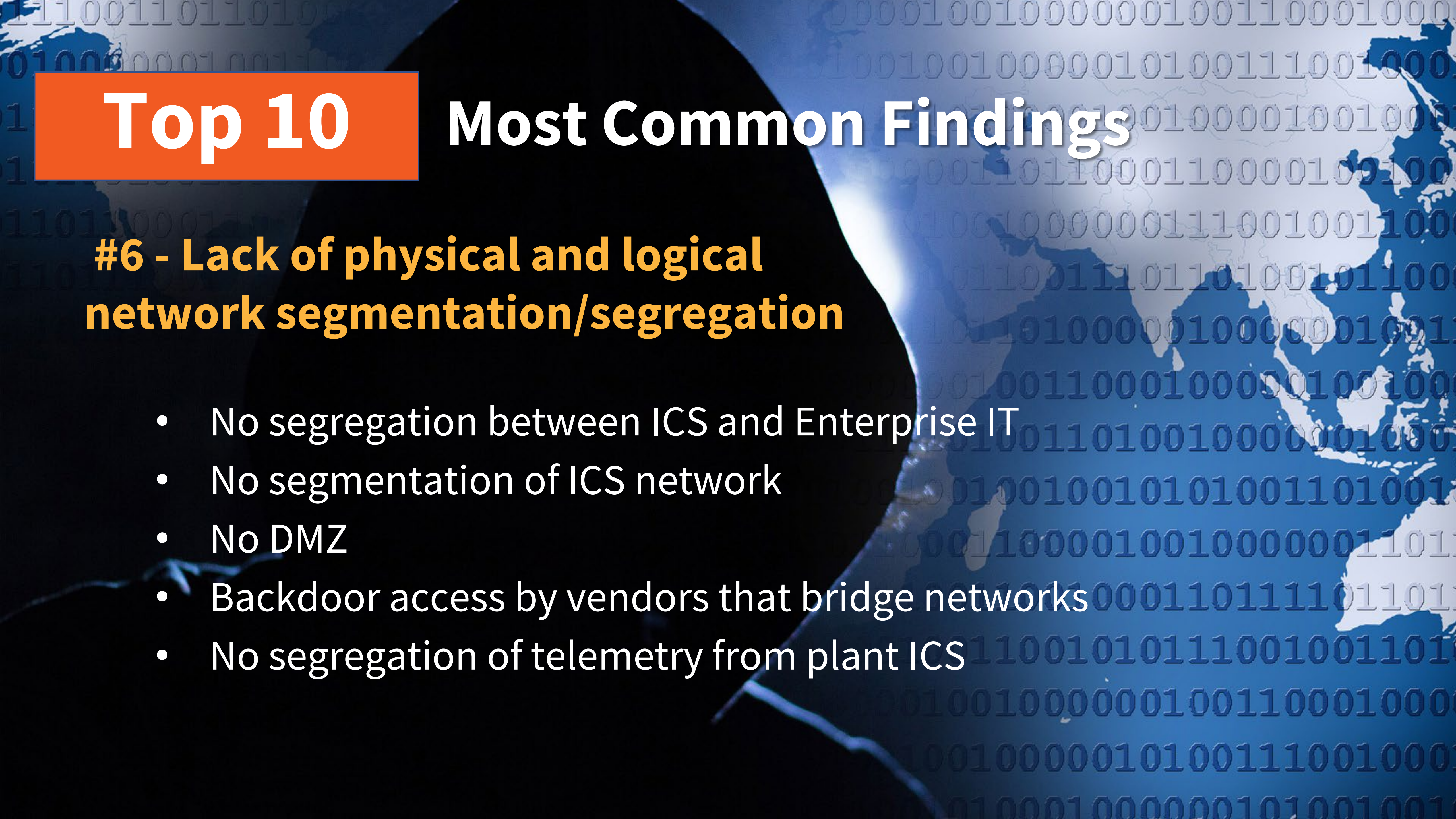
- *Develop Policy*
- *Institute and Change Management Board/Committee*
- *Develop procedure (forms, submittal process, review process)*
- *Develop log mechanism*

2 *Things to Consider*

- *Each submitted/proposed change should have backout/failback plan*
- *There should be an expedited process for emergency changes*
  - *Authority for change with retroactive approval?*

3 *Configuration Management*

- *Easier with software*
- *PLC, HMI, Network configs should be monitored*
- *Includes any vendor package system (always have copy of vendor PLC/OIT programs)*



Top 10 Most Common Findings

#6 - Lack of physical and logical network segmentation/segregation

- No segregation between ICS and Enterprise IT
- No segmentation of ICS network
- No DMZ
- Backdoor access by vendors that bridge networks
- No segregation of telemetry from plant ICS

How to Fix It –Network Segregation/ Segmentation

1 Segregate IT/OT!!!!!!!

- Top priority
- Do not share physical equipment between security zones
- Can use IT WAN transports via firewall /VPN tunnels

2 Implement DMZ if Required

(NIST SP 800-82 5.5.4)

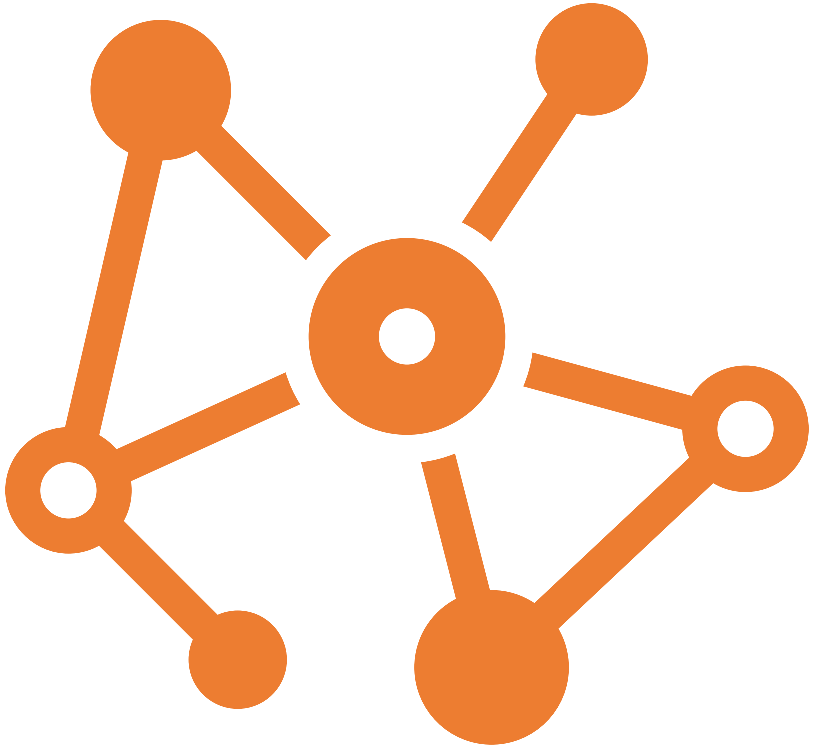
- Ensure no network bridging
  - Remote Access should be through DMZ and jump host
- Can have multiple DMZs

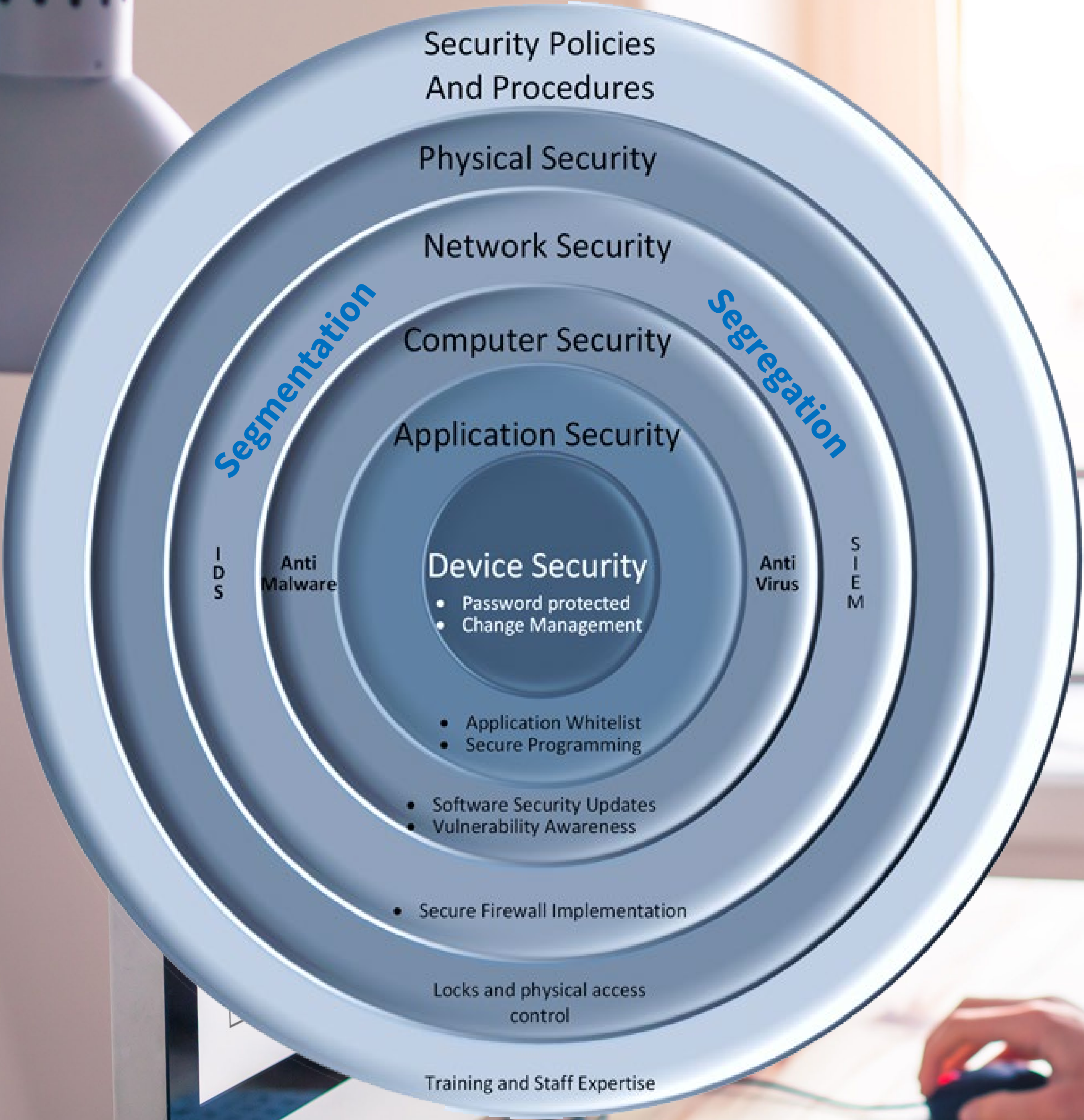
3 Use VLAN Segregation in the Control System Security Zone

- Helps protect sensitive control components
- Exclude windows protocols from PLC/Control VLAN

Network Segregation and Segmentation

“ ***NIST SP 800-82 R2 5.1-4 states:*** “Network segmentation and segregation is one of the most effective architectural concepts that an organization can implement to protect its ICS. The ICS network should, at a minimum, be logically separated from the corporate network on ***physically separate network devices.***”





Security Policies And Procedures

Physical Security

Network Security

Computer Security

Application Security

Device Security

- Password protected
- Change Management

Segmentation

Segregation

IDS

Anti Malware

Anti Virus

SIEM

- Application Whitelist
- Secure Programming

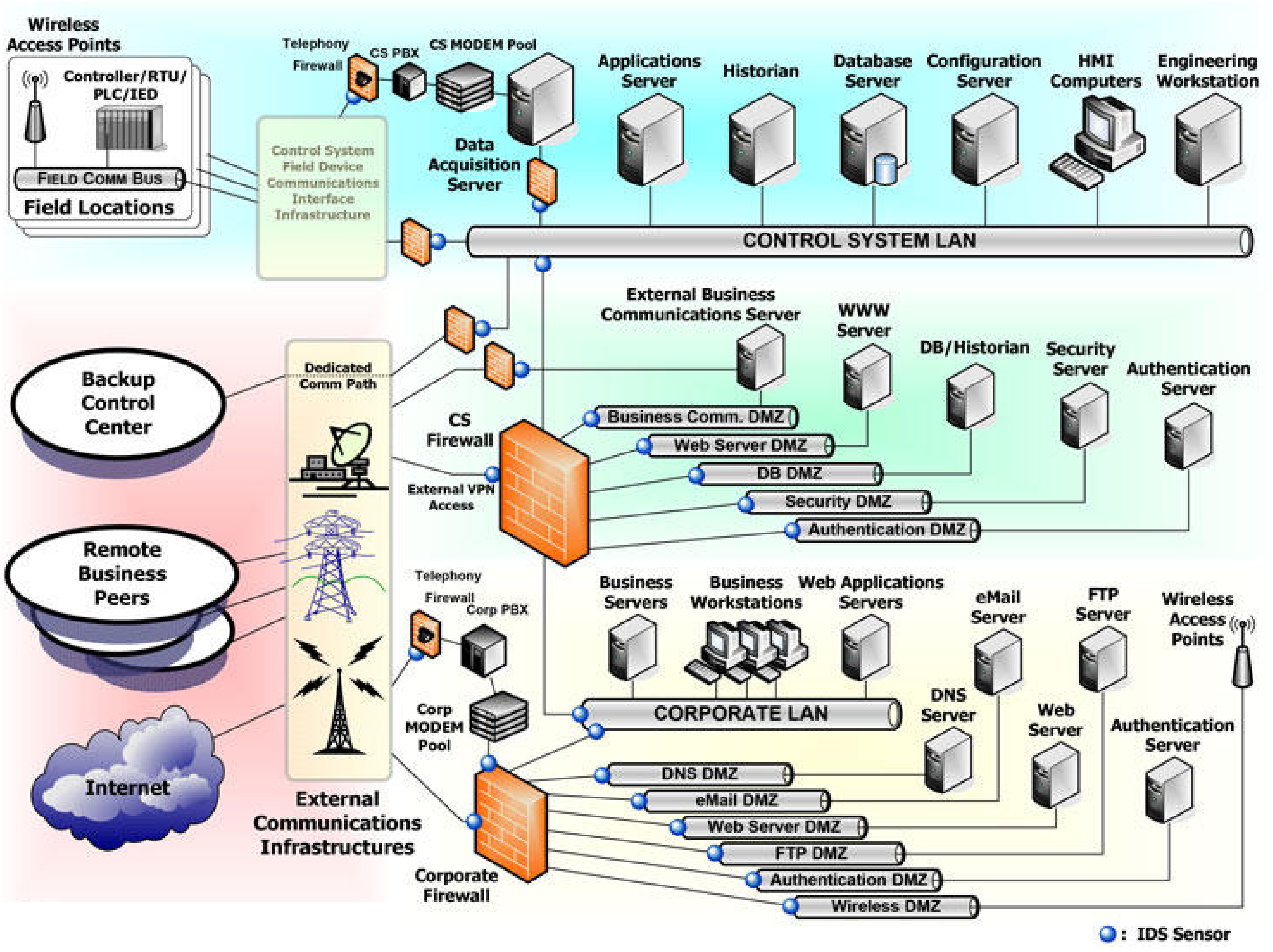
- Software Security Updates
- Vulnerability Awareness

- Secure Firewall Implementation

Locks and physical access control

Training and Staff Expertise

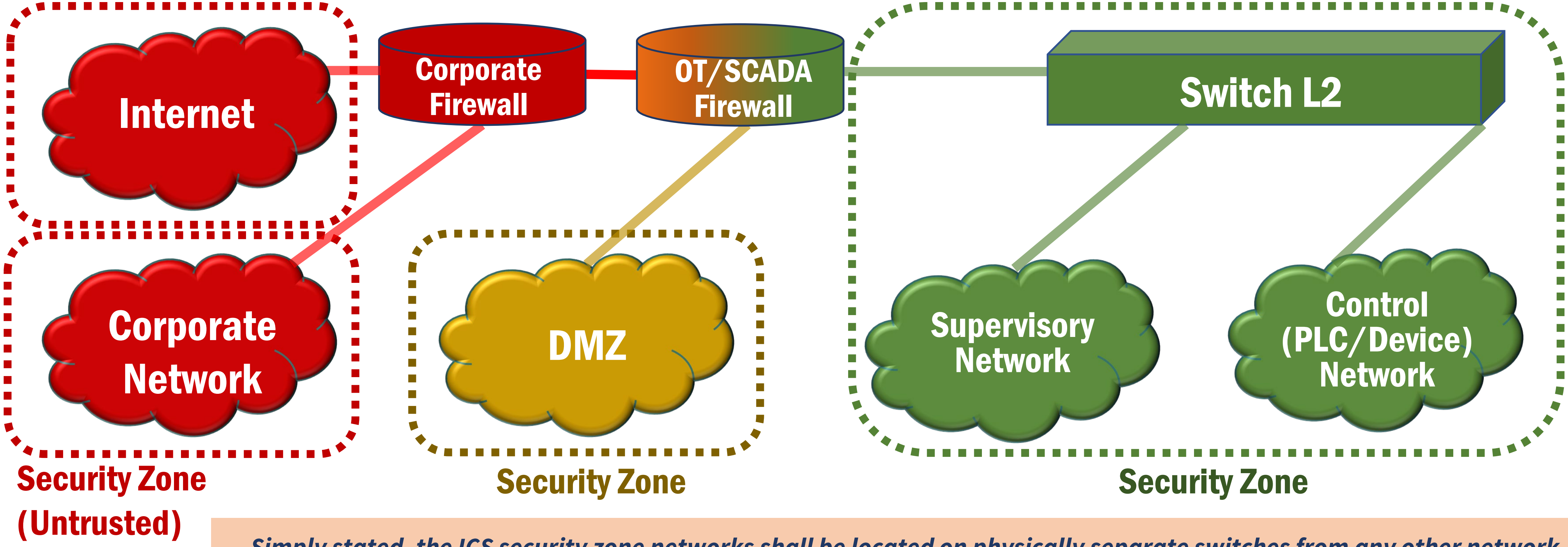
NIST Example ICS Diagram (From SP 800-82)



ICS Network Segmentation – Physical as Well as Logical

"The ICS network should, at a minimum, be logically separated from the corporate network on physically separate network devices."

it is strongly recommended that only minimal (single if possible) connections be allowed and that the connection is through a firewall and a DMZ."

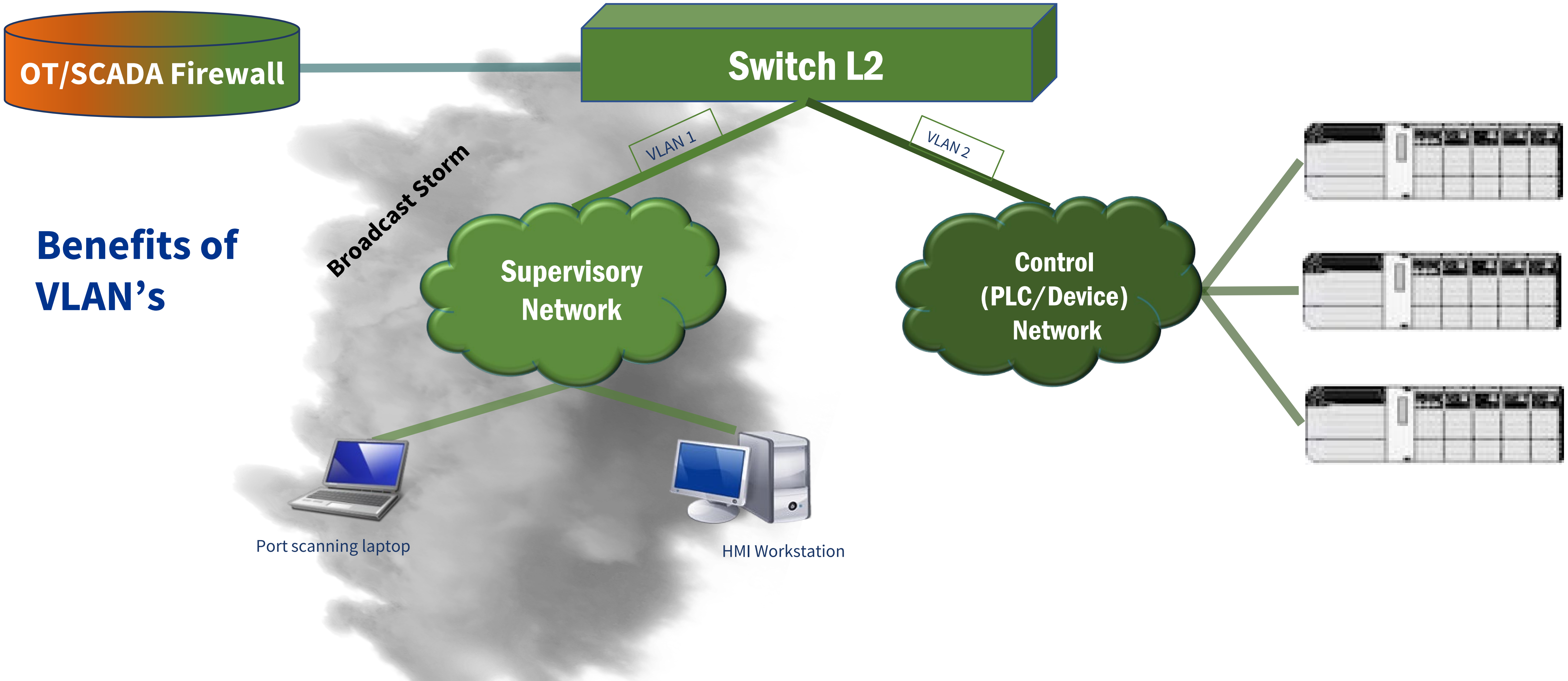


Simply stated, the ICS security zone networks shall be located on physically separate switches from any other network.

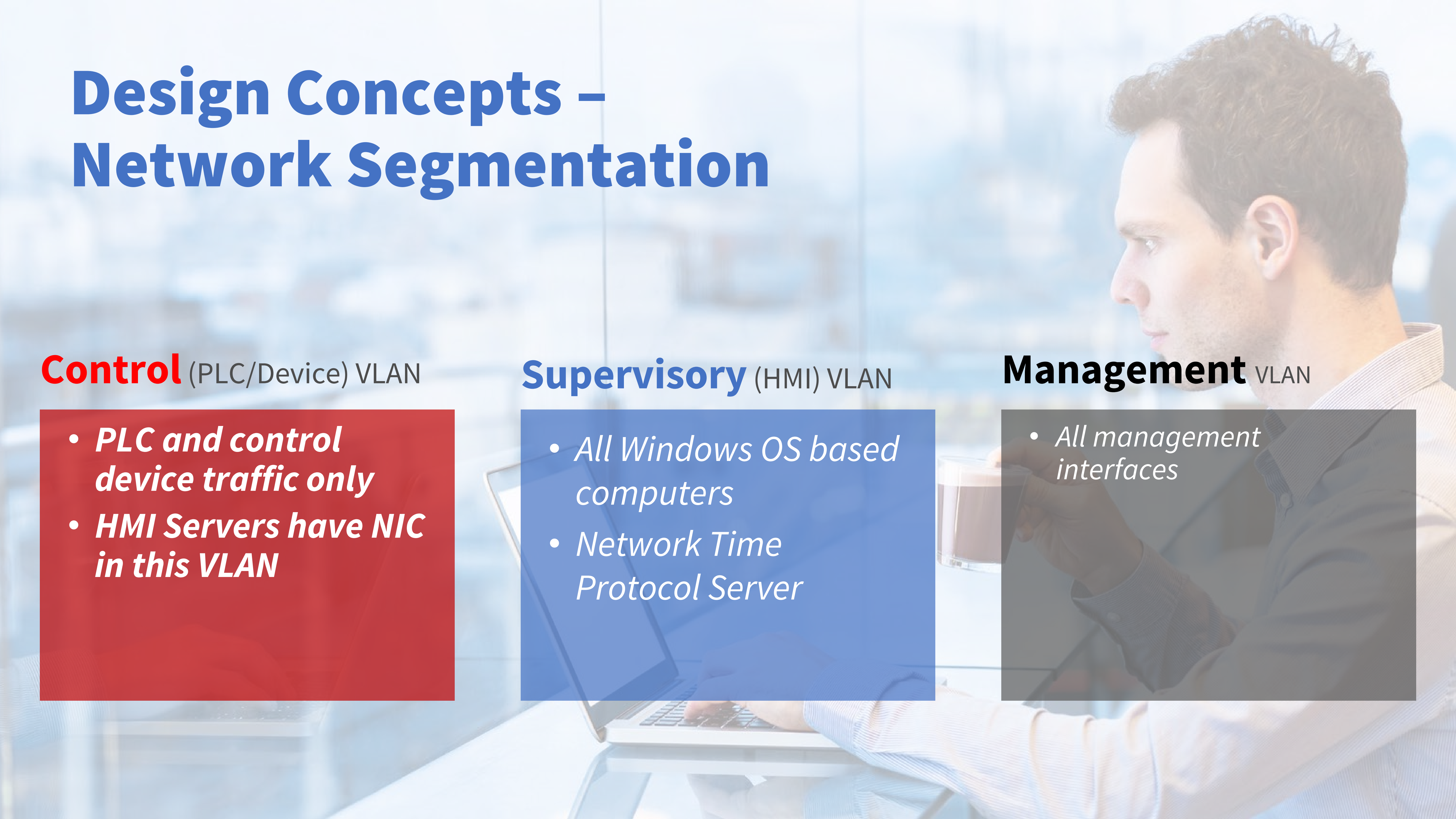
NIST SP 800-82r2 5.4 Logically Separated Control Network

Design Concepts – Network Segmentation

Benefits of VLAN's



Design Concepts – Network Segmentation



Control (PLC/Device) VLAN

- ***PLC and control device traffic only***
- ***HMI Servers have NIC in this VLAN***

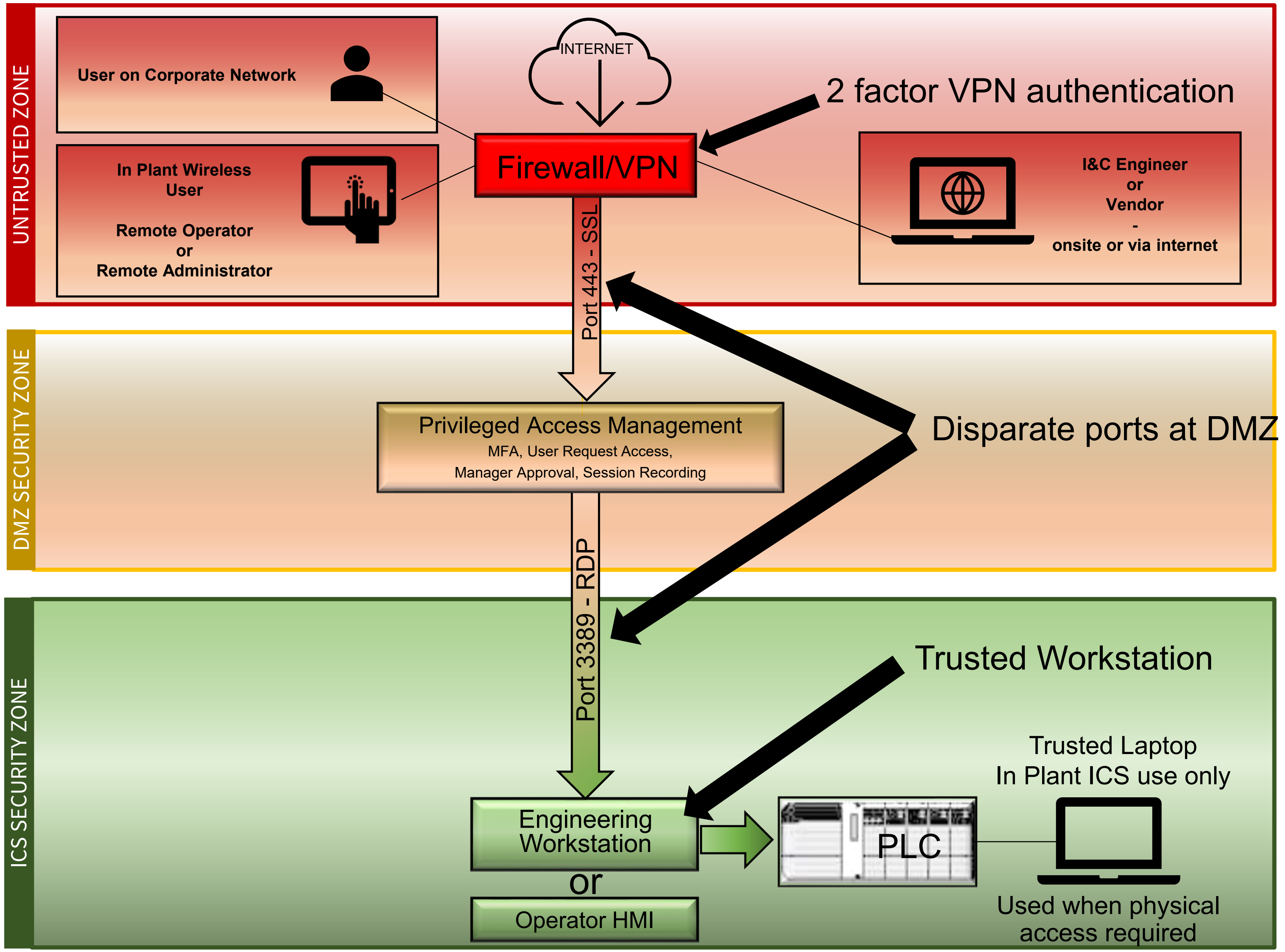
Supervisory (HMI) VLAN

- *All Windows OS based computers*
- *Network Time Protocol Server*

Management VLAN

- *All management interfaces*

Design Concepts - Secure Remote Access



UNTRUSTED ZONE

User on Corporate Network

In Plant Wireless User

Remote Operator
or
Remote Administrator

INTERNET

Firewall/VPN

2 factor VPN authentication

I&C Engineer
or
Vendor
-
onsite or via internet

Port 443 - SSL

DMZ SECURITY ZONE

Privileged Access Management
MFA, User Request Access,
Manager Approval, Session Recording

Disparate ports at DMZ

Port 3389 - RDP

ICS SECURITY ZONE

Trusted Workstation

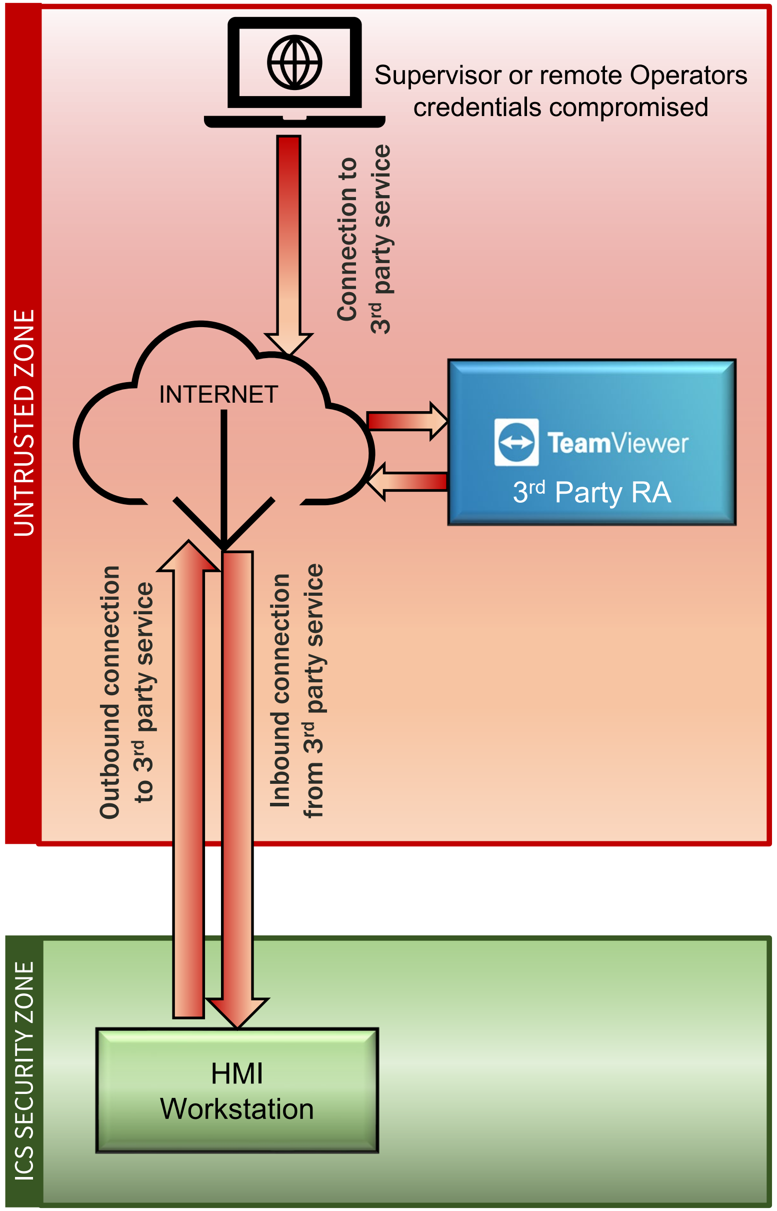
Engineering Workstation
or
Operator HMI

PLC

Trusted Laptop
In Plant ICS use only

Used when physical access required

Oldsmar Remote Access



UNTRUSTED ZONE

Supervisor or remote Operators credentials compromised

Connection to 3rd party service

INTERNET

TeamViewer
3rd Party RA

Outbound connection to 3rd party service

Inbound connection from 3rd party service

ICS SECURITY ZONE

HMI Workstation

Top 10 Most Common Findings

#7 - Staffing Issues

- No trained OT staff
- No designated cybersecurity staff
- Limited SCADA staff
- SCADA Staff expected to handle cybersecurity
- No CISO or similar position

How to Fix It –Staffing Issues

1 Designate Someone as Responsible for ICS Cybersecurity

- *Top priority*

2 Use Enterprise IT or Third Party for OT Support

- *If lacking OT skills within utility*
- *Using IT can be tricky, need clear SLAs/MOUs and proper ICS specific training*
  - *Staff changes can affect support*
- *Training SCADA staff to be OT/Cyber experts is very difficult*

3 Ensure Adequate SCADA Staff

- *Can help keep system updated and secure*
- *Can limit dependency on third party support during adverse events that affect large geographic areas*

Top 10 Most Common Findings

#8 - Lack of Standardization

- No PLC standards
- No HMI standards
- No networking standards
- No engineering/construction requirements to use standardized components

How to Fix It – Lack of Standards

Develop Standards

- ***Develop Standards***
- ***PLC, HMI, Alarm, Historian***
- ***Hardware, Software***
  - *Network*
  - *Servers*
  - *Firewalls*
  - *PLCs*
  - *OITs*
  - *Communications*
- ***Panels***
- ***Testing***

Ensure standards are in All Engineering Packages for CIP Projects

Top 10 Most Common Findings

#9 - Access Control Issues

- Logged on operator workstations (with no compensating control)
- No HMI security
- No security group delineation (Supervisors vs Operators)
- Common accounts (no non-repudiation)
- No account management
- No centralized access control/authentication

How to Fix It – Access Control Issues

Develop Policies & Procedures

- ***Access control policy***
- ***Access control settings***
- ***Security architecture***
  - *Security groups*
  - *Security policies*
  - *Application-level security*
- ***Use compensating security controls***

Policy for Termination/Departure

- ***Accounts disabled***
- ***Access revoked (electronic & physical keys)***

Physical Security

- Physically Secure
- Network Equipment
- Server Equipment
- Control Rooms
- PLC’s
- Radios
- Use Intrusion Alarms

Top 10 Most Common Findings

#10 - Anti-Virus/Anti Malware

- None
- Outdated
  - *No current definition updates*
  - *No engine updates*
- Old school products
- No AI-based detection
- No management

How to Fix It – Anti-Virus/Anti-Malware

Install Something

- *Check HMI vendor exclusions and recommendations*

Use EDR/XDR

- *Can be expensive*
- *The absolute best protection from ransomware*
- *Architectures use cloud services or substantial on-prem server infrastructure*

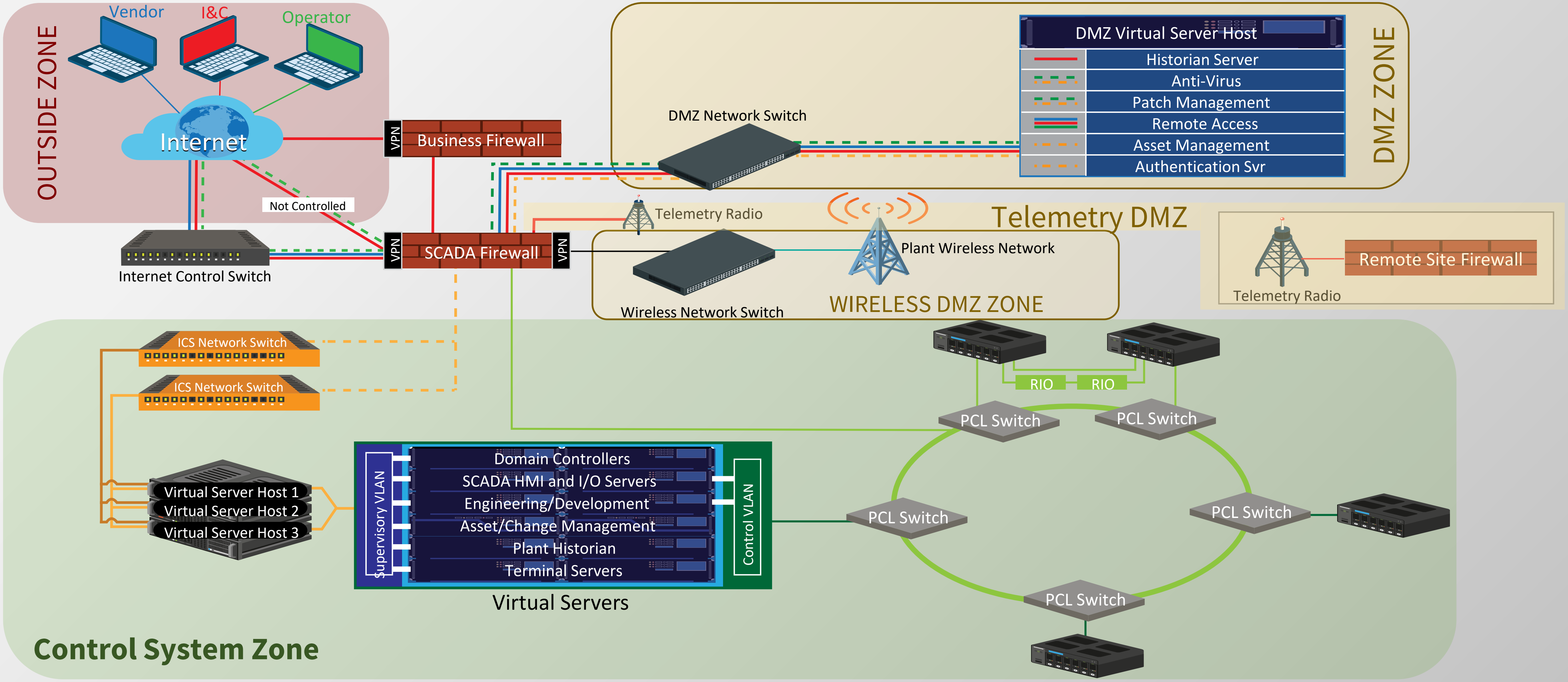
Other Common Findings

- No network logging (historian for the network)
- No network monitoring (lack of skillsets)
- Outdated/unsupported OS
- No current security patching
- No physical security on control panels, control room, server room
- Insecure remote access
- Insecure WiFi access
- No regular vulnerability or penetration testing
- No auditing ability (no accurate time source)
- 3rd Party devices allowed on ICS network (vendor laptops)
- Default credentials on devices
- Single points of failure

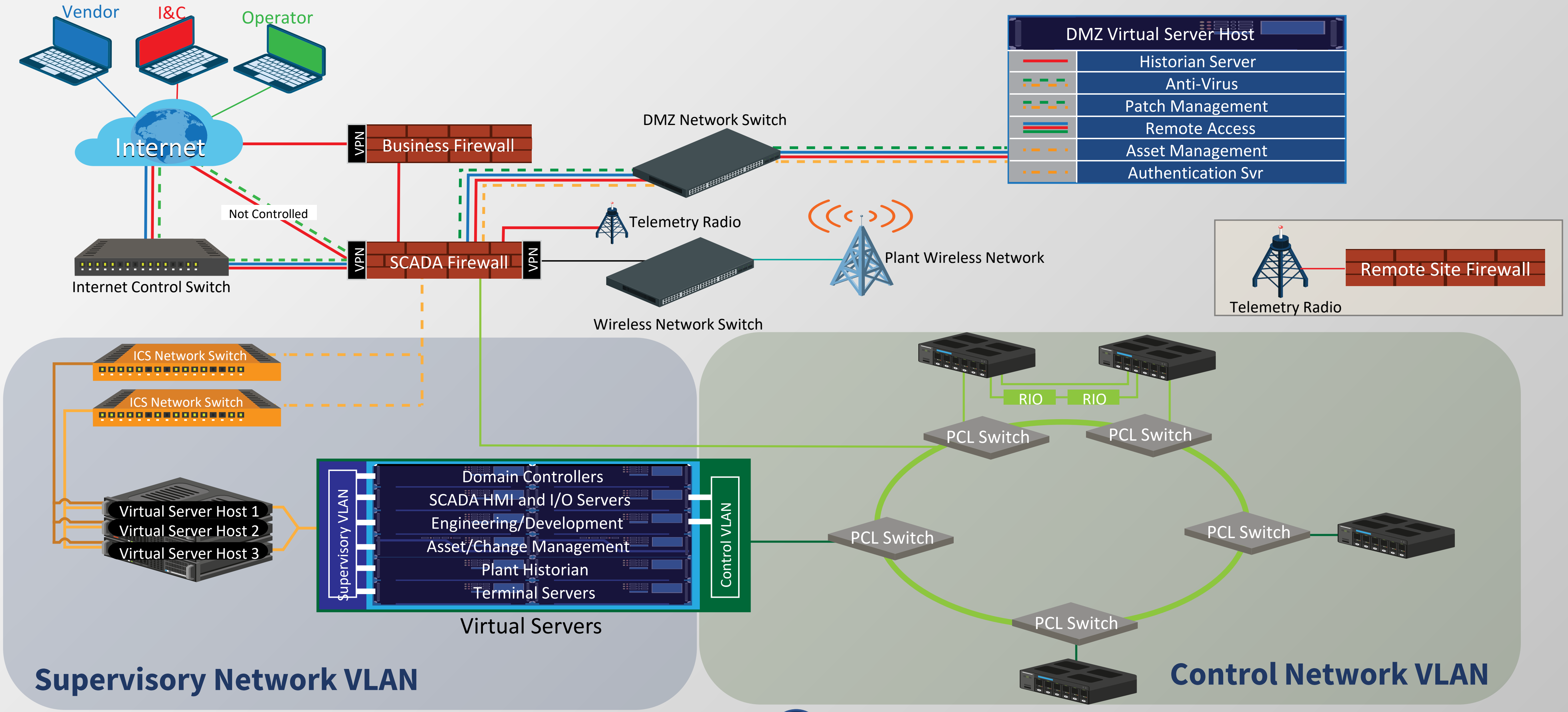
End of Presentation

Questions?

DESIGN CONCEPTS



DESIGN CONCEPTS



SP 800-82 Appendix G - ICS Overlay

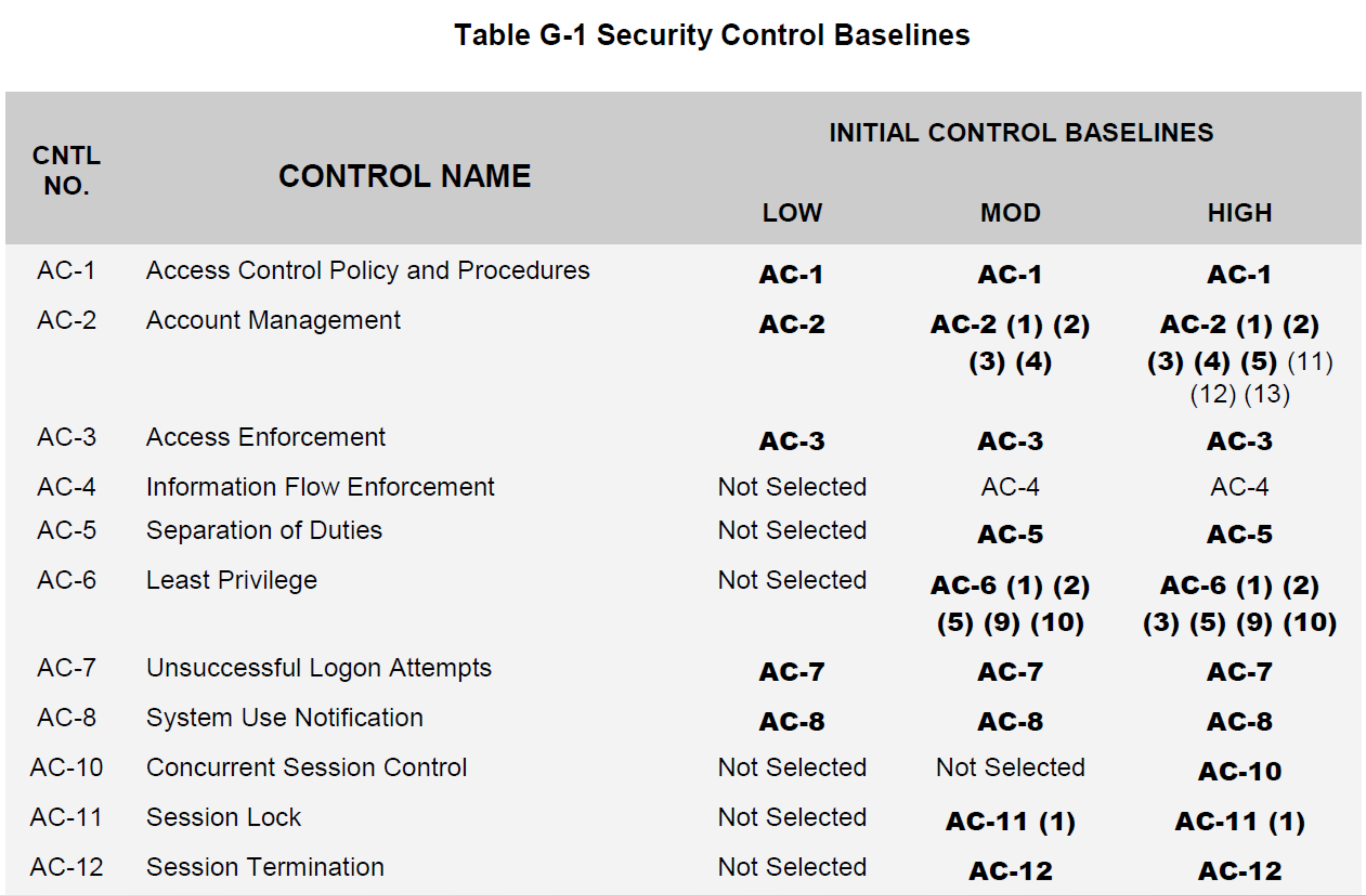
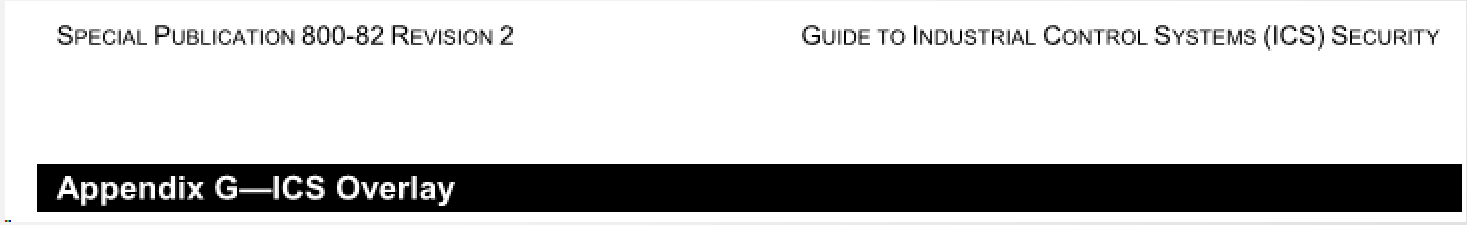


Table G-1 Security Control Baselines

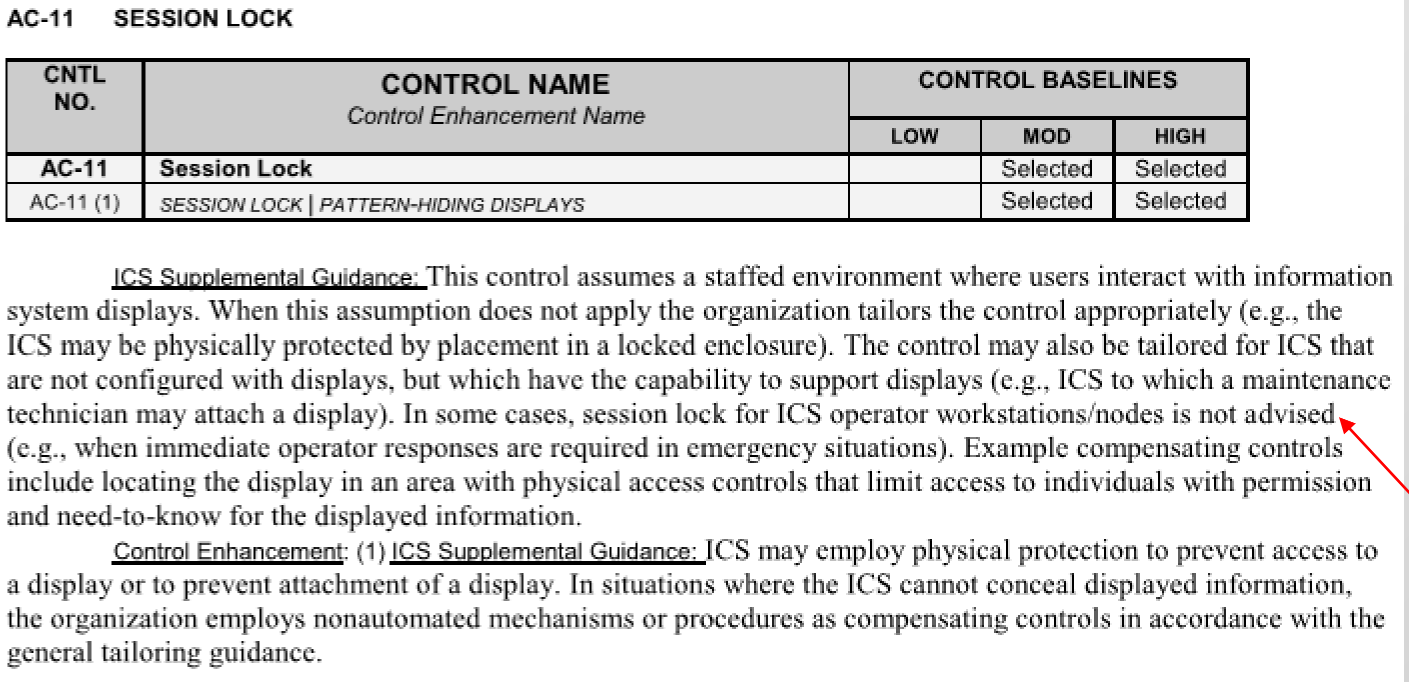
CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
AC-1	Access Control Policy and Procedures	**AC-1**	**AC-1**	**AC-1**
AC-2	Account Management	**AC-2**	**AC-2 (1) (2) (3) (4)**	**AC-2 (1) (2) (3) (4) (5)** (11) (12) (13)
AC-3	Access Enforcement	**AC-3**	**AC-3**	**AC-3**
AC-4	Information Flow Enforcement	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	Not Selected	**AC-5**	**AC-5**
AC-6	Least Privilege	Not Selected	**AC-6 (1) (2) (5) (9) (10)**	**AC-6 (1) (2) (3) (5) (9) (10)**
AC-7	Unsuccessful Logon Attempts	**AC-7**	**AC-7**	**AC-7**
AC-8	System Use Notification	**AC-8**	**AC-8**	**AC-8**
AC-10	Concurrent Session Control	Not Selected	Not Selected	**AC-10**
AC-11	Session Lock	Not Selected	**AC-11 (1)**	**AC-11 (1)**
AC-12	Session Termination	Not Selected	**AC-12**	**AC-12**

System Cybersecurity Details - NIST SP 800-82 Appendix G



SPECIAL PUBLICATION 800-82 REVISION 2 GUIDE TO INDUSTRIAL CONTROL SYSTEMS (ICS) SECURITY

Appendix G—ICS Overlay



AC-11 SESSION LOCK

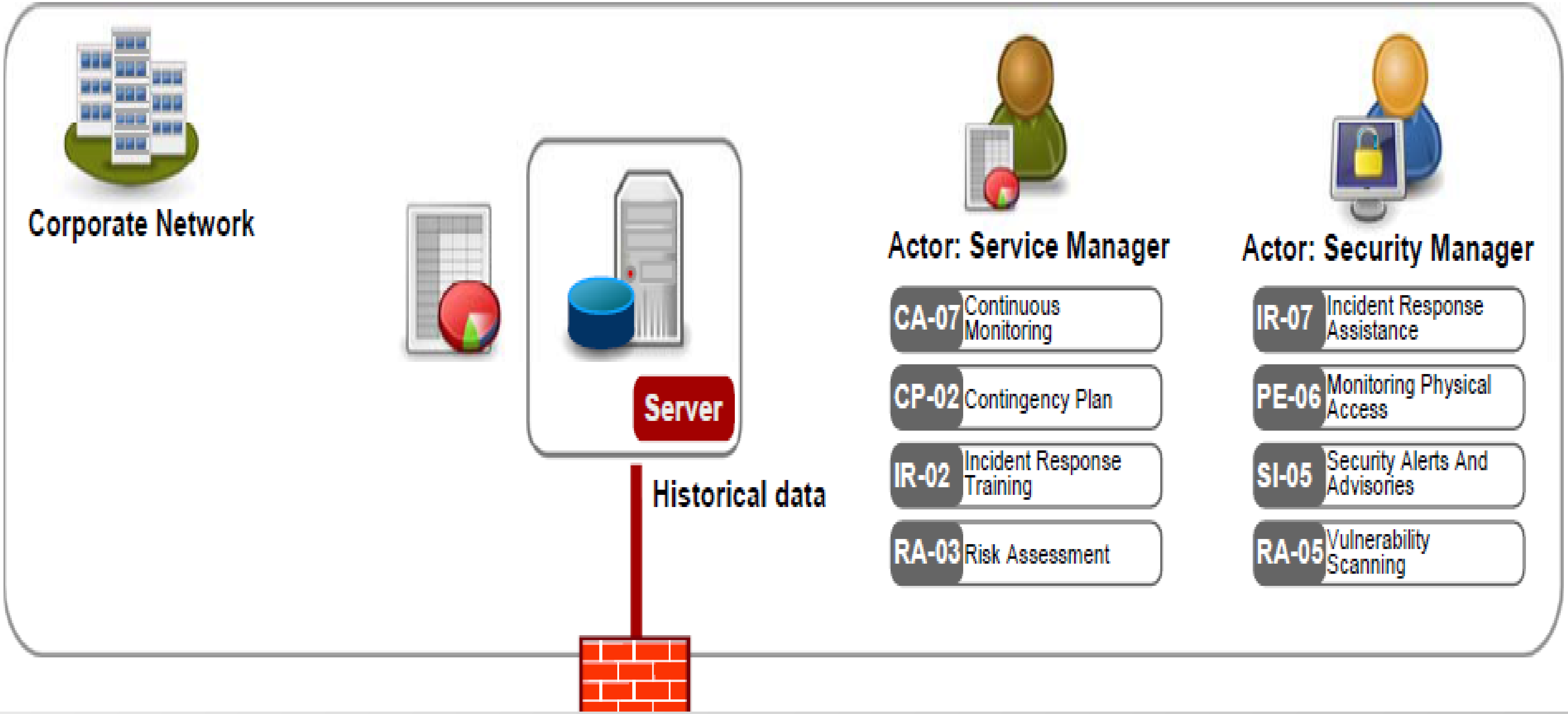
CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-11	**Session Lock**		Selected	Selected
AC-11 (1)	*SESSION LOCK | PATTERN-HIDING DISPLAYS*		Selected	Selected

ICS Supplemental Guidance: This control assumes a staffed environment where users interact with information system displays. When this assumption does not apply the organization tailors the control appropriately (e.g., the ICS may be physically protected by placement in a locked enclosure). The control may also be tailored for ICS that are not configured with displays, but which have the capability to support displays (e.g., ICS to which a maintenance technician may attach a display). In some cases, session lock for ICS operator workstations/nodes is not advised (e.g., when immediate operator responses are required in emergency situations). Example compensating controls include locating the display in an area with physical access controls that limit access to individuals with permission and need-to-know for the displayed information.

Control Enhancement: (1) ICS Supplemental Guidance: ICS may employ physical protection to prevent access to a display or to prevent attachment of a display. In situations where the ICS cannot conceal displayed information, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

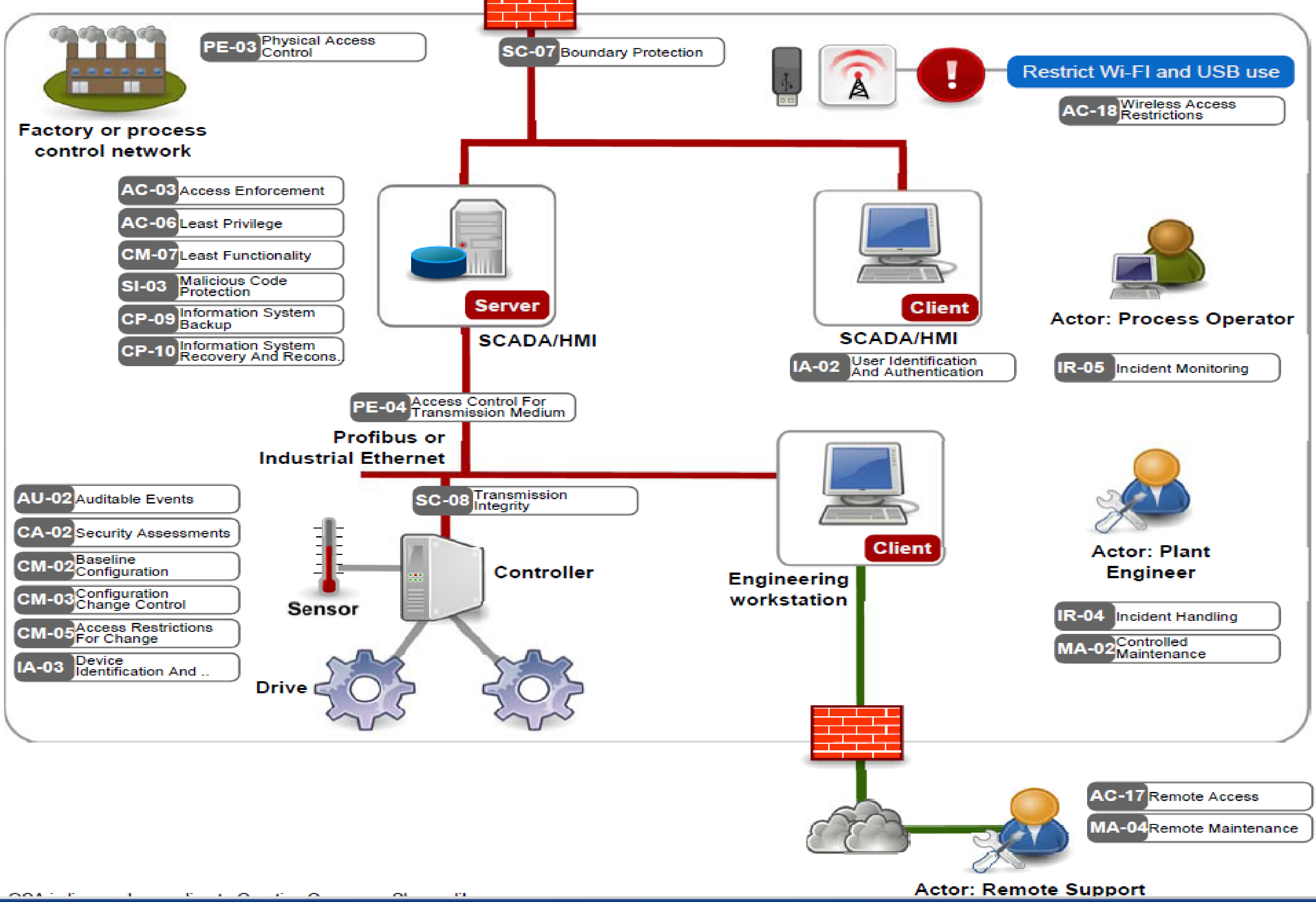
In some cases, session lock for ICS operator workstations/nodes is not advised

Policies and Procedures



Corporate Network
Server
Historical data
Actor: Service Manager
CA-07 Continuous Monitoring
CP-02 Contingency Plan
IR-02 Incident Response Training
RA-03 Risk Assessment
Actor: Security Manager
IR-07 Incident Response Assistance
PE-06 Monitoring Physical Access
SI-05 Security Alerts And Advisories
RA-05 Vulnerability Scanning

Policies and Procedures


Factory or process control network
PE-03 Physical Access Control
SC-07 Boundary Protection
Restrict Wi-FI and USB use
AC-18 Wireless Access Restrictions
AC-03 Access Enforcement
AC-06 Least Privilege
CM-07 Least Functionality
SI-03 Malicious Code Protection
CP-09 Information System Backup
CP-10 Information System Recovery And Recons.
Server
SCADA/HMI
Client
SCADA/HMI
IA-02 User Identification And Authentication
Actor: Process Operator
IR-05 Incident Monitoring
PE-04 Access Control For Transmission Medium
Profibus or Industrial Ethernet
AU-02 Auditable Events
CA-02 Security Assessments
CM-02 Baseline Configuration
CM-03 Configuration Change Control
CM-05 Access Restrictions For Change
IA-03 Device Identification And ..
SC-08 Transmission Integrity
Sensor
Controller
Drive
Client
Engineering workstation
Actor: Plant Engineer
IR-04 Incident Handling
MA-02 Controlled Maintenance
AC-17 Remote Access
MA-04 Remote Maintenance
Actor: Remote Support