Test & Measurement System Security in an IT World

NI Security Summit

Derek Mayer

October 13, 2021

Jacobs

Challenging today.
Reinventing tomorrow.

Abstract

- Automated test and measurement systems are coming under increased cybersecurity scrutiny. Most of these systems fall under the “Operational Technology” designation, as defined by NIST, and often have unique requirements that conflict with enterprise security policy. These systems are typically not well understood by traditional enterprise IT personnel, which leaves them ill-supported or invalidated.
- This presentation attempts to help Test System owners recognize the security landscape, determine their unique system requirements and concerns, and negotiate a peer-level working arrangement with an existing IT department while maintaining a NIST-recommended level of autonomy and sovereignty.

Objective

- Stimulate thinking/discussion

Caveat

- You know your operational/political environment, I do not

Preparing to Deal with the IT Department

- Stonewalling, misdirection, strategic omission, Buffaloing/overwhelming, strong-arming, out-maneuvering, etc.
- Working with the IT Dept is INEVITABLE
  - Want to enter agreements on equal footing
  - Ideas, experiences and resources to get there

Agenda

Design/Build Your System
- Keep cybersecurity in mind
- Let IT Dept help you, where appropriate

Cooperate/Integrate
- Cooperate with IT Dept
- Articulate to upper mgmt
- Defend your sovereignty

Learn Some IT/ Cybersecurity
- Be able to communicate effectively with IT Dept

Leverage OT Platform
- NIST Standards

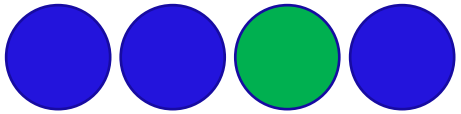
Understand My System
- Capture requirements
- Articulate priority

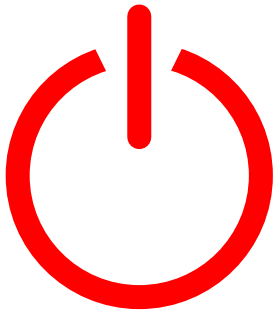
My Background is

- University education: Nuclear Engineering (emphasis plasma physics)
- Onsite contractor for NASA's MSFC for 22+ years
- Primary responsibility: Design, build and support LabVIEW-based measurement and control systems for the Test Laboratory.
  - Recent emphasis on IT capability and OT cybersecurity.
- MSFC Test Lab:
  - Rocket engine testing
  - *Wind tunnel*
  - *Environmental Test (space qualification)*
  - *Turbomachinery component performance testing*
  - Material Strength testing
  - Metrology – Calibration Lab for common equipment

Why are you here?

- Because my system is different from Enterprise/IT systems
  - My system cannot properly function with some IT security policies





Shutdown Day

- The IT department has/tried to shut down my system, or I am concerned they will try
- My company has to meet cybersecurity metrics for regulatory reasons, which includes my test systems

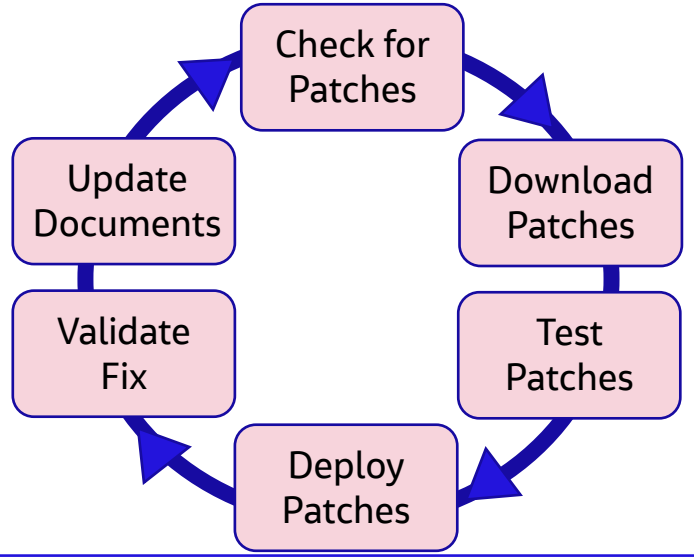
- I need to figure out how to work with the IT department to get what I need if my system is going to survive.
  - I want a solid platform that the IT Dept is forced to respect

My system is special because..

Can't tolerate a random reboot during "operations"?

Do you interface specialized hardware? Specialized software?

Configuration Control:
"freeze until change" or
An endless bi-weekly patching cycle?



Don't see your reason here?
Add it to the chat box to share!

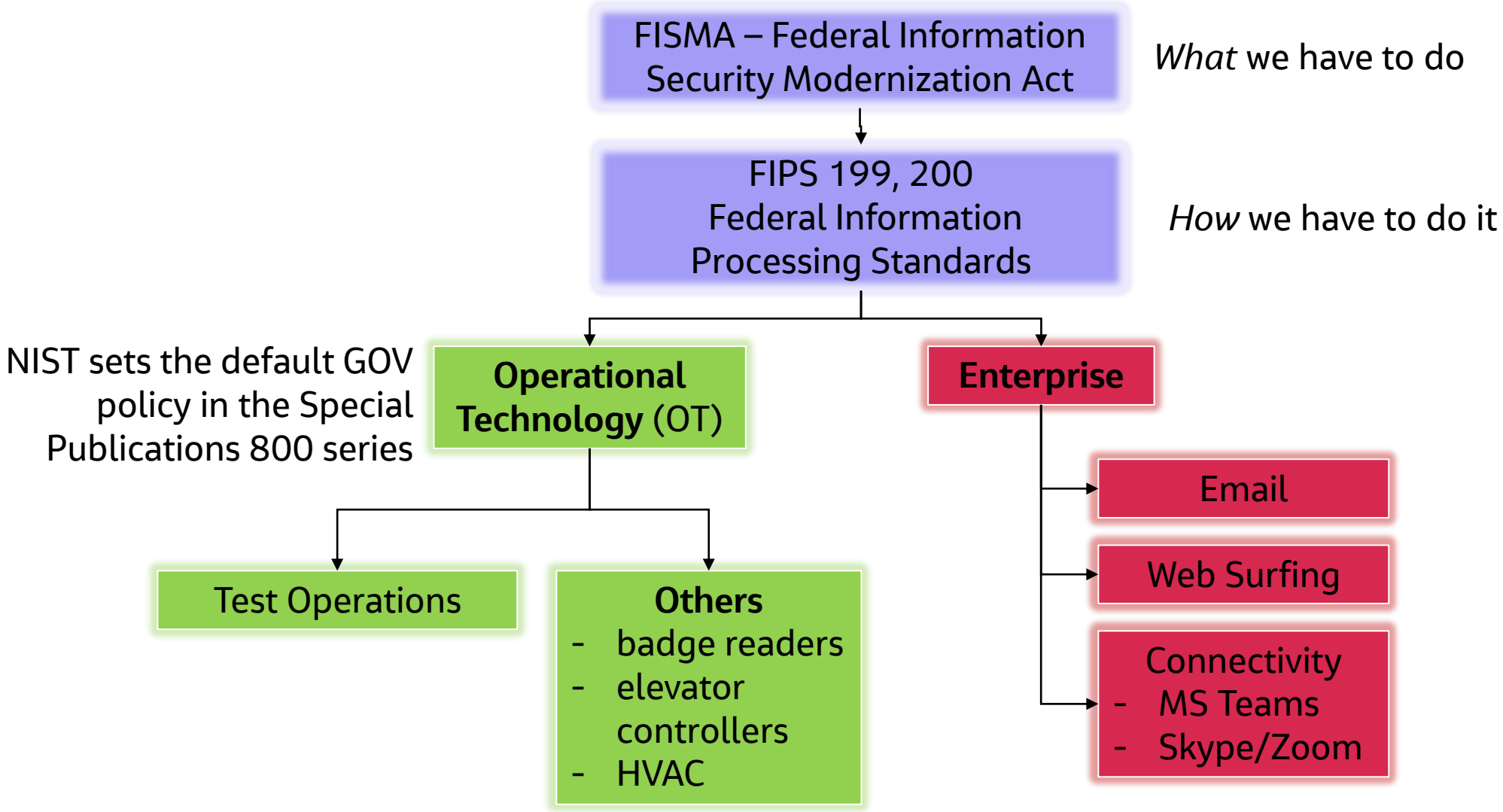
* Capture the requirements of your system that are incompatible with IT/Enterprise policy

What are your concerns?

- Application-Specific
  - Test Operations
    - Personnel/Test Facility/Test Article **SAFETY**
  - Production Line
    - Anything that impacts the quality or quantity of production
  - R&D Lab
    - Interference with product development or system testing
  - Other?
    - List it in the chat!
- Systemic
  - IT Dept assumes the worst-case consequence is that a user is forced to restart
    - Issues remaining after forced patching can be addressed through existing support channels
  - IT Dept assumes Enterprise metrics apply, when they may not.

* Compile and be able to articulate your concerns. Exaggerate (slightly) if necessary.

Information Technology = Enterprise + Operational Technology



* OT security policy has more freedom than Enterprise. This can be disorienting to Enterprise personnel.

Operational Technology is..

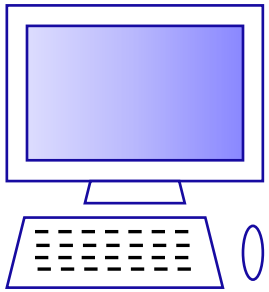
- *"hardware and software that is physically part of, dedicated to, or essential in real time to the performance, monitoring, or control of physical devices and processes*"
  - NASA OT Security Handbook
- "hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events."
  - NIST, Wikipedia









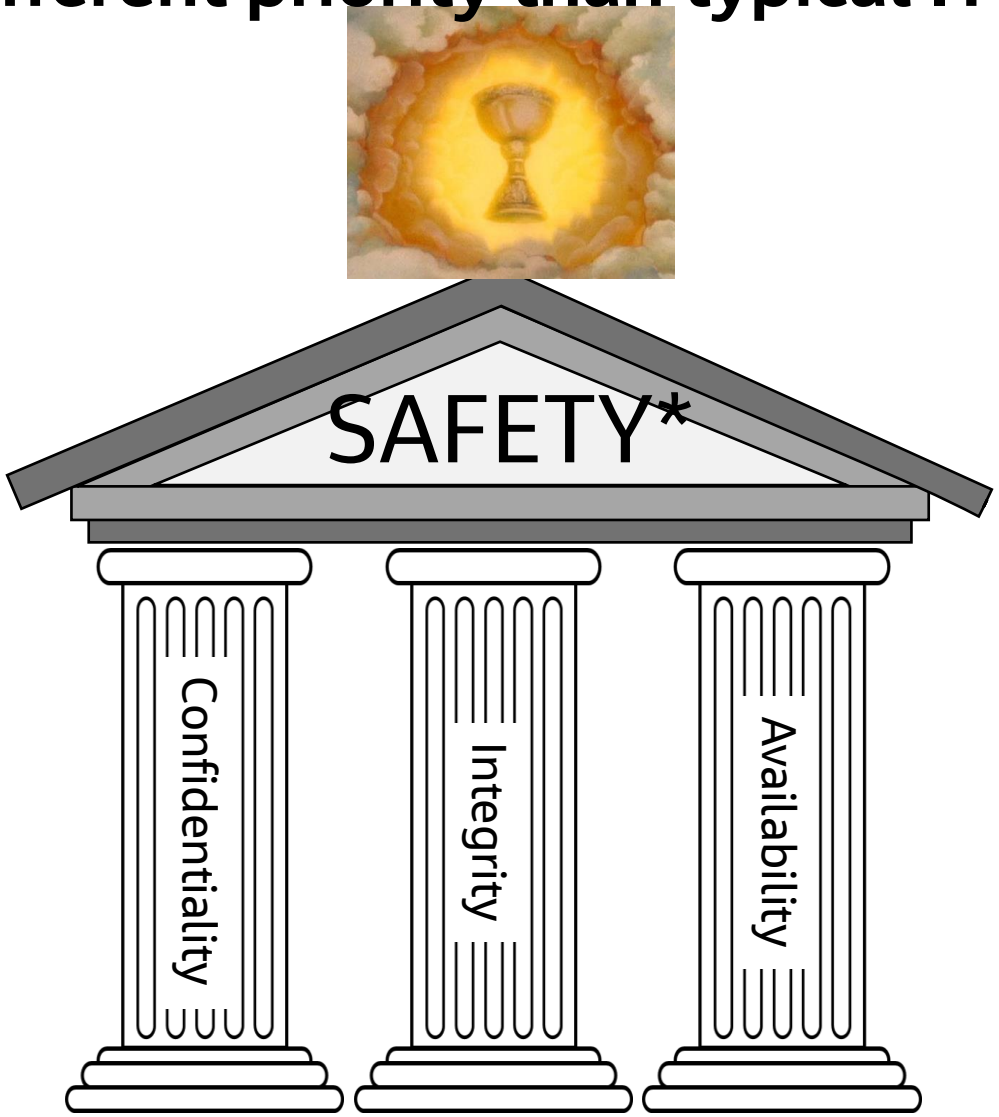



Critical Infrastructure is..

- “Critical infrastructure describes the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety. The Nation's critical infrastructure provides the essential services that underpin American society.” (https://www.cisa.gov/infrastructure-security)
- Examples include:
  - Power plants/grids
  - Banking (ATMs)
  - Transportation
    - Fuel Pumps
    - Fuel Refining
    - Fuel Delivery Pipelines
    - Municipal Water Supply
    - Waste Treatment

https://news.sky.com/story/hackers-try-to-poison-florida-town-by-changing-chemical-levels-at-water-treatment-plant-12212892

OT Systems have a different priority than typical IT cybersecurity

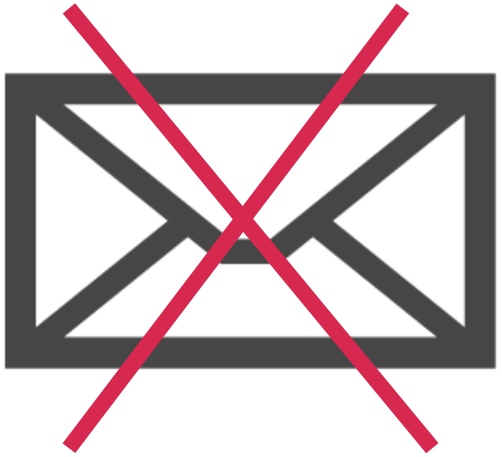


* Be able to articulate your highest priority (Production? Product development?)

Address Some Cybersecurity Concerns Early

- Historically, the biggest threat vectors have been:

Web surfing



Email

File Transfer

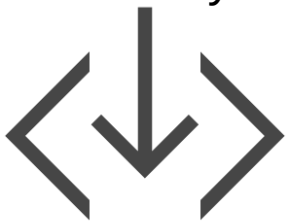
Agreeing with IT/Enterprise on a Process to Define Security Controls

Confidentiality

Integrity

Availability

Security Controls Overlay



Identify System
- Define Boundary(s)
- System Descriptions
- Inventory Contents

Categorization
- Assess as LOW, MEDIUM, or HIGH
- Law/Regulations

Apply Security Controls
- NIST Risk Management Framework
- Overlay(s) for OT

Tailor as Necessary
- Controls are overlapping/redundant
- Who authorizes RBDs?

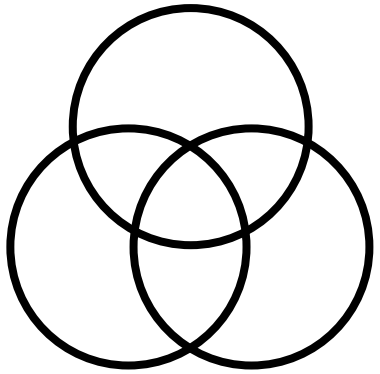
* Ask what the process is at your organization. Be prepared for chaos/no direct answer.

So, I have a list of security controls to apply. Now what?

- Do It Yourself
  - Do you have the time/interest/experience?
  - Does IT have a script/automation to use?
- Let IT Dept setup your system?
  - Can you trust this arrangement? Will it give them control of your system?
  - The IT Dept may have mandates to install “agent” software that functions as a back door to alter the configuration of your system
- Get some help:
  - Collaborate with IT Dept
  - Hire consultant/support
  - For medium/large systems, consider centralized control

Why are there so many controls?

- Each control requirement forces the system designer to consider a particular aspect of security



- Controls are designed to be overlapping
  - In engineering: “factor of safety” or “2-fault tolerant” or generally “robust”
  - In Cybersecurity-speak: “defense-in-depth”

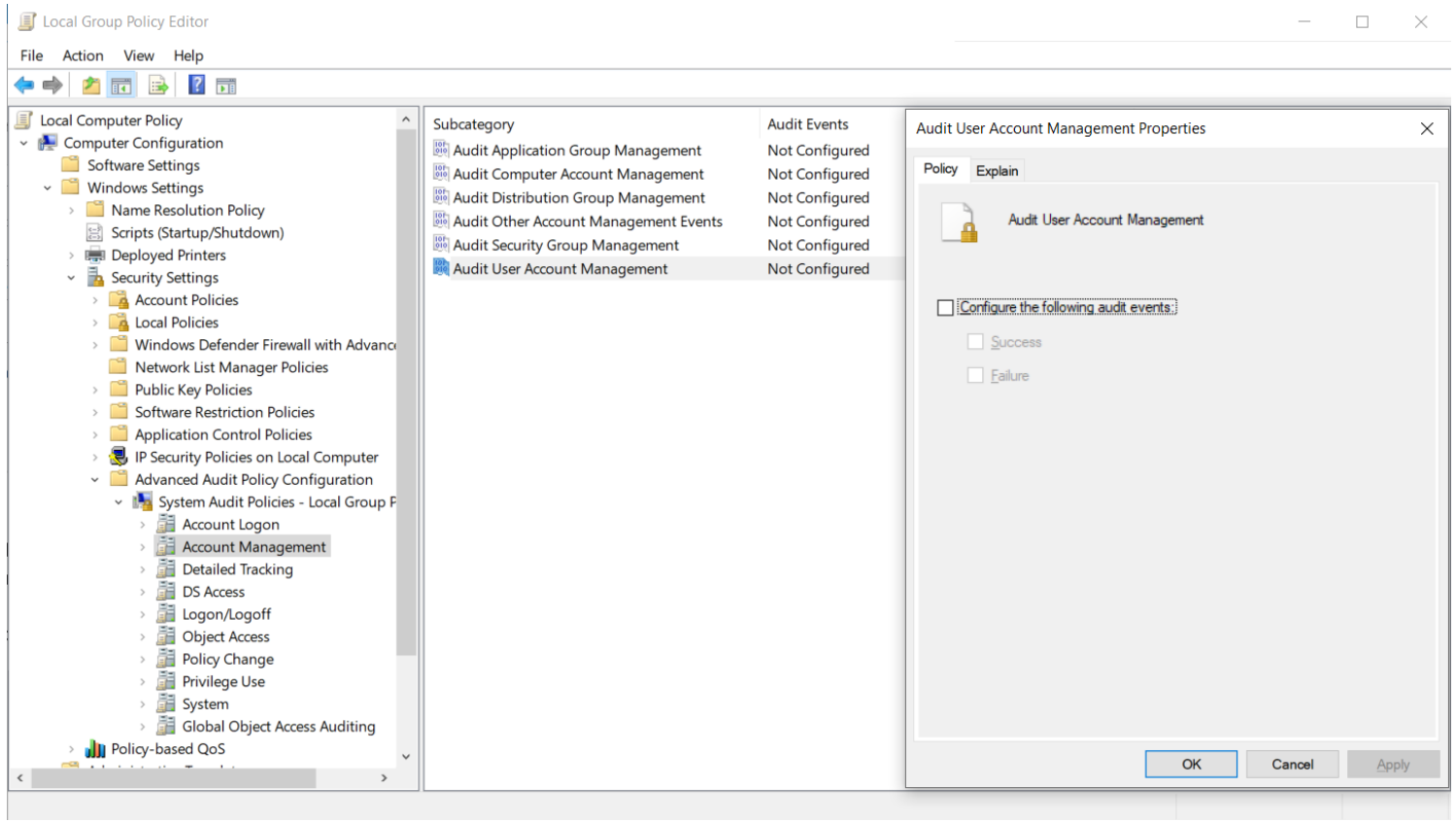
- *Cybersecurity modeling is based not only on surviving component failures, but also hacking.*

Security Control Example

- Many controls are designed to work directly with OS settings. Simply turn them ON.

AC-2(4)	ACCOUNT MANAGEMENT | *AUTOMATED AUDIT ACTIONS*	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-2(4)[1]	*the information system automatically audits the following account actions:*
	AC-2(4)[1][a]	*creation;*
	AC-2(4)[1][b]	*modification;*
	AC-2(4)[1][c]	*enabling;*
	AC-2(4)[1][d]	*disabling;*
	AC-2(4)[1][e]	*removal;*

NIST SP800-53 Security & Privacy Controls



Audit User Account Management (Explain tab)

This policy setting allows you to audit changes to user accounts. Events include the following:

* A user account is created, changed, deleted; renamed, disabled, enabled, locked out, or unlocked.
* A user account's password is set or changed.
* A security identifier (SID) is added to the SID History of a user account.
* The Directory Services Restore Mode password is configured.
* Permissions on administrative user accounts are changed.
* Credential Manager credentials are backed up or restored.

Relevant NIST Standards

- **NISTSP800-37** Guide for Applying Risk Management Framework for Federal Info Systems
- **NISTSP800-53** Security and Privacy Controls for Federal Information Systems
- **NIST800-82** Guide to Industrial Control Systems Security
  - Ch 3 – ICS Risk Management and Assessment
  - Ch 4 – ICS Security Program Development and Deployment
  - Ch 5 – ICS Security Architecture
- Available at: https://csrc.nist.gov/publications/sp800
  - Learn some IT/Cybersecurity
  - Get ideas about how to defend your sovereignty

Highlights of NIST-Recommended Changes from Enterprise to OT

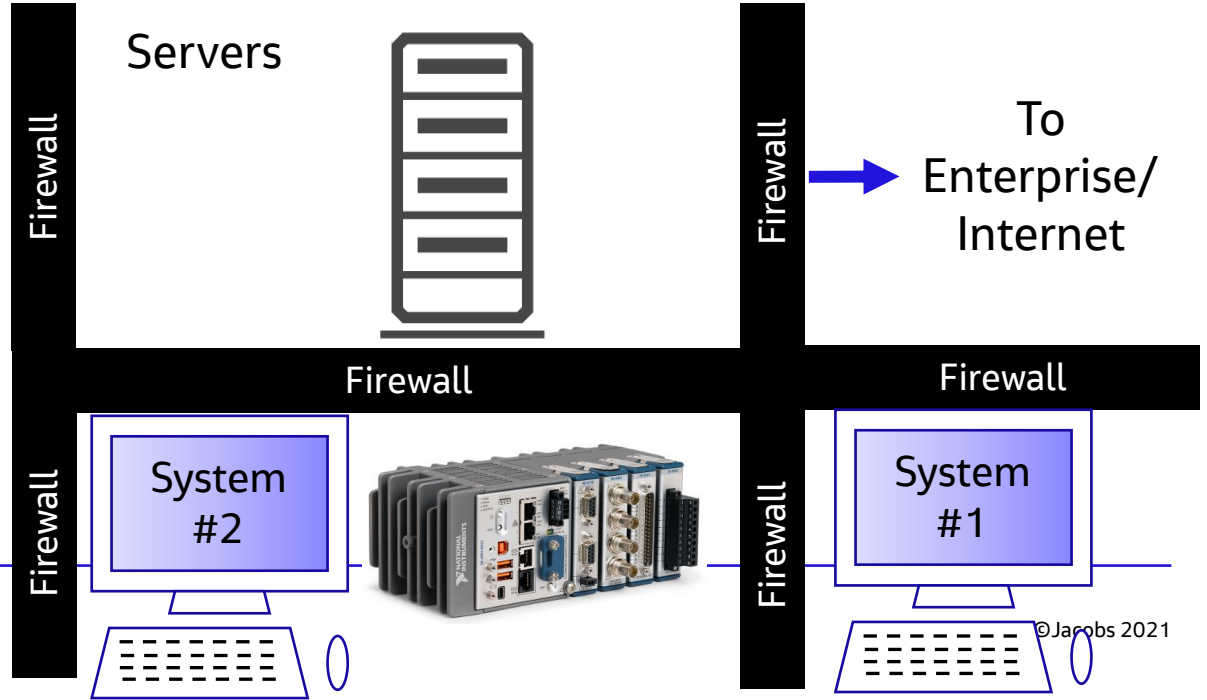
- Network
  - Static IP addressing, no DHCP
  - Firewalled protection from Enterprise/internet
    - Written and signed Interconnect Agreement
  - Various Demilitarized Zone (DMZ) configurations
- Authentication
  - Credential separately on OT systems (compared to Enterprise)
  - No trust relationship between OT credentialing and Enterprise
  - Multiple users may need access to the same user account
- A computer/system or user account may be assigned to a purpose
- Network isolation is not cybersecurity

Taken from NIST800-82 Guide to Industrial Control Systems Security, §5 ICS Security Architecture

I Challenge You to Build: Network

- Totally different than Enterprise design
  - Static IP addressing (No DHCP)
  - Segmentation - numerous subnets, mostly isolated from eachother
  - Only necessary ports/protocols open, everything else CLOSED/DISABLED by default
- Firewalled Connectivity to Enterprise/Internet
- Keep all system components together

* "Firewall" is virtual or appliance; ACL, traditional or NGFW



NIST-Recommended Network Layout

- OT Networks and Devices need greater security than Enterprise systems
- DMZ (Demilitarized Zone) Approach
  - All traffic begins or ends in the DMZ
  - No traffic is allowed through both firewalls

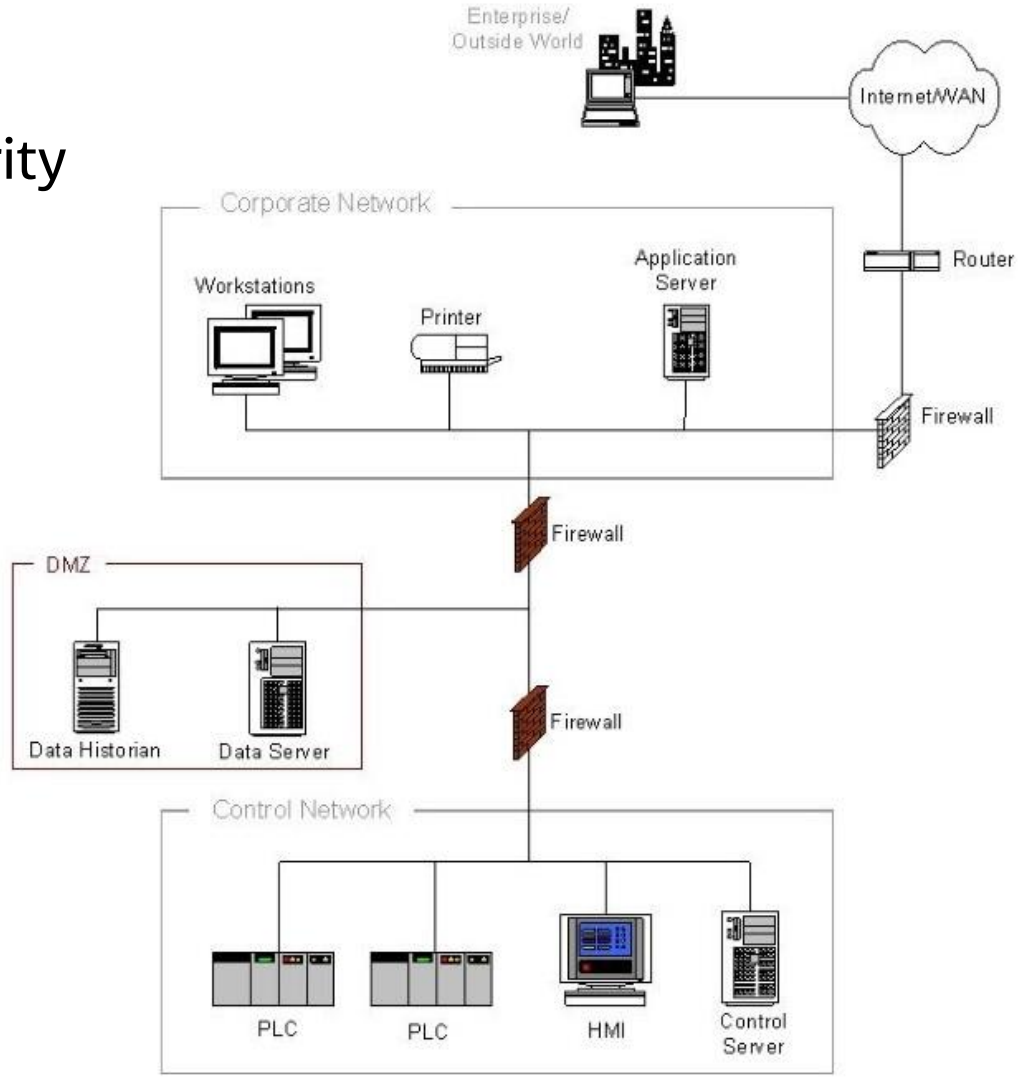


Figure 5-4. Paired Firewalls between Corporate Network and Control Network

NIST SP800-82r2 Guide to Industrial Control Systems

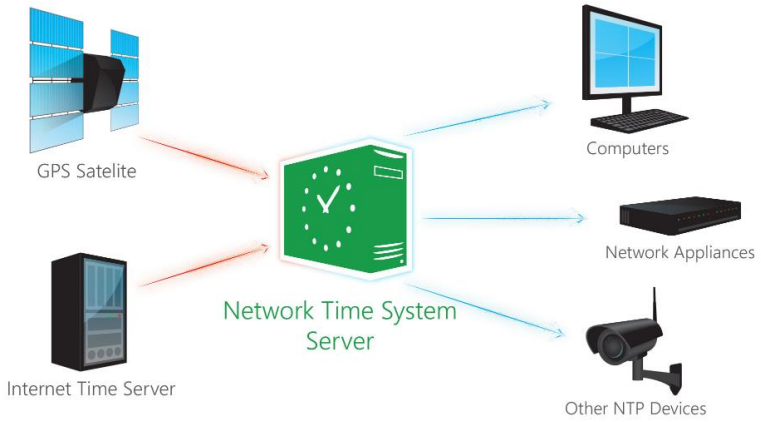
With Servers and a Reliable Network, Enterprise Tools are available

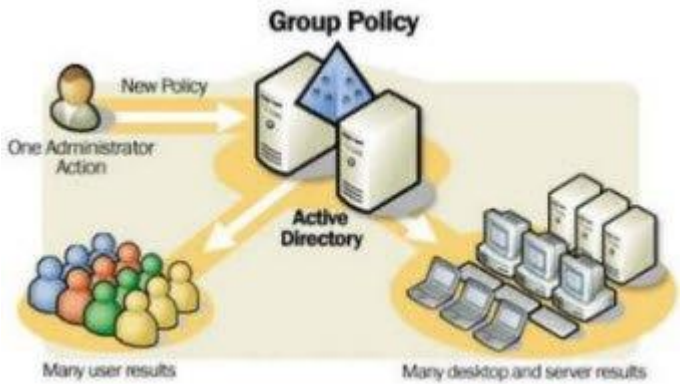
Symantec.

Symantec™ Endpoint Protection

Windows Server Update Services

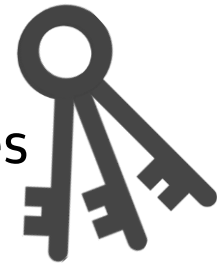
Active Directory



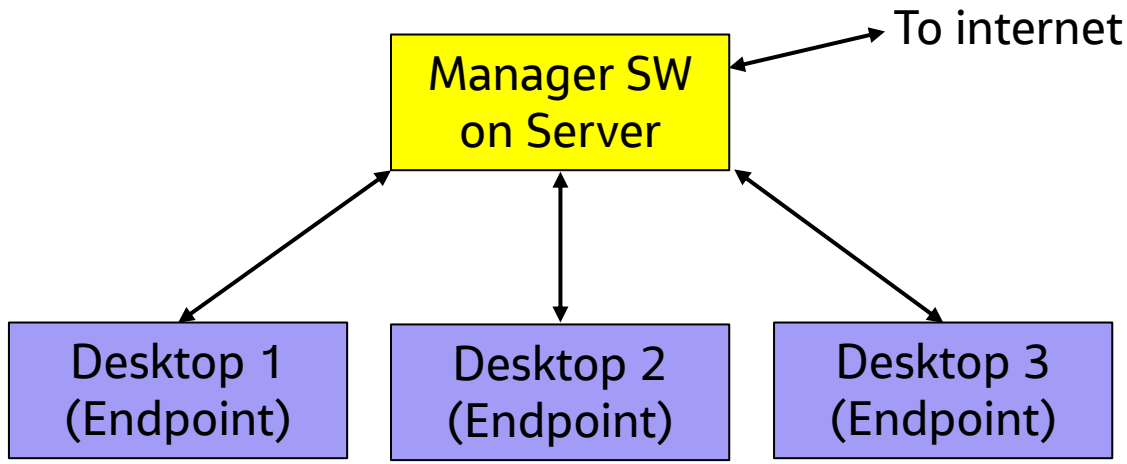


Guard the Keys to Your Kingdom CAREFULLY, from the Beginning

- Administrator Access
  - Network/Firewall
  - Servers and desktop devices



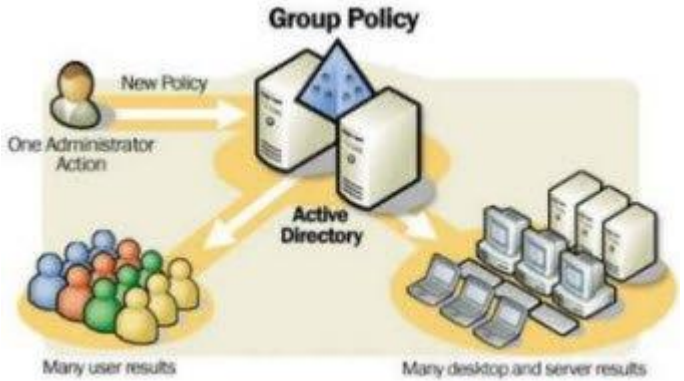
- Agents and Managers
  - SCCM/BigFix managing agents
  - Endpoint/virus protection agents
  - Windows Server Update Services (Patch Server)
  - These software systems can un/install, upgrade, reboot, etc. WITHOUT your permission.



- GOAL - Do not allow installation of any agent/manager that is not under your control!!

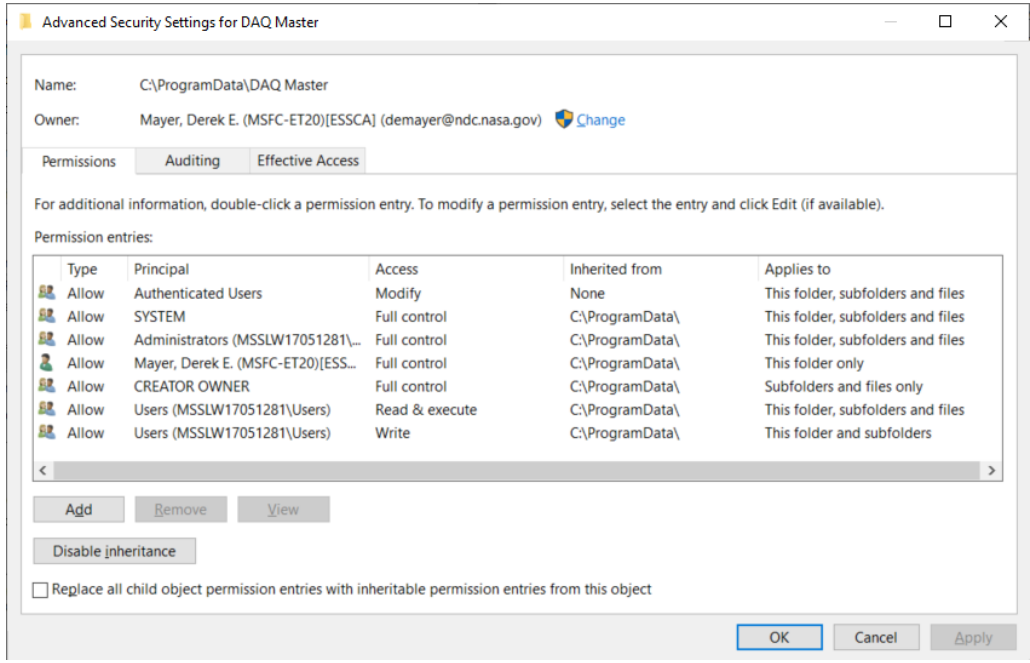
Using an Active Directory Domain

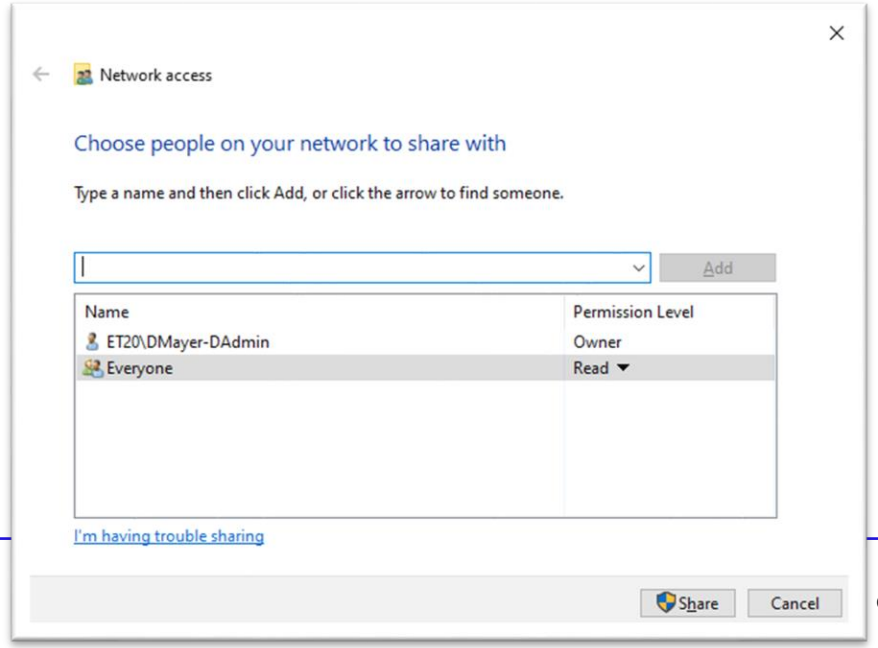
- Common credentialing
  - 1 user account/password works everywhere
  - Change password in 1 place, reflected everywhere
- Simplified 2-factor authentication rollout
- Group Policy
  - Centrally administered security policy
- Do NOT install/configure Email server
- How to Setup?
  - Start with a Windows Server
  - Promote to Domain Controller
  - Join each client to the domain
  - Best Practice – Don't use the DC Server for any other functions



File Permissions

- Critical element of cybersecurity
- File permissions are different than SHARE permissions
- Good Advice:
  - "If you don't manage file permissions by script, in 5 years you won't be doing file permissions."
    - File permissions can be manually set, but those are VERY difficult to maintain
    - On Windows, ICACLS handles file permissions well enough
  - "Full Control" is an administrative function, and should be reserved for Administrators.





Windows File Server or Network-Attached Storage (NAS)?

Windows-based File Share

- Uses existing server
- Antivirus automatically detects/scans new or changed files
- Requires independent backup system
- Provides FILE and SHARE permissions
- *Exposes all the potential cyber vulnerabilities of Windows Server*
- Authenticates as Windows device

Network-Attached File Share

- Requires a dedicated HW/SW system
- Threat management tools available, must be configured
- Vendor-provided backup tools
- Provides FILE and SHARE permissions
- Exposes only the cyber vulnerabilities of the dedicated, embedded platform
- Authentication integrates with Active Directory, more challenging for stand-alone

Encryption

- Data in Transit
  - File sharing SMB v3.0+ (Windows 10 automatically supports it, Win7 does not)
- Data at Rest
  - Desktops/Servers
    - Windows – BitLocker integrated into OS
      - No user interaction required to unlock drives at bootup
        - Data drives can store BitLocker keys on Boot drive, if boot drive is encrypted
        - Boot drive can store BitLocker key on Trust Protection Module (TPM) chip, if installed and configured
      - Automatically store BitLocker recovery keys for all drives?
        - Use Active Directory Domain
  - Network Attached Storage (NAS)
    - Encryption possible, but not as well supported (performance affected, too)
    - Generally requires the encryption key at bootup, no TPM option available

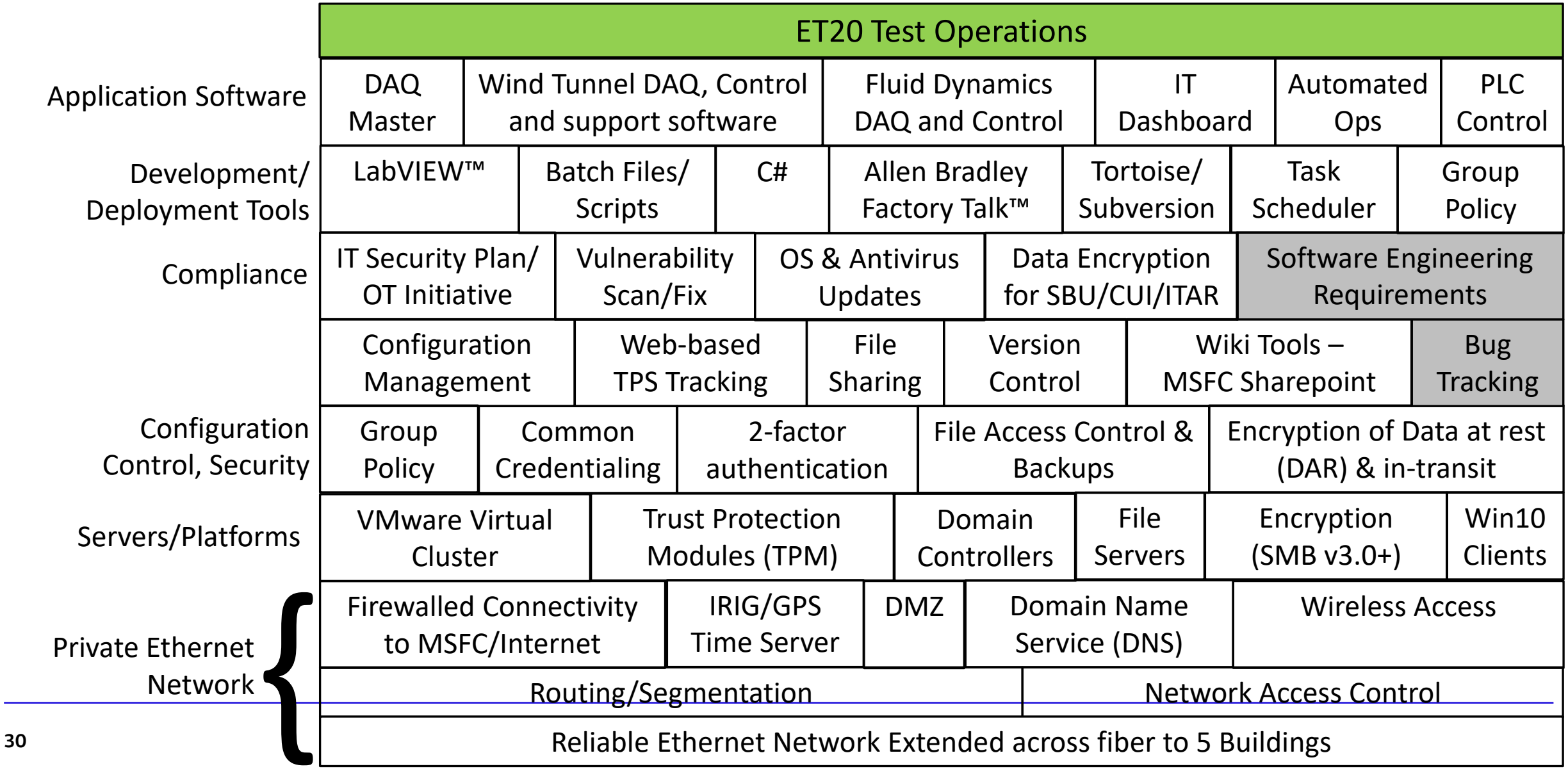
What is a Vulnerability Scan?

- A scan of all network ports/ protocols across a defined network range
  - Full discovery requires permission from firewalls (network and host-based)
  - "Credentialed scans" provide the *administrator password* for computers to verify patch/system status and vulnerabilities
- Examples:
  - Acunetix, Burp Suite, GFI Languard, Frontline, Nessus, Nexpose, Nmap, Qualys, SAINT
- Promise:
  - "The scan does not change any settings on any discovered targets"
- Reality:
  - Often scans open connections that are not properly closed
    - Enterprise devices can often recover but OT components can be left in denial-of-service state
  - Solution: FULLY power-down all OT devices after a scan

Suggestions for Handling Vulnerability Scans

- Scans from the Enterprise network are blocked by your firewall.
  - Either arrange when you will allow a scan through your firewall and across your network
  - Or have the IT Dept bring a laptop with scanner software to your network.
- YOU schedule/coordinate the scan
  - Create a detailed procedure/checklist to follow
    - Assign the scanner IP address (if device is admitted to your network)
    - Specify the range of addresses to be scanned
    - Arrange for all network traffic to be allowed from the scanning address, only during the scan
    - Create an exemption in your endpoint security for the scanner address to perform “port scan”
    - Give the scanner an administrator password to all your computers
      - Disable that account(s) once the scan is complete
- Use the scan results!
  - Identify all devices
  - Address the vulnerabilities

This is how I support my customer



Any questions?

Backup Slides