OT Cybersecurity

State of the Industry, Practical Steps, and Stories

Ben Stirling

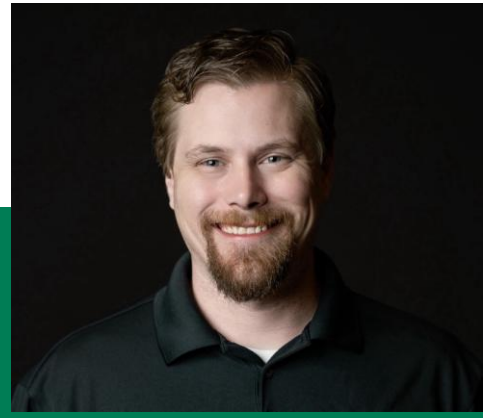
Gregg Gray

Jacobs

Challenging today.
Reinventing tomorrow.

Biography

Jacobs



Benjamin (Ben) Stirling
Director Cybersecurity
& Operational Technology

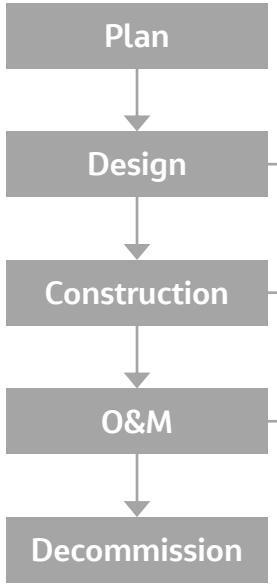
Ben has over 15 years of experience in the Power, Oil & Gas, and Industrial sectors. As a thought leader in securing industrial environments, Ben works with end users and OEMs to develop technology stacks and secure architectures. He has a passion for control systems and securing the world's infrastructure combined with deep knowledge of NERC CIP, NIST, ITIL, ISA 99/IEC 62443, and MITRE ATT&CK for ICS. He has a long-established track record of working with industry to recognize and ameliorate cybersecurity risks to infrastructure and human safety.

Jacobs' Business Overview

Jacobs is the market leader in water sector OT cybersecurity

OT Cyber Team Delivers Throughout Jacobs Delivery Lifecycle

Jacobs Delivery Lifecycle



OT Cybersecurity Solutions

OT System Architecture:
- Select, design and develop 30%, 60% and 90% designs for integrated OT systems

Network Design:
- Determine required network
- Develop Ring Topology
- Develop network design below and including DMZ

Technology Integration:
- Fabrication and integration of variety of OT technologies
- UFT/WFT

Cybersecurity Threat Detection & Remediation:
- Network monitoring
- Patching and vulnerability maintenance

- 40 unique water utility sites served with OT cybersecurity in FY2024
- 30 cybersecurity assessments
- 10+ active projects in design and integration of control systems & OT
- 20+ water utility sites served with O&M cybersecurity services including managed services
- Major wastewater OT cybersecurity projects in Wilmington and Clark Regional Wastewater

45,000 employees

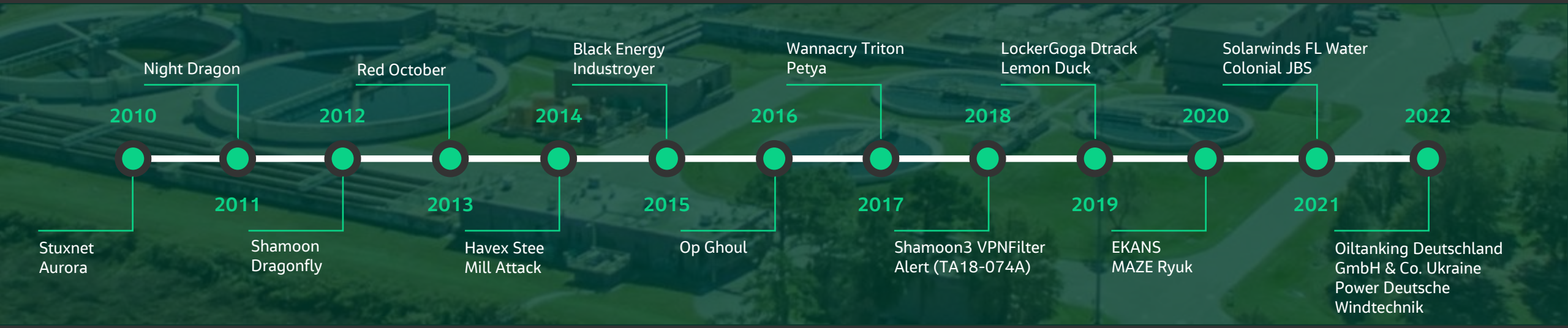
Serve 6 markets in geographies around the world

Global leader in water sector

5,000 employees in US water sector/9,000 employes in water sector globally

Unrivaled bench strength in water sector OT cybersecurity and I&C personnel

Increase of Cyber Attacks in Critical Infrastructure



May 2021

Colonial Pipeline
- victim of a ransomware
- halted operations.

Impact to operations because of concerns over safety due to impacts to operations monitoring and visibility.

April 2022

PIPEDREAM
- seventh ICS specific malware
- designed to disrupt industrial processes.

Affects libraries used across vendors. Lists of effected control processor may not be comprehensive.

February 2023

U.S. Energy company
- adversaries reached their OT network
- infected with Royal ransomware.

It's believed that the ransomware was general and not intended for the ICS environment.

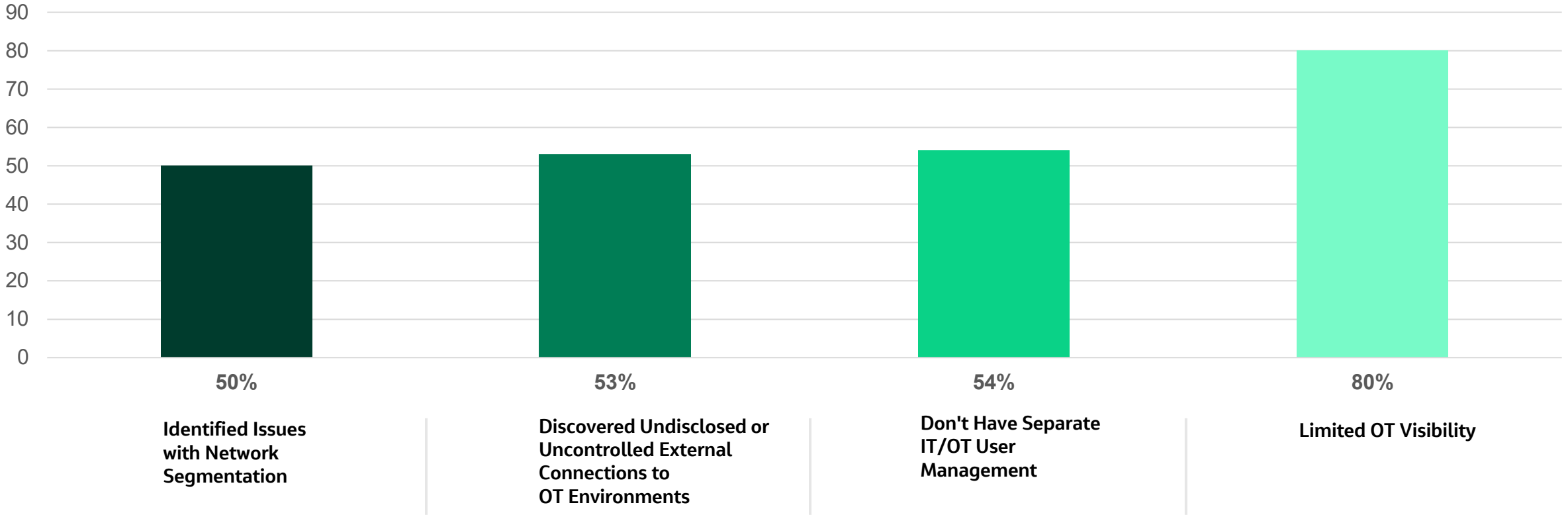
September 2024

Hezbollah attacks,
- pagers and two-way radios exploded
- resulting in at least 37 fatalities

This highlighted a long-standing warning from cybersecurity experts: our global supply chains for electronic devices are vulnerable.

Unprepared – OT vs. IT

SCADA Cybersecurity is not a “copy/paste” of IT Security



https://www.dragos.com/year-in-review/#section-report

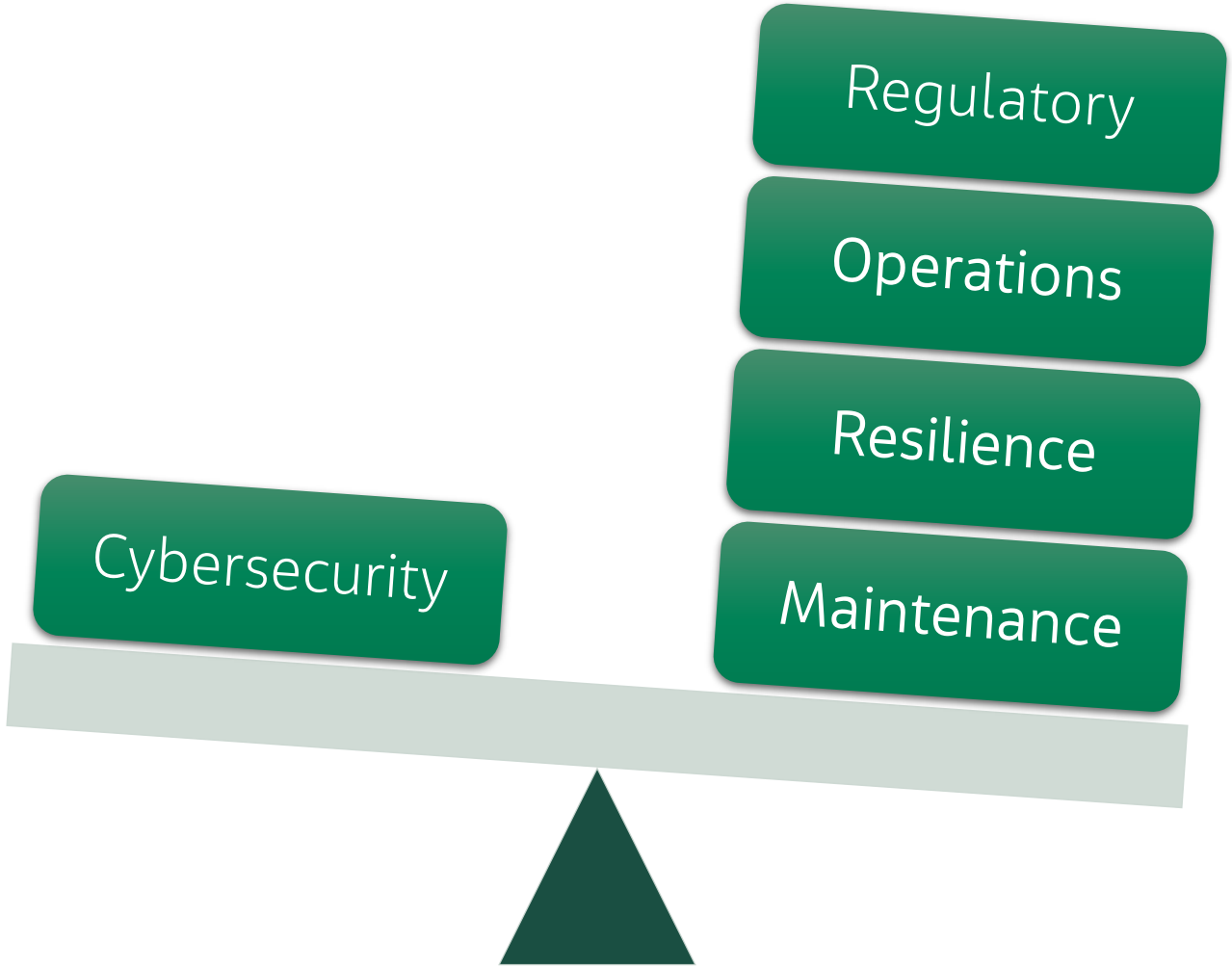
https://www.sans.org/white-papers/state-ics-ot-cybersecurity-2022-beyond

Leadership Perception vs. Operational Reality

- Everything is working
- There’s time to do it later
- Bad things happen to someone else
- This was reviewed last year

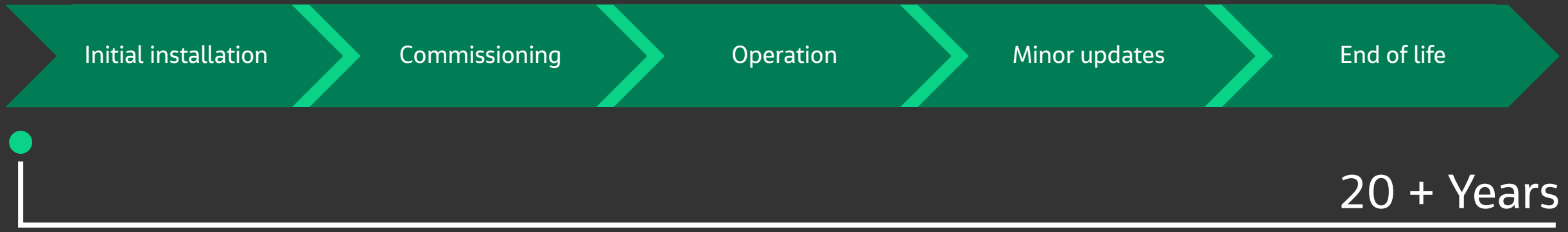
- Underfunded, understaffed, undertrained
- Functional, but ageing systems are at higher risk
- One click could lead to an incident
- Threat landscape is constantly changing

Competing Priorities



ICS Environment Life Cycle

- Control systems have long lives
- Plants of low economic value are very unlikely to upgrade
- Footprint changes are a challenge for any facility
- Legacy components often survive upgrades



Controls have Changed

Experimental Breeder Reactor I First operation August 24, 1951

How we protect them should too

XP and the Public IP

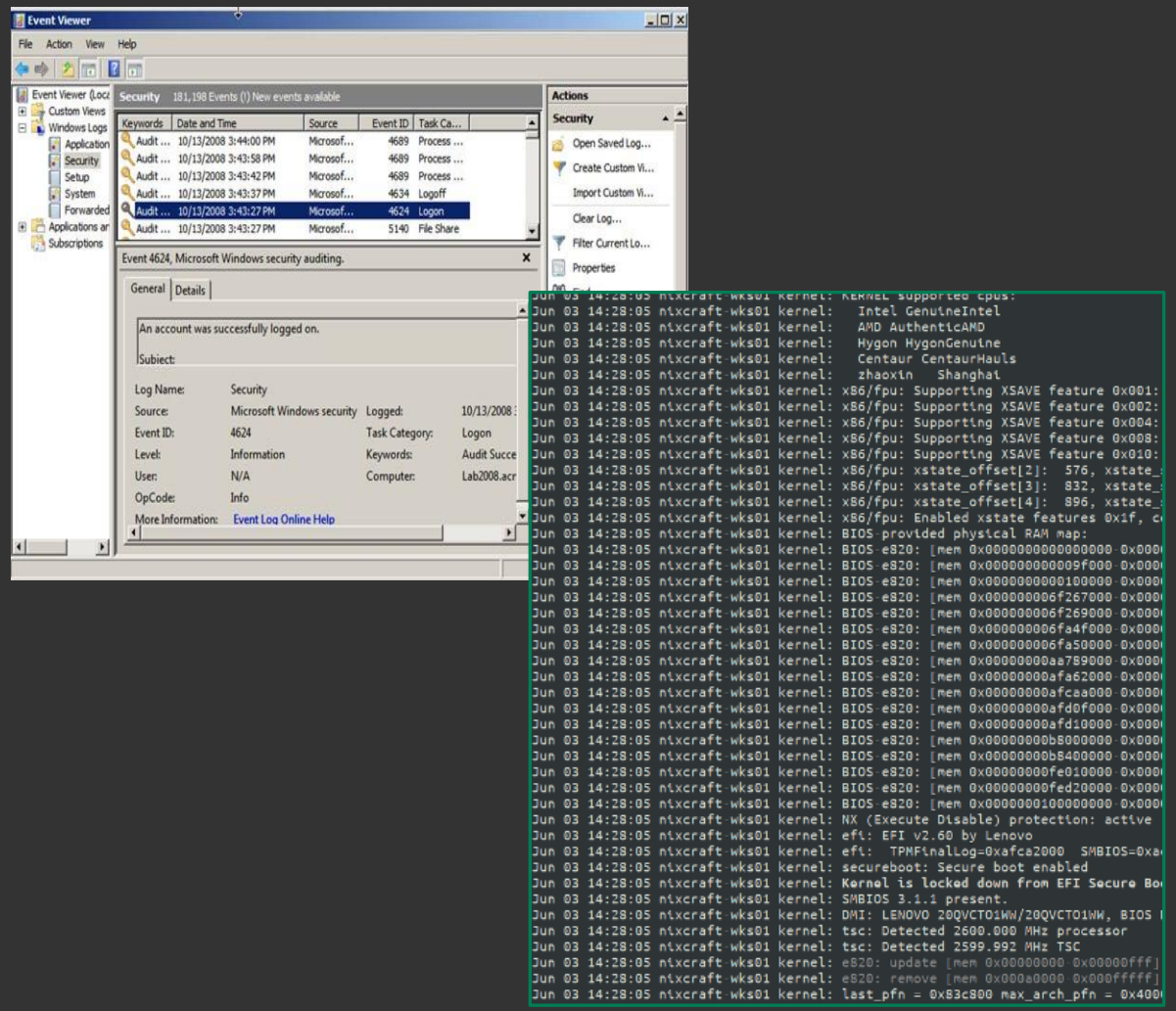
What's Wrong with this picture

Is your unit running?

What the Heck Happened

- Tuesday the 3rd 7:21ISO Calls site
- Plant Confirms Unit is online
- Cybersecurity Kicked off IR call
- Morning of the 4th Dragos and Customer IR on site
- Pulling of Memory and Hard drive images Starts
- Logic Reviewed by Controls and IR Team
- Analysis of images Started
- No indications of compromise found
- End of investigation

Where is that D*mn log



- Log location and retention
- Why its important after inventory
- Role in incident response
- Uses for automation

Know your logs: Collection Management Framework (CMF)

	A	B	C	D	E	F	G	H	I	J	K
1	Common Name	Hostname	Criticality	Description	IP Address	Physical Location	Manufacturer	Model	Serial Number	Log Retention	Log Locations
2	Operator 01	Oper_01	Medium	Operator Workstaion	192.168.0.22/24	Control room Unit 1	DCS vendor	T1000	t1000-1234	30 days	c:\Logs\
3	Engineering	Eng_01	High	IDE workstation	192.168.0.20/24	Electronics room Unit 1	DCS vendor	T-800	t800-0001	90 days	c:\Logs\ c:\application\log\
4											
5											

Beyond Asset Inventories:

- While asset inventories are crucial, they are not sufficient on their own. A CMF goes beyond just listing assets to understanding what data can be collected from each asset and how it can be used.

Structured Approach:

- A CMF is a structured method for identifying data sources and determining the type of information that can be obtained from each source.

Attributes of Data:

- The framework incorporates attributes such as the reliability, trustworthiness, accuracy, and completeness of the data. This helps in evaluating the quality of the collected information[1].

Meeting Analysts' Needs:

- The primary goal of a CMF is to collect data that can be turned into actionable information. The framework should be tailored to the specific needs of the organization.

Incident Response:

- A CMF supports incident responders and security operations by providing necessary data to investigate and respond to adversary effectively.

What are the Odds?

…whatever remains, however improbable, must be the truth.

Where to Start?

Start with the SANS ICS 5 Critical Controls

SCADA Incident Response Plan

Defensible Architecture

SCADA Network Visibility and Monitoring

Secure Remote Access

Risk-Based Vulnerability Management

Note: that the order of the controls is the recommended order of implementation

Jacobs Joins Dragos Community Defense Program

- OT specific IR
- Consulting and implementation of Defeasible Architecture
- Dragos Platform implementation
- Secure remote access (announcement Coming)
- Risk based Maintenance and vulnerability management

https://www.jacobs.com/newsroom/news/jacobs-and-dragos-collaborate-strengthen-cybersecurity-vulnerable-us-water-facilities

What Now?

Are your Safety, Cybersecurity, and Operations teams prepared?

Be proactive

- Start now - Incorporate cybersecurity into current management procedures
- Help mangers gain understanding of existing system
- Identify equipment and assets that could be targeted in a cybersecurity incident
- Enhance organizational awareness of external connections
- Develop OT/ICS/SCADA specific plans (both inventory & incident response plans)
- Seek EPA guidance outlining response strategies

Biography

Jacobs

Gregg Gray, PE

Senior Instrumentation & Control (I&C) Engineer

Gregg has over 30 years of experience in the Municipal Water and Wastewater industry. At Jacobs, he is responsible for I&C/OT design activities for projects throughout the Southeast. In this role, Gregg develops hardware and software standards for SCADA/OT master plans, control system upgrades, develops network design drawings and specifications, and provides services during construction to ensure that project implementation meets the client's needs. Previous experience included engineering and management roles for a systems integration company and with the USAF as a computer engineer.

Could your control system be vulnerable?

- Legacy proprietary control networks such as Data Highway (DH), Data Highway Plus (DH+), Modbus, Modbus Plus (MB+), and others offered a built-in layer of security. They used proprietary cable, proprietary connectors, and were installed inside the plant with no connection to the outside. Proprietary (and expensive) network cards were required in computers to gather information from their partner PLCs.
- Then along came Ethernet … the adoption and standardization of Ethernet-based communications quickly became the dominant and preferred control network architecture. Implementation of Ethernet networks offered faster and cheaper solutions than the legacy proprietary solutions. Placing SCADA computers at all levels of an organization became more common.
- However, that inherent “security by obscurity” network design also became a thing of the past.

Could your control system be vulnerable?

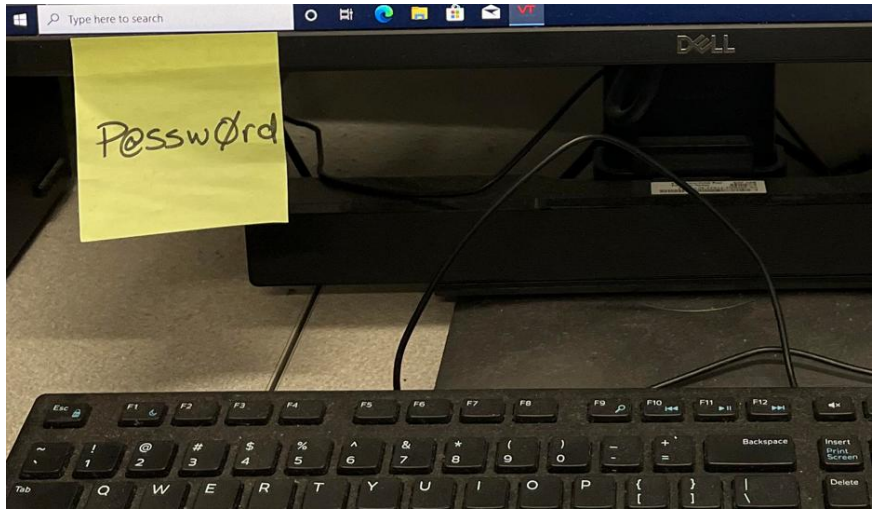
- Early implementations of Ethernet networks used “hubs”, switches, and simplistic network addressing. Basically, there was not any traffic analysis or routing – every device appeared on the network and every device could listen to and transmit to every other device. You may hear this referred to as a “flat” network.
- While enterprise and business networks have long since evolved to utilize advanced routing protocols, VLANs (Virtual LANs) for segmentation, firewalls and data diodes for protection from outside threats, often times the control network has lagged behind.
- Because of the long life of many control systems, your control network may still be using some or all of the legacy Ethernet infrastructure; potentially exposing your control system to cyber threats.

How your Control Network could be exposed!

- Thinking that your plant's control network or SCADA system is "on an island" and isolated from the outside world.
- Exposure resulting from remote support access.
  - PLC Support Providers (ISP or VPN access)
  - Packaged Vendor Control Panel (cellular access)
- Plant personnel, contractors, or visitors using SCADA (or other Enterprise connected) computers for personal use (USB ports, Internet access)
- Open (unsecured) network ports inside your plant control panels or control rooms
  - Example: Graceport (implement with caution):

Other Typical Vulnerability Concerns

- Unencrypted wireless (radio) communications. Many older telemetry networks transmit unencrypted data. Even many newer radios may be operating in an unencrypted mode to allow compatibility with legacy radios.
- Minimal or no physical security on facility access gates, buildings, electrical rooms, control rooms, or control panels.
- No user login requirements or shared generic logins. Anyone with physical access may have full access and no traceability.
  - The classic example:



Implementation Examples

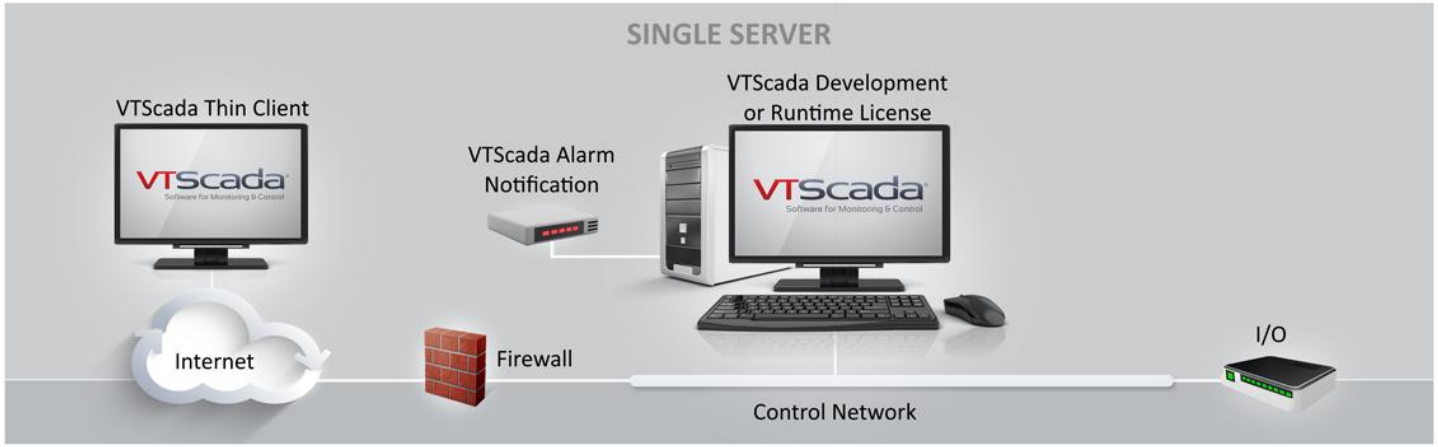
- Once security gaps are identified and assigned a threat level, budgets and an implementation plan should be developed to address those vulnerabilities.
- The organization must balance the investment cost to protect their system versus the potential cost of a breach or a cyber incident.
  - Lost production or downtime.
  - Damaged public reputation or trust.
  - Real monetary costs. The average "ransom" demand estimates range from $500k - $1M at minimum. Could you be stuck with that as your only alternative?
- Some examples of Jacobs involved project solutions in and around Alabama follow.

Physical Security

- Secure facility gates, building access doors, control rooms, and operator interface equipment (computers, panel touchscreens or OITs).
- Implementing a secured Server Room with tracked, access control is ideal. Utilizing lockable server equipment racks may also be an option.
- Securing the Control Room is also a necessary layer of protection. If the control room cannot be secured, use of auto-logout of SCADA system users should be enforced.
- Only allow authorized personnel to have physical access to control system equipment (this includes control panels). Add intrusion alarms and lock the enclosures. Password protect the PLC programs.

Secured control room

Network Security



- Network security is accomplished through the use of firewall devices, managed (Layer 2) Ethernet switches, and an applied IP addressing schema which all work together to segment, isolate, and protect devices on the control network.
- Firewall devices are the first line of defense for network security. These devices monitor “incoming and outgoing network traffic and decide whether to allow or block specific traffic based on a defined set of security rules” [Cisco].
- Firewalls are essential for external connections to wireless devices. Such connections are considered “untrusted” and must be routed through firewall rule sets.

Network Security - continued

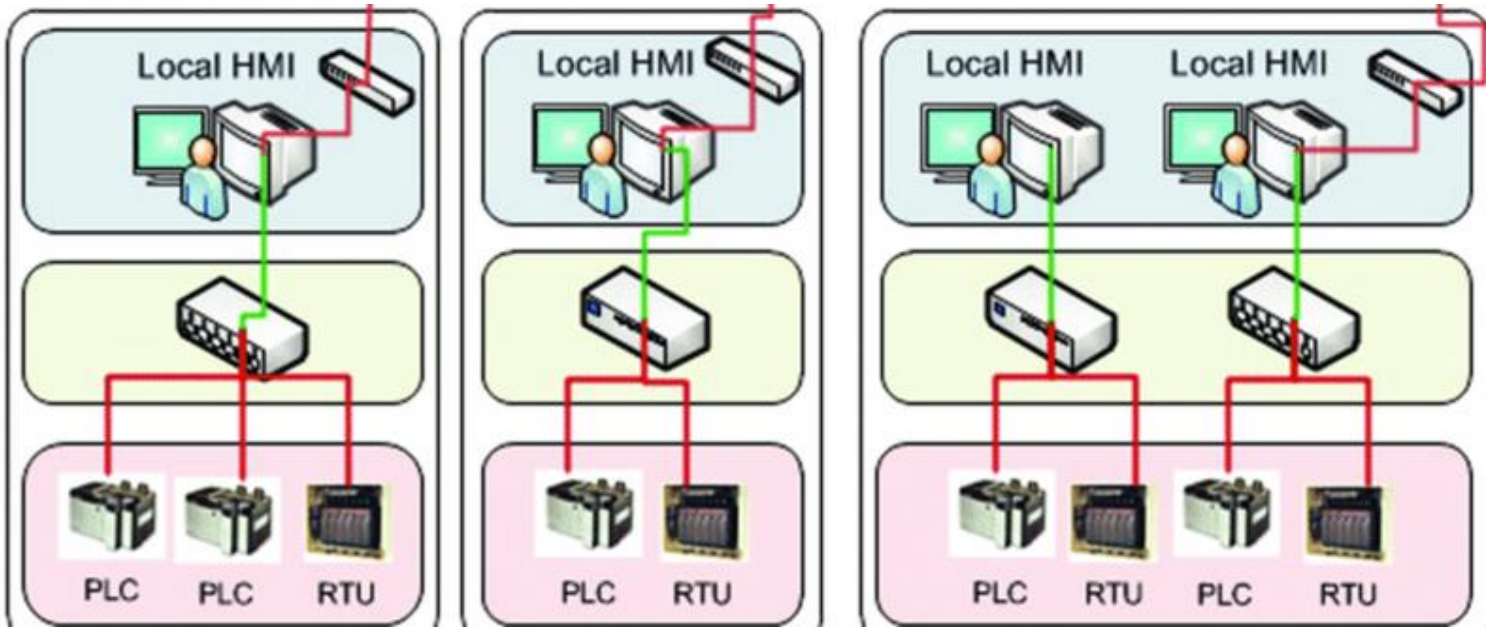
- By using managed Ethernet switches and a purposeful **IP address schema**, control networks can be segmented into **virtual local area networks (VLANs)**. Network segmentation provides a layer of protection against cyber attacks by restricting unauthorized access and by isolating a compromised device.

Area 10 (X = 10) Area 20 (X = 20) Area 30 (X = 30) Y = device number

Operations VLAN 10.100.X.Y

Control VLAN 10.20.X.Y

Device VLAN 10.10.X.Y



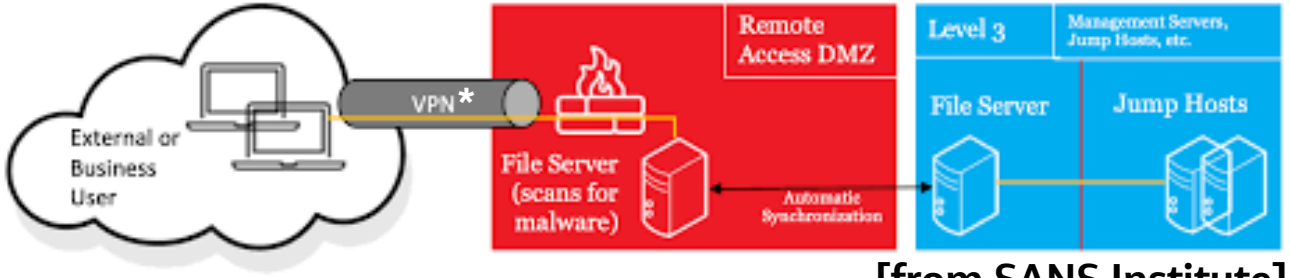
[from UpKeep.com]

Examples:
10.10.20.1 is a controller in Area 20

10.100.10.1 is a computer in Area 10

Remote Access Security

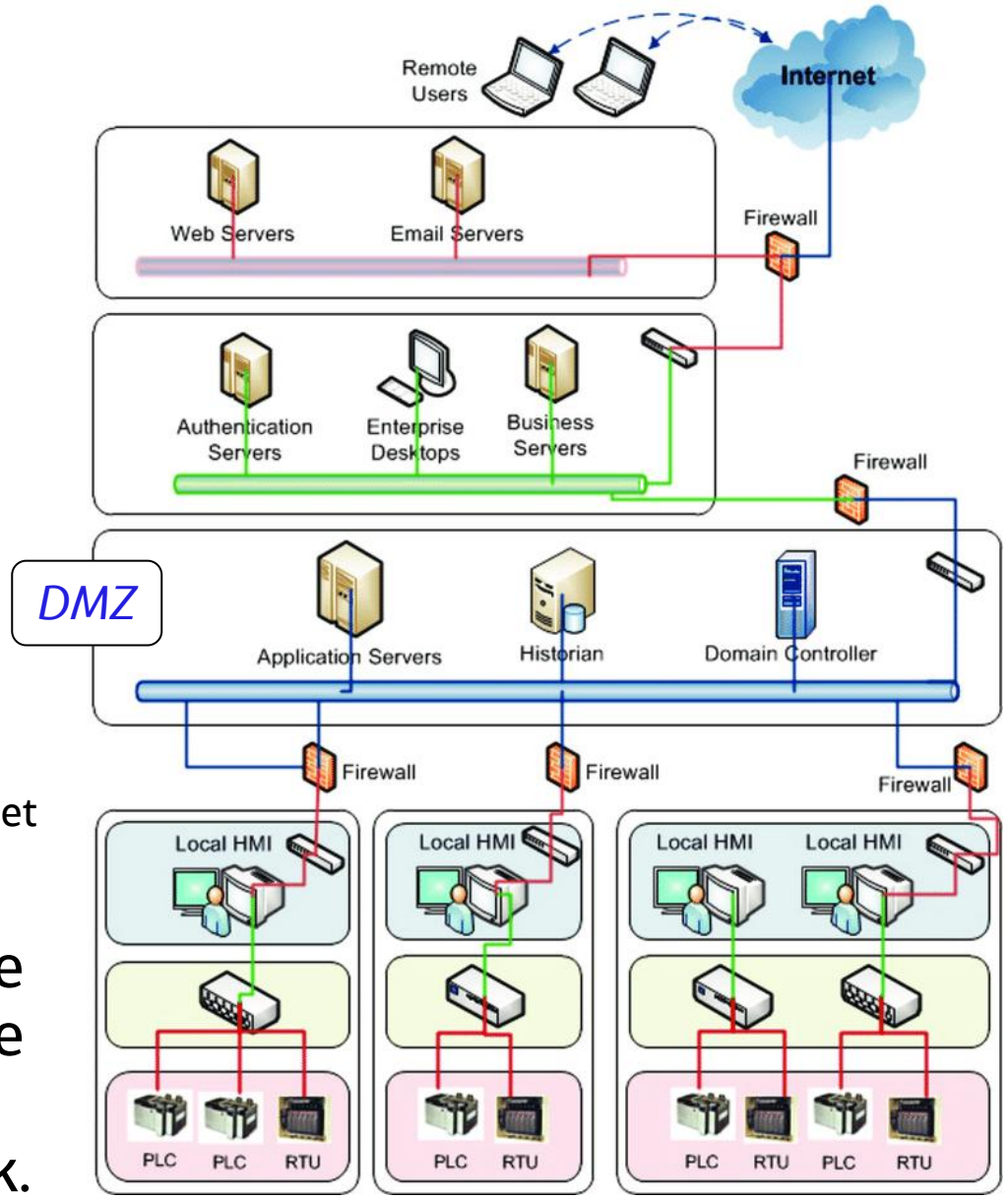
- Remote access to the system must provide protection for the control system. This may be done with a **De-Militarized Zone (DMZ)** or a Screened Subnet.



[from SANS Institute]

*** VPN = Virtual Private Network;** encrypted private network over Internet

- The DMZ separates the OT environment from the enterprise (or "business") network. Remote users access a copy of the SCADA system in the DMZ rather than directly connecting to the SCADA system attached to the control network.



[from UpKeep.com]

User Authentication

- User names, passwords, and permissions are managed through an OT Domain Controller and are integrated into the SCADA system such that the user only has one login/password for the computer and for the SCADA system.
  - The Domain Controller is an OT server that is dedicated to handling user authentication within the control system. The Active Directory (or AD) is the user database of passwords and credentials that exists on the Domain Controller.
- All users must have unique logins and have assigned privileges based on group membership. Determination of user permissions is an iterative process with input from all stakeholders (management, operations, and IT to name a few).
- **Multi-Factor Authentication (MFA)** is also used. This method of authentication requires two (2) or more types of user validation.
  - Something you know (password, PIN code, security question)
  - Something you have (authentication app on your phone, badge, token)
  - Something you are (facial recognition, fingerprint scan)

[from EDAFIO.com]

Integrated Cyber Security & Disaster Recovery

User Configuration (AD and HMI)

- Name, Token Type, Email Address
- HMI Realms
- HMI Group Privileges
- HMI Groups and User Assignment
- Alarm Groups and Remote Alarm notifications

Privileged Access Management:

- Integrated with AD for Users and Privileges
- Required approvals for external remote access
- Monitoring and recording of remote sessions
- Device and application control

Firewall and Switch Policies

- Allow by exceptions (Default-Deny)
- Port restrictions and monitoring

Backup and Recovery

- Automated machine, PLC, and applications backups
- Local and remote backup storage (3-2-1 strategy)
  - 3 copies
  - 2 media types
  - 1 offsite

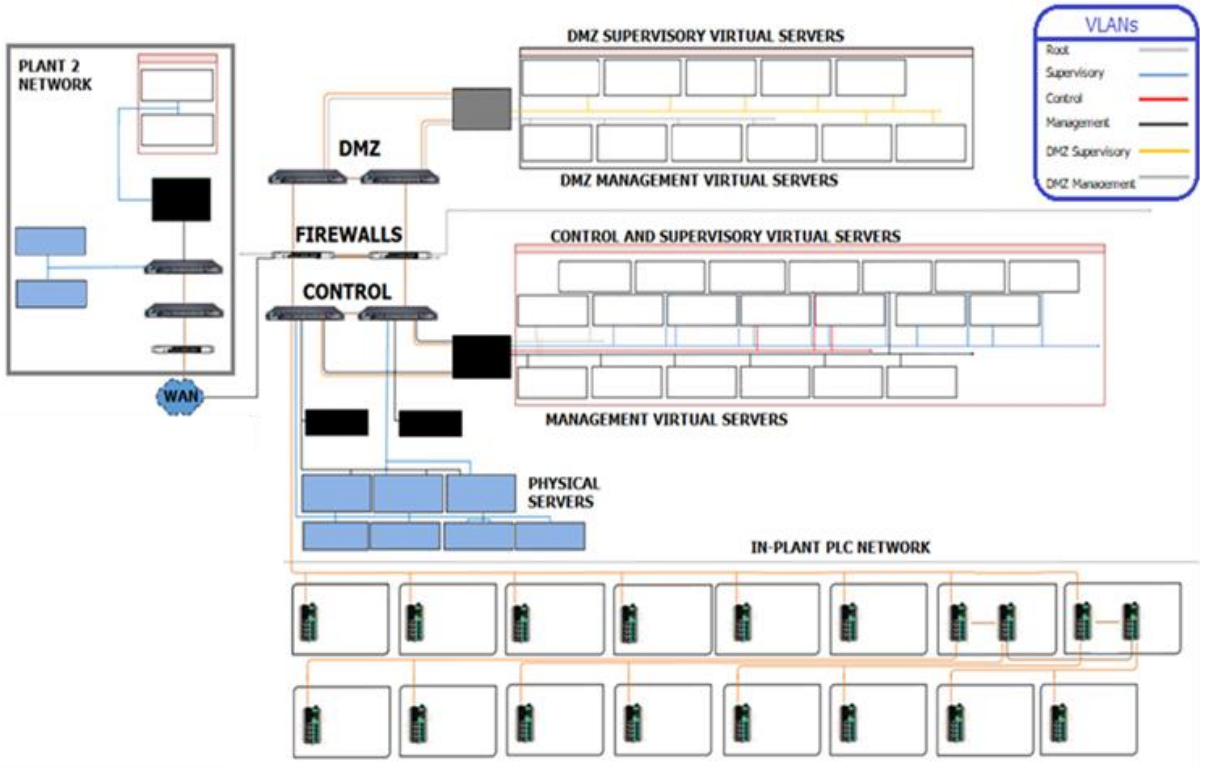
Documentation is essential!

- The infrastructure required to support today's OT solutions is intentionally multi-layered (aka, "defense in depth") to make it hard for cyber criminals to infiltrate your system.

- This adds complexity that must be managed and maintained. Cybersecurity is an ongoing process and accurate documentation is essential.

Some examples of System Documentation include:

- Overall System Architecture
- Network Maps
- Component Lists
- VLAN Assignments
- Password vault
- IP address tracking
- Warranty, support, and subscription information



Questions or Comments?

Copyright notice

Important