SANS

The SANS Five ICS Cyber Security Critical Controls - Control #4 Secure Remote Access

Bruce Large
Principal Cyber Security Architect, BLARGE
bruce@blarge.io

/whois

- Principal Cyber Security Architect at *BLARGE*
- Worked in IT and OT in Network & System Engineering and Cyber Security roles for over 15 years
- SANS Certified Instructor Candidate for ICS410 and Teaching Assistant for ICS612
- Worked in Electricity Generation and Transmission, Rail, Aviation, Emergency Services and Consulting
- Chartered Professional Engineer (CPEng) in Information, Telecommunications and Electronics Engineering (ITEE) & Registered Professional Engineer Queensland (RPEQ)
- Bachelor Engineering (Telecomms) QUT and Master Business (Applied Finance) QUT
- Check out some of my previous presentations on the SANS ICS Youtube Channel

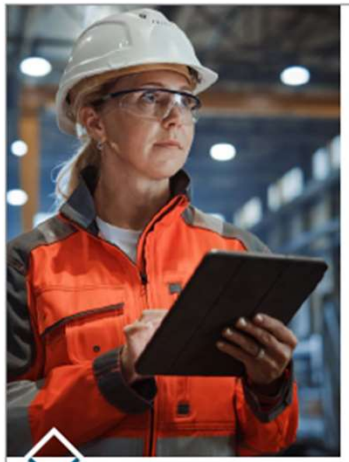
Why this presentation?

Agenda

1. Introduction to the SANS Five ICS Critical Cybersecurity Controls
2. SANS 2024 State of ICS/OT Cybersecurity Report and insights for Secure Remote Access
3. A Defensible Security Architecture Supports Secure Remote Access
4. People Perspective
5. Process Perspective
6. Technology Perspective
7. SANS ICS Cybersecurity Community Resources
8. Summary

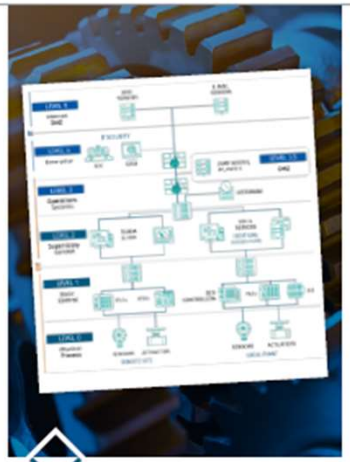
1. Introduction to the SANS Five ICS Cybersecurity Critical Controls (5CC)

Introduction to the Five ICS Cyber Security Critical Controls (5CC)



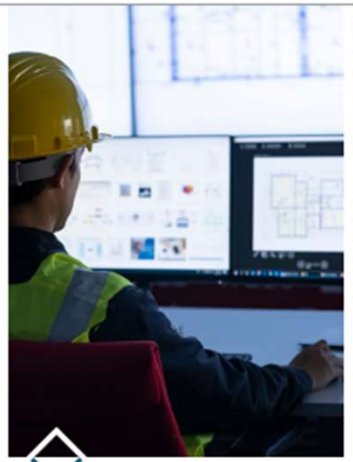
ICS INCIDENT RESPONSE

Operations-informed IR plan with focused system integrity and recovery capabilities during an attack. Exercises designed to reinforce risk scenarios and use cases tailored to the ICS environment



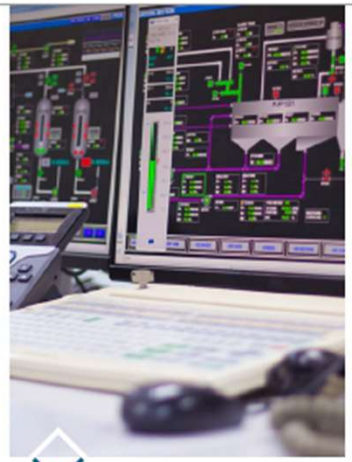
DEFENSIBLE ARCHITECTURE

Architectures that support visibility, log collection, asset identification, segmentation, industrial DMZs, process-communication enforcement



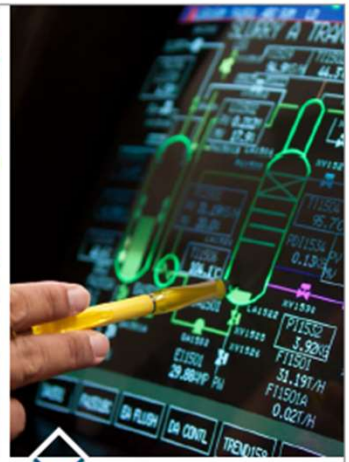
ICS NETWORK VISIBILITY MONITORING

Continuous network security monitoring of the ICS environment with protocol-aware toolsets and system of systems interaction analysis capabilities used to inform operations of potential risks to control



SECURE REMOTE ACCESS

Identification and inventory of all remote access points and allowed destination environments, on-demand access and MFA where possible, jump host environments to provide control and monitor points within secure segment



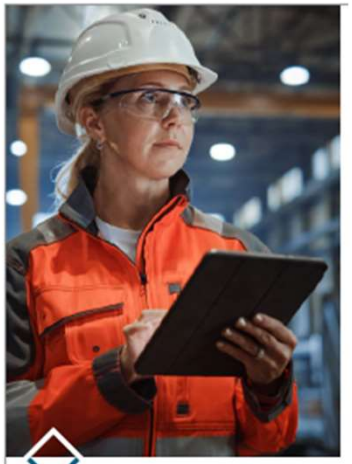
RISK-BASED VULNERABILITY MANAGEMENT

Understanding of cyber digital controls in place and device operating conditions that aid in risk-based vulnerability management decisions to patch for the vulnerability, mitigate the impact, or monitor for possible exploitation

Source - https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/

Control #1 – ICS Incident Response

- Start security with the end in mind!
- Understand Risk Scenarios and Prioritise remediation and investment efforts
- Your Scenario Planning should start with real world incidents and be cyber threat intelligence informed
- Consider worst case high-consequence scenarios as well but don't become overwhelmed
- Critical that you tabletop the scenarios and prepare



ICS INCIDENT RESPONSE

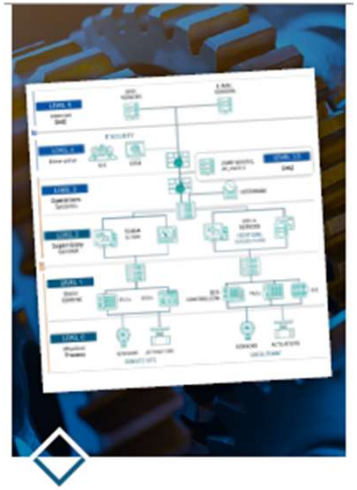
Operations-informed IR plan with focused system integrity and recovery capabilities during an attack. Exercises designed to reinforce risk scenarios and use cases tailored to the ICS environment

SANS

Source - https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/

Control #2 – Defensible Architecture

- How are you building systems that can be defended by your cyber teams?
- Need to define your crown jewel assets and know your assets
- Know your network chokepoints and your defensible cyber position
- It's not just the IT/OT Edge DMZ but needs to consider traffic flows between ICS zones



DEFENSIBLE ARCHITECTURE

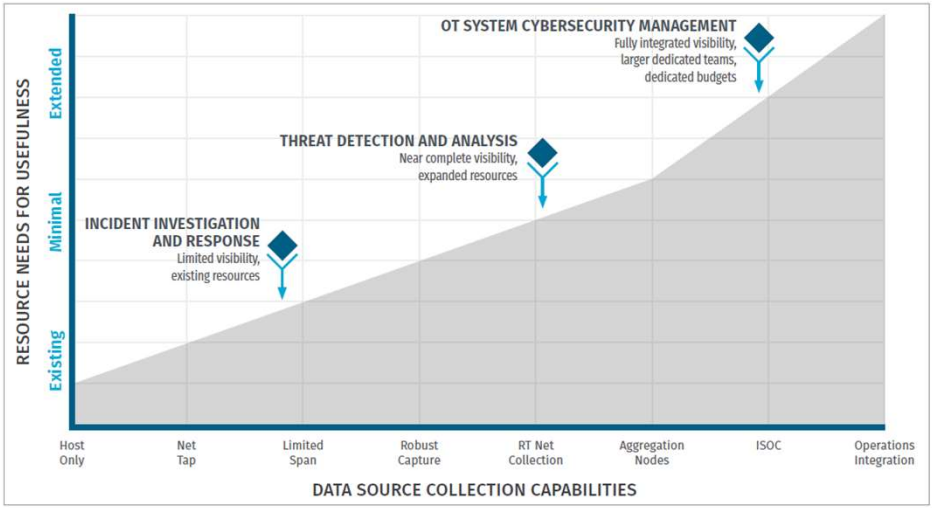
Architectures that support visibility, log collection, asset identification, segmentation, industrial DMZs, process-communication enforcement

SANS

Source - https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/

Control #3 – ICS Network Visibility Monitoring

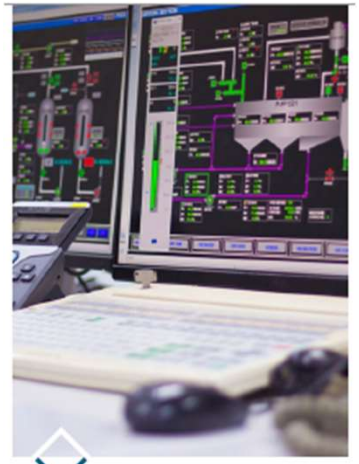
- OT is Systems of Systems – the network is key
- Use your scenarios and understand your threat actor TTPs to ensure you have the right visibility



Source - https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/

Control #4 – Secure Remote Access

- **The focus of today's presentation**
- More than just MFA
- COVID-19 has seen the attack surface increase
- Your Stage-1 Kill Chain may now be in your third parties



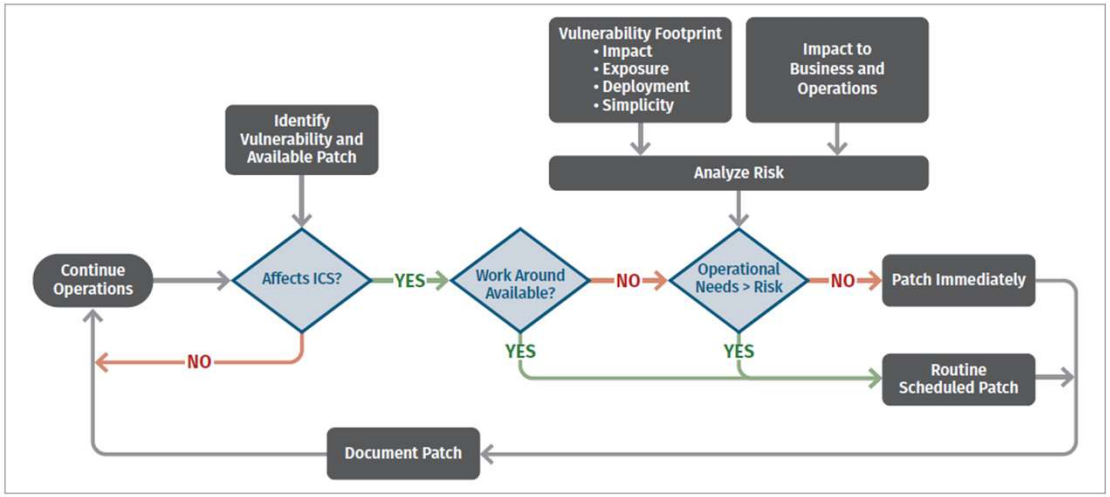
SECURE REMOTE ACCESS

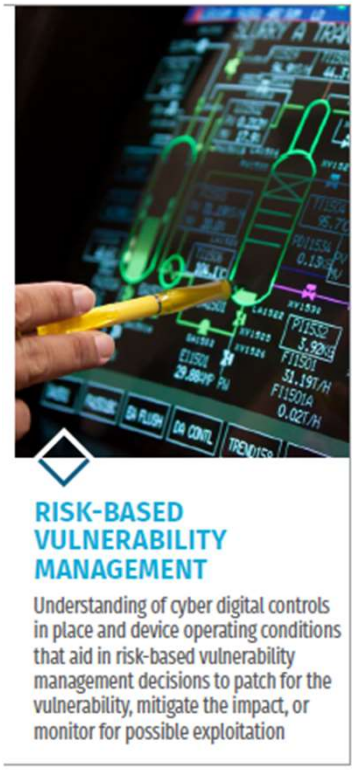
Identification and inventory of all remote access points and allowed destination environments, on-demand access and MFA where possible, jump host environments to provide control and monitor points within secure segment

Source - https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/

Control #5 – Risk Based Vulnerability Management

- Use the Now, Next, Never Approach
- Patching is not the only answer –
  only 4% of Patches are a “now” level
- There are other mitigations that are better strategies to manage risk





Source - https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/

2. 2024 State of OT/ICS Cyber Security Survey Insights

SANS State of OT/ICS Cyber Security Insights for Secure Remote Access

- Over 80% of Respondents have a Formal or Informal Remote Access Program
- Strong Response of MFA but concerningly still 25% not using MFA
- Read the report or watch the webinar for more insights about OT/ICS Cyber Security Programs

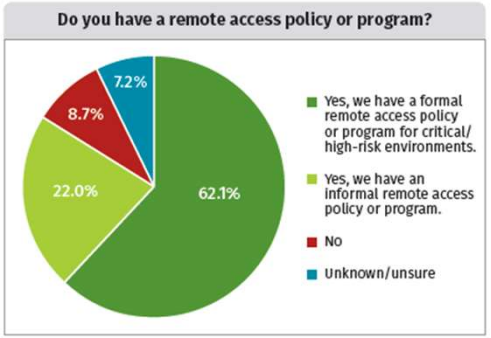


Figure 24. Remote Access Policy and Program Implementation

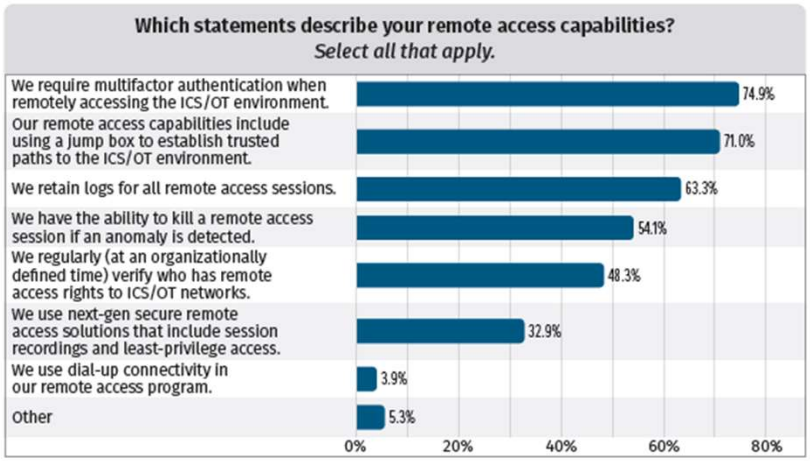


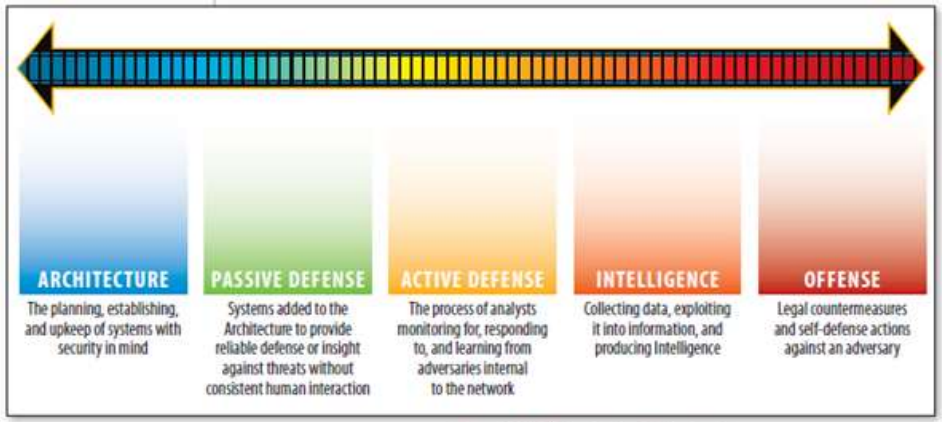
Figure 25. Secure Remote Access Capabilities

Source - https://www.sans.org/white-papers/sans-2024-state-ics-ot-cybersecurity/

3. Security Architecture Perspective

Sliding Scale for Cyber

From the The Sliding Scale of Cyber Security Architecture *"Architecture refers to the **planning**, **establishing**, and **upkeep** of systems with security in mind. Ensuring that security is designed into the system provides a foundation upon which all other aspects of cyber security can build."*



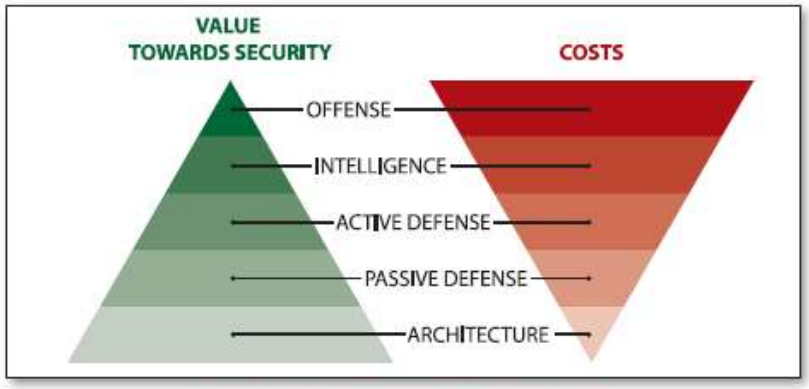
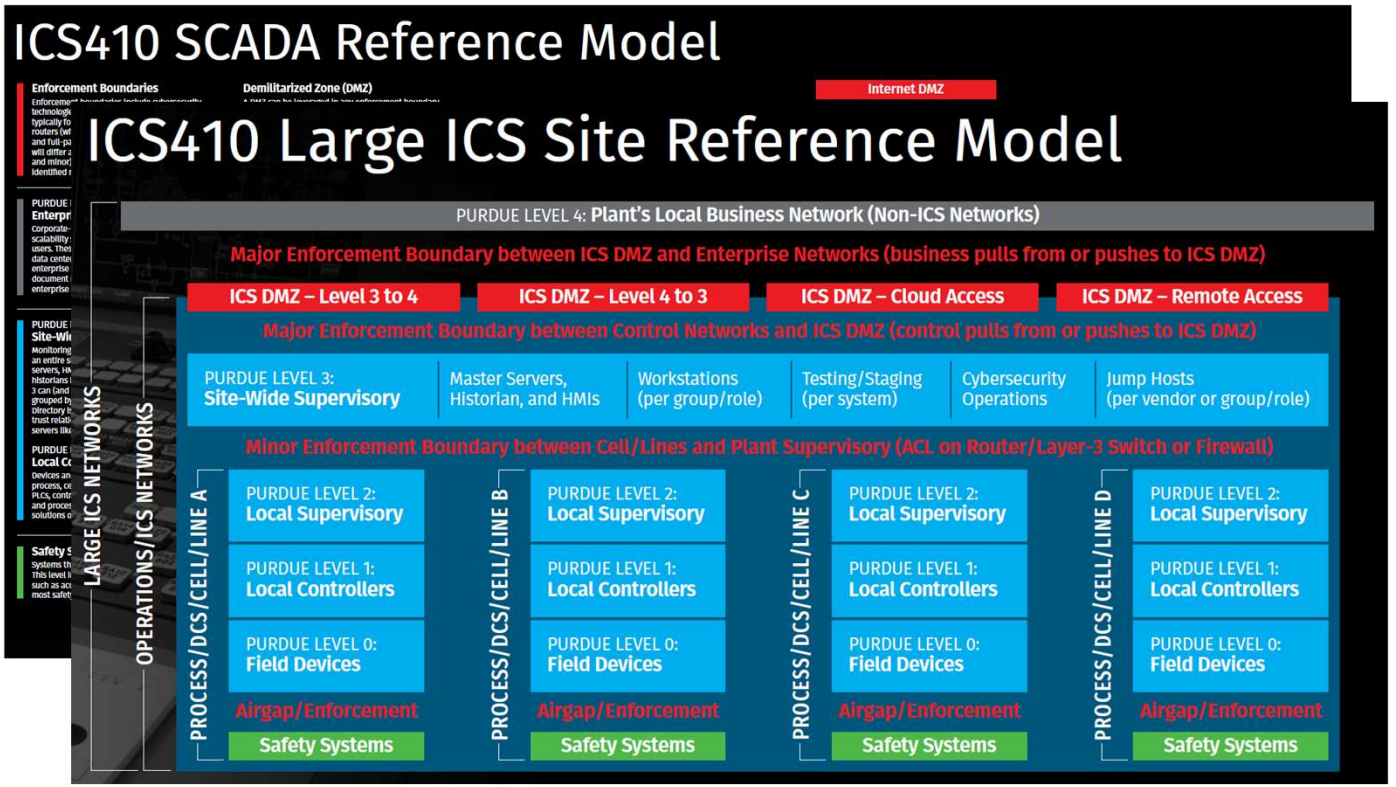


Figure 2. Value Towards Security (Left) vs. Cost (Right)

Source - https://www.sans.org/reading-room/whitepapers/ActiveDefense/paper/36240

A Defensible Security Architecture Supports Control #4

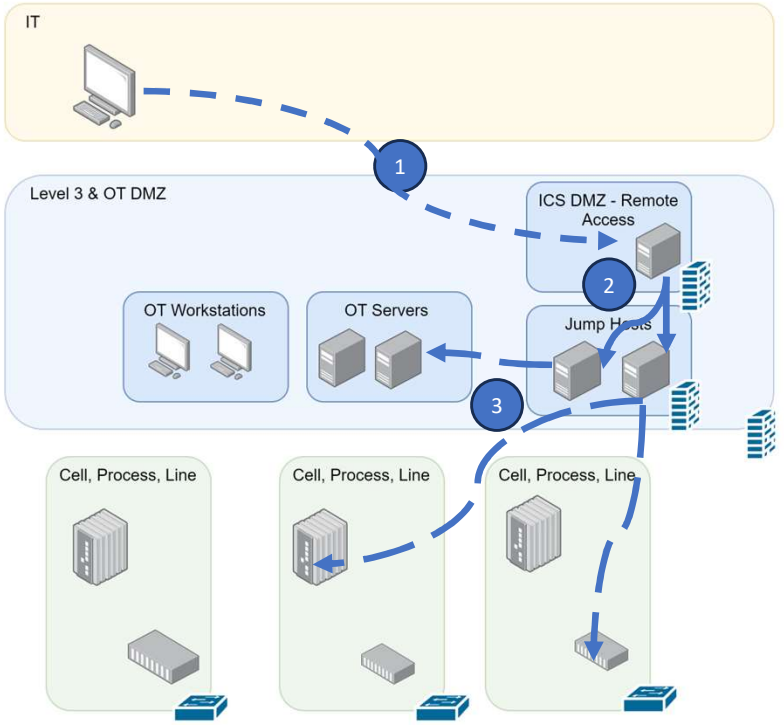
- **A Strong Perimeter and Segmentation Model** is a critical foundation to support secure remote access
  - The SANS ICS410 SCADA Reference architecture is a great reference
- Separate IT and OT Identities
  - ***On Average 54% <u>Lacked</u> separate IT and OT Identities***
    Dragos 2022 YIR Review
- Embed and support with Policies & Procedures



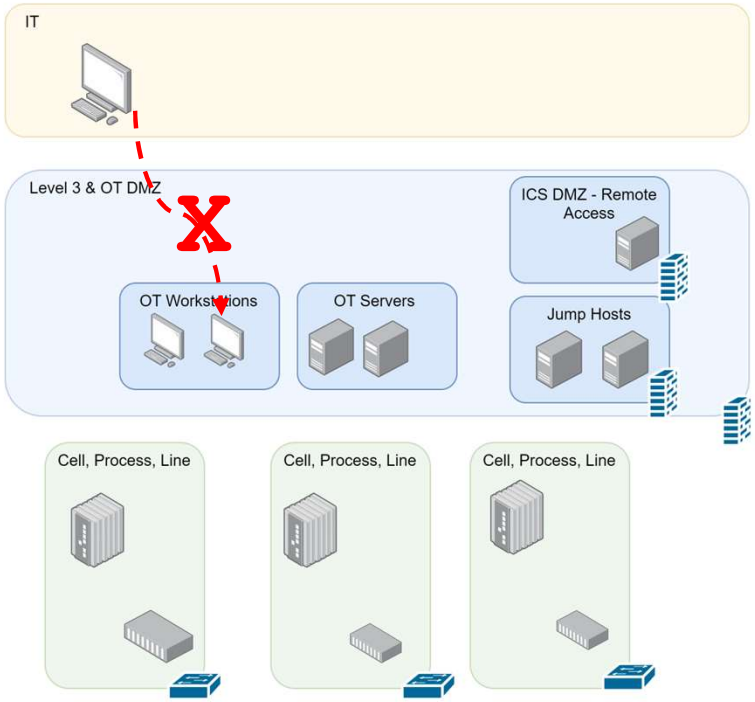
Source - https://www.sans.org/posters/control- systems-are-a-target/

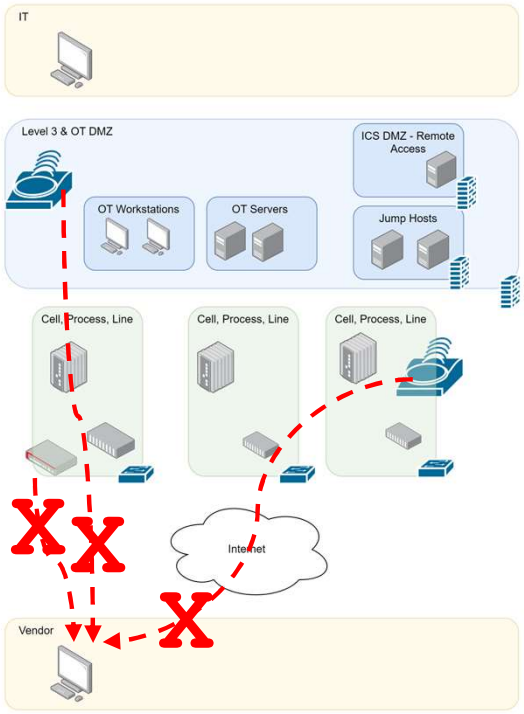
A Defensible Security Architecture Supports Control #4 (cont.)

1. A user in the Business Network connects to the ICS DMZ Remote Access Device using an IT Identity and MFA. This device could be a server, connection broker or a VPN pool
2. The User then connects to the Jump Host using an OT Identity and OT MFA if required
3. Jump Boxes can be restricted to different functions/use cases. Network Access to Cell, Process, Line can be controlled using Network Access Control Lists in local switching infrastructure



A Defensible Security Architecture Supports Control #4 (cont.)





Example Anti-Patterns for Remote Access

4. People Perspective

People Perspective

- It is vital that your staff understand the critical risks that insecure remote access presents
  - Share examples of how insecure remote access was a factor in security incidents
- Train your staff on the importance of secure remote access
  - Make sure you spend time to explain the why to your staff
  - Consider demonstrations of sites such as Shodan to demonstrate how insecure remote access can be discovered online
- Always consider the impact to your Staff and make sure you respect the impact it will have to their work

People Perspective (cont.)

- For example, consider Oldsmar Water Treatment Facility Incident
- Publicly known that an Operator Workstation had Internet Access and Team Viewer Remote Access Software Installed
- This is a good example for educating users of the risks of having exposed OT systems on the internet with remote administration software

https://www.abc.net.au/news/2021-02-09/hackers-remotely-gain-access-to-a-florida-city-water-treatment/13134818

Ref https://www.dragos.com/blog/industry-news/recommendations-following-the-oldsmar-water-treatment-facility-cyber-attack/

5. Process Perspective

Process Perspective

- ACSC ICS Remote Access protocol identifies:
  - Design Principles
  - Implementation Principles
  - The “Protocol”
- Key Things to consider:
  - Manage Third Party & Vendor Access
  - Enforce Multi Factor Authentication
  - Know how to disconnect from external networks quickly
  - Avoid generic accounts
  - Avoid “always on” connections – limit to one day or a shift duration
  - Avoid direct connections to OT systems from Vendors
  - Use time limited passwords where possible
  - Retain logs for ideally a 5 year period

Ref - https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/critical-infrastructure/industrial-control-systems-remote-access-protocol

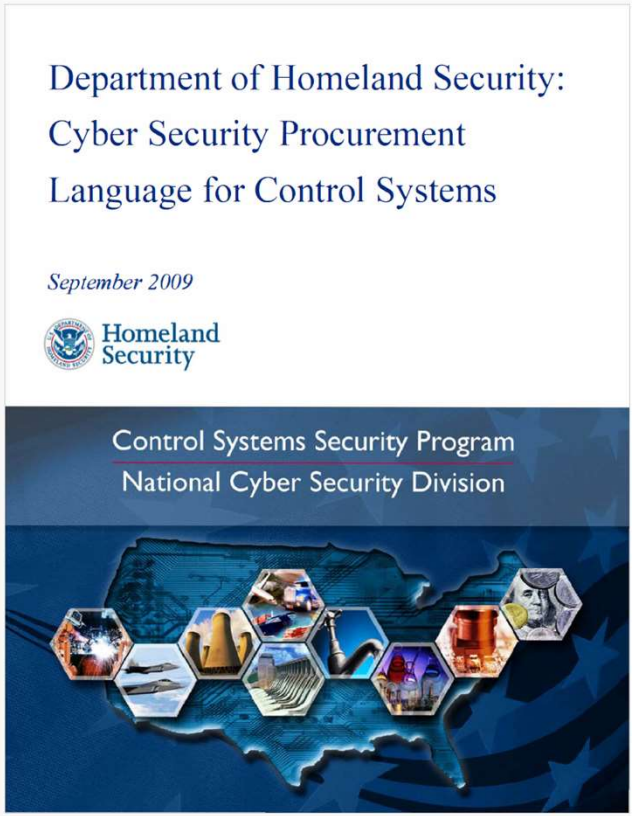
Process Perspective (cont.)

- To support the Remote access systems, how do you monitor and audit access attempts?
- How can you quickly disable user access? Have you tested this? Is this required for your incident response playbooks?
- Who authorises remote access to systems? How often is this reviewed and audited?
- Consider AESCSF Identity Practices & Anti-Patterns for this as well, for example -
  - ARCHITECTURE-AP2 - Remote or third-party access to assets circumvents network security controls
  - ACCESS-AP4 - Non-public, Internet-facing assets can be accessed using single-factor authentication
  - ACCESS-AP7 -Identities (users) cannot be individually identified and attributed to a person
  - ACCESS-AP9 - Unknown or unauthorised identities (users) and assets can connect to known assets

Ref - https://aemo.com.au/en/initiatives/major-programs/cyber-security/aescsf-framework-and-resources

Process Perspective (cont.)

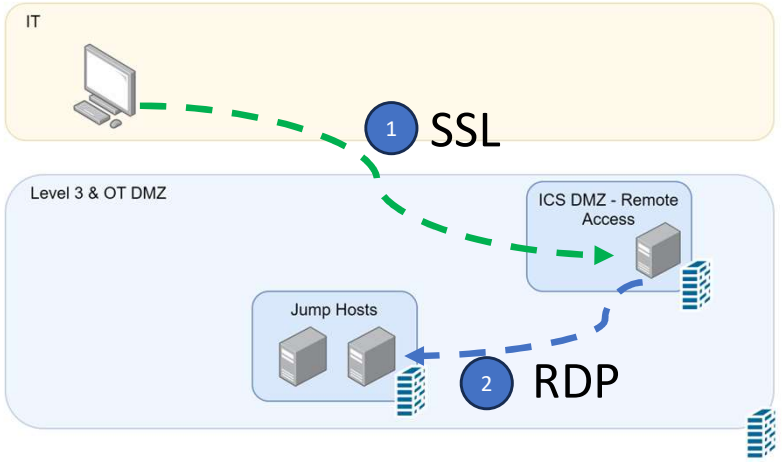
- ICS-CERT Procurement Language considers Remote Access
  - Dial-Up Modems
  - Dedicated Line Modems
  - TCP/IP
  - Web-Based Interfaces
  - Virtual Private Networks
  - Serial Communication Security
- Defines
  - Basis
  - Language Guidance
  - Procurement Language
  - FAT & SAT Measures
  - References



6. Technology Perspective

Technology Perspective

- Microsoft Remote Desktop Gateway Services is a good solution
- Break of protocol, uses SSL to the Connection Broker and then RDP From the broker to the jump host
- The Remote Desktop Gateway can use Corporate Identities and the Jump Box can use the OT Identities
- SANS ICS612 has a hands on lab using RDS to provide a secure remote access architecture
- Learn more at https://learn.microsoft.com/en-us/windows-server/remote/remote-desktop-services/



Technology Perspective (cont.)

- Other Example Vendor Remote Access Solutions
- Other OT security solutions are also including Secure Remote Access
- Consider Secure File Transfer capabilities as well

CYBERARK

citrix

ConsoleWorks
Cybersecurity Operations Platform

BeyondTrust

Technology Perspective (cont.)

- These devices should be considered highly critical and need to be hardened
- Remote administration tools such as Powershell and other system utilities
- Ensure you have adequate logging and monitoring to detect system abuse or privilege escalation
- Thanks to Gus' 2023 SANS ICS Summit Presentation for the tip – lessons from the field from Dragos Penetration Testers

Technology Perspective (cont.)

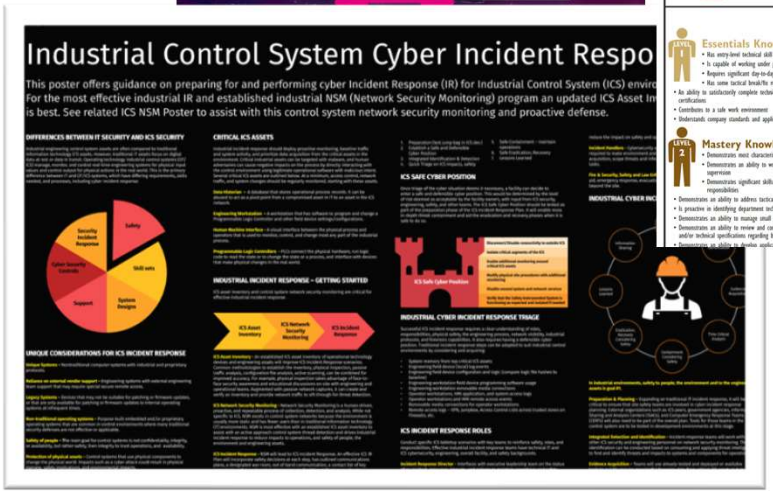
- One of the coolest “low tech” examples I have seen was an Unmanaged switch powered by a Circuit Breaker controlled by the control system
- The Circuit breaker had a remote operated power mode and the Plant Operators were able to control the circuit breaker via the HMI/OWS
- It is a simple and intuitive interface for plant operators to enable remote access to third party vendors

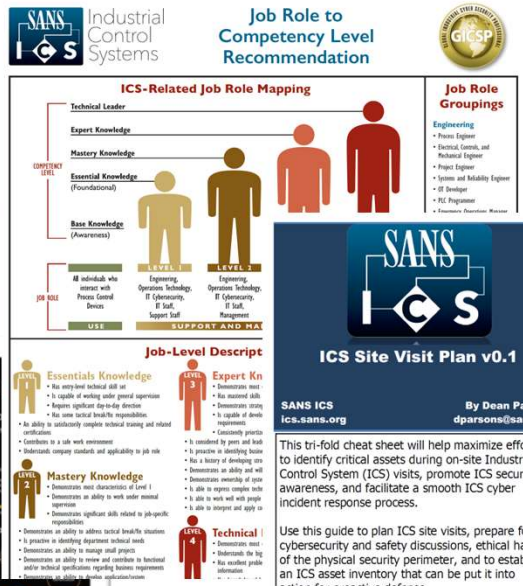
Image - https://blog.isa.org/design-tips-effective-industrial-machine-process-automation-hmi

7. SANS ICS Community Resources

SANS ICS Community Resources

1. SANS ICS Field Manual
2. SANS ICS Youtube – Concepts Series, Summit Recordings and many more resources
3. SANS ICS Community Forum – https://ics.sans.org
4. SANS Posters –Active Defense Poster, Site Visit, Job Poster and Many More





SANS Videos About Secure Remote Access

https://www.youtube.com/watch?v=-XEdb-B4dCo

https://www.youtube.com/watch?v=izTUNegXskw&t=281s

Summary

- **Review SANS Five ICS Critical Cyber Security Controls**
  - Read the White Paper
  - Watch the Webinar Recording
- **SANS 2024 State of ICS/OT Cybersecurity insights for Control #4**
  - Read the Report
  - Watch the Webinar Recording
- **Security Architecture Supports Control #4 Secure Remote Access**
  - SANS ICS410 SCADA Reference Architecture
  - Refer to Security Patterns and ensure Anti-Patterns are not present
- **People Perspectives**
  - Make sure your people understand why Secure Remote Access matters – use examples of security incidents where insecure remote access was critical
- **Process Perspectives**
  - Consider using parts of the ACSC Remote Access Protocol
  - Review how Remote Access is provisioned and reviewed
  - Ensure adequate logging and monitoring is present
  - Use the Practices and Anti-Patterns to support your identity capability
- **Technology Perspectives**
  - There are many Vendor Options and the MS Remote Desktop Services Option
  - Make sure you harden and reduce attack surface on jump boxes
  - Think about “low tech” like Circuit Breakers controlled via Operator Work Station (OWS) or HMI
- **SANS Community Resources**
  - **https://ics.sans.org/**

Thank you, Questions?

bruce@blarge.io
https://www.linkedin.com/in/blargeau/
https://github.com/belarge/SANSICS