USAID
FROM THE AMERICAN PEOPLE

USEA
United States Energy Association

Secure Remote Access and Cloud Security in the Electricity Sector

- Justin Searle

Cybersecurity and Digitalization:
Supply Chain Risks in the Electricity
Sector

SANS Five Critical Controls for ICS/OT Cybersecurity

1. ICS incident response plan
2. A defensible architecture
3. Visibility and monitoring
4. Secure remote access
5. Risk-based vulnerability management

Secure remote access depends on a defensible architecture!

SANS ICS/OT Control 2: A Defensible Architecture

- Networks should be organized into security zones using
  - Purdue levels are the most common security zone naming scheme used
  - Purdue model is first and foremost a linguistical tool!!!

- ICS410 reference model is based on guidance in ISA/IEC 62443
  - Each level has different components, services, and functions
  - A single Purdue level can contain multiple subnets
  - Network defenses can be placed between subnets in the same Purdue level

- Enforcement boundaries are where we place cybersecurity network defenses
  - Limit communications through the boundary (think firewalls)
  - Record and inspect communications through the boundary

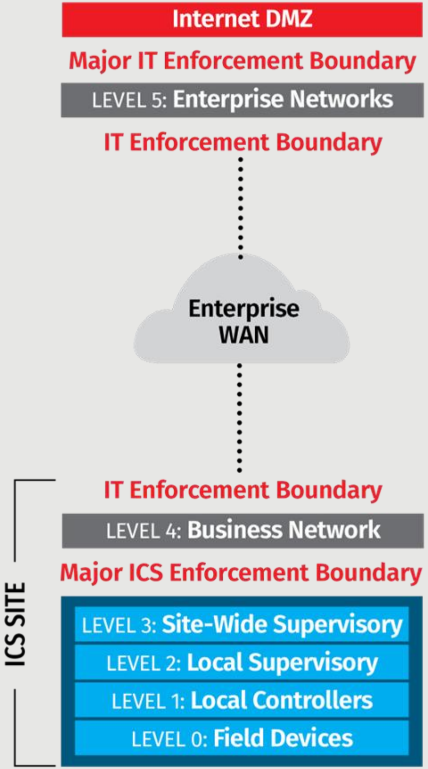
IT/OT Demarcation

- Segmentation between IT and OT is key
  - OT environments are overly dependent on network defenses
  - Host-based security solutions are harder and sometimes impossible to deploy

- Vendor and commissioning restrictions make endpoint security harder
  - Older software because of longer life cycle requirements
  - Less ability to harden or patch endpoints

- Determining the demarcation between IT and OT
  - Assets that make up the OT processes are usually obvious
  - Other OT assets should be determined by their ability to directly or indirectly affect OT

Levels 4 and 5: Business and Enterprise Networks



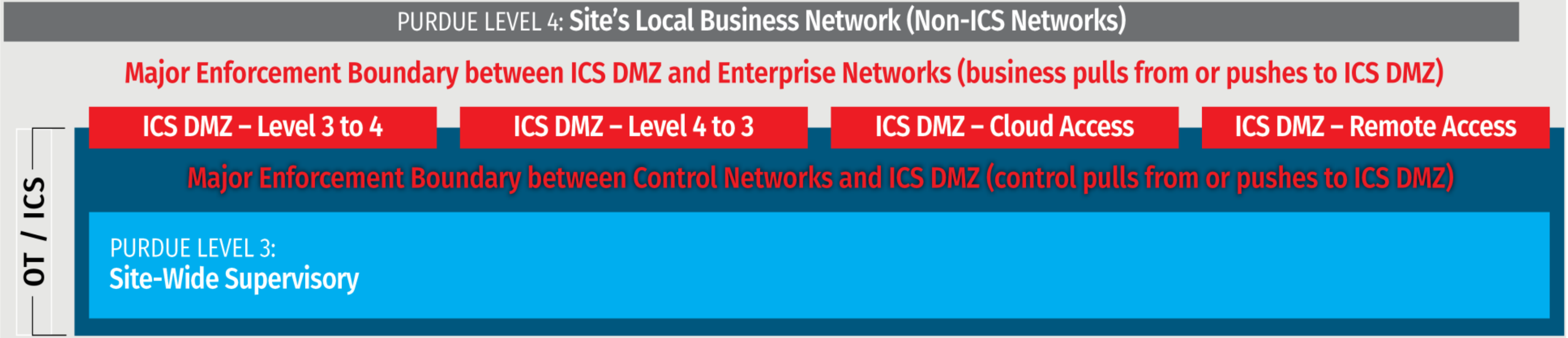
Internet DMZ
Major IT Enforcement Boundary
LEVEL 5: Enterprise Networks
IT Enforcement Boundary
Enterprise WAN
IT Enforcement Boundary
LEVEL 4: Business Network
Major ICS Enforcement Boundary
LEVEL 3: Site-Wide Supervisory
LEVEL 2: Local Supervisory
LEVEL 1: Local Controllers
LEVEL 0: Field Devices
ICS SITE

- Most OT/ICS sites are connected back to the enterprise
  - MPLS or satellite links are common
  - Enterprise provides many important services to the plants

- Each larger site, plant, or facility usually has a business network
  - This is Purdue Level 4
  - Supporting services, data, etc.
  - HR systems, email servers, print servers
  - Enterprise Security Operations Center (SOC)

- General cybersecurity guidelines
  - Internet access and email should not go deeper than Level 4
  - Level 4 machines should be provided for OT staff to access this data
  - Enterprise Active Directory (AD) should not extend below this point

A Strong ICS Perimeter Includes a DMZ


PURDUE LEVEL 4: Site's Local Business Network (Non-ICS Networks)
Major Enforcement Boundary between ICS DMZ and Enterprise Networks (business pulls from or pushes to ICS DMZ)
ICS DMZ – Level 3 to 4
ICS DMZ – Level 4 to 3
ICS DMZ – Cloud Access
ICS DMZ – Remote Access
Major Enforcement Boundary between Control Networks and ICS DMZ (control pulls from or pushes to ICS DMZ)
PURDUE LEVEL 3:
Site-Wide Supervisory
OT / ICS

- ICS DMZ and its enforcement boundaries are your primary ICS perimeter
  - Scale number of ICS DMZs to complexity of IT/OT traffic
  - Use micro-segmentation to minimize lateral movement in DMZ
  - Web proxies should be avoided since they blindly pass on exploits
  - Don't place patch management and other security services here, instead place them in Purdue Level 3
- The most secure communications should look like this
  - Level 4/5 pushes to this DMZ, and Level 3 pulls from it
  - Level 3 pushes to this DMZ, and Level 4/5 pulls from it
  - Larger sites can use multiple DMZ to further separate traffic and mitigate risk
  - Smaller sites can use a single ICS DMZ

Avoid Sharing Management Solutions

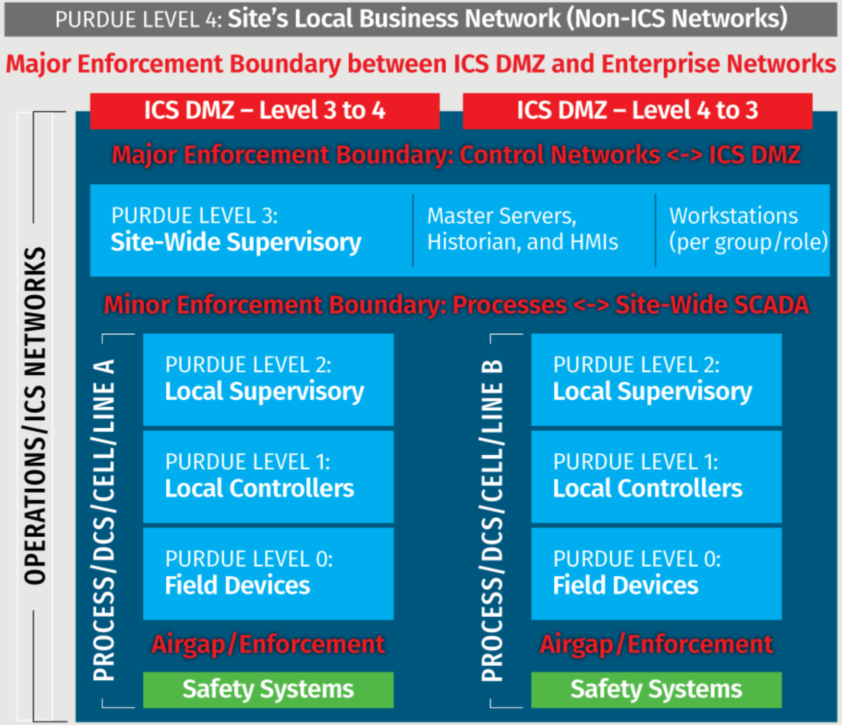
- Sharing management solutions between IT/OT increases complexity
  - Increases firewall rules
  - Shared Active Directory (AD) exposes OT credentials to AD attacks in IT
  - Shared network and virtualization management leads to IT/OT perimeter bypasses
  - Leads other future management solutions to also span IT/OT perimeter
  - **Makes islanding OT more difficult, less effective, and maybe impossible**

- Recommendation: Separate all management solutions between IT/OT
  - Use separate AD for IT and OT with no trust relationships between them
  - Manage OT networks, virtualization, backups, patching, and EDR from within OT

- Use the same solution in IT/OT where feasible, but with different management servers
  - Takes advantage of bulk licensing
  - Allows for skill sharing and shared knowledge between IT/OT

Enforcement Boundaries between Level 3 and Processes

- Identify major process groups at each site
- Consider minor enforcement boundary between them and Purdue Level 3
- Isolate any safety system communication from the rest of the ICS network


PURDUE LEVEL 4: Site's Local Business Network (Non-ICS Networks)
Major Enforcement Boundary between ICS DMZ and Enterprise Networks
ICS DMZ – Level 3 to 4
ICS DMZ – Level 4 to 3
Major Enforcement Boundary: Control Networks <-> ICS DMZ
OPERATIONS/ICS NETWORKS
PURDUE LEVEL 3: Site-Wide Supervisory
Master Servers, Historian, and HMIs
Workstations (per group/role)
Minor Enforcement Boundary: Processes <-> Site-Wide SCADA
PROCESS/DCS/CELL/LINE A
PURDUE LEVEL 2: Local Supervisory
PURDUE LEVEL 1: Local Controllers
PURDUE LEVEL 0: Field Devices
Airgap/Enforcement
Safety Systems
PROCESS/DCS/CELL/LINE B
PURDUE LEVEL 2: Local Supervisory
PURDUE LEVEL 1: Local Controllers
PURDUE LEVEL 0: Field Devices
Airgap/Enforcement
Safety Systems

Individual Remote Access – Two Separate Steps

1: From the Internet to the ICS DMZ

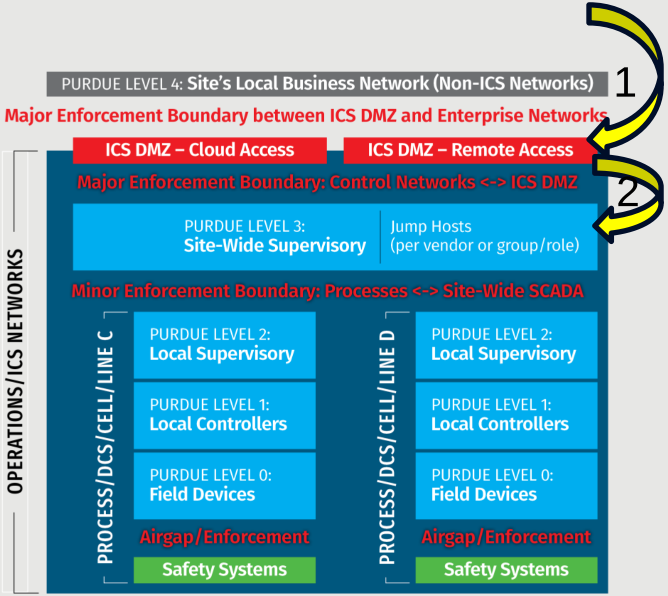
- Leverage a VPN or Zero Trust Architecture (ZTA) remote access solution
- Two-factor authenticates REQUIRED
- Use standalone authentication or Enterprise AD

2: From ICS DMZ to individual assets or jump host in Level 3

- Use OT AD authentication
- Leverage different jump hosts per employee role or vendor
- ZTA solutions could provide limited access direct to asset

Additional recommendations:

- Solution in step 1 or 2 should record session
- Prevent most remote users from bringing data
- If permitted, use file server in ICS DMZ or ZTA to
  - Hash files for IR and forensics
  - Scan files for malware,
    if passes, enables download from jump host
  - Prevent most from using of software on remote host



PURDUE LEVEL 4: **Site's Local Business Network (Non-ICS Networks)**

1

Major Enforcement Boundary between ICS DMZ and Enterprise Networks

ICS DMZ – Cloud Access

ICS DMZ – Remote Access

Major Enforcement Boundary: Control Networks <-> ICS DMZ

2

PURDUE LEVEL 3: **Site-Wide Supervisory**

Jump Hosts (per vendor or group/role)

Minor Enforcement Boundary: Processes <-> Site-Wide SCADA

OPERATIONS/ICS NETWORKS

PROCESS/DCS/CELL/LINE C

PURDUE LEVEL 2: **Local Supervisory**

PURDUE LEVEL 1: **Local Controllers**

PURDUE LEVEL 0: **Field Devices**

Airgap/Enforcement

Safety Systems

PROCESS/DCS/CELL/LINE D

PURDUE LEVEL 2: **Local Supervisory**

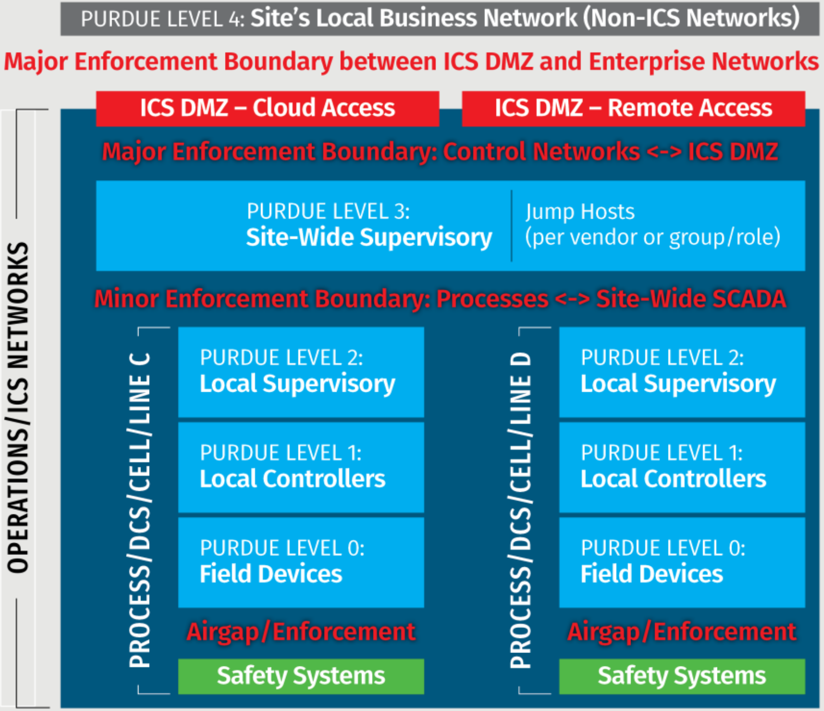
PURDUE LEVEL 1: **Local Controllers**

PURDUE LEVEL 0: **Field Devices**

Airgap/Enforcement

Safety Systems

Cloud Connectivity and IIoT


PURDUE LEVEL 4: Site's Local Business Network (Non-ICS Networks)
Major Enforcement Boundary between ICS DMZ and Enterprise Networks
ICS DMZ – Cloud Access
ICS DMZ – Remote Access
Major Enforcement Boundary: Control Networks <-> ICS DMZ
PURDUE LEVEL 3: Site-Wide Supervisory
Jump Hosts (per vendor or group/role)
Minor Enforcement Boundary: Processes <-> Site-Wide SCADA
OPERATIONS/ICS NETWORKS
PROCESS/DCS/CELL/LINE C
PURDUE LEVEL 2: Local Supervisory
PURDUE LEVEL 1: Local Controllers
PURDUE LEVEL 0: Field Devices
Airgap/Enforcement
Safety Systems
PROCESS/DCS/CELL/LINE D
PURDUE LEVEL 2: Local Supervisory
PURDUE LEVEL 1: Local Controllers
PURDUE LEVEL 0: Field Devices
Airgap/Enforcement
Safety Systems

Cloud connectivity should be considered very carefully

- Is it required?
- Does it affect security, reliability, and safety?
- Treat traditional 24x7 vendor remote access like cloud

When needed, assume attack and isolate traffic patterns

- Use TLS protected protocols or VPNs
- Firewall rules should use IPs if possible, hostnames if not
- Firewall rules should be highly specific in both directions
- All traffic should move through a system in ICS Cloud DMZ
  - Either a server that brokers traffic between cloud and ICS assets
  - Or a web proxy with allow lists between specific systems and services
  - Both solutions should support logging, tuned appropriately
- If connections to level 2, 1, or 0 are needed, place secondary defenses around those assets to block pivots

Conclusion

- If you do not have a defensible perimeter between IT and OT
  - Remote access to IT pivots to remote access to OT
- If you do not have enforcement boundaries inside OT
  - Remote access to low value assets pivots to critical access
- Cloud connectivity to one asset or process needs to be isolated from other assets and processes
  - This requires a defensible network architecture

Justin Searle
jsearle@inguardians.com

USAID
FROM THE AMERICAN PEOPLE

USEA
United States Energy Association