

An Overview of the SANS Five ICS Cybersecurity Critical Controls

Focus on Control Number 1 - ICS-Specific Incident Response Plan

SANS DFIR
APAC DFIR
SUMMIT & TRAINING
デジタルフォレンジック&インシデントレスポンス



/whoami

- Cyber Security Architect with an interest in OT Active Defense and Cyber Security Operations
- Worked in IT and OT in Network & System Engineering and Cyber Security roles for over 15 years
- Worked in Electricity Generation and Transmission, Rail, Aviation, Emergency Services and Consulting
- Chartered Professional Engineer (CPEng) in Information, Telecommunications and Electronics Engineering (ITEE)
- Bachelor Engineering (Telecomms) QUT and Master Business (Applied Finance) QUT



Agenda

1. A brief overview of Operational Technology & Industrial Control Systems
2. The SANS Five ICS Cyber Security Critical Controls
3. Deep Dive into Critical Control #1 – ICS Specific Incident Response Plan
4. Key OT Incident Response Concepts from ICS515
5. SANS ICS Security Community Resources
6. Summary

SANS DFIR

APAC DFIR

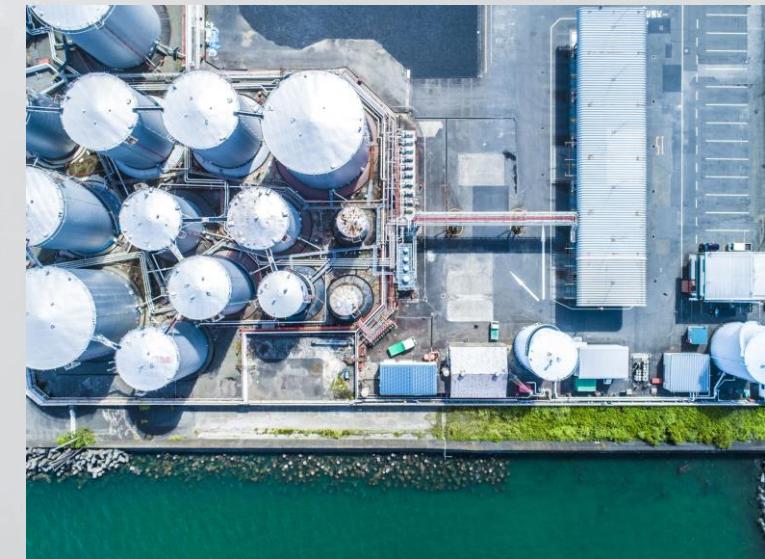
SUMMIT & TRAINING

デジタルフォレンジック&インシデントレスポンス

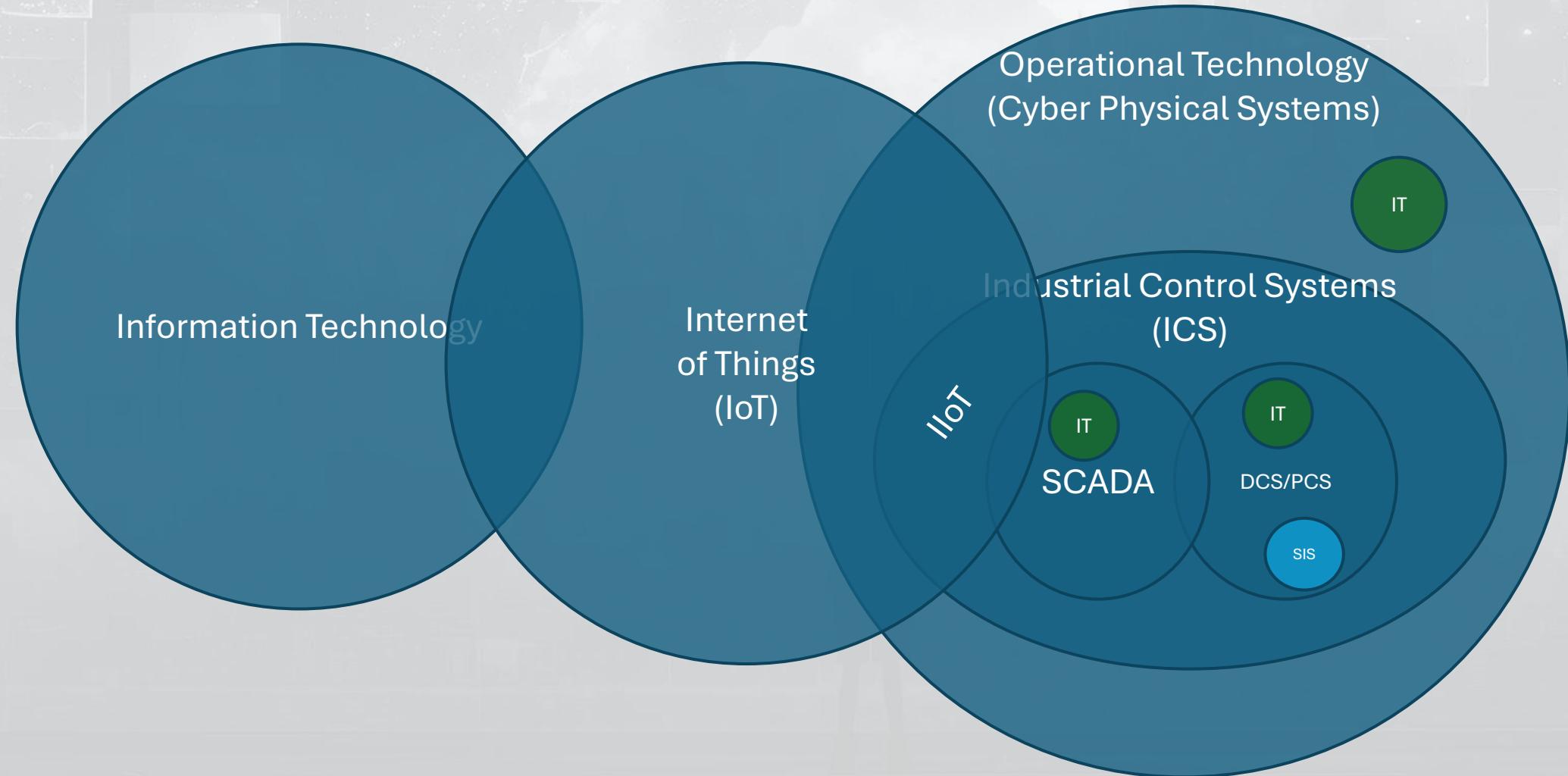
A brief overview of
Operational Technology and
Industrial Control Systems

What is Operational Technology (OT)

- Operational Technology are the systems that monitor and control the physical world
- It is a nebulous term and is also referred to as:
 - Industrial Control Systems
 - Cyber Physical Systems
- The International Society of Automation (ISA) Defines Industrial Automation and Control Systems (IACS) as -
 - *“Collection of personnel, hardware, software, and policies involved in the operation of the industrial process and that can affect or influence its safe, secure and reliable operation.”*



What is Operational Technology (cont.)

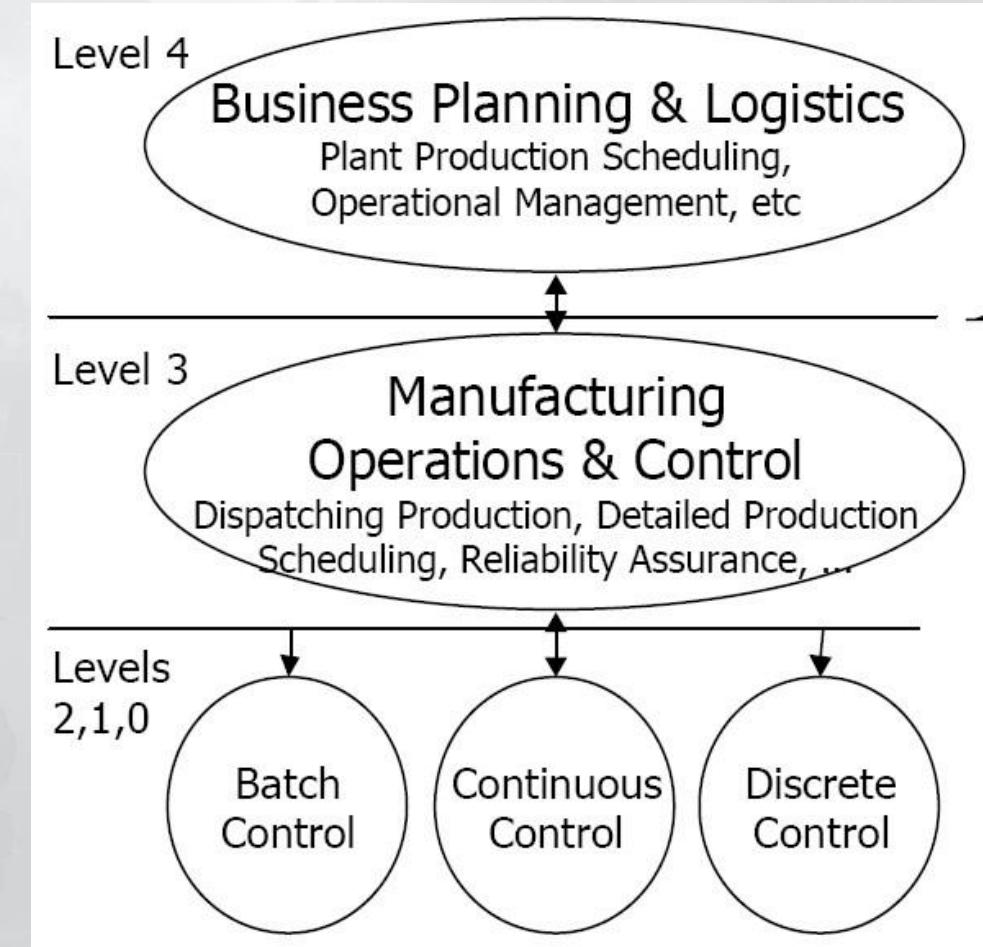


Key OT Assets

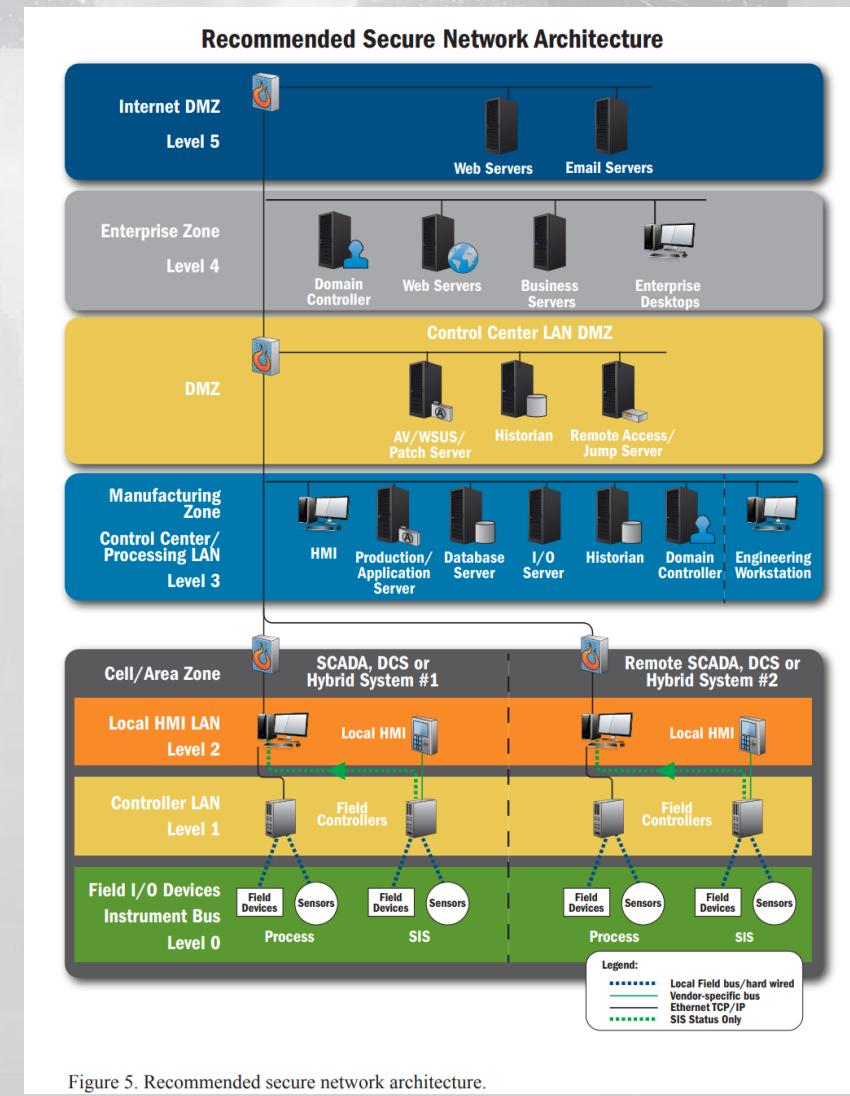
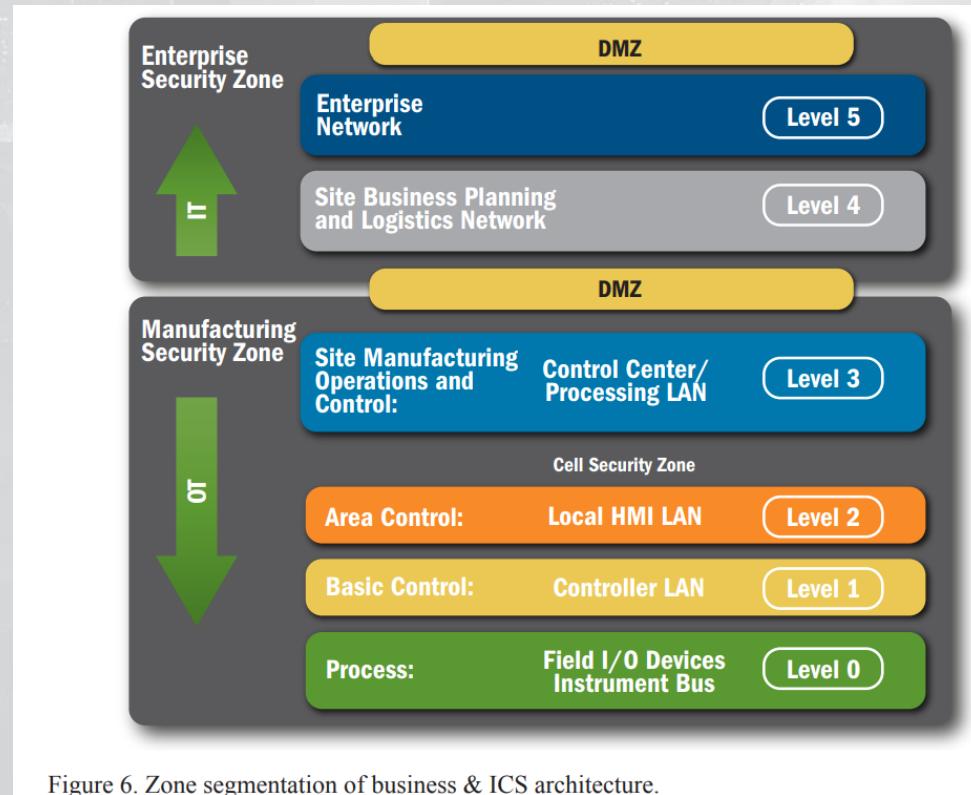
- SCADA/Control Server/DCS Server
- Human Machine Interface (HMI)
 - Operator Work Stations (OWS)
 - Local HMI
- Engineering Work Stations (EWS)
- Local Controllers
 - Programmable Logic Controller
 - DCS Controller
 - Remote Terminal Unit
- Safety Instrumented System (SIS)

The Purdue Enterprise Reference Architecture (PERA)

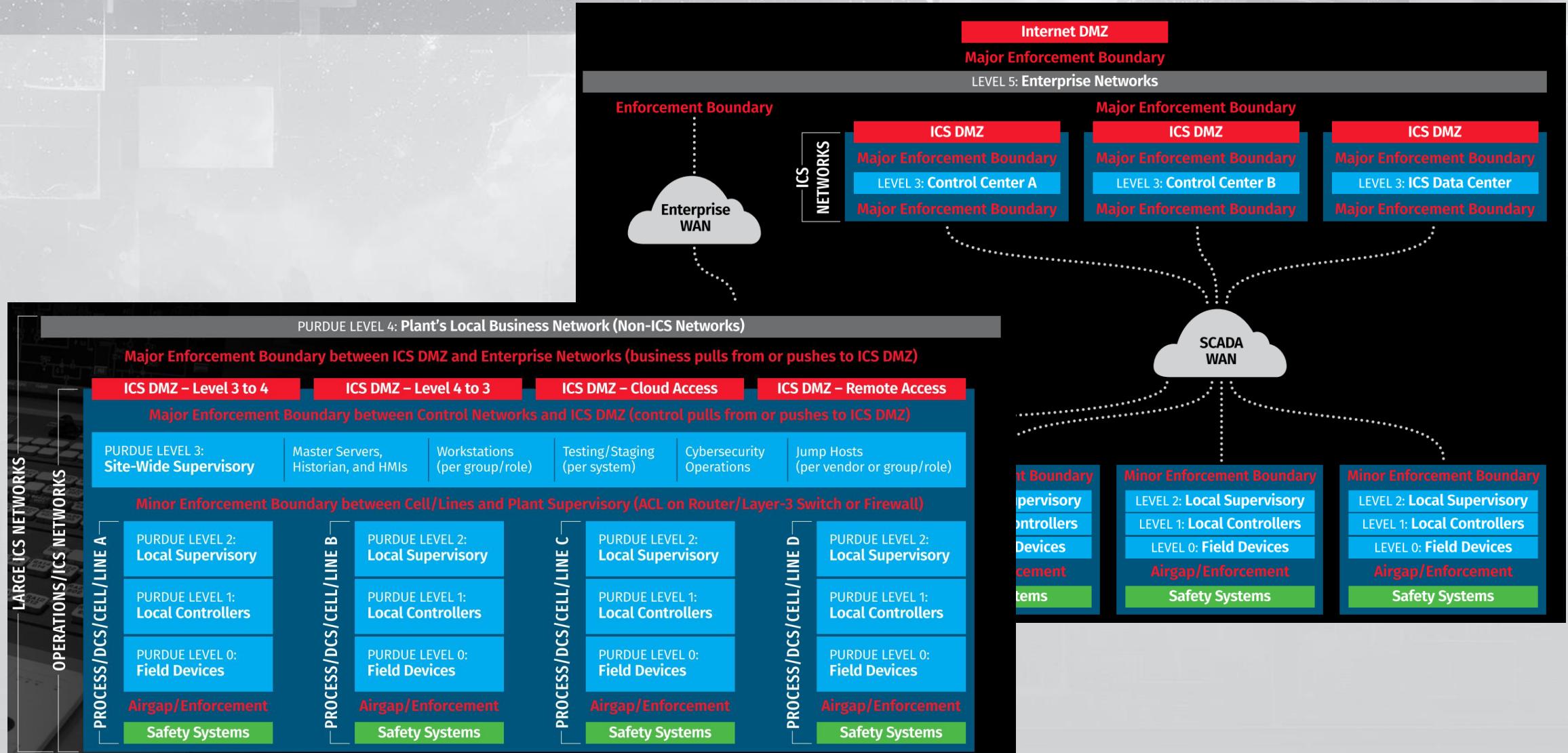
- Often referred to as the “Purdue Model”
- Is often mistaken as a network segmentation model ...
- Rather, it is a **functional model** and describes time
- Referenced by ISA-95 to describe how to integrate IT and ICS Networks in the 1990s



ICS-CERT Recommended Architecture



The SANS ICS410 SCADA Reference Model



MITRE ATT&CK for ICS

ICS Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for ICS.

[View on the ATT&CK® Navigator](#)

[Version Permalink](#)

Initial Access 12 techniques	Execution 10 techniques	Persistence 6 techniques	Privilege Escalation 2 techniques	Evasion 7 techniques	Discovery 5 techniques	Lateral Movement 7 techniques	Collection 11 techniques	Command and Control 3 techniques	Inhibit Response Function 14 techniques	Impair Process Control 5 techniques	Impact 12 techniques
Drive-by Compromise	Autorun Image	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Change Operating Mode	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Command-Line Interface	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Execution through API	Project File Infection	Rootkit	Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System	Block Reporting Message	Spoof Reporting Message	Loss of Availability	
Internet Accessible Device	Graphical User Interface	System Firmware		Spoof Reporting Message	Wireless Sniffing	Program Download	Detect Operating Mode	Block Serial COM	Unauthorized Command Message	Loss of Control	
Remote Services	Hooking	Valid Accounts	System Binary Proxy Execution	System Binary Proxy Execution	Remote Services	I/O Image	Monitor Process State	Change Credential	Loss of Productivity and Revenue		
Replication Through Removable Media	Modify Controller Tasking	Native API			Valid Accounts	Point & Tag Identification	Denial of Service	Device Restart/Shutdown	Manipulate I/O Image		
Rogue Master	Scripting	Scripting	User Execution			Program Upload	Modify Alarm Settings	Modify Alarm Settings	Rootkit		
Spearphishing Attachment	User Execution	User Execution				Screen Capture	Rootkit	Service Stop	Service Stop		
Supply Chain Compromise						Wireless Sniffing	System Firmware	System Firmware			
Transient Cyber Asset											
Wireless Compromise											

SANS DFIR

APAC DFIR

SUMMIT & TRAINING

デジタルフォレンジック&インシデントレスポンス

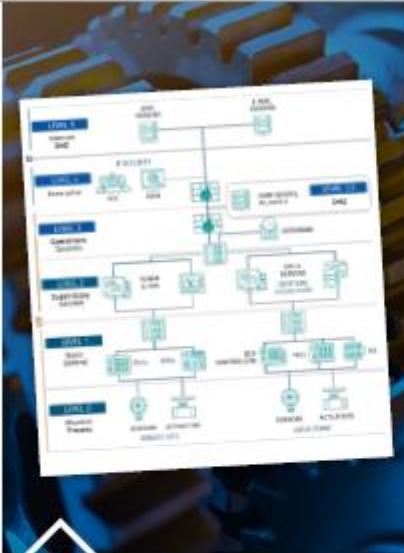
The SANS Five ICS Cybersecurity Critical Controls

The Five ICS Cyber Security Critical Controls



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

#1 ICS Incident Response

- Starting 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
- We will come back to go into this one in more detail later in this presentation

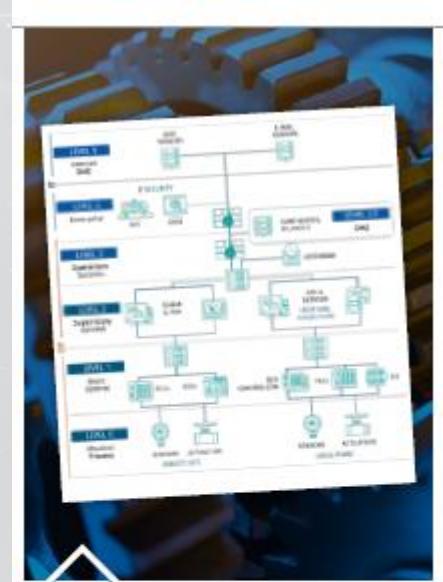


ICS INCIDENT RESPONSE

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

#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

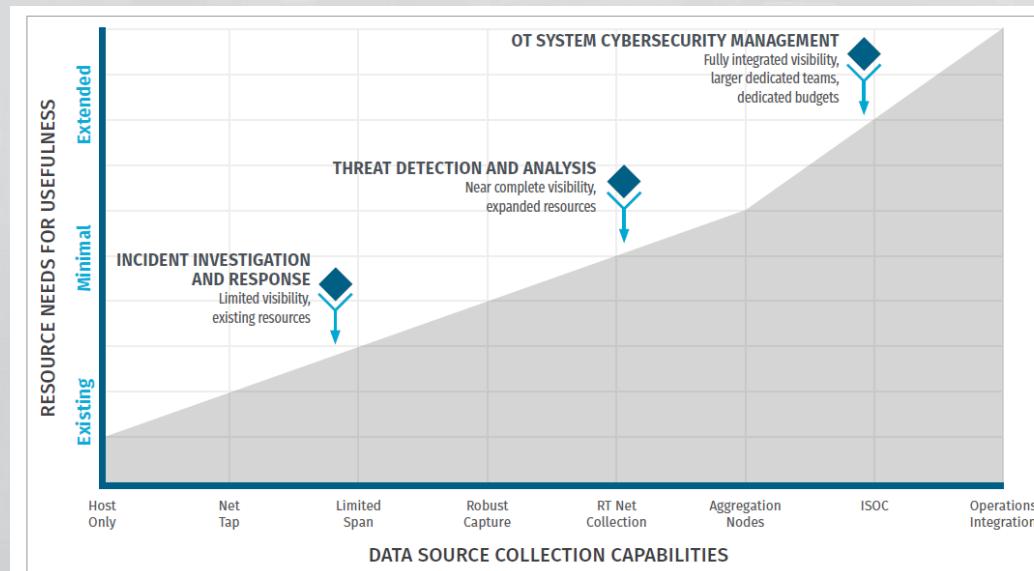


DEFENSIBLE ARCHITECTURE

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

#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

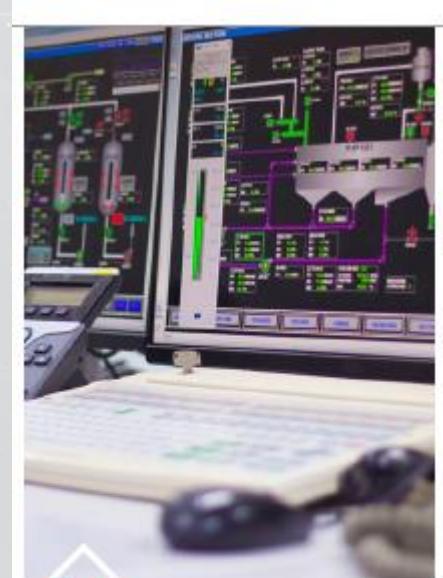


ICS NETWORK VISIBILITY MONITORING

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

#4 Secure Remote Access

- It's not just MFA
- COVID-19 has seen the attack surface increase
- Your Stage-1 Kill Chain may now be in your third parties

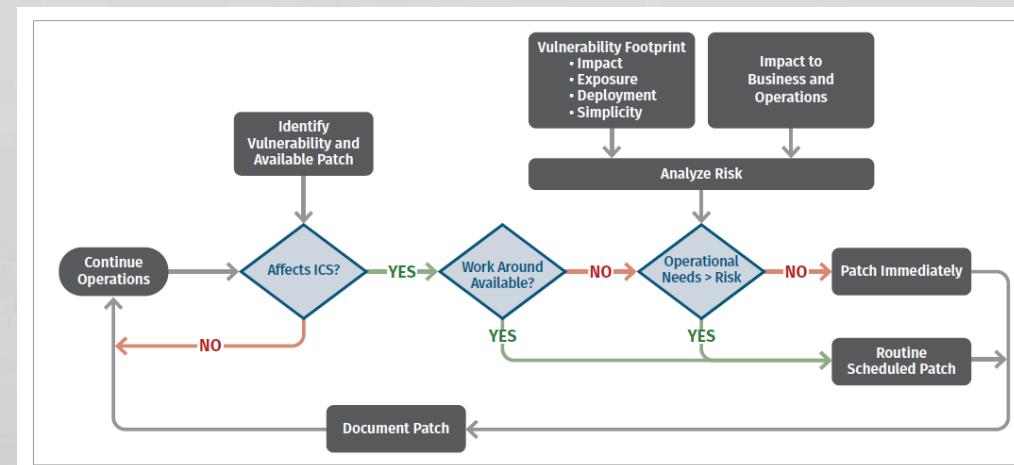


SECURE REMOTE ACCESS

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

#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



SANS DFIR

APAC DFIR

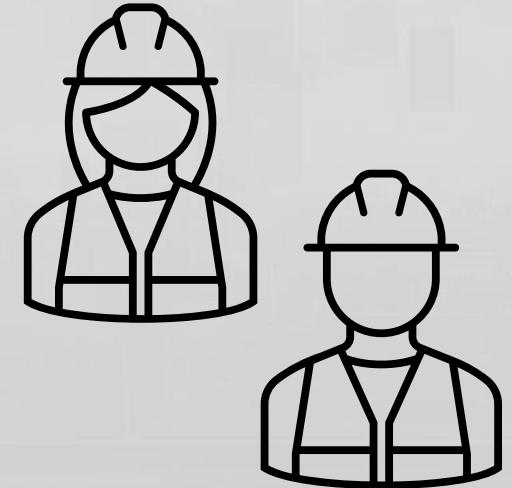
SUMMIT & TRAINING

デジタルフォレンジック&インシデントレスポンス

#1 ICS Incident Response Deep Dive

Safety

- **Personal Safety is Critical in ICS Incident Response**
- Vital to understand physical hazards especially ones that the ICS controls
- The response team must have correct inductions, site permits/tickets and appropriate Personal Protective Equipment (PPE)
- Ideally the team should be familiar with sites prior to an incident



Define and Prioritise Scenarios

- The most critical activity in Control #1
- Ransomware must be considered for all Industries
- Electric:
 - Ukraine 2015 and Ukraine 2016 (CRASHOVERRIDE)
- Oil & Gas:
 - TRISIS
- Also consider high-consequence low likelihood events:
 - Work with your Engineering and Operations teams and ask “What does a really bad day look like”

Top 5 Recommended Tabletops

- Dean Parson's Top 5 Recommended Tabletops:
 - Scenario 1 – Living off the Land: Native Industrial Control System Protocol Abuse
 - Scenario 2 – Human Machine Interface Hijack: On-Screen Suspected Activity
 - Scenario 3 – Physical Access to Cyber Access Event
 - Scenario 4 – Ransomware on IT or ICS/OT Networks
 - Scenario 5 – IT or ICS Network Pivot through Trusted Connections/OT Networks
 - BONUS SCENARIO – Contaminated Transient Device
- Read the blog at <https://www.sans.org/blog/top-5-ics-incident-response-tabletops-and-how-to-run-them/> which also has a link to a video session



Backdoors and Breaches – ICS/OT

- A card game developed by industry practitioners to help people learn about OT Incident Response
- A great stakeholder engagement tool for teams outside of the core OT Cyber Security Team
- Learn more at
www.backdoorsandbreaches.com
- Online version
<https://play.backdoorsandbreaches.com/play.backdoorsandbreaches.com-Engine-V1/App/>



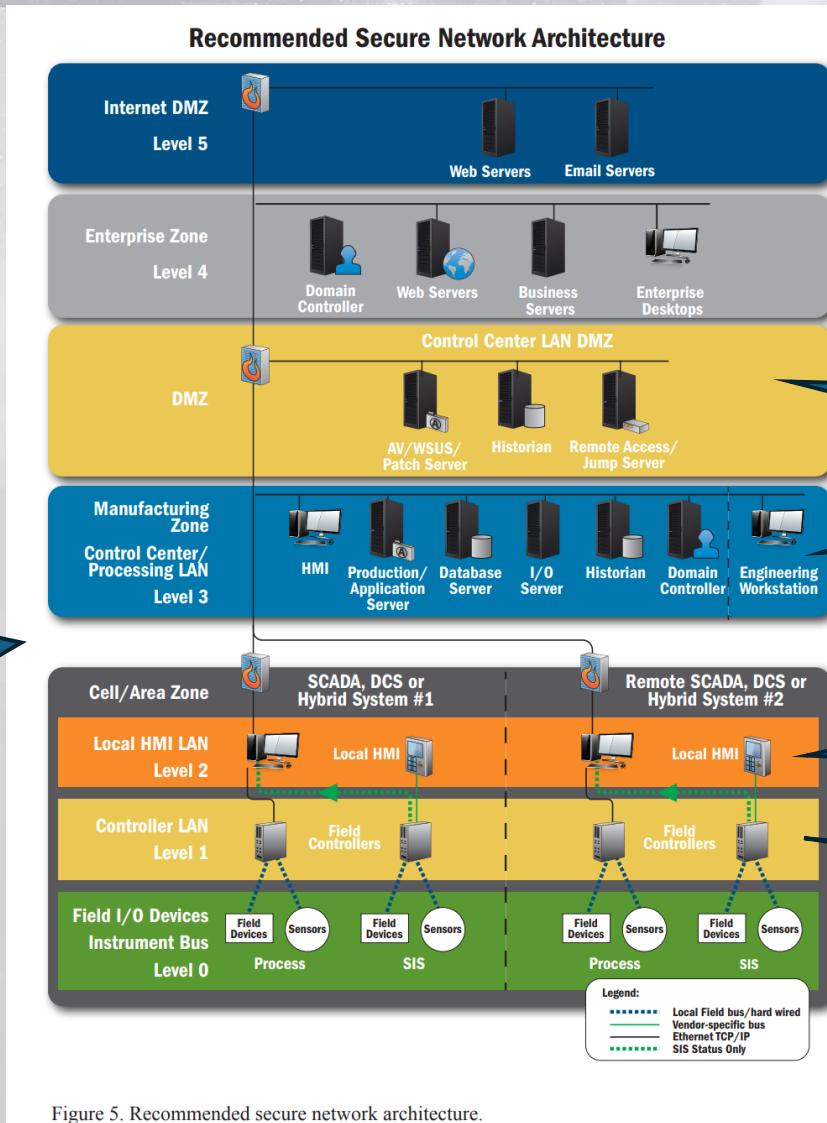
Know your Assets!

- You can't defend what you don't know
- Methods to collect:
 - Physical Inspection
 - Configuration Analysis
 - Traffic Capture
 - Active Scanning (Requires Risk Based considerations!)
- Determine how you can find baselines of what is normal configuration and behaviour and what tools exist to find “weird”

What to collect?

Network Visibility
Can work at all levels:

- Need to understand chokepoints
- Need to understand SPAN and Network Tap Capabilities
- Also consider existing switch capabilities (Netflow, local collectors etc.)



Typical IT Assets and Collection Acquisition –
IT IR can really help here!

Likely Legacy Operating Systems
Essential Reliability and Availability Requirements

Local HMIs may be older OS and use
embedded operating systems

Custom Electronic Devices, will have
specialist software and may require vendor
support

Figure 5. Recommended secure network architecture.

Collection Management Framework (Dragos)

	CONTROL CENTER	CONTROL CENTER	CONTROL CENTER	TRANSMISSION SUBSTATION	TRANSMISSION SUBSTATION
ASSET TYPE	Windows Human Machine Interface	Data Historian	Network Monitoring Appliance	Windows Human Machine Interface	Remote Terminal Units
DATA TYPE	Windows Event Logs	Alarms	Alerts	Windows Event Logs	Syslog
QUESTION TYPE (KILL CHAIN PHASES)	Exploration, Installation, Actions on Objectives	Actions on Objectives	Internal Reconnaissance, Command and Control, Delivery, Actions on Objectives	Exploitation, Installation, Actions on Objectives	Installation, Actions on Objectives
FOLLOW-ON COLLECTION	Registry Keys	Set Points and Tags	Packet Capture	Registry Keys	Controller Logic
DATA STORAGE LOCATION	Enterprise SIEM	Local	Enterprise SIEM	Local	Local
DATA STORAGE TIME	60 Days	120 Days	30 Days	30 Days	7 Days

SANS DFIR

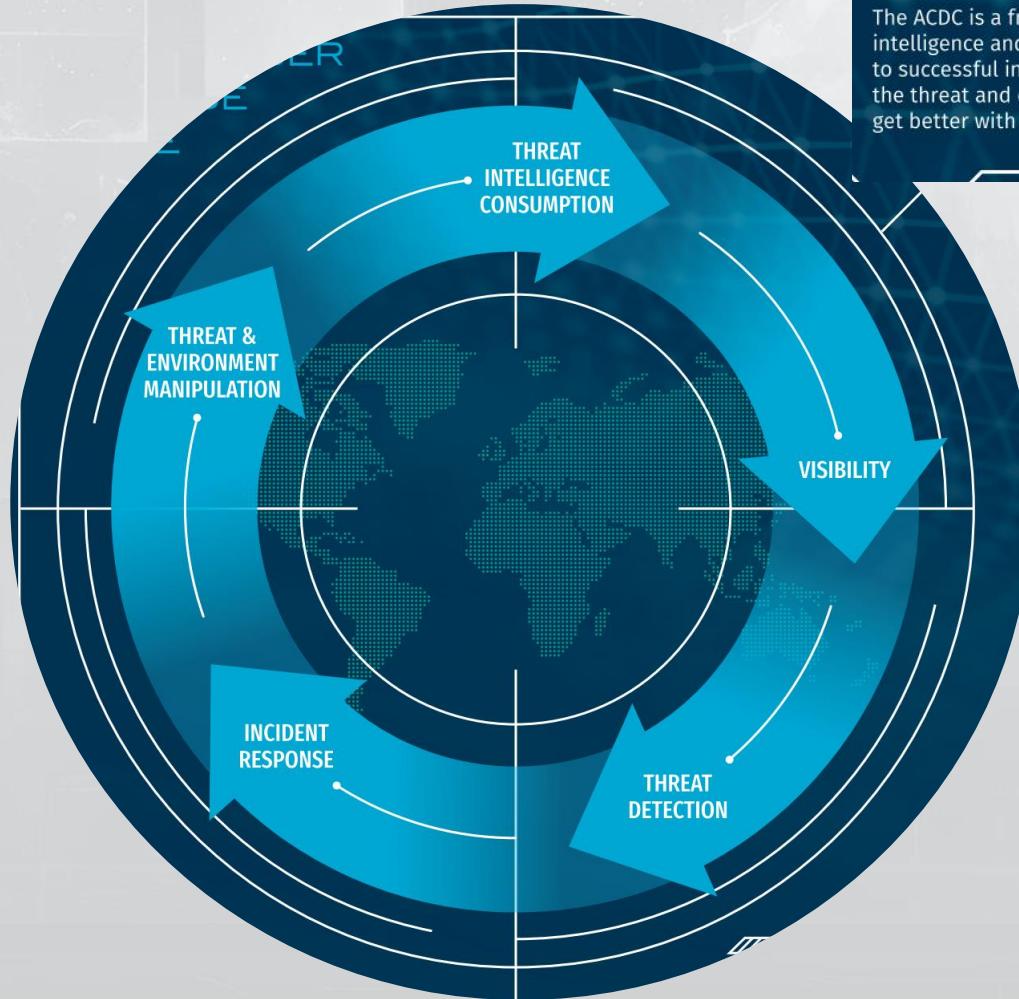
APAC DFIR

SUMMIT & TRAINING

デジタルフォレンジック&インシデントレスポンス

Key OT Incident Response Concepts from SANS ICS515

Active Cyber Defense Cycle (ACDC)



The Active Cyber Defense Cycle (ACDC)

The ACDC is a framework used in [SANS ICS515](#) to teach students how to consume intelligence and leverage it to drive monitoring efforts. This framework will lead to successful incident response engagements and an improved understanding of the threat and our systems. Consistently utilizing this framework, defenders will get better with every engagement with an adversary.

Focus on ICS threat behaviors (tactics and techniques); Indicators of Compromise (IOCs) can be valuable but should be secondary to a focus on threat behaviors which will provide more coverage and a more durable detection strategy.

- **Threat Intelligence Consumption –** Determine how to source and apply Cyber Threat Intelligence for defending your ICS
- **Visibility –** Ensuring you have adequate visibility of your environment
- **Threat Detection –** Combining Visibility with knowledge of Threats to detect
- **Incident Response –** How to Contain and Respond to ICS Threats
- **Threat & Environment Manipulation –** How to safely manipulate threats and determine how to make changes to neutralise or delay their objectives

ICS Safe Position

- Disconnect/Disable connectivity to outside the ICS
- Isolate critical segments of the ICS
- Enable additional monitoring around critical ICS assets
- Modify physical site procedures with additional monitoring
- Disable unused system and network services
- Verify that the Safety Instrumented System is functioning as expected and isolated if needed

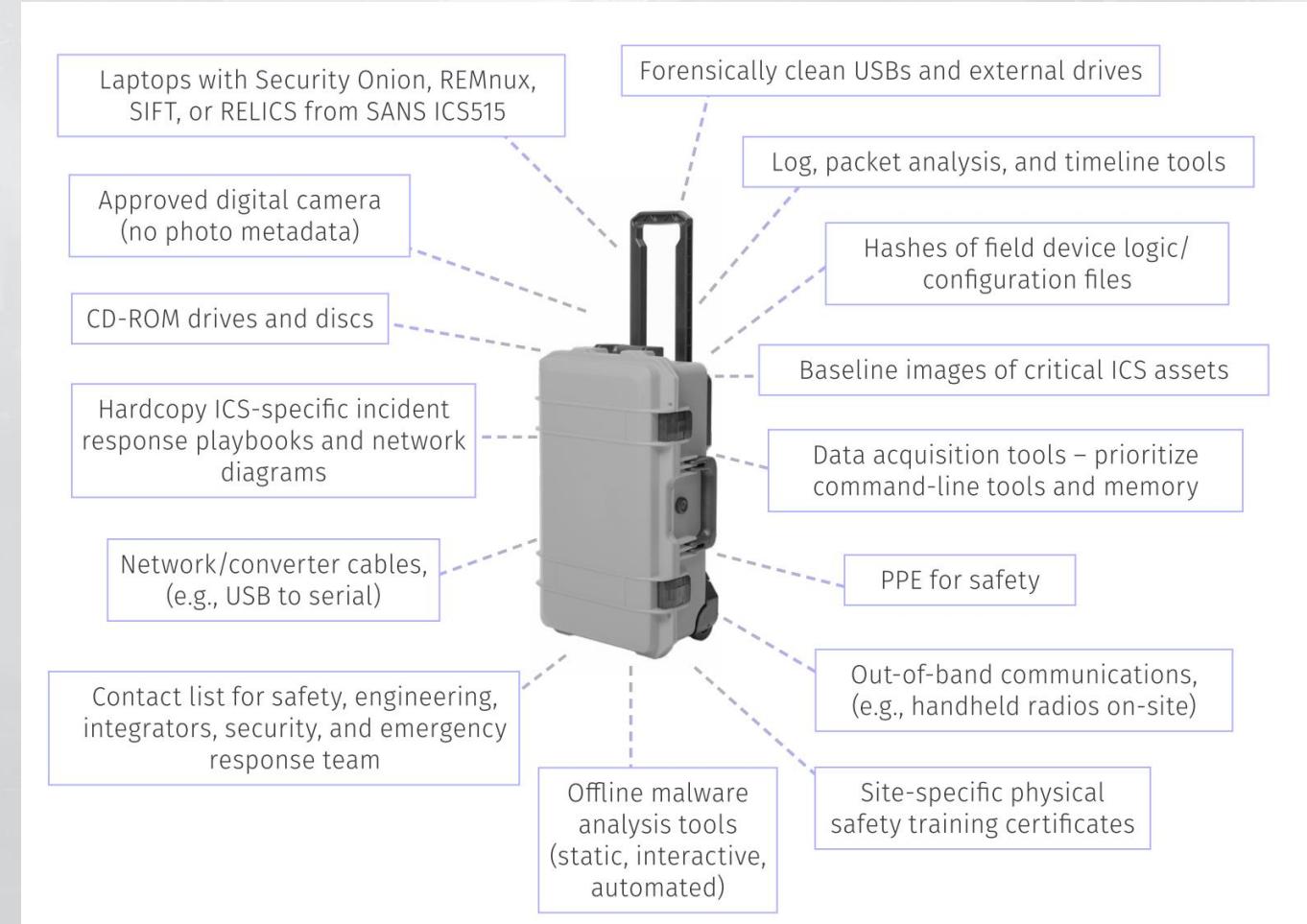
ICS Response Life Cycle



Source - <https://www.sans.org/posters/industrial-control-system-cyber-incident-response/>

ICS Jump Bag Contents

- Essential equipment to have this ready to go prior to an incident
- Ideally have them pre-deployed at your OT Sites and train site teams on how to use acquisition tools



Tying it all Together – SANS ICS IR Poster

Industrial Control System Cyber Incident Response

This poster offers a quick reference for incident response. For the most effective response, it's best. See related resources.

Differences Between IT and OT/ICS

Industrial engineering control systems are different from information technology (IT) assets. However, data at rest or data in transit. Operational Technology (OT) systems manage, monitor, and control real-world processes, including physical values and control output for physical safety. The difference between IT and OT/ICS systems is needed, and processes, including cybersecurity.

Unique Considerations

- Unique Systems** – Nontraditional computing protocols.
- Reliance on external vendor support** – Team support that may require specialized expertise.
- Legacy Systems** – Devices that may not be available for patching or updates at infrequent times.
- Non-traditional operating systems** – Platforms used by operating systems that are common in the IT world but are not effective or are not available for change.
- Safety of people** – The main goal for cybersecurity is not availability, but rather safety, then security.
- Protection of physical assets** – Controls that change the physical world. Impacts such as damage, safety implications, and environmental impact.

WHERE IS THE ADVERSARY IN THE ATTACK

After reviewing detection data from NSM and gaining an initial understanding of the malicious actions, incident response steps will be determined by where the adversary is, what the impact has been already, and what the potential impact is moving forward for control system operations and safety. An essential question is "How far along is the adversary in the attack?"

Is the adversary stealing sensitive data to build a harmful industrial attack?

Is the adversary attempting to move laterally towards the control environment?

Is the adversary attempting to elevate permissions to maintain a foothold in the control environment?

Is the adversary attempting to enumerate and map out the control network?

Is the adversary attempting to communicate with field devices to disable safety protections or affect quality assurance?

Is the adversary attempting to disrupt, manipulate, or damage physical assets or cause harm to people or the environment?

Has the adversary established a C2 and is the adversary enumerating the control network, laterally moving in the environment, attempting to access a Human Machine Interface, or accessing PLCs or other field devices on programming service ports?

WHEN TO INITIATE ICS INCIDENT RESPONSE

Analysis drawing on ICS NSM will contribute to escalating the factors that will ultimately determine when industrial incident response steps are to be invoked. Use the questions listed above to help determine the potential risk that an intrusion will disrupt the industrial process or safety, and to understand the progression of an attack already in progress. Answers to these questions will help drive defense steps and shift to potential incident response steps.

Malicious Code, Unauthorized Access Detected	Exfiltration of sensitive industrial system information	Loss of visibility of control process	Loss of process controls	Manipulation of control system operations	Physical Damage to assets or safety concerns
Malicious Code, Unauthorized Access Detected	Exfiltration of sensitive industrial system information	Loss of visibility of control process	Loss of process controls	Manipulation of control system operations	Physical Damage to assets or safety concerns
Malicious Code, Unauthorized Access Detected	Exfiltration of sensitive industrial system information	Loss of visibility of control process	Loss of process controls	Manipulation of control system operations	Physical Damage to assets or safety concerns

Posters are intended for general guidance only. They are not intended to be comprehensive, nor do they provide legal advice. They are not intended to be relied upon for specific circumstances. It is recommended to consult with legal counsel and industry experts for specific guidance.

ICS INCIDENT RESPONSE TABLETOPS

An incident response tabletop is a paper-based exercise that facilitates security discussions across several teams and focuses on existing preparedness. A tabletop exercise can help verify deployed security technologies, controls, event monitoring, and security processes to help identify areas for improvement. Beyond traditional ICS incident response tabletops, industrial tabletops must consider additional teams, controls, and environments built for industrial operations, which have a different nature than IT.

Regularly conducted incident response tabletop exercises as part of a mature ICS Security Program serve to identify weak points in security efforts and enable proactive defense to address the range of threats.

Validation – Tabletop exercises validate readiness by comparing optimal defense controls against existing controls. Areas in need of improvement are identified in industrial incident response plans and security and safety playbooks. Simultaneously, tabletops help train both new and established team members about the industrial process and ICS-specific security.

Situational Awareness and Team Building – Reviewing threat intelligence with the teams involved educates them about adversary capabilities and attack techniques. Regular tabletops also establish communication channels and operational relationships needed for incident response events that could span multiple industrial sites across large geographic regions.

Practical Defense Actions – Tabletop exercises can identify gaps in such critical areas as threat detection, data source collection, log correlation, network segmentation changes, access control updates, security and safety process changes, and the communication of roles and responsibilities. Effectiveness in all these areas is key for a successful incident response. These gaps can be addressed to reduce overall response time, reduce impacts on the engineering process, and increase safety.

ICS INCIDENT RESPONSE JUMPPAGE

The objectives in industrial environments during a cyber incident is to maintain safety and operations. Use these tools for quick analysis and triage to understand the threat(s), operational impacts, and present options to facility owners to minimize loss and ensure safety. Store Jump Bag (ideally rolling protective cases) at critical sites or deploy them with the IR team as they conduct IR.

- Data acquisition tools (prioritize memory)
 - Laptops with Security Onion, REMnux, ShIFT
 - Sniffers
 - Hashes of field device logic/configuration files
 - Log, packet analysis, and timeline tools
 - Approved digital camera (no photo metadata)
 - Human machine interface (HMI) diagrams
 - Site physical safety training certificates
 - Network/convertor cables (USB → Serial)
 - Contact list for safety, engineering, integrators, security, emergency response teams
 - Out-of-band communications, handheld radios on site
 - Forensically clean USBs, external drives
 - CD-ROM drives and discs
 - Personal protective equipment (PPE) for safety
 - Mobile analysis tools (static, automated)

INDUSTRIAL IR TABLETOPS KICK-START GUIDE

Validate Incident Response Readiness

- Identify detection gaps
- Improved understanding of operations
- Training

Awareness – ICS Attacks Adversary Capabilities

- Communicate & designate roles and responsibilities for ICS security
- Educate Other Teams
- Building cross-team relationships for incident response
- Focus sessions with several teams – Convergence

Improved Detection & Safety

- Identify detection gaps
- Improved understanding of operations
- Training

ICS INCIDENT RESPONSE MUST-HAVES

- ICS-Specific Incident Response Plan**
- ICS-Specific Network Security Monitoring**
- Trained ICS-Specific Security Defenders**
- ICS INCIDENT RESPONSE IN PRACTICE**

Successful ICS incident response requires a clear understanding of roles, responsibilities, physical safety, the engineering protocols and process, network visibility, detection, and forensics capabilities. Facilities benefit when having a tested safe defensible cyber position. Consider adapting traditional IR steps to suit industrial control environments:

- Acquire forensics data from key ICS assets
- Quickly triage to understand the threat via static or automated malware analysis
- Establish a containment plan
- Contain threats while running operations
- Eradicate the threat if safe for operations
- Analyze the impact of any reliance on external vendors and IT
- Apply the appropriate ICS incident response plan
- Regularly conduct ICS incident response tabletop exercises
- Examine the connectivity and isolation of legacy devices
- Determine operational impacts
- Develop a communication plan
- Use indicator “hits” to scope infection
- Compare production and baseline config to detect tampering in controllers etc.
- Present analysis and options (blocking C2 access, running ICS in manual mode, removing remote access, etc.) to management
- Identify and agree lessons learned (e.g., detect gaps in defense measures, deploy additional ICS network visibility, detection capabilities, determine whether threats are malware or human adversaries).

Source - <https://www.sans.org/posters/industrial-control-system-cyber-incident-response/>

SANS DFIR

APAC DFIR

SUMMIT & TRAINING

デジタルフォレンジック&インシデントレスポンス

SANS ICS Security Community Resources

Free SANS Community Resources

- SANS ICS Field Manual
- SANS ICS Youtube – Concepts Series, Summit Recordings and many more resources
- SANS Posters –Active Defense Poster, Site Visit, Job Poster and Many More
- SANS ICS Community Forum – ics.sans.org



A thumbnail image of the SANS ICS Site Visit Plan v0.1. It features the SANS ICS logo and the title "ICS Site Visit Plan v0.1" in a blue header area.

A chart titled "Job Role to Competency Level Recommendation". It shows a mapping between job roles and competency levels. The job roles include "Technical Leader", "Expert Knowledge", "Mastery Knowledge", "Essential Knowledge (Foundational)", "Base Knowledge (Awareness)", "Engineering", "Operations", "Programmer", "Management", and "Support Staff". The competency levels range from "LEVEL 1" to "LEVEL 4". A legend indicates that yellow figures represent "USE" and red figures represent "DESIGN".

A large poster titled "Industrial Control System Cyber Incident Response". It contains several sections of text and diagrams. At the top left is a pie chart showing "Safety" (yellow), "Cyber Security" (orange), "Health" (red), and "Safety & Security" (green). Below the chart is a section titled "UNIQUE CONSIDERATIONS FOR ICS INCIDENT RESPONSE". Other sections include "DIFFERENCES BETWEEN SECURITY AND ICS SECURITY", "CRITICAL ICS ASSETS", "ICS SITE CYBER POSITION", "INDUSTRIAL INCIDENT RESPONSE - GETTING STARTED", "INDUSTRIAL CYBER INCIDENT RESPONSE TRIAGE", "ICS INCIDENT RESPONSE ROLES", and "Job-Level Descriptions". The poster also includes a "Job Role to Competency Level Recommendation" chart and a "Job Role Groupings" section.

SANS DFIR

APAC DFIR

SUMMIT & TRAINING

デジタルフォレンジック&インシデントレスポンス

Summary

Summary

- The Five ICS Cyber Security Critical Controls
 - Read the [White Paper](#)
 - Watch the [Webinar Recording](#)
- Control #1 – ICS Specific Incident Response Plan
 - Determine your scenarios and prioritise
 - Run the [5 SANS ICS Table tops](#)
 - Practice, Practice, Practice
- SANS ICS515 Resources
 - Apply the Active Cyber Defense Cycle (ACDC)
 - Know your Cyber Safe Position – practice it
 - Review the Incident Response Poster
- SANS ICS Community Resources
 - Read the [ICS Field Manual](#)
 - Watch the [SANS ICS Youtube Channel](#)
 - Review the [SANS ICS Posters](#)

Thank you! Questions?



<https://linkedin.com/in/blargeau>



<https://github.com/beLarge>



@beLarge