612.4

ICS System Management

SANS | GIAC CERTIFICATIONS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

All reference links are operational in the browser-based delivery of the electronic workbook.

ICS612.4 | ICS Cybersecurity In-Depth

SANS

ICS System Management

SANS ICS612: This course is focused on the implementation and support of a secure control system environment through a hands-on, in-depth course that is designed to change how students engineer and support ICS environments.

Jeffrey Shearer
Mr. Shearer is a member of the SANS Institute ICS team focused on developing courseware in support of the ICS curriculum. Jeffrey also acted as a Subject Matter Expert (SME) for the Global Industrial Cyber Security Professional (GICSP) certification and is a content contributor for ICS NetWars. He also participates as an advisory board member for the ICS Security Summit and Training events.

Prior to joining SANS Institute, Mr. Shearer worked at Rockwell Automation for 23 years, where his most recent role was a Senior Security Architect for Rockwell Automation's Commercial Engineering group focused on network and security designs for Industrial Automation Control Systems (IACS) and Industrial Demilitarized Zones (IDMZ). Mr. Shearer was a contributing member of the Rockwell Automation and Cisco Systems Converged Plantwide Ethernet (CPwE) team, where he participated in architecture design and validation efforts. He also co-authored publications such as *Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture*, *Site-to-Site VPN to a Converged Plantwide Ethernet Architecture*, and *Securely Traversing IACS Data across the Industrial Demilitarized Zone*.

Jason Dely
Jason Dely is responsible for leading the critical infrastructure and industrial control systems (ICS) security practice for Cylance. Prior to joining Cylance, Jason held many roles at Rockwell Automation, where he assisted clients with their research, design, integration, testing, and response activities across a variety of application, security, and infrastructure initiatives. During this time, Jason gained in-depth ICS product, protocol, and operational experiences that are invaluable when it comes to evaluating and building defenses within critical infrastructure organizations. His security passion over the past 18 years of experience with ICS is founded upon balancing business requirements against people, process, and technologies unique to each organization to ensure their operations are safe, reliable, and secure.

Tim Conway

Tim Conway is currently the Technical Director – ICS and SCADA programs at SANS, and is responsible for developing, reviewing, and implementing technical components of the SANS ICS and SCADA product offerings. Additionally, he performs contract and consulting work in the areas of ICS cybersecurity with a focus on energy environments. Recognizing the need for ICS-focused cybersecurity training throughout critical infrastructure environments and an increased need for hands-on training, Tim assisted in authoring, and instructs, the ICS curriculum's newest courses and ICS NetWars challenges. Outside of SANS, Tim continues to work on projects that blend cybersecurity, operations technology, and critical infrastructure protection with a focus on the energy sector.

Chris Robinson

Chris Robinson graduated from the United States Naval Academy with a B.S. in Computer Science and served over 6 years in the United States Navy. He then began his IT security career as a consultant for Booz Allen Hamilton before he attended graduate school full time at San Diego State University, earning an M.S. in Computer Science. Following graduation, Chris worked as Computer Scientist for the Navy and was an Adjunct Professor at San Diego's Mesa Community College. Chris then transitioned into ICS security, where he is currently an ICS Principal Consultant at Cylance, applying his expertise to various ICS cybersecurity projects to ensure solutions meet the needs of a modern industrial control system. Chris has learned firsthand the unique requirements and operational constraints for securing ICS environments. Chris currently holds and maintains multiple certifications, including the CISSP, OSCP, GICSP, GISP, GISF, and CEH. Chris teaches both the SANS MGT414 and MGT415 courses and currently resides in London, UK.

Contributor

Ted Gutierrez

Ted Gutierrez, CISSP, GICSP, and GCIH, is the ICS & NERC CIP Product Manager at the SANS Institute. Mr. Gutierrez was most recently the Director of Operations Technology & NERC Compliance at Northern Indiana Public Service Company (NIPSCO), where he was responsible for compliance to NERC 693 and CIP Standards and the support of the related operations technology systems. Mr. Gutierrez has more than 25 years of experience working in the electric utility, information technology, and manufacturing industries.

ICS612 Course Outline

- Section 1: The Local Process
- Section 2: System of Systems
- Section 3: ICS Network Infrastructure
- Section 4: ICS System Management
- Section 5: Covfefe Down!

This page intentionally left blank.

ICS612 Section 4 Outline (1)

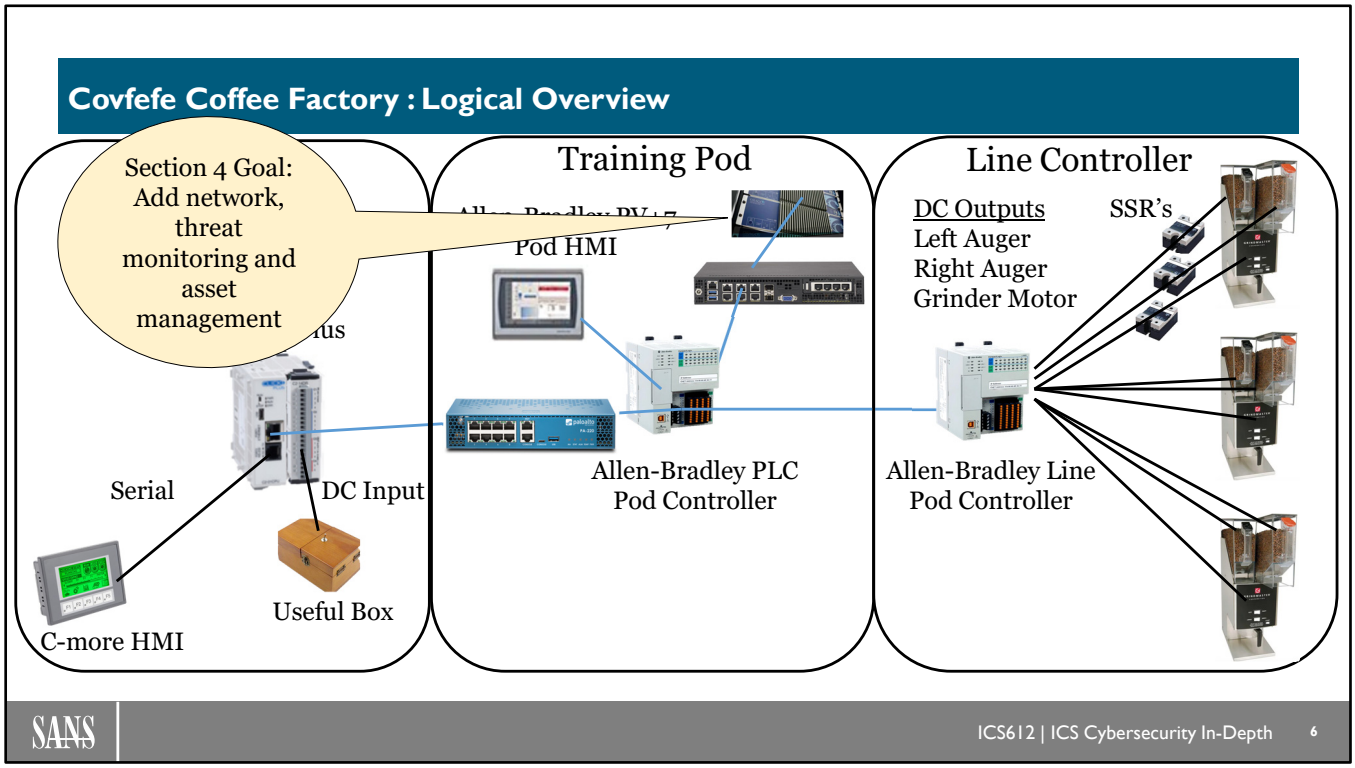
- ICS Security Monitoring
- Lab 4.1: Local Monitoring
- Lab 4.2: Process Environment Monitoring
- ICS Logging and Alerting
- Lab 4.3: Monitoring Tool Integration in ICS
- ICS Asset Management
- Lab 4.4: ICS Asset Inventory and Management
- Importance of Time
- Lab 4.5: Kiss of Death (KoD) Attack
- Asset Validation and Restoration
- Lab 4.6: ICS Device Backup
- Lab 4.7: ICS Device Restoration

This page intentionally left blank.

ICS612 Section 4 Outline (2)

- ICS Security Monitoring
- Lab 4.1: Local Monitoring
- Lab 4.2: Process Environment Monitoring
- ICS Logging and Alerting
- Lab 4.3: Monitoring Tool Integration in ICS
- ICS Asset Management
- Lab 4.4: ICS Asset Inventory and Management
- Importance of Time
- Lab 4.5: Kiss of Death (KoD) Attack
- Asset Validation and Restoration
- Lab 4.6: ICS Device Backup
- Lab 4.7: ICS Device Restoration

This page intentionally left blank.



As we look at Levels 0 and 1 hands-on exercises, we will use two systems to achieve the PLC and HMI learning objectives. In the middle of the slide, you will see the training Pod hardware that consists of an Allen-Bradley PanelView HMI and the Allen-Bradley (A-B) CompactLogix PLC. The training Pod also contains push buttons, indicator lights and remote breakers that the A-B PLC will use for input and output control.

The student kit as shown on the left contains the Click Plus PLC and the C-more HMI that will be used during student labs. The Click Plus PLC will communicate with the A-B PLC via Modbus TCP sharing data register information and I/O status. The student kit also contains a Useless Box that will be transformed into a Useful Box that will be controlled by the Click Plus PLC in order to show you how "useful" a simple input switch, motor circuit, and power source can be to gain knowledge about PLC systems. The student kit also contains a K-type thermocouple to demonstrate analog input capabilities of the Click Plus PLC.

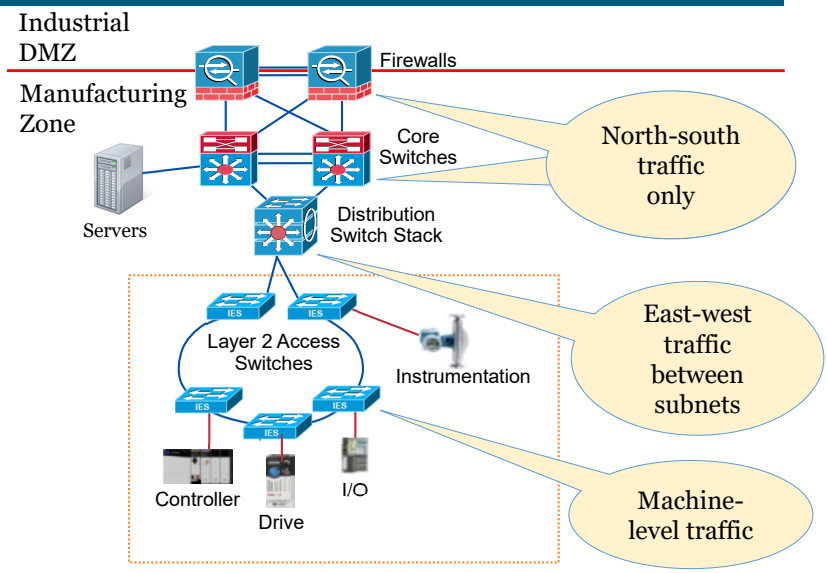
ICS Security Monitoring

Device Placement
Collection
Visualization

This page intentionally left blank.

Network Sensor Placement

- Passive is preferred
- Considerations
  - CPU usage
  - Packet rate (minimal)
  - Network bandwidth
- Proper placement determines anticipated captured traffic in and out of target devices
- Use local capture and store devices for air-gapped, bandwidth, or latency constrained systems



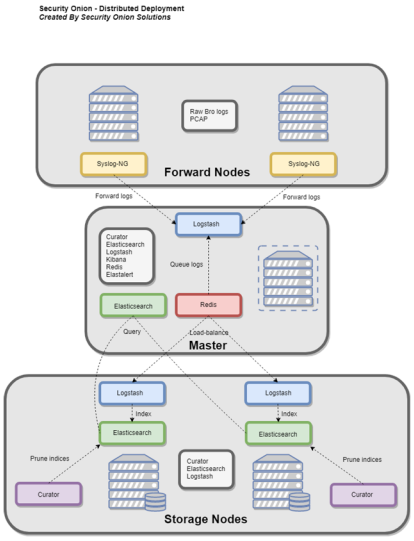
Network sensors are placed strategically in the network to capture traffic for future analysis and to alert an interested party that some unusual pattern or type of traffic is occurring. Network sensors can help gain an understanding of network traffic and it is especially important to place the sensors lower in the network in order to gain visibility to control system traffic.

In ICS environments it is not common to place a sensor in line with the traffic with the intention of actively dropping traffic much like a firewall. Typically network sensors are wired to a switch or router port that is mirroring the port(s) of interest in a passive mode.

Considerations for sensor capabilities are packet processing rates, network bandwidth, and CPU capabilities. Ultimately you want the sensor to be able to process all the traffic.

Sample Open-Source NSM Solution

- Free and open-source NSM solution
  - Will need to fund people to implement it
- Targeted at monitoring IT networks
- Fully capable platform – Security Onion
  - Snort, Bro, Wazuh, Elastic Stack, etc.
- Can be used for ICS networks
  - Out-of-box has no ICS-specific configurations
  - Allows exact fit to organization
- Sensors can run on any PC platform
- Extremely flexible



Open-source solutions do exist for NSM, and the most common one out there is Security Onion. This all-in-one solution is extremely flexible, making it very usable within an ICS environment. Because of this it makes a great entry platform for an organization starting to build out an ICS-specific NSM solution. However, the scalability of Security Onion does make it a contender as a long-term solution.

Image Source:

- https://raw.githubusercontent.com/Security-Onion-Solutions/securityonion-docs/master/images/elastic-architecture/distributed.png

Lab 4.1: Local Monitoring

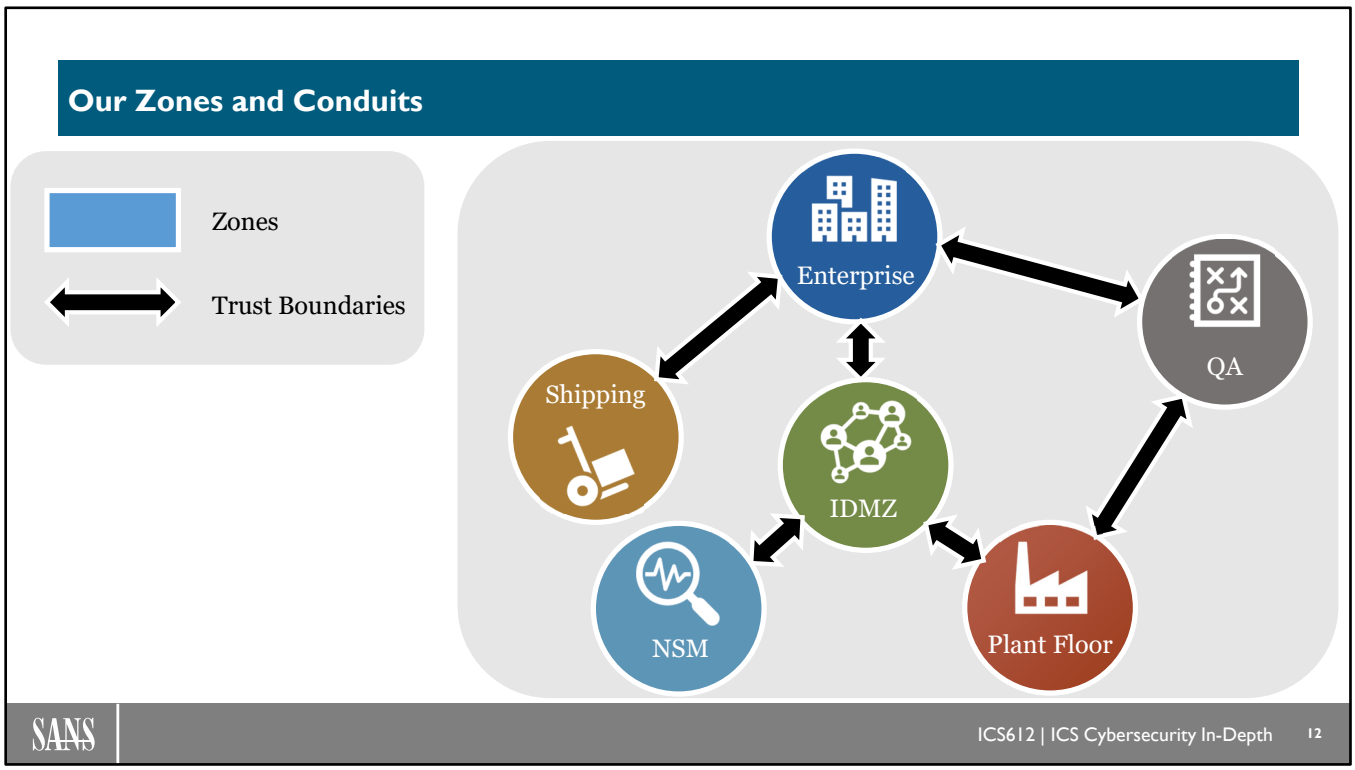
Go to the Lab Workbook: Lab 4.1

This page intentionally left blank.

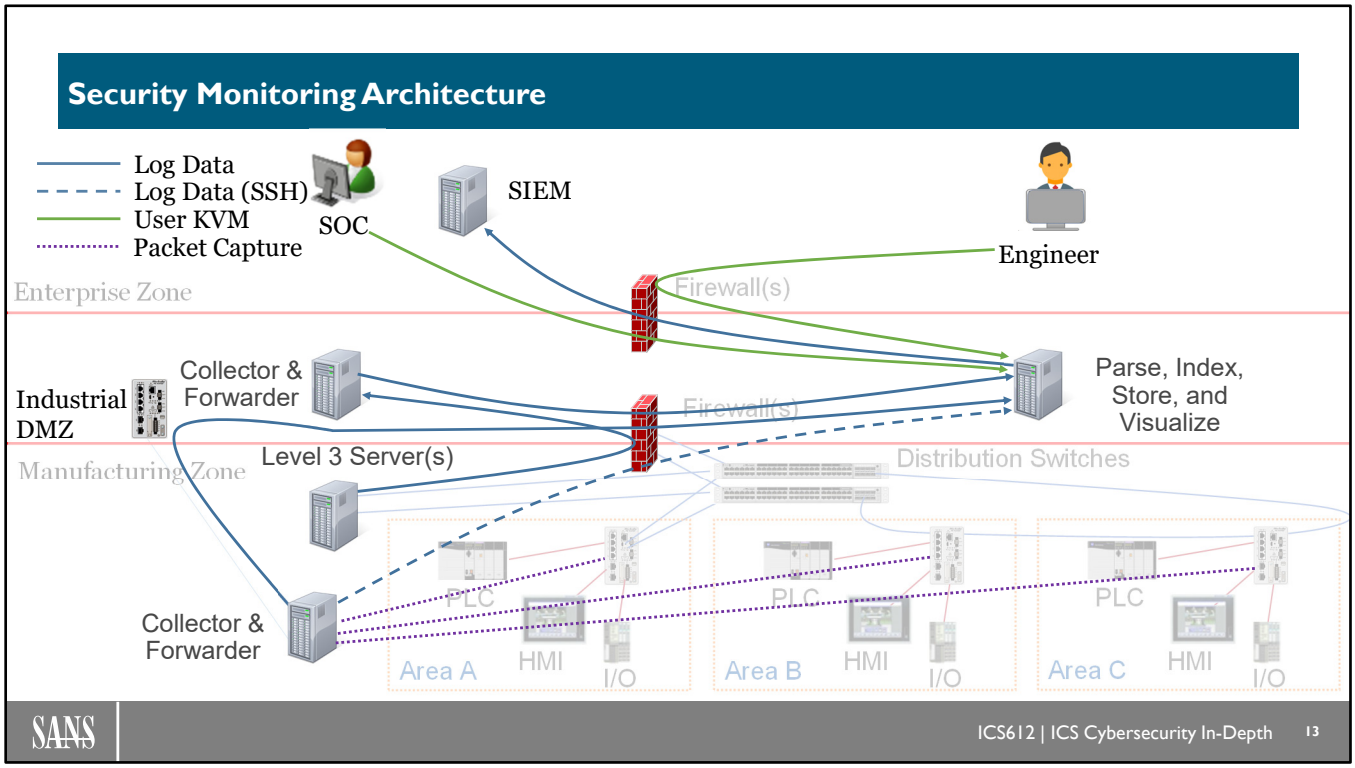
ICS Security Monitoring Checkpoint 4.1

- Network monitoring is crucial for creating a baseline of expected network traffic
- Sensor placement for control traffic will require sensors located near the controllers to catch unusual patterns or types of traffic
- Using automated network monitoring tools to find ICS assets can be problematic as some assets may be powered off during the scan while others may not be accessible from the scanning device's network
- Manual inspection of a facility, including opening up control cabinets to find all the network switches, is required if you really want an accurate inventory of networking equipment

This page intentionally left blank.



As we refer back to the model of our security zones and communication conduits, observe that we have placed the Network Security Monitor (NSM) device(s) within their own security zone. The desire is to have a separate network segment that will manage the configuration and data retrieval from the network sensors. We need to secure and limit the access to the monitoring system as any adversary activity to cover their tracks would include tampering with the NSM sensors and logs.



The security monitoring architecture is heavily dependent on the capabilities of the security monitoring solution selected as well as the network complexity and challenges unique to the ICS environment being monitored. This diagram depicts, in concept, specific ICS-related best practices.

The Level 3 servers, laptops, and capable Level 2 devices should forward logs to an isolated collector and forwarder. If possible, though unlikely without using a third-party agent, this traffic should be encrypted. For large and heavily segmented environments, placing multiple collectors and forwarders may make more sense. Some level of parsing capabilities, especially for packet capturing, should be considered for the remote collectors and forwarders to reduce storage and bandwidth requirements. Due to network constraints such as remote pump stations, remote collectors with local storage and no forwarding capabilities may make the most sense; however, a procedure to manually collect and forward these logs will need to be followed.

Since the log collectors and forwarders (also known as sensors) are far-reaching across the environment, they should operate in isolation and passively to reduce their abuse against the environment. This isolation could be over an out-of-band network for remote sensors, which may only be feasible for small geographical process facilities such a water treatment facility, refinery, or manufacturing plant. Otherwise, isolation of remote sensors could be in-band but forwarded through an encrypted tunnel.

The primary platform used to parse, index, store, and visualize should operate in an isolated network separate from the collectors and forwarders as well as the users and analysts that require access. Ideally there should be no network services, such as http, that are available for the users to access this system remotely. Extending the keyboard, video, and mouse (KVM) from this network to a secured control room should be the only method allowed.

Lab 4.2: Process Environment Monitoring

Go to the Lab Workbook: Lab 4.2

This page intentionally left blank.

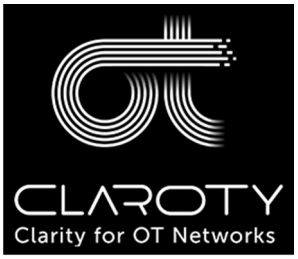
ICS Security Monitoring Checkpoint 4.2

- Expanding our network monitoring beyond the local networks, we see there are Systems of Systems, which is more representative of an industrial environment
- Sensor placement at routers and higher-level switches will catch the system-to-system communications. The data flow diagrams will show much more traffic flowing from the controller layers to the higher levels.
- Sensors at the higher levels will see larger streams of data while the lower-level sensors will see smaller, more rapid streams.

This page intentionally left blank.

Sample ICS-Ready Monitoring Solution

- Commercial solution
  - May need architecture/network changes
- Varying levels of NSM capabilities
- Incorporates ICS capabilities
  - May need some development for unique software or protocol
- Hardware sensor form factor is vendor specific
- Network and host visibility are vendor specific
- Somewhat flexible



There has been an emergence of network monitoring solutions due to the explosive adoption of Ethernet-based and heavily networked control systems. Because control system products have a heavy reliance on Ethernet networks, they can be considered a reasonable option for customers looking to support their security programs. Network monitoring solutions can alert a customer that unexpected network traffic is occurring, also giving the customer the ability to capture and analyze the unusual traffic.

Image Sources:
- https://www.nozominetworks.com
- https://www.indegy.com
- https://www.claroty.com
- https://dragos.com/

ICS612 Section 4 Outline (3)

- ICS Security Monitoring
- Lab 4.1: Local Monitoring
- Lab 4.2: Process Environment Monitoring
- ICS Logging and Alerting
- Lab 4.3: Monitoring Tool Integration in ICS
- ICS Asset Management
- Lab 4.4: ICS Asset Inventory and Management
- Importance of Time
- Lab 4.5: Kiss of Death (KoD) Attack
- Asset Validation and Restoration
- Lab 4.6: ICS Device Backup
- Lab 4.7: ICS Device Restoration

This page intentionally left blank.

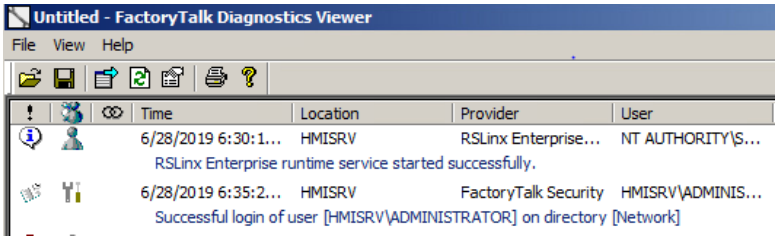
ICS Logging and Alerting

Device Configuration
Network Architecture
What to Log
What to Alert

This page intentionally left blank.

Examples of Log Sources

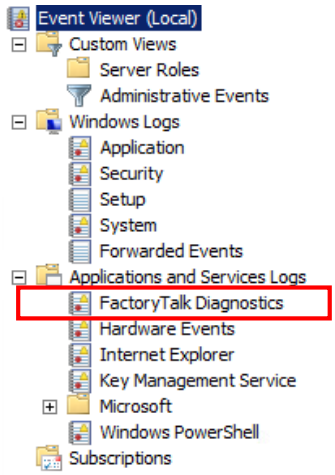
- Routers/Switches/Firewalls
- Servers/Workstations
- Active Directory
- Security Tools
  - Anti-malware solutions
  - IDS/IPS
- Applications
  - OPC
  - DCS/SCADA
  - Alarms



There can be many devices that are capable of participating in logging efforts, including routers, switches, and firewalls. The challenge is correlating events as they are logged, especially if the time source between these devices are not shared. It should be noted that most routers, switches, firewalls, and Windows servers use Network Time Protocol (NTP). It is important to coordinate the time of all the infrastructure nodes to sync to the same NTP source.

Examples of Log Types

- Windows
  - Application
  - Security
  - System
  - Applications and Services Logs
- Linux
  - /var/log/messages
  - /var/log/auth.log
  - /var/log/cron.log
  - /var/log/kern.log

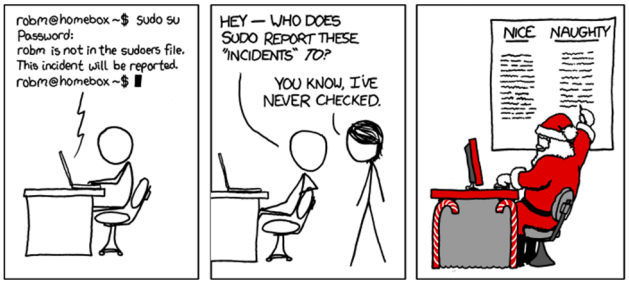


The logs types listed are examples of some very common and well-known logs, but this is by no means an exhaustive list.

As the image shows, applications will usually create their own logs. The quality and format of these logs will vary widely.

Log Aggregation

- Syslog
- Windows Event Forwarding
- WMI
- Agent-based Forwarders



As we have seen, the systems and applications used throughout the processing environment produce a wide variety of logs. Reviewing those logs and correlating events between various log sources can be difficult if the logs are scattered throughout the environment and not in a central location.

Log Aggregation collects logs from the various log sources and stores them in a central location. With all the logs in a central location, Security Information and Event Management (SIEM) products can correlate events from different sources, produce alerts on certain events, display informational charts to visualize activity within the environment, produce reports for compliance purposes, aid in forensics, etc.

There are many ways to aggregate logs to a central location, including:

- Configuring systems to send syslog messages to a syslog server
- Using Windows Event Forwarding (WEF) to forward events to a Windows Event Collector (WEC) server
- Using Windows Management Instrumentation (WMI) to connect to a remote Windows system and pull the logs
- Agent-based Forwarders that are installed on a system and forward logs

Another benefit of having logs collected in a central location is it makes it harder for an attacker to cover their tracks by clearing logs on a compromised system. Of course, this means that the central location (e.g. log server) must be well protected.

Image Source:
- https://imgs.xkcd.com/comics/incident.png

Syslog

- Syslog is a standard for message logging
- Allows separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them
- Each message is labeled with a facility code, indicating the software type generating the message, and assigned a severity level
- Severity levels range from 0 (Emergency) to 7 (Debug)
- Syslog uses UDP Port 514
- Syslog over TLS uses TCP Port 6514

Syslog is a very popular and widely used standard for message logging. It allows separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Each message is labeled with a facility code and assigned a severity level.

A facility code is used to specify the type of program that is logging the message. Messages with different facilities may be handled differently.

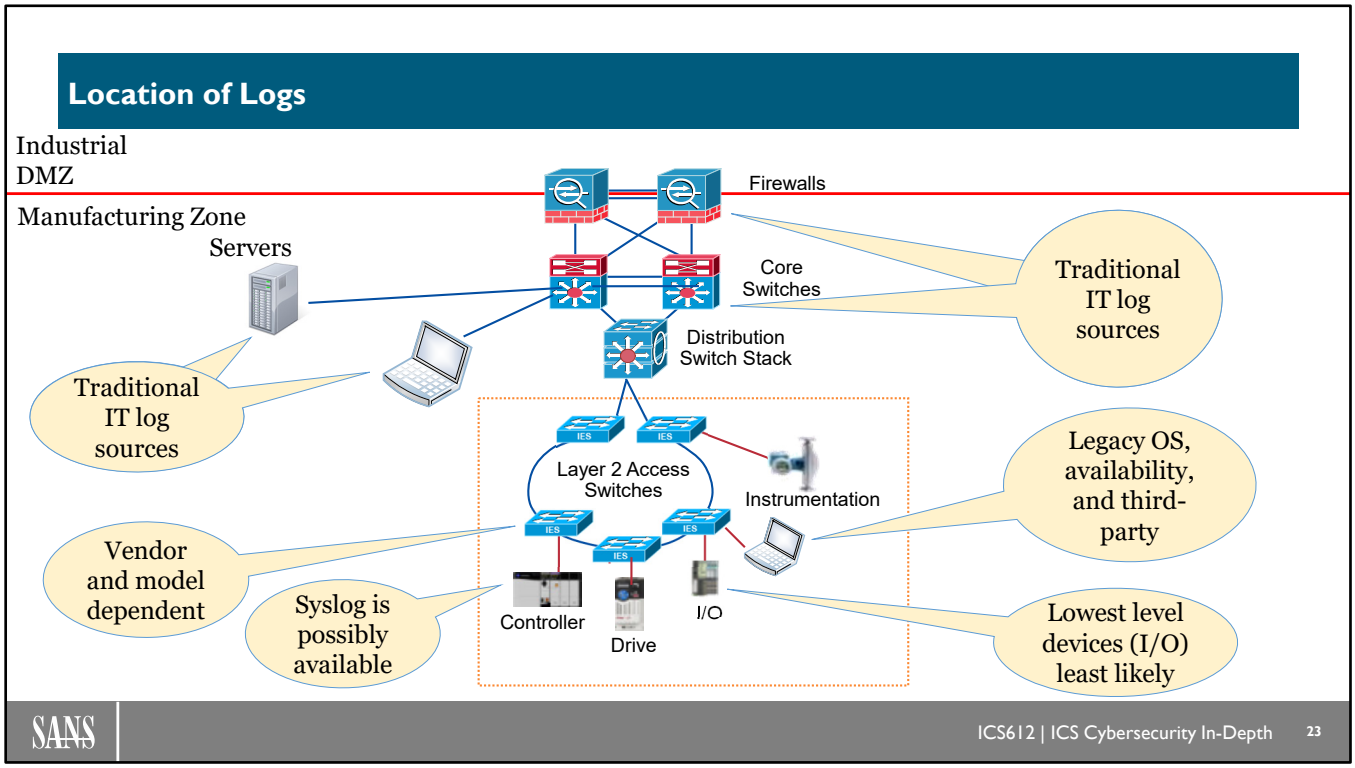
The list of severities is defined by the standard.

Value	Severity	Keyword	Description
0	Emergency	emerg	System is unusable
1	Alert	alert	Action must be taken immediately
2	Critical	crit	Critical conditions
3	Error	err	Error conditions
4	Warning	warning	Warning conditions
5	Notice	notice	Normal but significant conditions
6	Informational	info	Informational messages
7	Debug	debug	Debug-level messages

While the syslog standard defines the facility codes, severity levels, and the message component, the content of the message is not defined so the content will be dependent upon the application, etc. that is creating syslog messages.

When operating over a network, syslog uses a client-server architecture where the server listens for messages from clients. Syslog uses UDP Port 514 and syslog over TLS uses TCP Port 6514.

Reference:
- https://en.wikipedia.org/wiki/Syslog



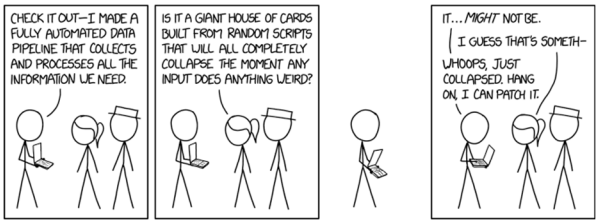
Understanding where logs reside in the environment and whether those logs can be collected based on their location is nontrivial. From the Purdue Model, most Level 3 and some Level 2 logs should be easier to identify and collect since they are based on more traditional IT technologies.

Both computers and embedded devices (e.g., PLC) lower in the control systems will be more challenging. There are likely laptops and other traditional computing assets operating at these lower levels, however the following challenges with many of these assets should be anticipated:

- They operate with legacy operating systems (e.g., Windows 95)
- They are not continuously available on the network (i.e., stored on a shelf in maintenance office)
  - Limited collection software updates and configurations
  - Limited log collection
- They are used in various ways to connect to the device (e.g., directly to the devices on serial or over local Ethernet)
- They are owned and operated by a third-party contractor

Log collection and aggregation should start with the traditional log sources within the higher-level systems before tackling the lower-level systems. In a properly architected network, the initial attack paths will include the higher-level systems and traditional IT assets.

Logging Considerations (1)



- Bandwidth and Latency
  - Remote Telemetry
  - Legacy Communications
- CPU and Memory Limitations
  - Embedded Devices
- Poor Logging Implementations
- Variations of Log Information/Format

When vendors create products to solve operational problems, logging is not usually a priority. Logging quality at its foundation is controlled by the device's ability to detect and record an event. This requires the implementer to consider not only the operational use of the OT or IT device but also its ability to support situational reporting like logging.

As we deal with control system devices like PLCs, I/O, and instrumentation the ability to store log data onboard becomes finite. Most embedded devices are designed to support storage for the operating system, operational code, configurations, log data, and some type of RAM for program variable creation. If event history is important, then it becomes important to design the logging infrastructure to support a highly available network for those devices considered to be critical for alarm and event forensics.

One other point: Not all lower-level devices should be required to participate in the logging campaign because of their limited event capabilities and their limited CPU processing capabilities. These simpler devices may only contain messages about configuration or running error codes that would not be troubleshot from a higher-level log but rather from the disparate control system log, the engineering workstation, or perhaps a hand-held instrument calibration device.

Image Source:
- https://imgs.xkcd.com/comics/data_pipeline.png

Logging Considerations (2)

- Log all the things?
  - Probably not
- Forward all the logs to the Enterprise SOC?
  - Probably not
- Maximum log size
  - Overwrite events
  - Archive log file
  - Do not overwrite events

Should you log all the things? Probably not, especially if you are just implementing logging. Logs can be very noisy with a lot of routine information that has no security implications. Trying to log everything will likely tax computing resources, especially for resource-constrained systems, and trying to forward all those logs can cause network congestion. Too much data, especially without proper analytics, will overwhelm security analysts. Also, many commercial SIEMs are licensed by how much data they ingest within a certain time frame, so logging everything can get pricey very quickly.

Many companies do not want to build an additional Security Operations Center (SOC) dedicated for the processing environment. Instead, companies want to utilize the people, processes, and technologies they already have available in their Enterprise SOC. So should you forward all the logs from the processing environment to the Enterprise SOC? Probably not, at least not initially. Enterprise SOCs understand the IT environment really well, but the OT environment operates differently; some things that may look malicious in the IT environment are just normal operations in the OT environment. Security analysts will need to be trained on the OT environment; processes and playbooks will need to be updated to address the OT environment; and technologies will need to be tuned. Additionally, SIEM licensing could be impacted if too much additional data from the OT environment is ingested.

Some logs will be noisier than others and will reach their maximum size quicker. There are several options, each with its own pros/cons, that can be performed when this happens.

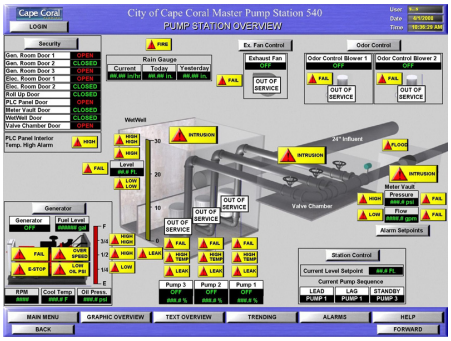
Overwrite events – When the maximum size is reached, the oldest events are overwritten with newer events. This means the newest events will always be available and a fixed amount of hard disk space will be used. For busy logs, this could mean that the logs contain a very short history of events.

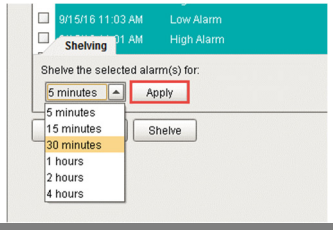
Archive log file – When the maximum size is reached, the log is archived, and a new log is created. This means a history of all the events is saved but this can eventually fill up the hard disk space on the system.

Do not overwrite events – When the maximum size is reached, the log stops storing new events. This means older events will always be available and a fixed amount of hard disk space will be used but newer events will be lost.

How to Alert in ICS

- Driven by corporate security but integrated with operations
- provide notification to operations for correlation with production activities
  - Careful to not overwhelm operations with alerts
  - Alert Shelving vs. Whitelisting
- Adopt principles of alarm management life cycle to drive standardization
  - Identify, document, and prioritize potential scenarios
  - Develop follow-up procedures





Critical industries such as energy, oil and gas, and chemical processing have found the need for efficient alarm reporting and management because an error in alarm interpretation and an incorrect response could lead to catastrophic outcomes. The major industry stakeholders came together to understand the technical capabilities of control systems; they also factored in the psyche of the operator and the possibilities of an operator being overwhelmed with too many alarm conditions. An overwhelmed operator leads to an unpredictable and non-repeatable response to the alarm conditions. This standard attempts to educate and inform the would-be alarm designer to implement a much more user-friendly alarm system. This standard highlights the alarm system as another system that needs thoughtful design rather than an afterthought of control system design.

References:

- ANSI/ISA-18.2-2016, *Management of Alarm Systems for the Process Industries*
- Image source: http://www.commercecontrols.com/images/graphic-overview-large.jpg
- Image source: https://docs.inductiveautomation.com/download/attachments/6046186/Shelving%2030%20Min%20Apply%20button.png?version=1&modificationDate=1475030480000&api=v2
- Ref: The Four Types of Threat Detection by Sergio Caltagirone and Robert M. Lee

Lab 4.3: Monitoring Tool Integration in ICS

Go to the Lab Workbook: Lab 4.3

This page intentionally left blank.

ICS Logging and Alerting Checkpoint 4.3

- System logging for forensics requires the devices' time sources are synchronized
- Standard NTP is not accurate enough to use on the control system layers; be aware that these time sources don't sync with NTP. Basically, don't assume it's NTP everywhere!
- Aggregation of logs can be difficult because of network architecture.
- Logging everything isn't a great strategy unless you have processing power, lots of storage, and some way to sort the relevant information
- Local control system specific event logs sometimes exist, so go hunting for them

This page intentionally left blank.

ICS612 Section 4 Outline (4)

- ICS Security Monitoring
- Lab 4.1: Local Monitoring
- Lab 4.2: Process Environment Monitoring
- ICS Logging and Alerting
- Lab 4.3: Monitoring Tool Integration in ICS
- ICS Asset Management
- Lab 4.4: ICS Asset Inventory and Management
- Importance of Time
- Lab 4.5: Kiss of Death (KoD) Attack
- Asset Validation and Restoration
- Lab 4.6: ICS Device Backup
- Lab 4.7: ICS Device Restoration

This page intentionally left blank.

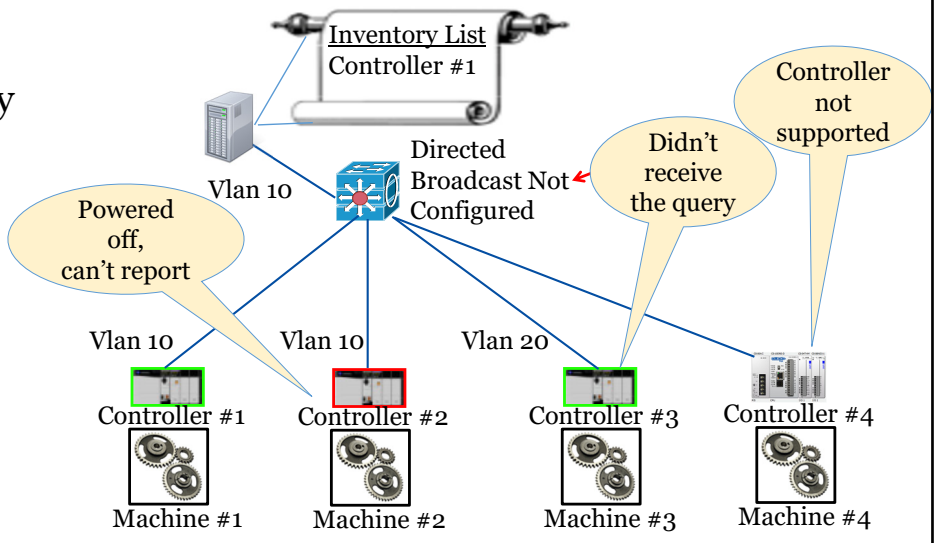
ICS Asset Inventory and Management

Inventory of ICS Devices
Change Management for Process Environments
Patching in Process Environments

This page intentionally left blank.

Inventorying Challenges

- Offline assets won't show up in inventory list
- Network configuration block scanning tools
- One-time versus continuous
- Unsupported ICS protocol(s)



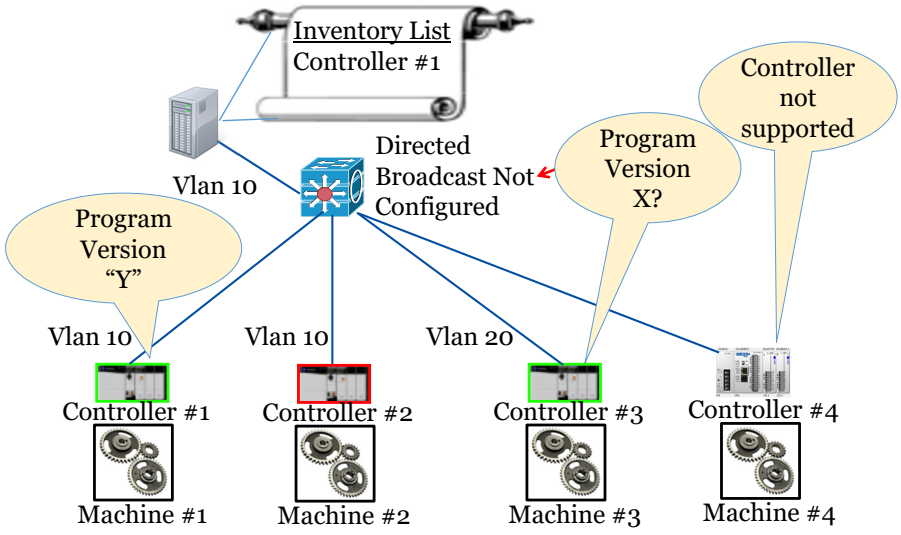
Collecting asset inventories can be challenging for a number of reasons. Some are:

- It's possible for machines to be powered off or broken when the inventory tool is running
- Network infrastructure is configured in such a manner as to not allow the scanning tool to cross VLANs or the assets are hidden behind a firewall
- The device may be spotted by a simple "ping", but the inventory asset software doesn't have a profile for the automation device in question

The idea of what data an inventory list should contain is quite varied. At a minimum the information should record the device type, hardware version, firmware or OS level, and any patch levels. This information will tell the interested party what features are supported and what the associated vulnerabilities are as reported by the vendor.

Inventorying Challenges – What about Configuration?

- Hardware versions are very important for knowing the supported features
- How can an asset be queried for program version?
- How can an asset be queried for changed critical data values?

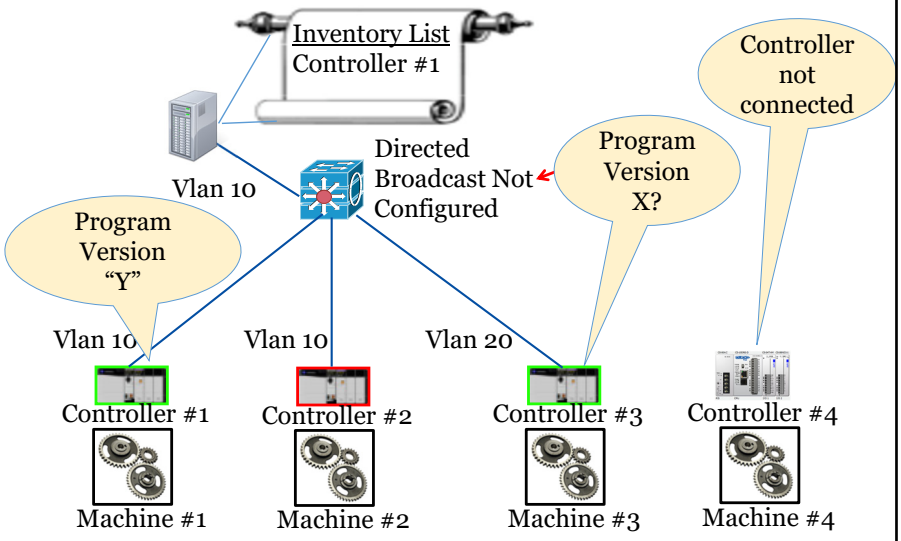


As mentioned before, when using automated inventory tools, they should report the hardware and firmware versions as this will dictate the available supported features. In order to interrogate the device, the inventory tool needs to support the ICS protocol supported by the device. Most ICS protocols will allow simple interrogation of the device to determine this level of information about the device.

A more integrated tool would be able to interrogate the asset to the level of comparing programs and critical data values as this will determine if the validated version of code and critical data has been loaded and is running in the controller.

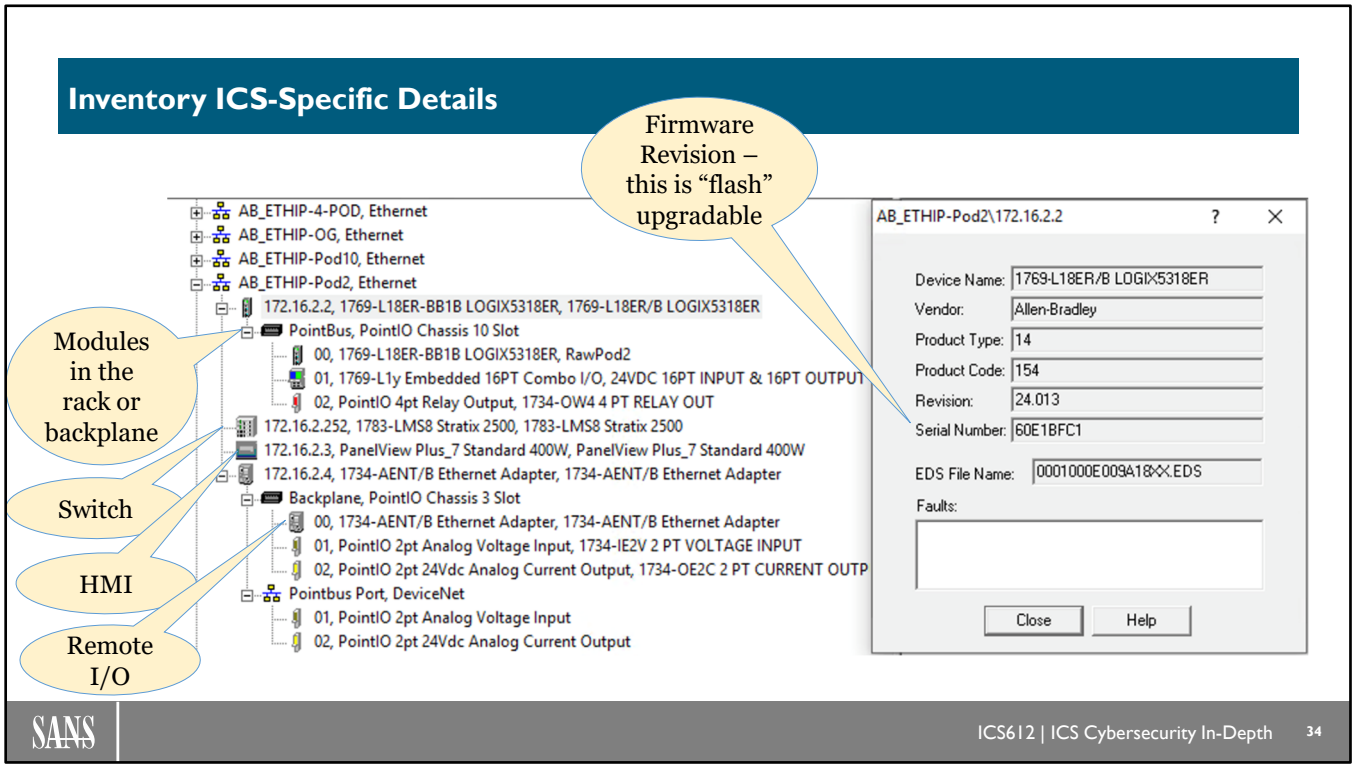
Inventorying Challenges – The Devices Are Not Connected to the Scanner's Network

- Non-networked or skid equipment
- Ancillary systems
- Third-party system
  - Power supply
  - Gas supply
  - Air or chemical supplier
- Shadow IT networks



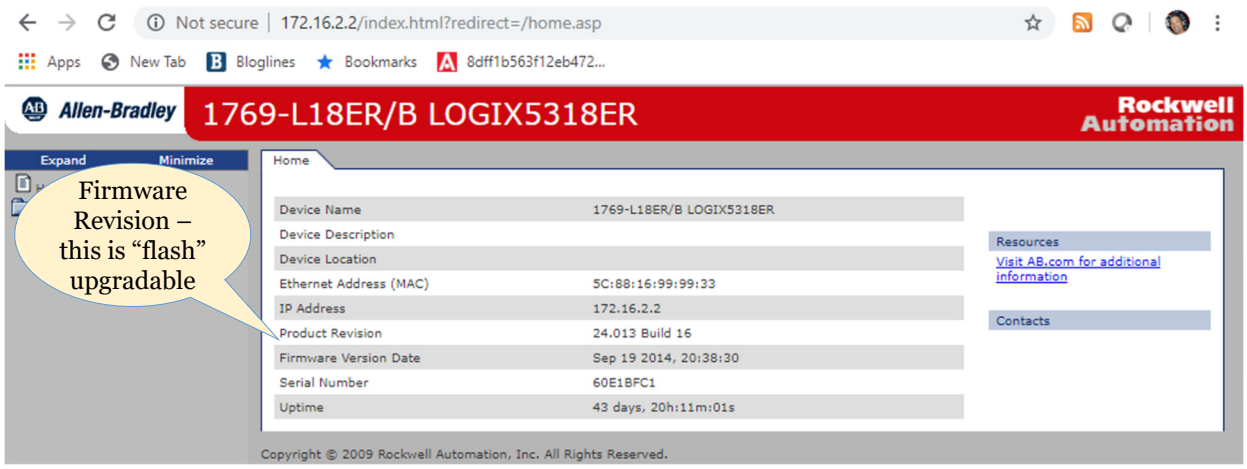
When doing automated inventory scanning it should be considered that the plant has installed non-networked skid(s) and the skid will not be seen by automated tools. It is also quite possible the plant personnel have run their own control network that is not connected to the main control network. We call this a "shadow IT network." Personnel who run these shadow networks often claim they do so because they don't want to rely on a "non-real-time" IT staff that may not be around in the middle of the night when equipment is down, and they need to get the equipment back up and running. If they feel their production targets are in jeopardy from slow responses of their network support team, they will find creative ways to put their destiny back in their own hands.

Another real-life lesson is the only way to get a true inventory is to put on your hard hat and steel-toed boots and go search for those assets that can't be reached by network scanning tools. This should include opening up control cabinets and visually inspecting shadow network assets and other control devices. Many network-type cabinets or closets will share IT assets and may contain many network devices which will become complex and confusing; be sure to document and justify everyone. Many unnecessary and/or forgotten devices and connections, including external ones, have been found while being thorough.



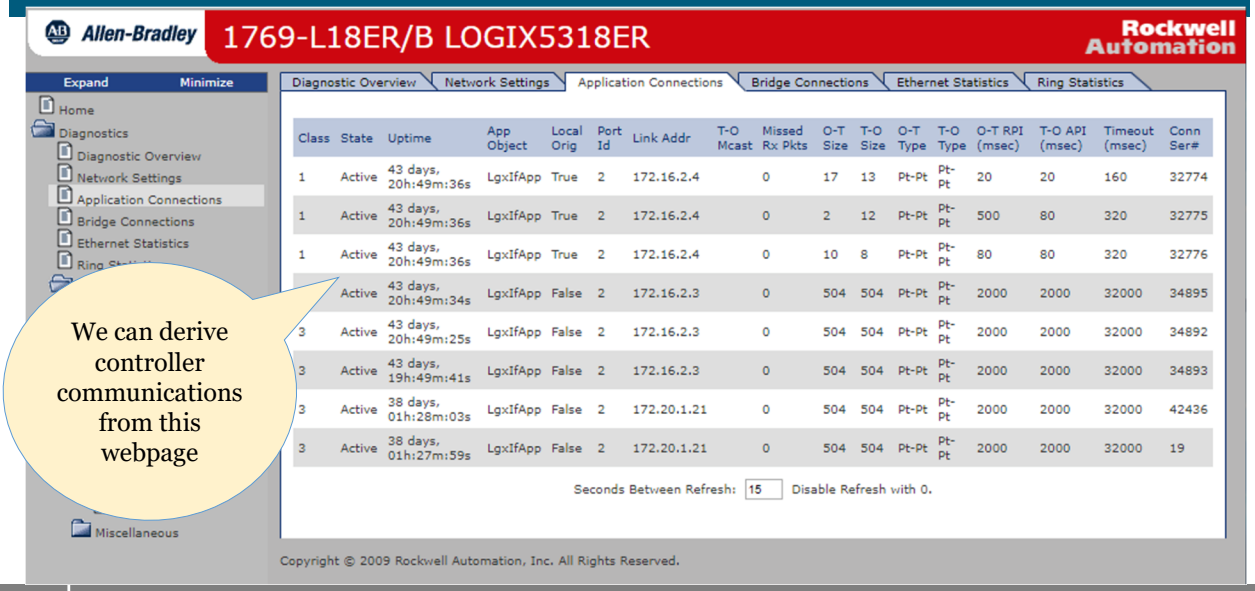
The data reported back to an inventory tool interrogation obviously depends on what a vendor decides to report back. Because a standard inventory tool vocabulary hasn't been established, some interpretation of the data being reported back to the tool may be required. For instance in the above scan, we see a "Revision" being reported back. What revision does this represent, a software revision, a firmware revision, or a hardware revision? In this particular case it represents a firmware revision that can be upgraded or even downgraded. The firmware revision will tell an educated interrogator what features, or vulnerabilities may exist when the controller is flashed to this level.

Inventory ICS-Specific Details through Webpage Interrogation



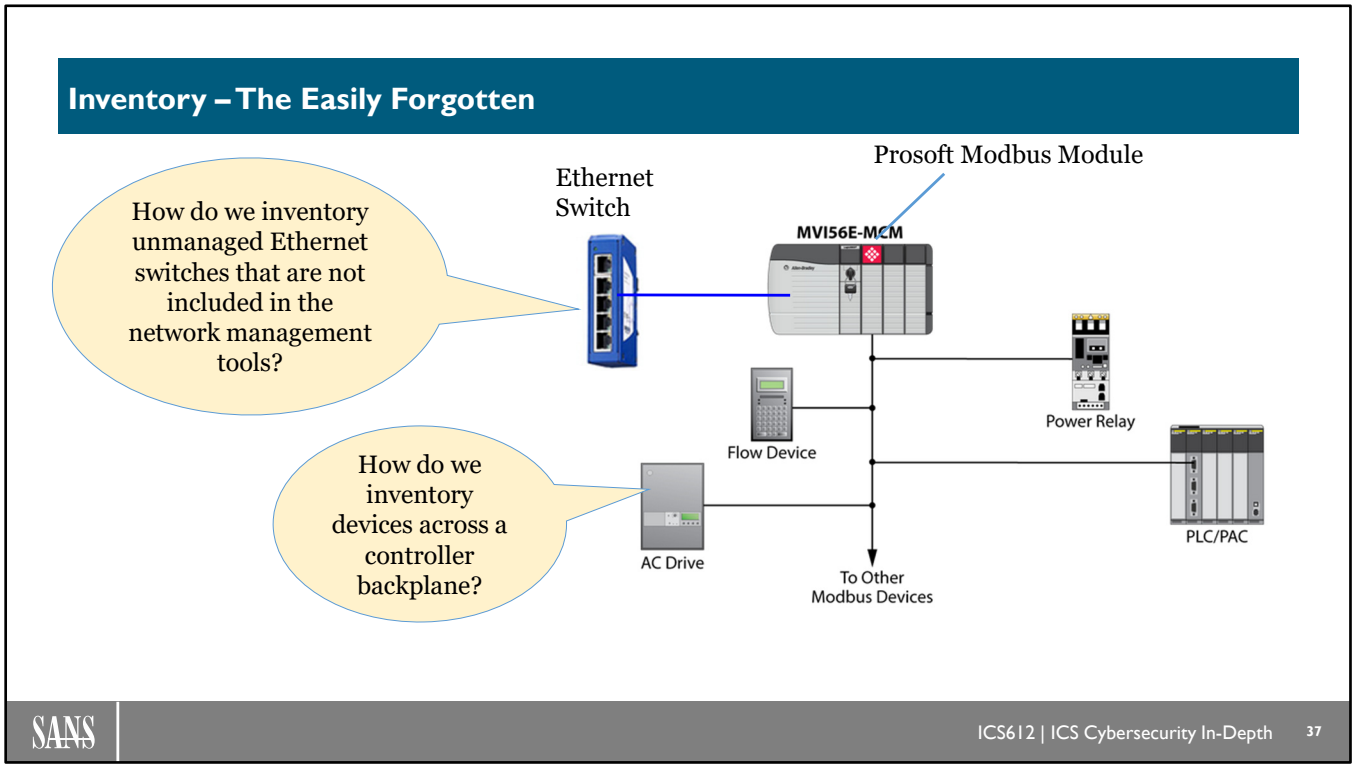
Most ICS devices that support Ethernet communications will also support an onboard management console such as an embedded web server. Many ICS devices will not have a software tool to show or extract the information, including the configuration file. We can enter the IP address into a browser window and obtain interesting information like the device type, MAC address, firmware revision, etc. Alternatively, some ICS-specific communication devices may use telnet or ftp as a method to communicate remotely. If remotely accessing the device isn't available, connecting directly to the device through a serial cable or physically reading the information off the product label may be the only option.

Inventory ICS-Specific Details – Controller Connection Details

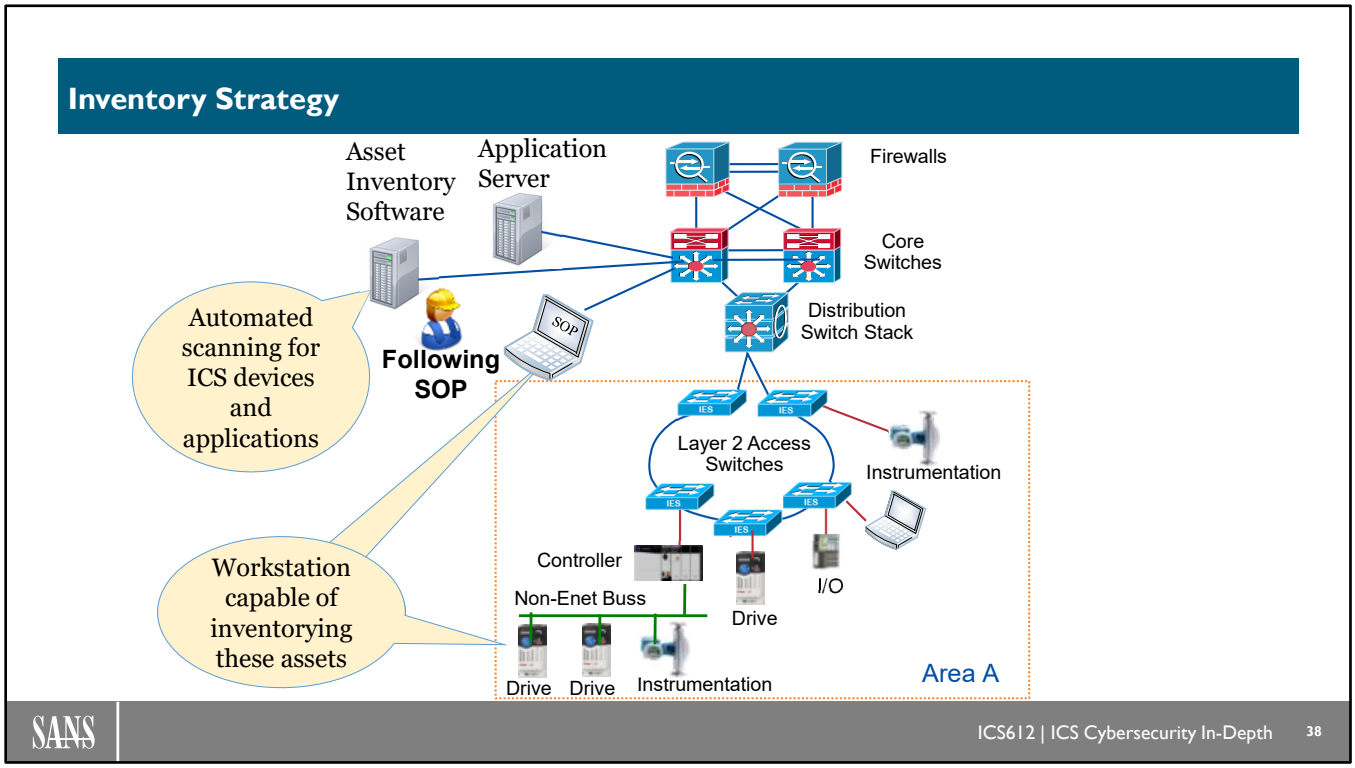


Some ICS devices offer visibility into the established connections routing tables and other interesting inventory information from their onboard management console. In our example above, we can see the open connections to and from the controller where "T" can be deciphered as "Targets" and "O" represents the controller that is the "Originator" of the communications. We can use this information to map a normal communication pattern and we can also use this to simply determine who the controller is currently communicating with at this snapshot in time.

Documenting the information available for every device on the onboard management console can be extremely useful for network security monitoring (NSM) or incident response.



When assets are hidden from the visibility of the inventory tool, these assets are oftentimes not included in the inventory list. Devices like unmanaged switches and assets that are not directly connected to Ethernet, which can be quite numerous, are an example of assets that may not end up on an automated asset tool scan. Successfully inventorying these types of assets will require coordination with people who are familiar with the different plant areas and who are also familiar with the various types of automation assets. Many times, these are a combination of engineering AND maintenance staff because maintenance staffs will have budgets to conduct automation projects that will not be coordinated with engineering.



Most manufacturing environments do not have everything network connected within the scope of the inventorying software's purview therefore you will need a combination of manual and automated inventory entries if you wish to see everything in a common view. For networks that are incapable of being scanned by the asset inventory software they can be verified through engineering design or configuration tools. An SOP should be created so the person conducting the inventory will know the assets and the type of information that should be collected.

We have focused our conversation on collecting data from the devices lower in the architecture because they may be foreign to traditional asset inventory software packages. However, it is still of paramount importance to gather the software inventory on each of the servers as well.

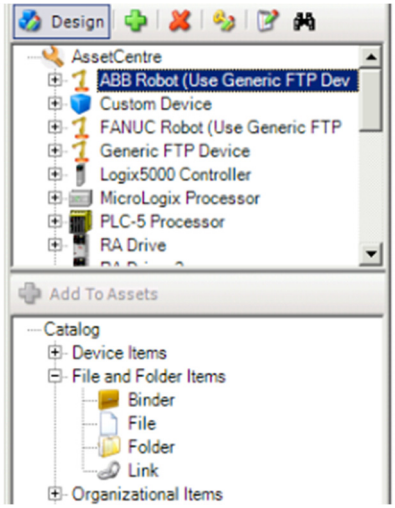
ICS Asset Management Checkpoint 4.4

- Asset interrogation requires the scanner to support the ICS protocol in order to get basic information beyond just a simple ping or NMAP scan
- If an asset is connected to a communication module in a PLC cabinet, then it's probable that asset discovery will not be successful because of the protocol encapsulation that must occur for the message to traverse a backplane
- To gain an entire asset inventory picture, you will end up aggregating data sources
- It is reasonable to put an SOP together in support of a manual procedure to capture device information

This page intentionally left blank.

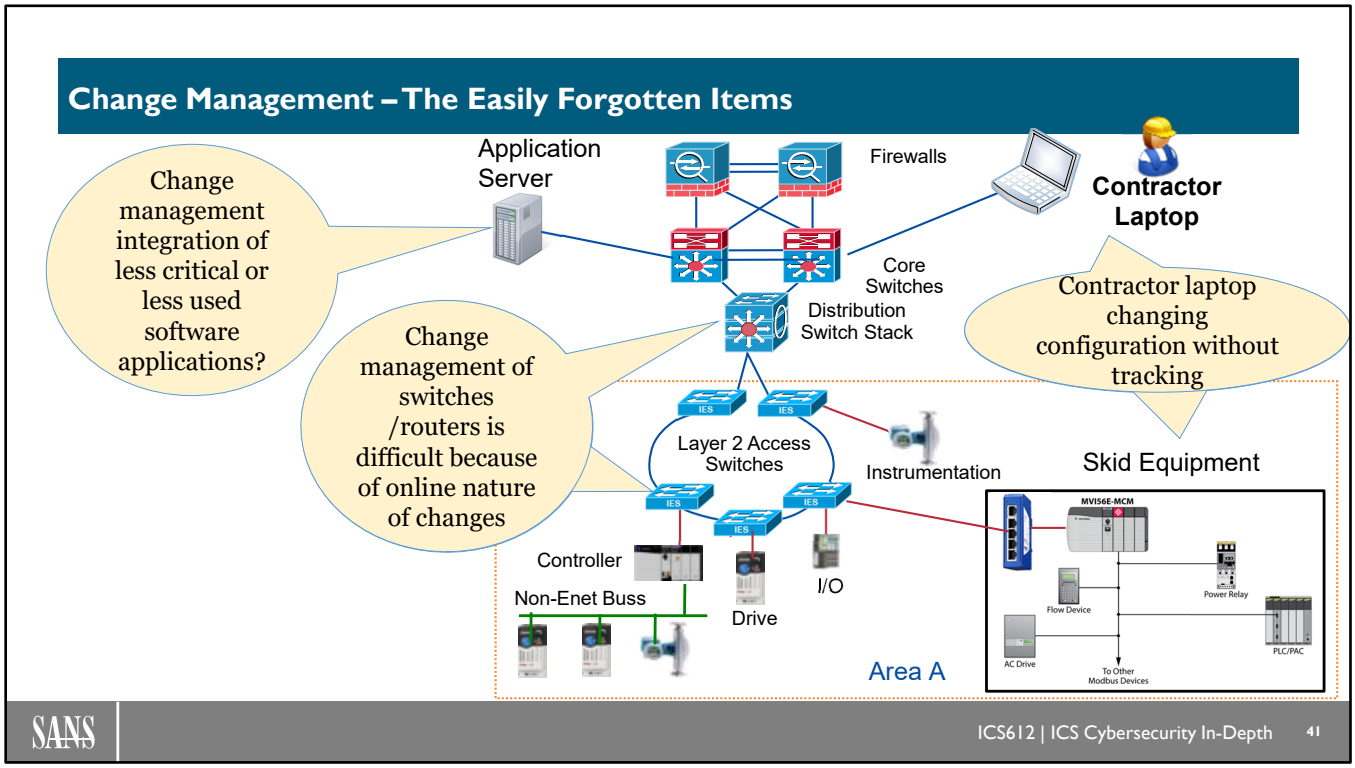
Change Management

- Ability to archive and compare "golden" copy
- Check in / check out capabilities to trace "who" made "what" changes and "when"
- Capabilities to store different vendor artifacts
  - Support of Plant Area Model for asset location relationship is helpful
- Capabilities to store multiple versions of automation artifacts



Change management, also known as Management of Change (MoC), is included in any serious security program. Change management software packages should support basic library functions like "checking in / checking out" of files. If the change management supports a code comparison feature it is extremely helpful to track down specific code changes that have been loaded in the control system. An offline comparison of the differences between running code and the "golden" or verified and validated code may also be required by regulations.

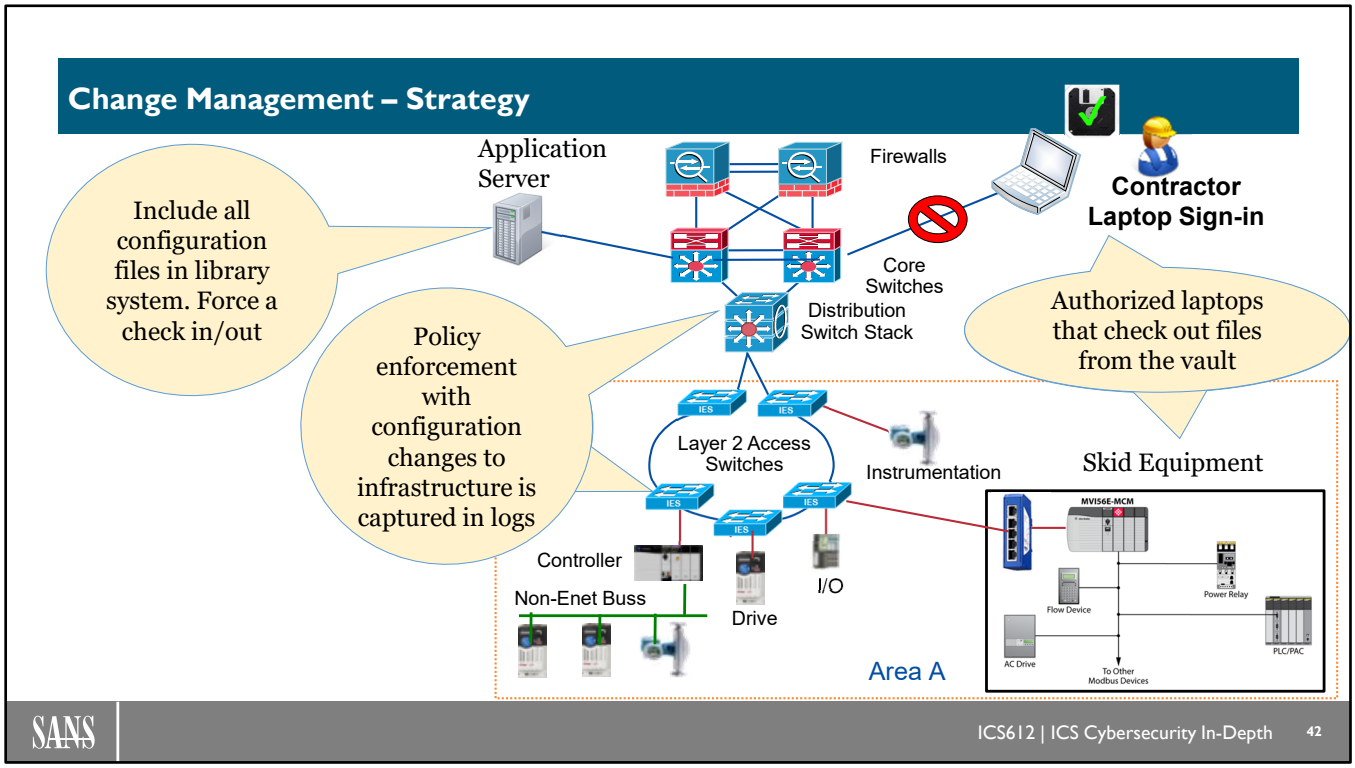
The change management software should support multivendor archiving even if it simply means enforcing check-in / check-out actions.



Consistent change management starts with changing the culture of the customer's personnel, who have the ability and responsibility for engineering, operating and maintaining their control systems and infrastructure. In the list of "easily forgotten items" to include in the change management systems are:

- Network switches and router configuration changes
- Modem or VPN endpoint configuration
- Enforcing contractor participation in change management procedures
- Including rarely used or less critical software into the change management process. Examples include alarm escalation software, standalone device-level configuration tools and smaller shadow network support tools.

Because many automation controllers allow online edits, it's possible for a contractor or other on-site person to change the configuration of an automation asset without checking the file out, making the changes, and checking the file back in. This capability is a fundamental reason to NOT allow third-party laptops into the environment. They may update the device configuration directly on the device and leave with the latest offline version and no documentation of change provided.



Change management enforcement can be tricky, especially with devices that can be altered by connecting and changing the configuration without the need for checking out an associated file. Change management guidelines and rules must be in place so anyone working in the plant must understand that in order to make a change, they must have a record of:

- What is the change to be made?
- What is the scope or duration of the change?
- Who or what is the impact of the change?
- Who is making the change?
- Who authorized the change?
- Do you need a signature of verification the change has been implemented successfully through an operational test?

For devices that can be changed without checking out an associated file, the device(s) should be configured to send a notification of configuration changes to the logging server.

The change management effort can be started by putting all the configuration files or code modules into a library system that forces a check-in / check-out of the associated file.

Also, implementing a contractor policy that enforces either a laptop check policy, or a company-supplied-laptop-only policy, with a documented issuance/access of the appropriate files upon request will help track approved changes. We have seen this type of policy work, especially if a customer provides contractor training as they come on site.

ICS Asset Change Management Checkpoint 4.5

- Change management helps us track "what" changes were made to an environment by "whom." With ICS devices, online change support was a product design requirement but in today's security-conscience environment that creates change management logistics issues.
- Controlling online configuration changes is part procedural and part technical controls. Automation and infrastructure vendors are giving us tools to help track changes such as code-compare tools and alerting capabilities when configurations are changed; some even provide time-limited authorization tools to enforce coordination of changes.

This page intentionally left blank.

Patching Strategy

Most ICS vendors will test their products with the latest OS vendor patches

- Your Standard Operating Procedure (SOP) should be to check with your vendor

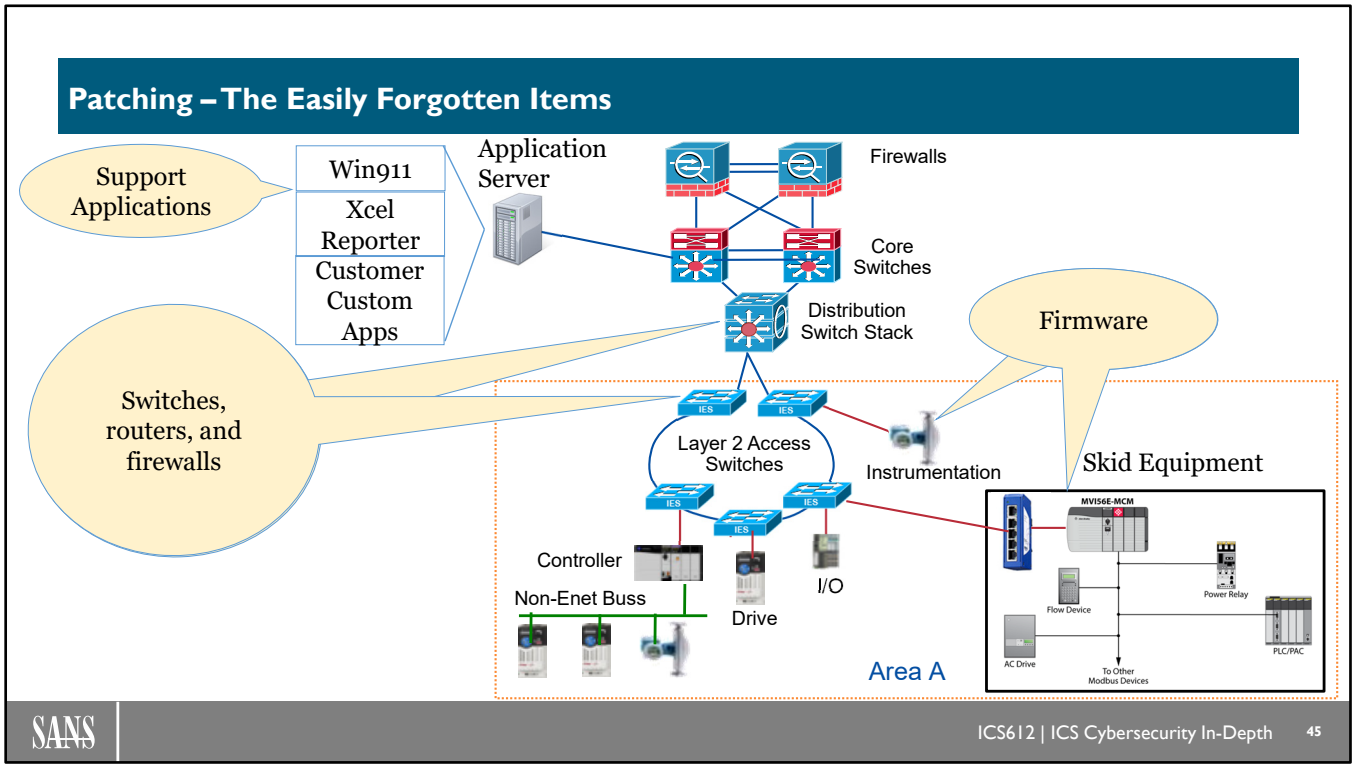
FAQ

Summary: What's New this Month

Last Updated: 7/19/2019

MS KnowledgeBase	MS Security Bulletin	Date Released	Qualification Status	Recommendation	CPR	Date Published	Details	OS	Title
KB4509410	None	7/9/2019	Published	Not Tested	NA	7/11/2019	PQUAL00166914	None	Update Rollup 29 for Exchange Server 2010 Service Pack 3 (KB4509410)
KB4509409	None	7/9/2019	Published	Not Tested	NA	7/11/2019	PQUAL00166913	None	Security Update For Exchange Server 2016 CU13 (KB4509409)
KB4509408	None	7/9/2019	Published	Not Tested	NA	7/11/2019	PQUAL00166912	None	Security Update For Exchange Server 2019 CU2 (KB4509408)
KB4507469	None	7/9/2019	Published	Not Tested	NA	7/11/2019	PQUAL00166911	None	2019-07 Cumulative Update for Windows 10 Version 1809 for x86-based Systems (KB4507469)
KB4507464	None	7/9/2019	Published	Not Tested	NA	7/11/2019	PQUAL00166910	None	2019-07 Security Only Quality Update for Windows Server 2012 for x64-based Systems (KB4507464)
KB4507462	None	7/9/2019	Published	Not Tested	NA	7/11/2019	PQUAL00166909	None	2019-07 Security Monthly Quality Rollup for Windows Embedded 8 Standard for x64-based Systems (KB4507462)

As we all know, one of the best ways to fight against an adversary is to patch against known vulnerabilities. In the manufacturing world, this can be easier said than done. Having a patching and control operation validation strategy can take a lot of effort but one way to help lessen this effort is to leverage the vendors' testing results. When many larger ICS and DCS vendors apply the OS patches they report their findings. This is certainly an efficient way to leverage their effort and it will give you some idea of whether their products have any ill effects from patching.



While the major software companies may offer a good notification of available patches, some of the niche companies may not have a security index or good notification method to easily identify current patches. In these particular cases, a company policy should drive an SOP for inventorying all the software and do a regular check for updates or patches. During the investigation of available patches, one must determine if the patch can be applied to the system without adverse side effects. It is typical for a non-production system to be patched and tested before the patch is applied to the production system.

Patching Strategy and Cadence

- Patching can be disruptive to operations
- Sometimes it will take longer than you expect to apply patches and get the system up and running
- Create a table with Operations Criticality vs. Security Criticality to determine patch cadence

Asset	Patching Priority	Days after vendor approval	Update during the week	Update during weekend
HMI Server	1	14	No	Yes
Engineering Workstation	5	60	Yes	Yes
Historian	1	30	No	Yes
QC Software Server	4	45	Yes	Yes
Industrial Switches	10	180	No	Yes
Industrial Firewall	1	30	No	Yes

Patching is a hand-in-hand walk between operations and the security team. The security team can create a table that can help identify the critical assets to patch and an established timetable on which they will commit to applying the patch. It should still be noted that working with the vendors can help establish when the patch is safe to apply. However, it is important to remember that applying the patches on a backup system to check the effects of the patch before applying the patch to the production system is a great way to mitigate risk.

Not every patch needs to be applied. From a prioritization standpoint, focus on software that does create a listening port, vulnerabilities that are more accessible from external networks, or risk of attack based on known threat group activities and active exploits.

Lab 4.4: ICS Asset Inventory and Management

Go to the Lab Workbook: Lab 4.4

This page intentionally left blank.

ICS Asset Management Checkpoint 4.6 (1)

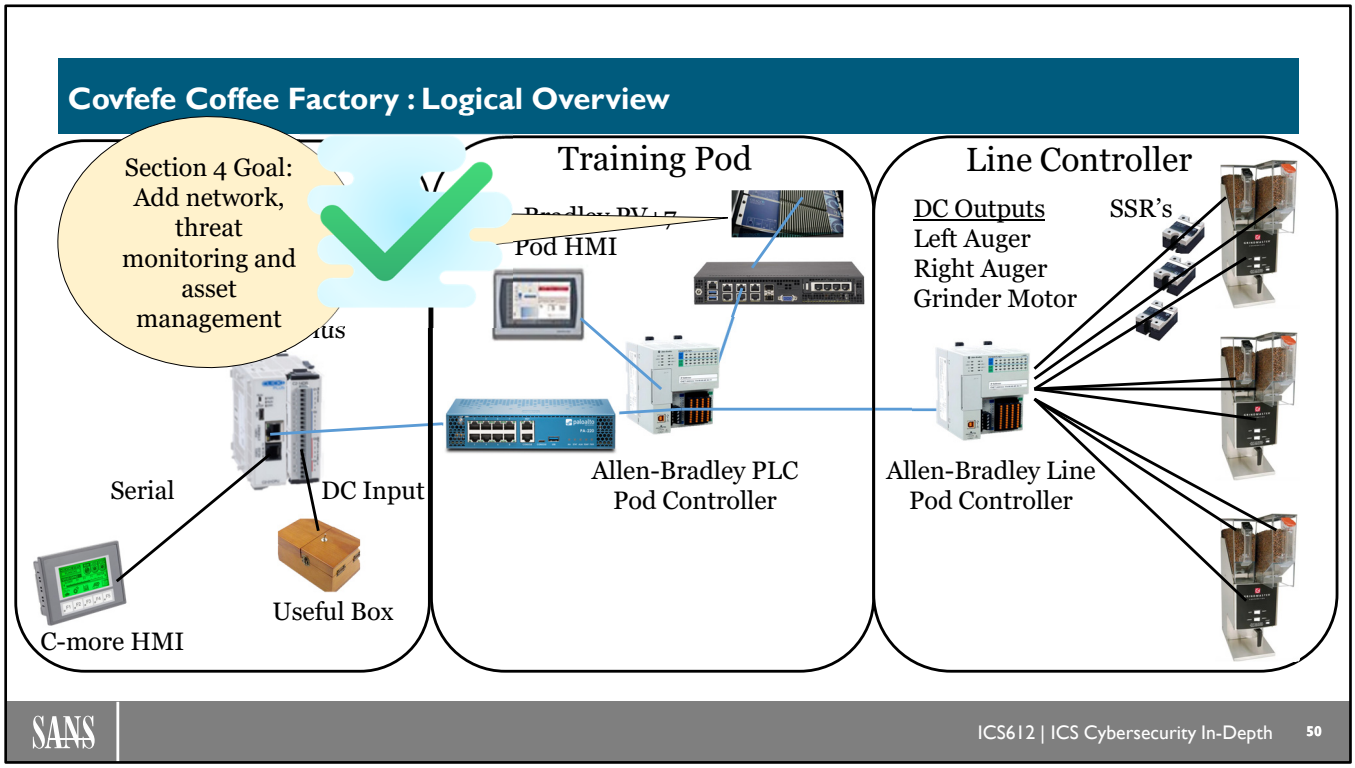
- Patches are typically created to make the software or firmware operate as intended. Patches may be issued to address functional anomalies that could lead to a threat actor using the anomaly in nefarious ways
- Patching can be viewed as a simple act of updating software, but in the industrial environment patching can be challenging: For instance a process environment may be running an old OS that is no longer offers patches; or there may be a requirement for thorough testing on a backup system before patches can be deployed on a production system

This page intentionally left blank.

ICS Asset Management Checkpoint 4.6 (2)

- ICS items like the controller, instrumentation, and I/O subsystems may rarely be patched in some environments, so being aware of the current firmware levels and the current list of vulnerabilities is important in case it is deemed necessary to apply the patches to these devices at some point
- Switches, routers, and firewalls in the ICS environment are oftentimes never patched, especially if an OT person is in charge of particular devices
  - For instance, the Stratix line has switches, routers, and firewalls that may never be touched by the IT staff and because they are "hidden" away, they never get patched

This page intentionally left blank.



As we look at Levels 0 and 1 hands-on exercises, we will use two systems to achieve the PLC and HMI learning objectives. On the left you will see the training Pod hardware that consists of an Allen-Bradley PanelView HMI and the Allen-Bradley (A-B) CompactLogix PLC. The training Pod also contains push buttons, indicator lights and remote breakers that the A-B PLC will use for input and output control.

The student kit as shown on the right contains the Click Plus PLC and the C-more HMI that will be used during student labs. The Click Plus PLC will communicate with the A-B PLC via Modbus TCP sharing data register information and I/O status. The student kit also contains a Useless Box that will be transformed into a Useful Box that will be controlled by the Click Plus PLC in order to show you how "useful" a simple input switch, motor circuit, and power source can be to gain knowledge about PLC systems. The student kit also contains a K-type thermocouple to demonstrate analog input capabilities of the Click Plus PLC.

ICS612 Section 4 Outline (5)

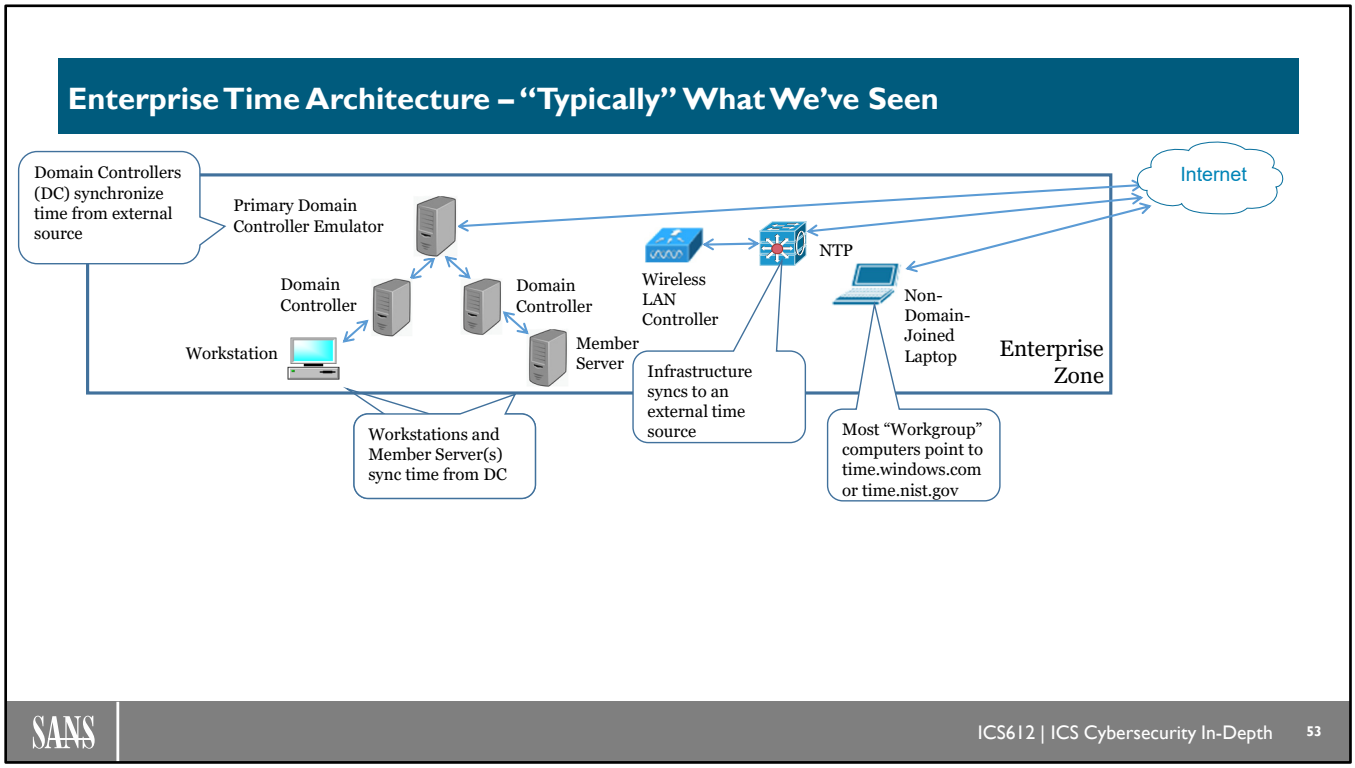
- ICS Security Monitoring
- Lab 4.1: Local Monitoring
- Lab 4.2: Process Environment Monitoring
- ICS Logging and Alerting
- Lab 4.3: Monitoring Tool Integration in ICS
- ICS Asset Management
- Lab 4.4: ICS Asset Inventory and Management
- Importance of Time
- Lab 4.5: Kiss of Death (KoD) Attack
- Asset Validation and Restoration
- Lab 4.6: ICS Device Backup
- Lab 4.7: ICS Device Restoration

This page intentionally left blank.

Importance of Time

Time Architecture
Types of Time Sources
Time Sources and PLCs

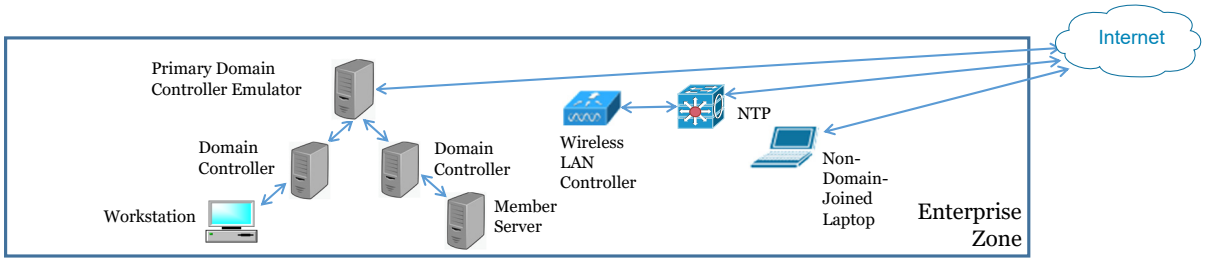
This page intentionally left blank.



From Microsoft: "Configure the Root PDC with an Authoritative Time Source and Avoid Widespread Time Skew"

Suggested Actions: "You can configure the Domain Controller holding the PDCE role to use an NTP Server to synchronize time"

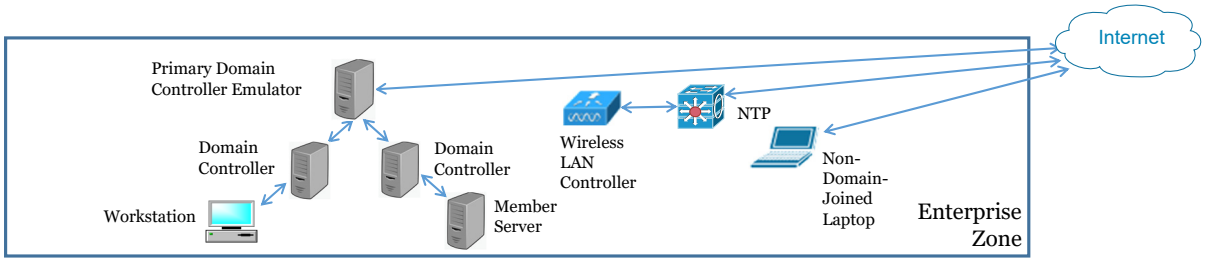
Enterprise Time Architecture – Accuracies



- NTP v3 is accurate to 1-2ms in a LAN and 10s of ms in WAN networks (http://www.cis.udel.edu/~mills/ntp.html)
- A recent survey from ntp.org suggests that 90% of the NTP servers have network delays below 100ms, and about 99% are synchronized within one second to the synchronization peer.

This page intentionally left blank.

Enterprise Time Architecture – What Happens during a "Malfunction"?

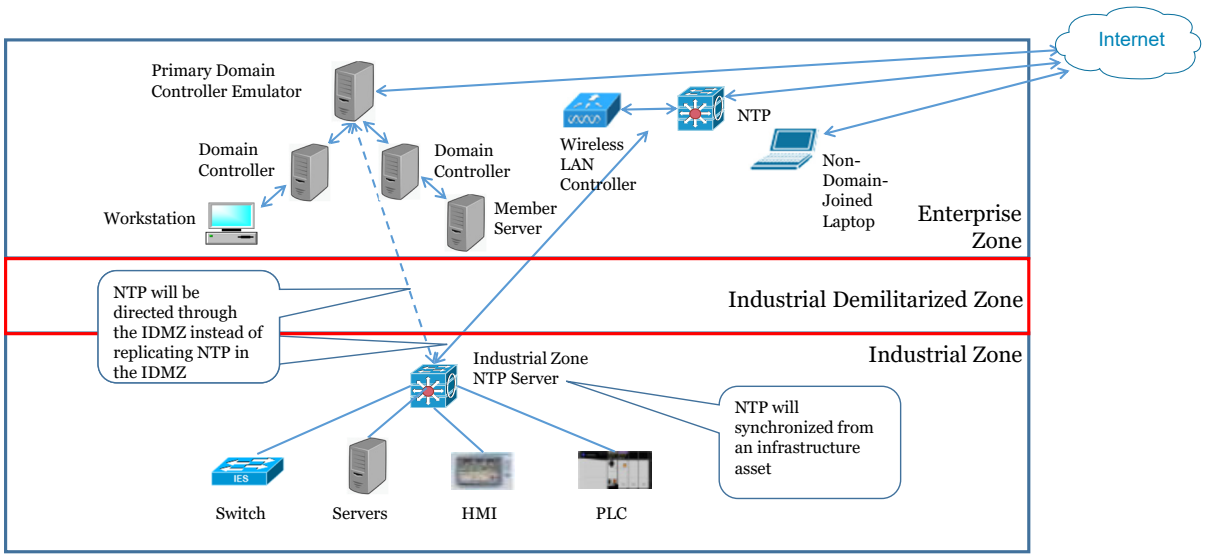


Time synchronization failures can cause a variety of problems:

- Logon failures. Kerberos authentication and claims-based single sign-on can fail due to time disparities.
- Forensics and Auditing software require accurate time synchronization.
- Wireless time synchronization is used for many different purposes including location, proximity, energy efficiency, and mobility to name a few.

This page intentionally left blank.

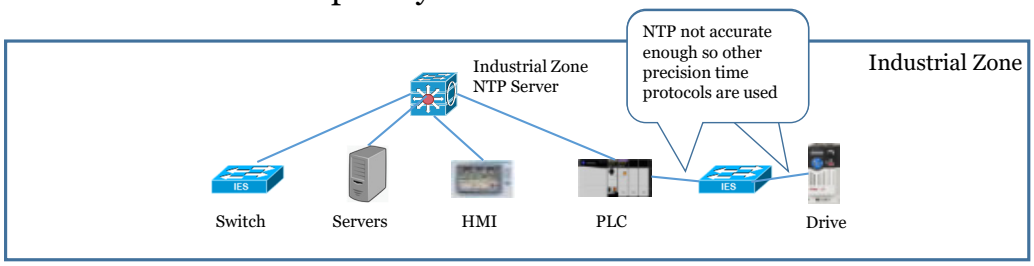
Industrial Zone Time Architecture – "Typically" What We've Seen



This page intentionally left blank.

Industrial Zone Time Architecture – Accuracies

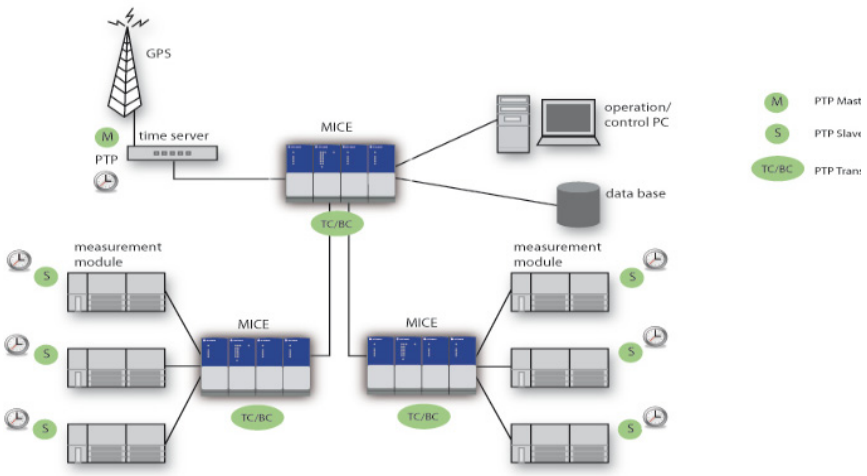
- NTP v3 is accurate to 1-2ms in a LAN which isn't precise enough for some applications
- Applications like Motion Control, First Fault Detection, Critical Sequence Of Events (SOE) processes, Packaging machines or sorters that have fast part cycles are often bottle-necked by controller scan times, so they move to a time-based solution do predictive events and schedule outputs to run things like diverters without having a scan time to match the part cycle time



This page intentionally left blank.

Time Source and PLCs

- Not all PLCs support NTP
- Automation applications require better time synchronization
- Precision Time Protocol (PTP)
- IEEE 1588
- Accuracy <1 µs over Ethernet



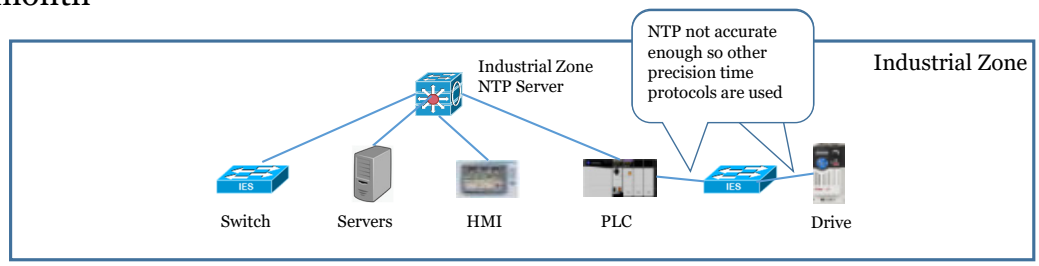
It should be noted that some PLC clocks cannot and do not synchronize to an NTP time source. Standards like IEEE 1588, also known as Precision Time Protocol (PTP), were designed for systems requiring accuracies beyond those supported by NTP. With control systems, precision time is required in support of deterministic I/O systems on Ethernet. The system latency must be calculated and used as a compensation for the deterministic I/O, drive, and motion control. Therefore, if a PLC is participating with the system logs it then becomes possible the other device using NTP for timestamps may not be synchronized to the devices supplying events that have been stamped with PTP. It is important to understand how the logging software handles the timestamping so correlation of events can occur.

Image Source:

- https://www.hirschmann.com/en/Hirschmann_Produkte/Industrial_Ethernet/Technologies/Precision_Time_Protocol/index.phtml

Industrial Zone Time Architecture – Accuracies

- Even with Precision Time Protocol (PTP), also known as IEEE 1588, it starts life from another time source like NTP or a GPS time source and is then converted into IEEE 1588 time
- PTP achieves clock accuracy in the sub-microsecond range
- Embedded devices like PLC's need time updates because time will skew at different rates depending on temperature. Examples could be over four (4) minutes per month



This page intentionally left blank.

Industrial Zone Time Architecture – What Happens during a "Malfunction"?

- Think about not processing a product for the right amount of time? Think about critical control parameters such as too short of a pasteurization cycle, or maybe moving to fast or too long on a robotic weld.
- Closed loop control depends on stable time measurement
  - Velocity = Distance / Time
- Automation vendors have had to overcome even before Ethernet with proprietary solutions

$$u(t) = \mathrm{MV}(t) = K_\mathrm{p} e(t) + K_\mathrm{i} \int_0^t e(\tau)\,d\tau + K_\mathrm{d} \frac{de(t)}{dt},$$

where

K_p is the proportional gain, a tuning parameter,

K_i is the integral gain, a tuning parameter,

K_d is the derivative gain, a tuning parameter,

$e(t) = \mathrm{SP} - \mathrm{PV}(t)$ is the error (SP is the setpoint, and PV(t) is the process variable),

t is the time or instantaneous time (the present),

τ is the variable of integration (takes on values from time 0 to the present t).

This page intentionally left blank.

NTP Rate Limit

- Network Time Protocol (NTP) servers indicate to a client they need to slow down the request rate by sending a special packet back to the client. This packet is called the kiss-o'-death (KoD) packet
  - One code "RATE" is sent by the server if the limited and KoD flags are set
- In order to make sure the client notices the KoD, the receive and transmit timestamps are set to the transmit timestamp of the client packet and all other fields left as in the client packet

This page intentionally left blank.

NTP Normal Transmit and Response

Transmit

```
> Flags: 0x0b, Leap Indicator: no warning, Version number: NTP Version 1, Mode: client
  [Response In: 2243821]
  Peer Clock Stratum: unspecified or invalid (0)
  Peer Polling Interval: invalid (0)
  Peer Clock Precision: 1.000000 seconds
  Root Delay: 0.000000 seconds
  Root Dispersion: 0.000000 seconds
  Reference ID: NULL
  Reference Timestamp: (0)Jan  1, 1970 00:00:00.000000000 UTC
  Origin Timestamp: (0)Jan  1, 1970 00:00:00.000000000 UTC
  Receive Timestamp: (0)Jan  1, 1970 00:00:00.000000000 UTC
  Transmit Timestamp: (0)Jan  1, 1970 00:00:00.000000000 UTC
```

Send a known bad time

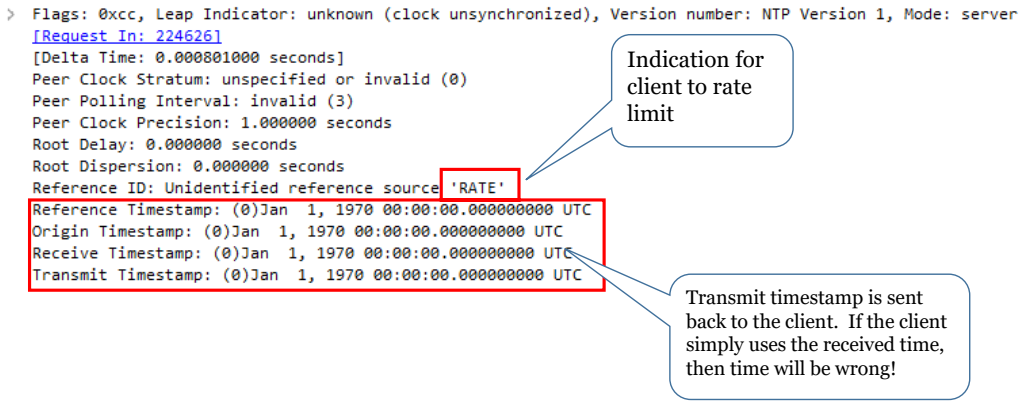
Response

```
> Flags: 0xcc, Leap Indicator: unknown (clock unsynchronized), Version number: NTP Version 1, Mode: server
  [Request In: 2243811]
  [Delta Time: 0.001349000 seconds]
  Peer Clock Stratum: unspecified or invalid (0)
  Peer Polling Interval: invalid (3)
  Peer Clock Precision: 0.000000 seconds
  Root Delay: 0.000000 seconds
  Root Dispersion: 0.006592 seconds
  Reference ID: (Initialization)
  Reference Timestamp: (0)Jan  1, 1970 00:00:00.000000000 UTC
  Origin Timestamp: (0)Jan  1, 1970 00:00:00.000000000 UTC
  Receive Timestamp: Apr  3, 2020 19:49:00.207349947 UTC
  Transmit Timestamp: Apr  3, 2020 19:49:00.207673550 UTC
```

You will see the time updated in the response

This page intentionally left blank.

Kiss of Death (KoD) Packet



This page intentionally left blank.

Lab 4.5: Kiss of Death (KoD) Attack

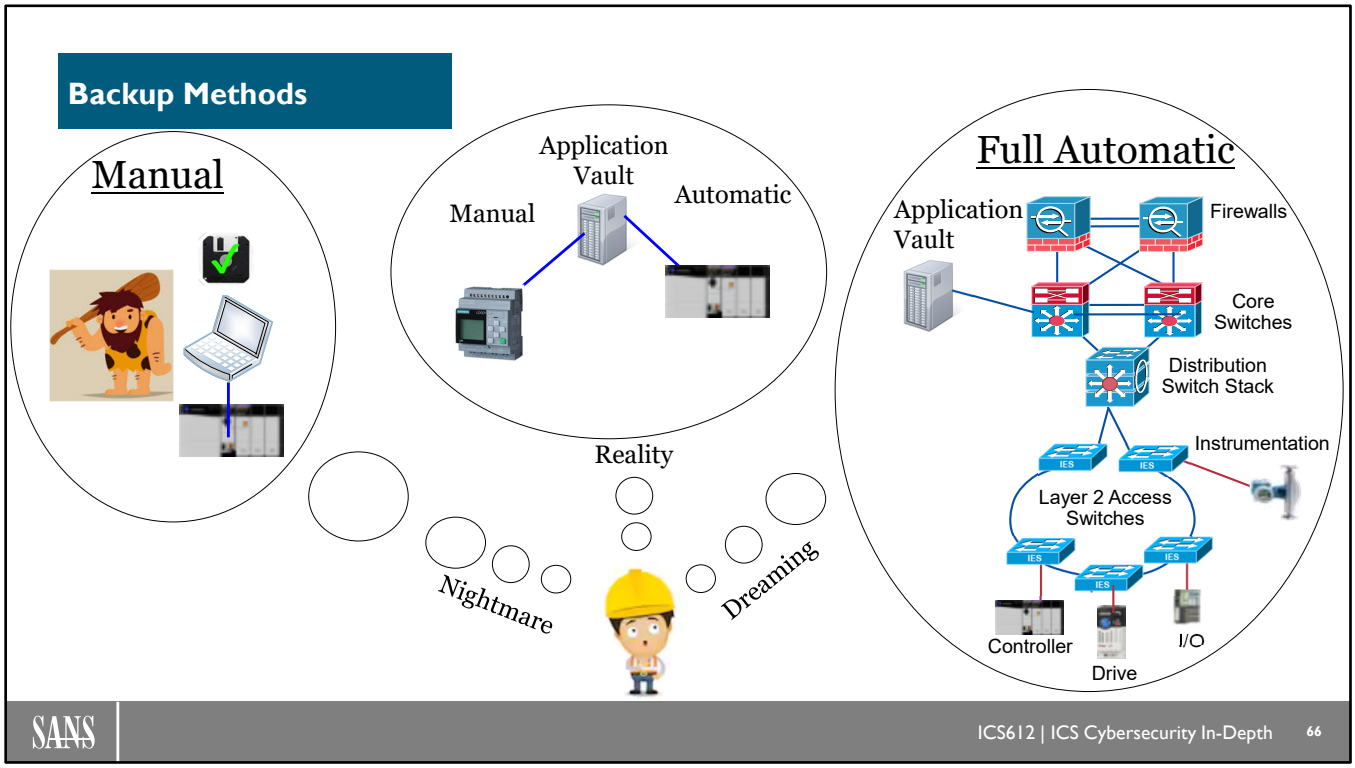
Go to the Lab Workbook: Lab 4.5

This page intentionally left blank.

Asset Validation and Restoration

Performing Backups of ICS Devices
Verification of the Backups
Restoring Impacted ICS Devices

This page intentionally left blank.



ICS vendors do supply automated backup tools which can be included into their change management software. The consideration for automatic backups will be determined if the software can connect to all the ICS devices and perform a backup. It is unlikely that all device configurations can be automatically archived, so manually backing up configurations will be necessary for some vendors, devices, and network devices.

In some cases, it may be necessary to utilize vendor-specific software, cables, and interface cards to devices to store or restore configurations.

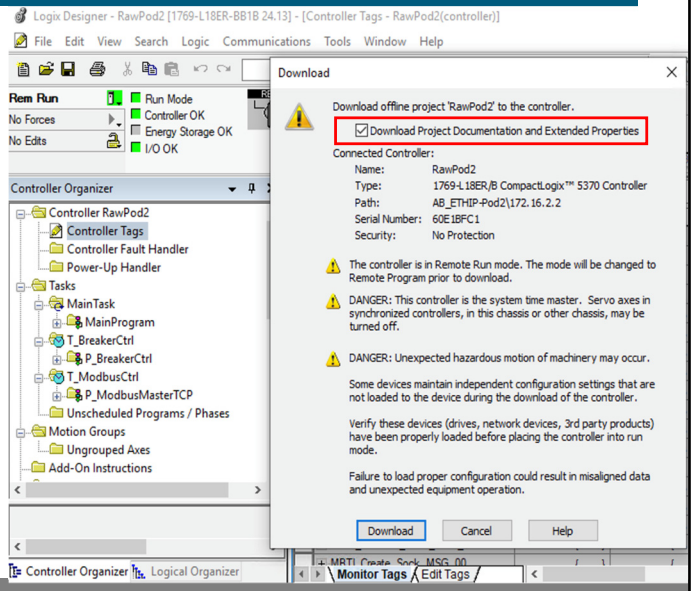
One design consideration for archiving is to determine where the backup storage location should be. Some considerations include that it should be:

- Secured
- Centralized
- On an actively managed server
- Protected with Authentication, Authorization, and Audit (great use of data loss prevention (DLP) type solution for early indicator of attacker interest)
- Not on a USB drive on a computer

Another consideration is determining how the backups will be tested and the frequency of exercising each backup.

ICS Restore – Having the Gold Copy Is a Start

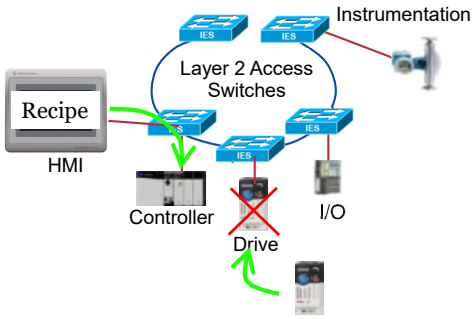
- Having the "gold" code copy is a good start but knowing if it includes "gold" data is key
  - Data in the backup is probably stale
- Difference in granularity in vendor software
  - Some vendors may allow backup of tag database and values
  - Comments within the configuration may be truncated on the device, requiring the latest offline file to maintain documentation



Restoring a device's code, configuration, and data can be a bit trickier than it seems because you must know not only if the code matches but also if the critical setpoint data is current. Most ICS vendors have faced this challenge and offer a method of backing up and restoring code only, data only, or both. It is also important to notice some ICS platforms store the tag, rung, function block, etc. on board so when the backup is conducted, it will contain these artifacts as well. "Why?" you might ask. The use case for most PLCs is to have the ability for a field service or engineer to walk up to the PLC, connect, and be able to troubleshoot the program without having access to the original file. It should be noted, older PLCs and some less expensive models will not have the documentation stored on board.

Drivers That Cause the Restore Process

- Cataclysmic
  - Something significant and event-driven
  - Operations is familiar with replacing failed devices
  - Vendors adopting Automatic Device Replacement (ADR) features
- We do restoration on a micro level with recipes
  - System has set parameters based on production objectives and is operations-driven



Automatic Device Replacement (ADR)

We typically don't do the restore process unless something cataclysmic occurs, like a device failure. ICS vendors have been supporting a "limited or no touch" method of replacing failed I/O, drives, and instruments with an Automatic Device Replacement (ADR) strategy. The workflow is this: The device fails; the new device is plugged into the network; then the PLC or higher-level master sends the configuration to the new device. This has made the restore operation much more automated, which is resulting in the operations team having less familiarity about how to restore from a software backup.

Lab 4.6: ICS Device Backup

Go to the Lab Workbook: Lab 4.6

This page intentionally left blank.

Asset Validation and Restoration Checkpoint 4.7

- Device backup can be an automated or manual process. Any automated change management or backup/restore software requires ICS protocol support to request a backup. It's likely you will use the ICS vendor's solution as they may have the only deep knowledge of how to request the backup from the device.
- If you have a wide variety of ICS assets, it is unlikely the entire backup process can be automated.
- Keep in mind the importance of having a "gold" copy of the logic, but also be aware that fresh or current data backup should be considered as required

This page intentionally left blank.

Asset Validation and Restoration Checkpoint 4.8

- Validation can occur by observing operational validation or by comparing device data sets against a known good set
- Operational validation is much more preferred because, just as people have personalities, so do devices.
  - If you build twenty machines, none of them will tune exactly the same
- Configurations can change based on the material being used in the process. This implicitly means that the "gold" data you restored may validate to a data set but operationally the process won't run the same

This page intentionally left blank.

Lab 4.7: ICS Device Restoration

Go to the Lab Workbook: Lab 4.7

This page intentionally left blank.

ICS Device Restoration Checkpoint 4.8

- Device restoration is typically triggered after a device has failed, which has typically caused downtime.
- Restoration is typically a two-step process. First, replace the device; and second, restore the code and configuration data
- Vendors realize sensors, drives, and instrumentation that touch the process are more likely to fail than the processors. For this reason, vendors have created more automated tools to allow the configuration to be downloaded to a new device.

This page intentionally left blank.

Section 4 Summary (1)

- In this section, we covered local and process environment monitoring. Sensor location to capture control asset traffic will be lower in the architecture than most IT deployments at the router layer
- Logging from the ICS layer is similar but different. Sending logs from switches, routers, and firewalls for enterprise switches, routers, and firewalls. Investigating ICS vendor specific logs may require running special tools to gather the Windows event logs for forensics.
- Be aware of NTP vs. other time protocols like IEEE 15888 as they may not be synchronized, which can make it very difficult to coordinate events

This page intentionally left blank.

Section 4 Summary (2)

- It is probably not realistic to assume that asset inventorying can be done in an automated fashion
  - Automation plus manual inspection to gain a realistic asset inventory is the reality
- Change management is easier with those assets that don't have online capability and require access to a file in order to change the program or configuration.
- Change management for assets that support online configuration changes will either need a way to compare the online program to the offline file or a method for announcing the configuration has changed, whether by a log or another means of visualization

This page intentionally left blank.

Section 4 Summary (3)

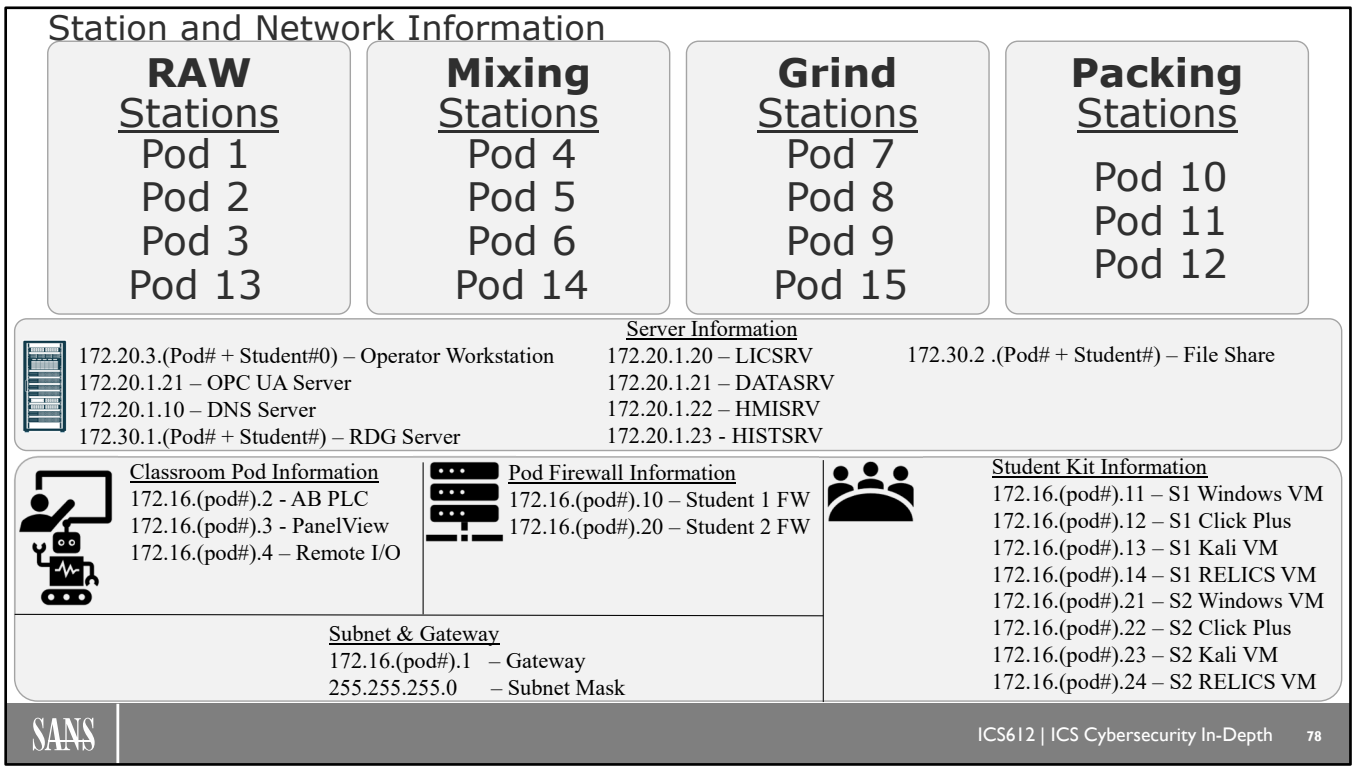
- Patching in the ICS environment may not be possible with some assets due to unsupported OS's or because the assets are part of a validated system and cannot be changed without revalidation efforts
- Backup and restoring activities should be part of the ICS security program. ICS engineers and maintenance personnel are typically quite familiar with restoring configuration to device-level assets as they are expected to fail and be replaced.
- ICS engineers and maintenance personnel are not typically familiar with backing up and restoring servers and other higher-level ICS assets

This page intentionally left blank.

Section 4 Summary (4)

- Testing backups is not often done until it comes time to do a restore of a failed device or system. Creating a backup testing plan is recommended.
- Having the ability to determine what specific device or configuration is potentially causing an issue is key, as you may cause more trouble in restoring a device that is not causing any issues. This is where troubleshooting skill sets, and systematic approaches are critical… And that is where we will begin Section 5

This page intentionally left blank.



This page intentionally left blank.