612.3

ICS Network Infrastructure

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.

ICS612.3 | ICS Cybersecurity In-Depth

SANS

ICS Network Infrastructure

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: Local Process
- Section 2: System of Systems
- Section 3: ICS Network Infrastructure
- Section 4: ICS System Management
- Section 5: ICS System Troubleshooting and Targeting

This page intentionally left blank.

ICS612 Section 3 Outline (1)

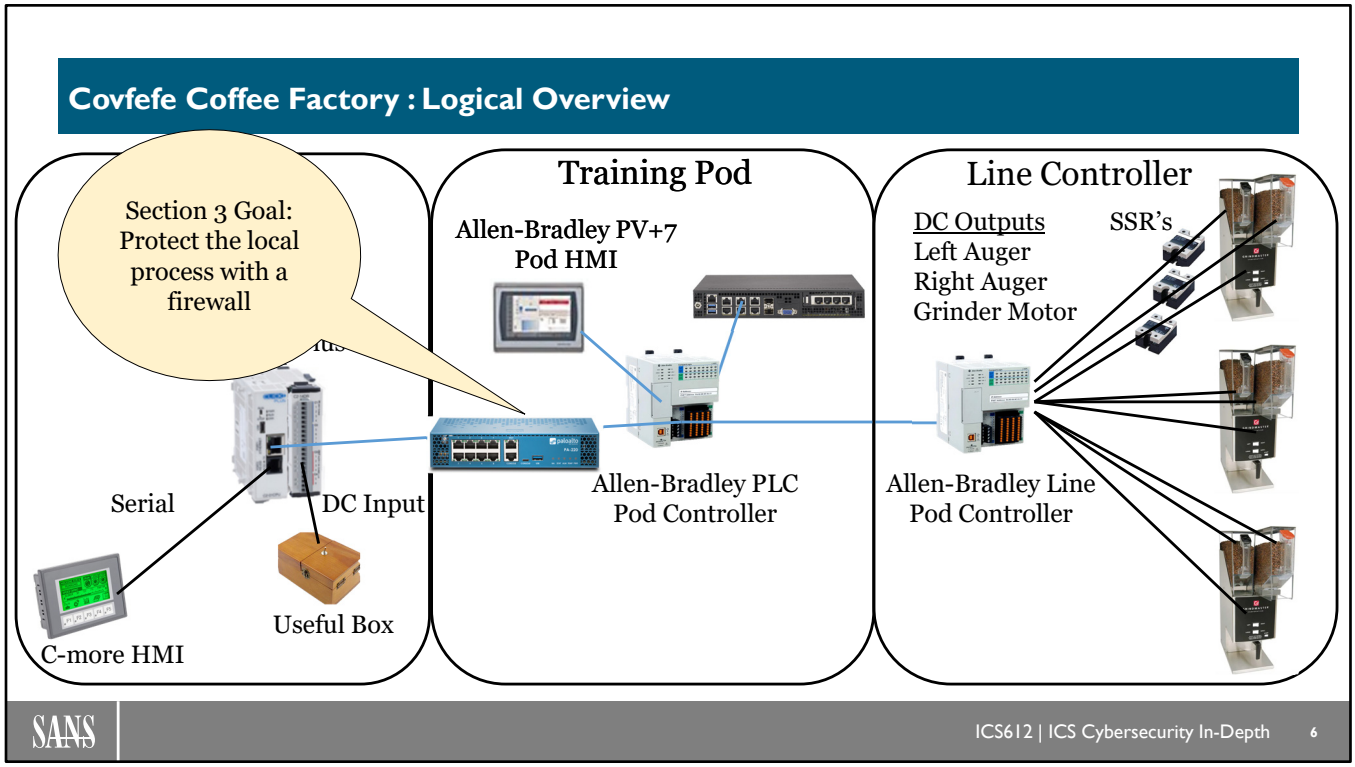
- Process Operation and Enforcement Zones
- Lab 3.1: Implementing Local Firewall
- Process Application Integration
- Lab 3.2: Process Historian
- ICS Environment Remote Access
- Lab 3.3: Configure and Establish Secure Remote Access
- Process Environment Network Protocol Attack Vectors
- Lab 3.4: SMB Attack
- Lab 3.5: RDP Pivot Attack
- Lab 3.6: Stage 2 Attack

This page intentionally left blank.

ICS612 Section 3 Outline (2)

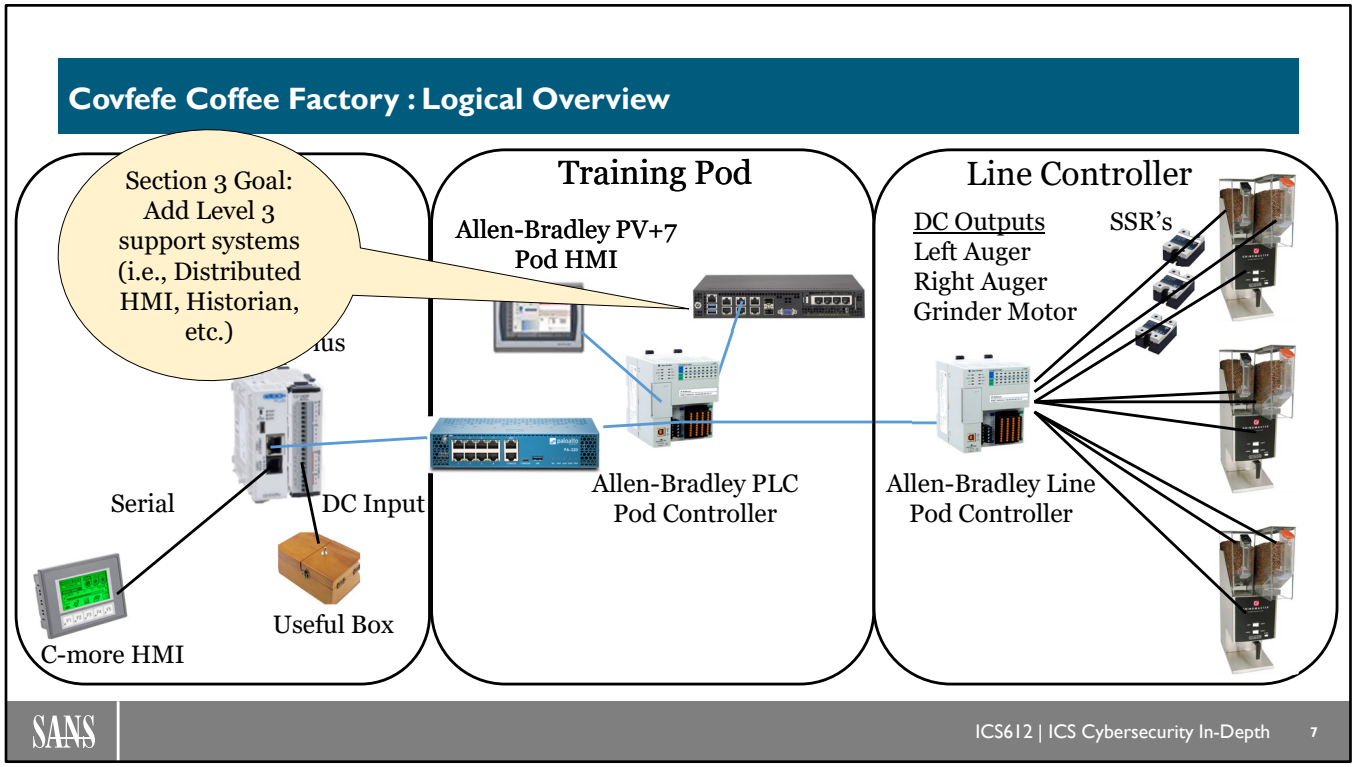
- Process Operation and Enforcement Zones
- Lab 3.1: Implementing Local Firewall
- Process Application Integration
- Lab 3.2: Process Historian
- ICS Environment Remote Access
- Lab 3.3: Configure and Establish Secure Remote Access
- Process Environment Network Protocol Attack Vectors
- Lab 3.4: SMB Attack
- Lab 3.5: RDP Pivot Attack
- Lab 3.6: Stage 2 Attack

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.



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.

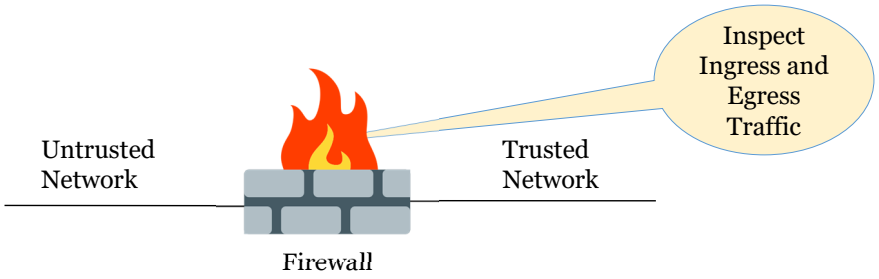
The student kit as shown on the left contains the Click Plus PLC and the C-more HMI that will be used during student labs. The Click Plus PLC will communicate with the A-B PLC via Modbus TCP sharing data register information and I/O status. The student kit also contains a Useless Box that will be transformed 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.

Process Operation and Enforcement Zones

Firewalls in ICS
Rule Specifics for Process Environments
Industrial DMZs

This page intentionally left blank.

Firewalls Define Trusted and Untrusted Security Boundaries

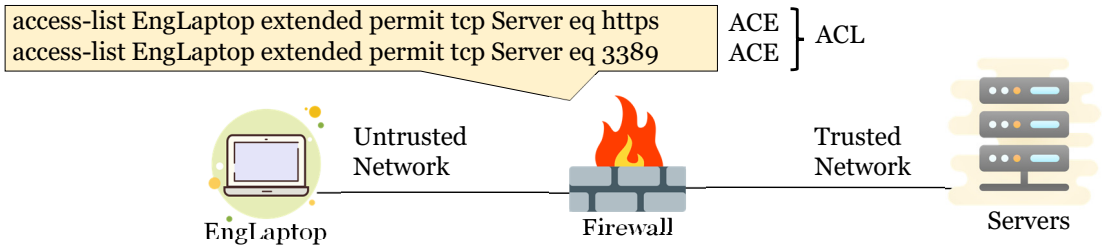


- Firewalls are used to define the edge of a security perimeter
- The firewall allows the network designer the ability to define the rules that permit or deny traffic

Firewalls are used in the majority of today's companies to define security perimeters. Firewalls allow us to define trusted and untrusted security boundaries through network rules on each interface and sub-interfaces. Firewalls allow us to configure the permitted and denied traffic between the networks through ACLs and inspect ingress and egress traffic between the trusted and untrusted network segments.

It should also be noted that a firewall by default will deny traffic. Therefore, the implementer must open or write permit rules to allow the traffic to flow between a source and destination.

Create Access Control Lists (ACLs) to Permit or Deny Traffic

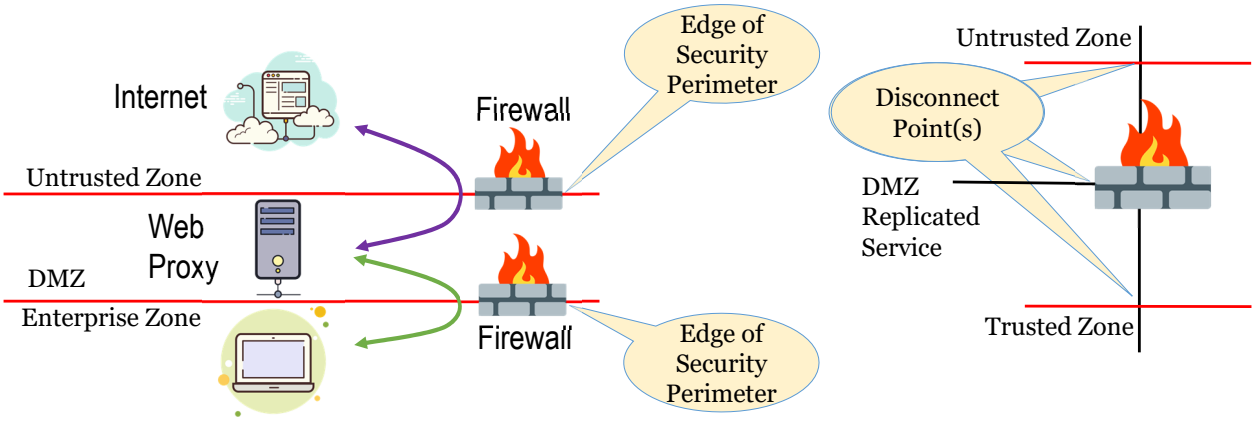


- Access Control Lists (ACLs) define which traffic is permitted between each interface (i.e., security zone)
- Explicit rules allow traffic to flow from the untrusted network to the trusted network
- With some vendors, traffic from the trusted to the untrusted network is permitted without explicit rules through setting security levels

Firewalls are designed to inspect traffic between networks by configuring "permit" and "deny" rules. ACL creations require that an implementer understand the expected data types as well as the permitted data flow between a source and a destination. ACLs are typically comprised of singular rules called Access Control Entries (ACEs). A firewall requires that the implementer open or permit the traffic between a source and a destination because by default a firewall will block or deny the traffic.

Many times, a firewall implementer will become frustrated and write an "any any" rule. In firewall vernacular, this should be interpreted as "allow any traffic to any destination on a particular network." This is commonly done to "just get the firewall to work" and/or because a firewall will not support dynamic port assignments.

Traditional DMZ Separation from the Internet and an Enterprise Zone



A Demilitarized Zone (DMZ) is sometimes referred to a special purpose network that is used to provide access to data or systems from a higher trust network to a lower trust network

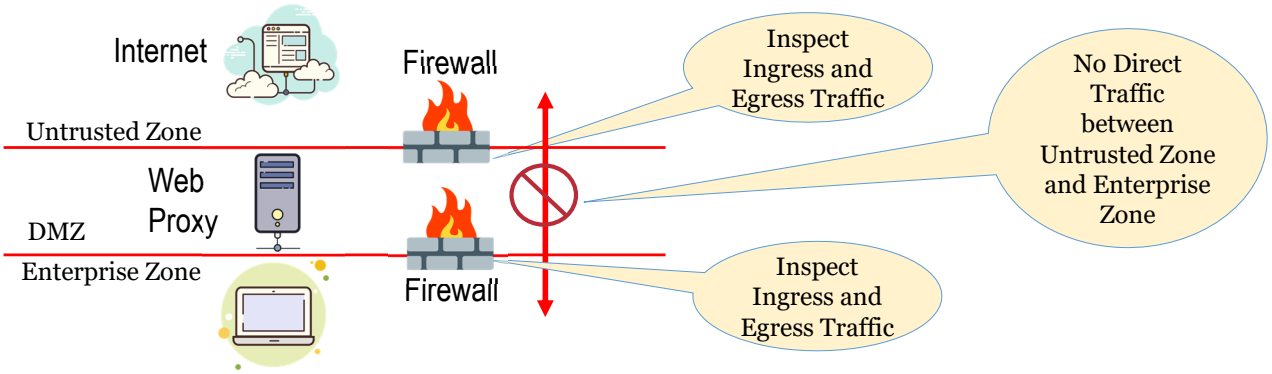
The DMZ is a network that contains replicated or brokered services in lieu of connecting an Enterprise resource directly to an untrusted network like the internet. The concept is to drive the untrusted traffic into the DMZ so it can be inspected. The DMZ is also the destination of the trusted network outbound traffic so this traffic can be inspected and directed to a brokered service in the DMZ. The purpose of the DMZ is to add an additional layer of security to the trusted network.

The firewall interfaces can act as a network disconnect point when an asset is compromised and is being used to pivot traffic to an unauthorized asset or network segment. The intent is for the firewall to inspect the traffic and determine if it is attempting to reach an unauthorized asset or pushing compromised traffic types to an authorized asset.

Reference:

- Source for DMZ definition: "DMZ (computing)," Wikipedia, https://en.wikipedia.org/wiki/DMZ_(computing)

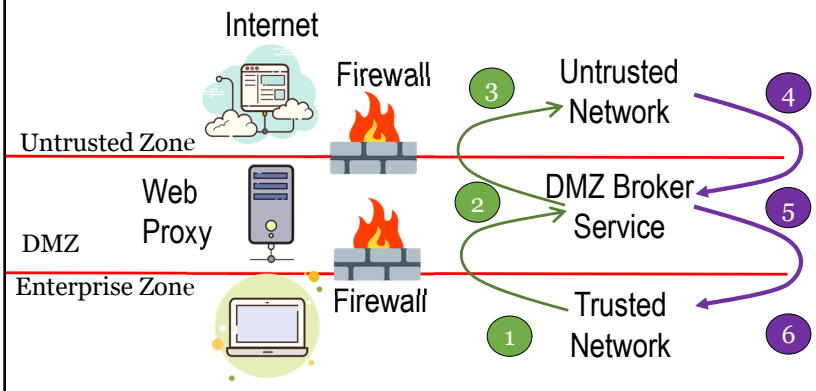
Traditional DMZ Separation of Internet from Enterprise Zone



- Access Control Lists (ACLs) applied to the ingress and egress traffic for the DMZ and the Enterprise Zone
- In most cases we won't allow direct traffic from the untrusted network (internet) into the Enterprise Zone

We have said that firewalls are used to define a security perimeter by explicitly declaring the trusted and untrusted networks that they are connected to. We have also said that firewalls are used to inspect traffic between networks by configuring "permit" and "deny" rules. We can permit or deny specific types of traffic to a particular asset in the DMZ through our ACLs. For instance, we could permit "HTTPS" traffic to the DMZ Web Proxy but deny "HTTP" traffic to the same DMZ Web Proxy server. We could also deny all traffic that is attempting to reach an Enterprise Zone asset from any network except the DMZ network.

Example of Utilizing a DMZ Web Proxy



1) Enterprise laptop requests an external webpage
2) The request is directed to a Web Proxy in the DMZ where the Web Proxy server approves or denies the requested website URL. The proxy does a URL rewrite to hide the client and forwards the request
3) The website receives the request from the Web Proxy
4) The website responds to the Web Proxy
5) The Web Proxy located in the DMZ receives the response, does a URL rewrite, and forwards the website information to the original requesting Enterprise Zone laptop
6) The Enterprise laptop receives the website information

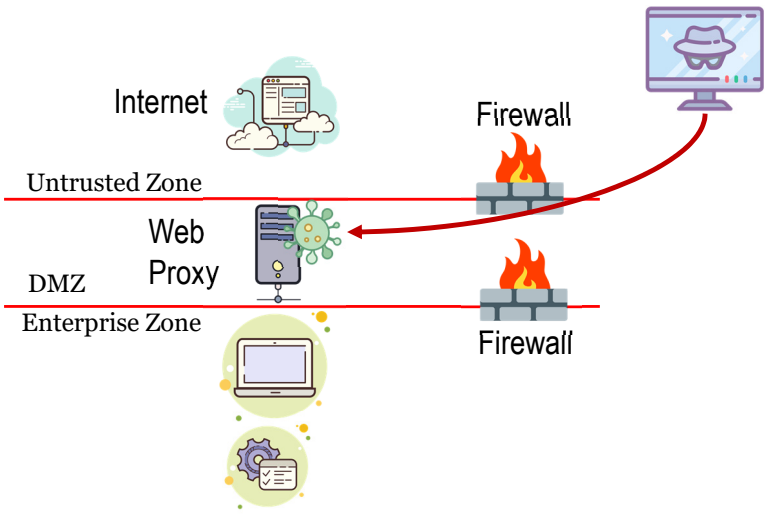
In this example, we are showing a laptop located in the Enterprise Zone that is requesting an externally located webpage. We see that instead of allowing the webpage request to move directly to the internet, we are using a Web Proxy for two functions:

- Used as a forward proxy to hide the client
- Used as a reverse proxy in the cases where we want to hide our Enterprise servers

The DMZ Web Proxy receives the web request, and it determines whether the request is authorized. If the request is approved, it will do a URL rewrite to hide the originating client request and forward the traffic to the destination. When the response is received from the internet web server, the DMZ Web Proxy has a couple of options:

- Inspect the webpage content and take the appropriate action (drop, warn, or permit)
- Rewrite the URL and pass the content intact to the Enterprise laptop

DMZ Assets Are Made to Be Disconnected after Compromise



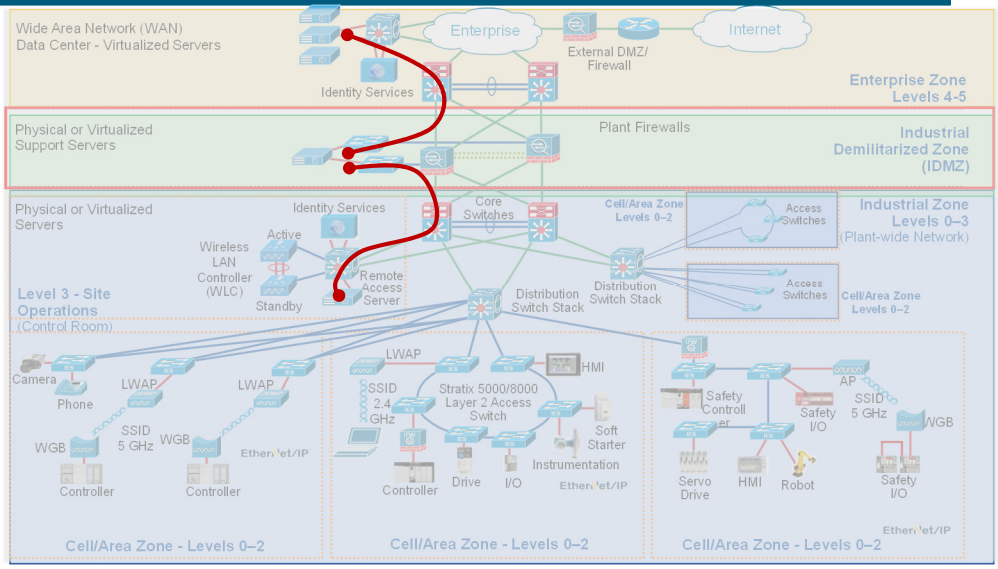
- The intent of the DMZ is so that when an adversary compromises an asset in the DMZ, the asset can be taken offline for rebuild, restore, and re-commissioning.
- Another intention of the DMZ is to buffer the Enterprise Zone from the compromised asset while the DMZ asset is taken offline. This allows the Enterprise asset to continue running while the DMZ asset is offline.

The intent of the DMZ is to provide not only the brokered service but also the capability to take a compromised asset offline without directly affecting the Enterprise Zone asset.

The intent of the perimeter firewalls in these architectures is to define permitted and denied traffic types as well as permitting and denying asset communication paths. For instance, if a DMZ Web Proxy is compromised and it is attempting to communicate to another unauthorized asset then it could be an indication of a compromise.

Industrial DMZ – Same Concept as Enterprise DMZ

- Industrial DMZ (IDMZ) buffers the Enterprise Zone from the Industrial Zone just like the corporate or Enterprise DMZ buffers the Enterprise assets from the internet.
- Traffic from the Enterprise that is destined for the Industrial Zone will be directed into the IDMZ
- The firewall(s) will inspect traffic into and out of the IDMZ



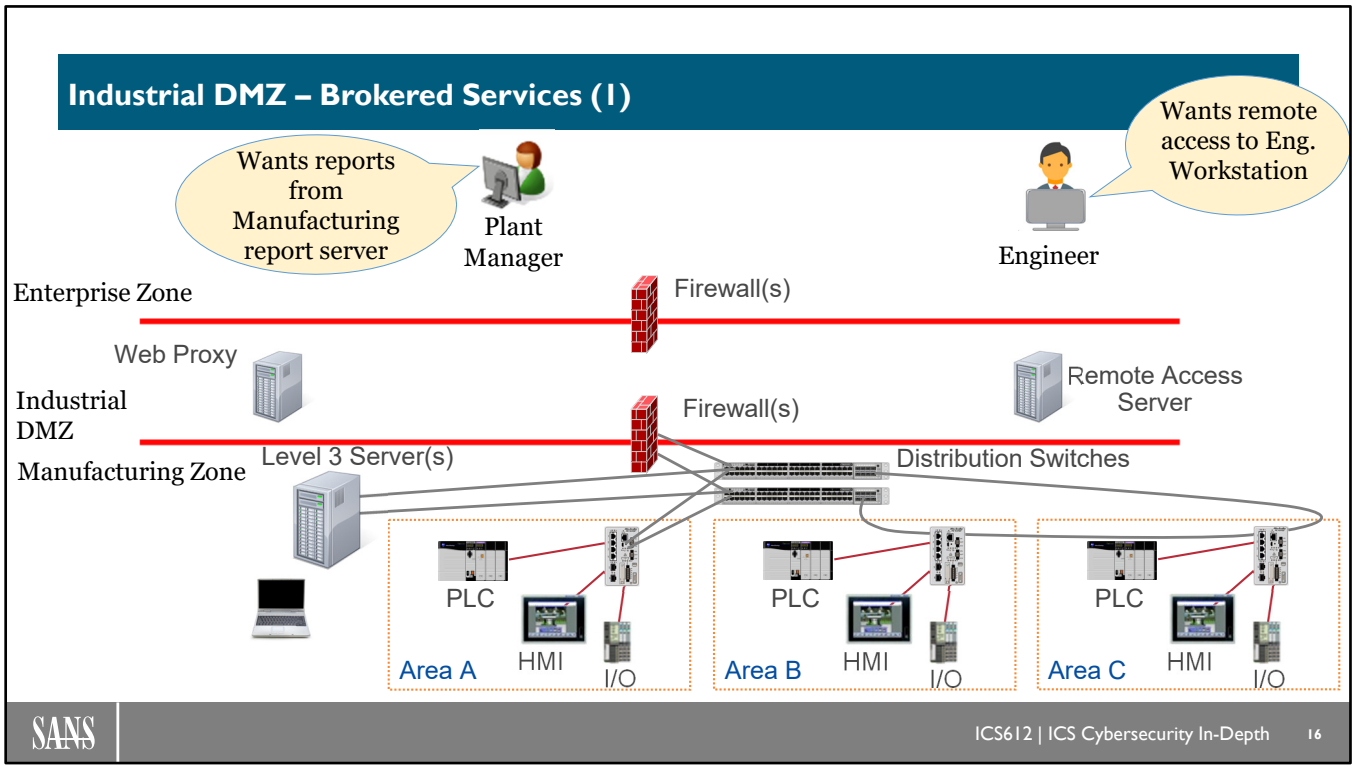
The intention of a DMZ is to protect or buffer the assets on a trusted network from assets on an untrusted network. With this in mind, we can see that the intention of an Industrial DMZ is to protect the Manufacturing assets from untrusted assets in the Enterprise Zone or even assets located outside the Enterprise Zone.

The firewalls facing the Enterprise Zone and the Industrial Zone (Manufacturing) will define the DMZ security zone. It is very typical to subdivide the IDMZ into smaller security zones so that if an IDMZ asset is compromised then the immediately affected network and related assets have a smaller security impact.

Another intention of creating multiple networks within the IDMZ is to catch a pivot of a compromised asset attempting to investigate and communicate with unauthorized assets.

Reference:

➢ Cisco and Rockwell Automation (2011), *Converged Plantwide Ethernet (CPwE) Design and Implementation Guide*. Retrieved from https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf

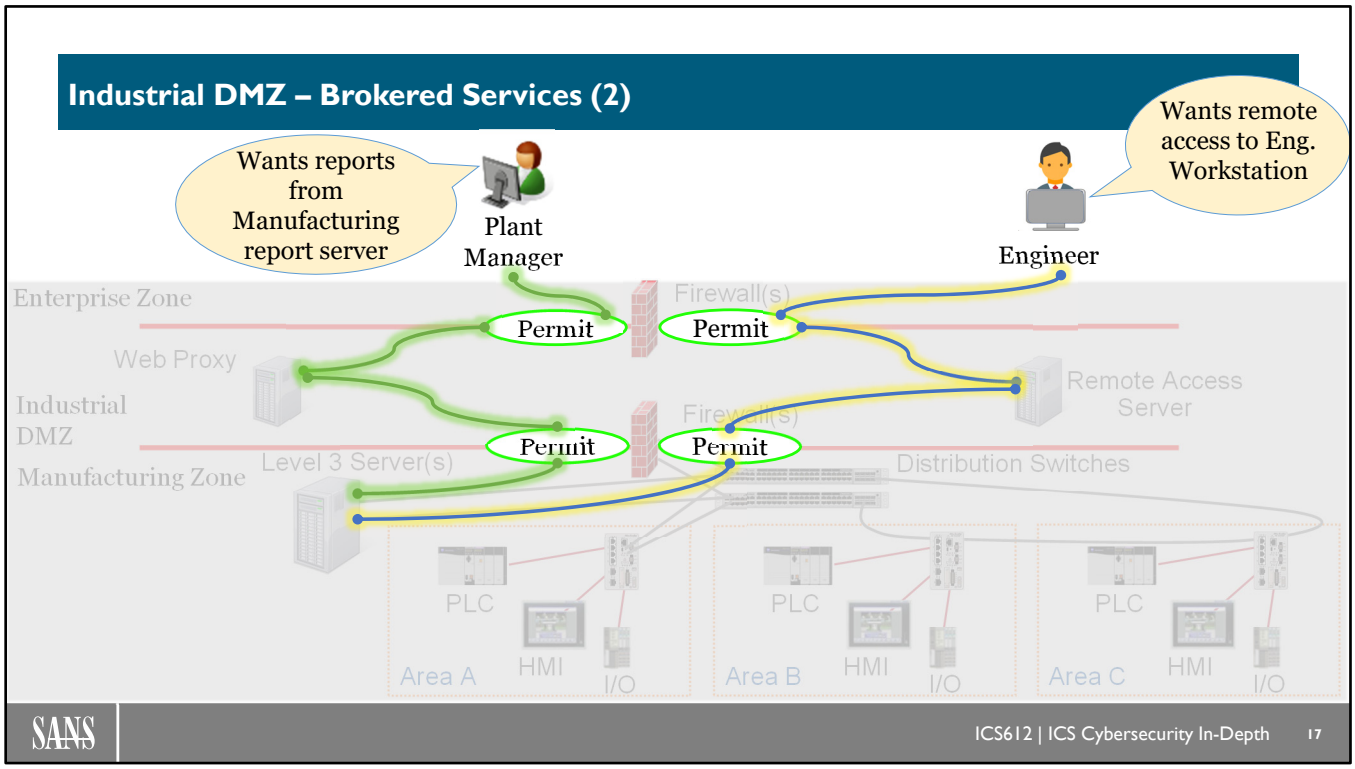


The IDMZ contains proxy or brokered services for users in the Enterprise Zone that wish to obtain access to data or assets in the Manufacturing Zone or vice versa.

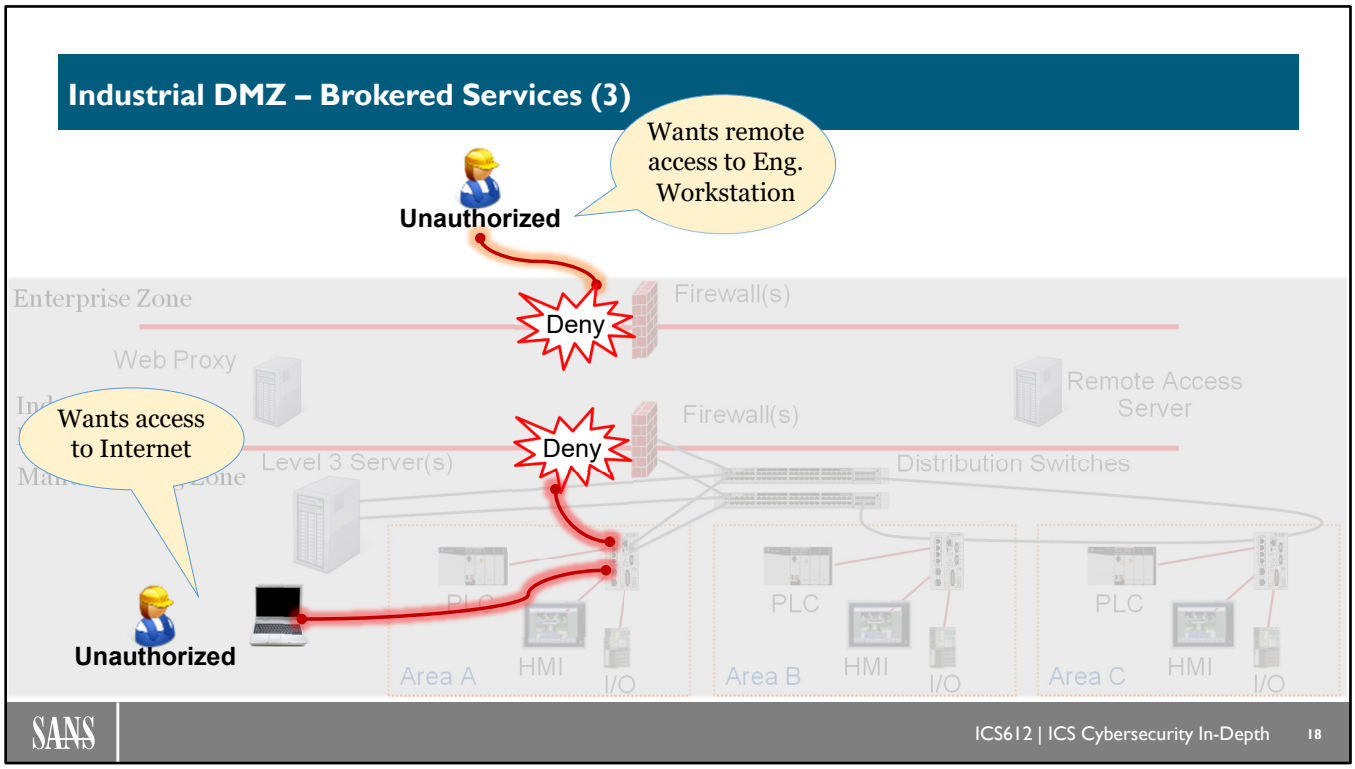
It is popular to find the following brokered services in the IDMZ:

- Web Proxy
- Managed File Transfer gateway
- Remote Access gateway (a.k.a. “jump host”)
- Historian and Database Data replication services
- Asset out-of-band management

When designing an IDMZ, one must create user scenarios and use cases to identify how Enterprise and Manufacturing users currently accomplish their daily tasks and then imagine how brokered services will enable them to continue accomplishing their daily task. It is common during the design of an IDMZ to establish a list of users, roles, and tasks along with a current data flow diagram to determine the systems that currently communicate between an Enterprise and a Manufacturing Zone asset. Doing this exercise will start to define the necessary IDMZ services required to keep the plant running while implementing the IDMZ.



Also, when designing an IDMZ one must consider what happens when an asset becomes compromised and is taken out of service for repair, replacement, or re-commissioning. Oftentimes, the Manufacturing Zone will continue running, store the important data, and then forward the information to the Enterprise systems once the IDMZ asset is reconnected and communications are restored.



For more information about designing an IDMZ see the publication *Securely Traversing IACS Data across the Industrial Demilitarized Zone*.

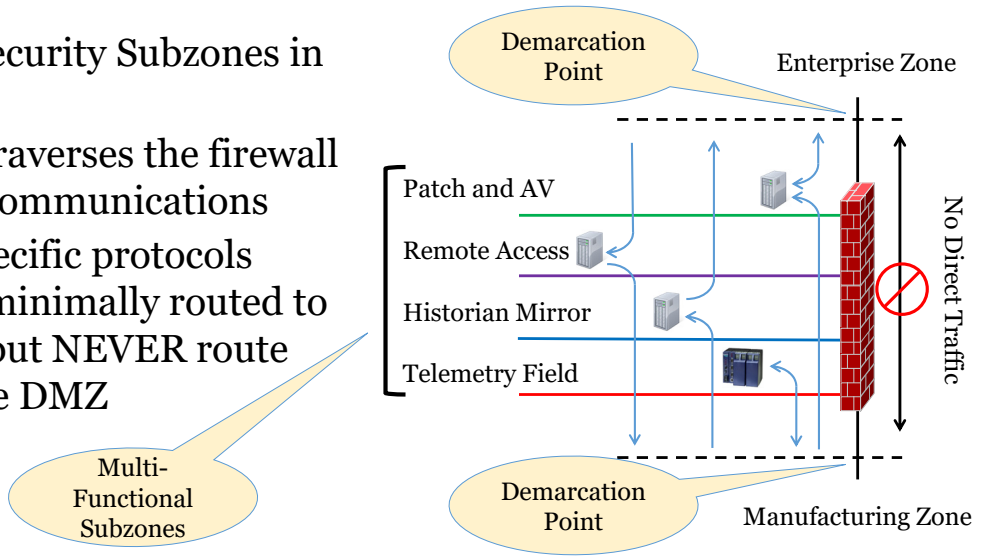
Reference:

- Cisco and Rockwell Automation (2017), *Securely Traversing IACS Data across the Industrial Demilitarized Zone*. Retrieved from https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td009_-en-p.pdf

Multizone Industrial DMZ

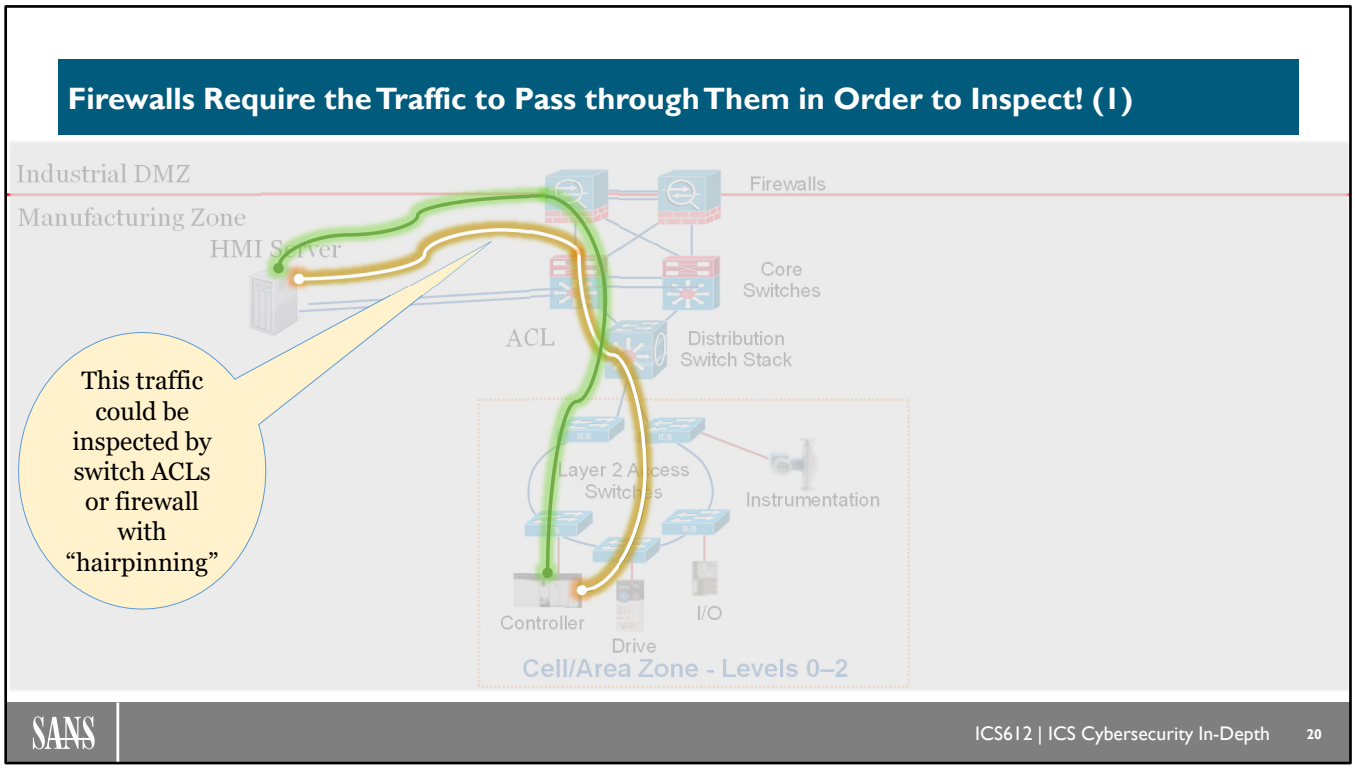
Functional Security Subzones in the IDMZ

- All traffic traverses the firewall for IDMZ communications
- Control-specific protocols should be minimally routed to the IDMZ but NEVER route through the DMZ



One method of limiting exposure of potentially vulnerable IDMZ broker services to untrusted networks is to initiate the communication from within the protected area. There are, however, times when many services need to operate across a security perimeter trust boundary and the communications need to initiate from outside the protected area. Operating multiple brokers from a single IDMZ provides the opportunity for lateral movement between brokers within the IDMZ in search of a pivot into the ICS environment. Each brokered service is typically role-specific and may have minimal, if any, relationship with the other brokered services. The level of trust between the Manufacturing Zone and the brokers should also vary depending on multiple factors including communication flow, criticality, etc. Additionally, having one broker per subzone allows complete inspection and visibility of all IDMZ communications.

For example, the telemetry field devices may have the highest level of trust (75%) to the Manufacturing Zone, but not 100% trust as it may communicate over a lower trust network medium. The Patch and AV system may have the lowest level of trust (25%) as it has two-way communication between the Enterprise and cloud services.

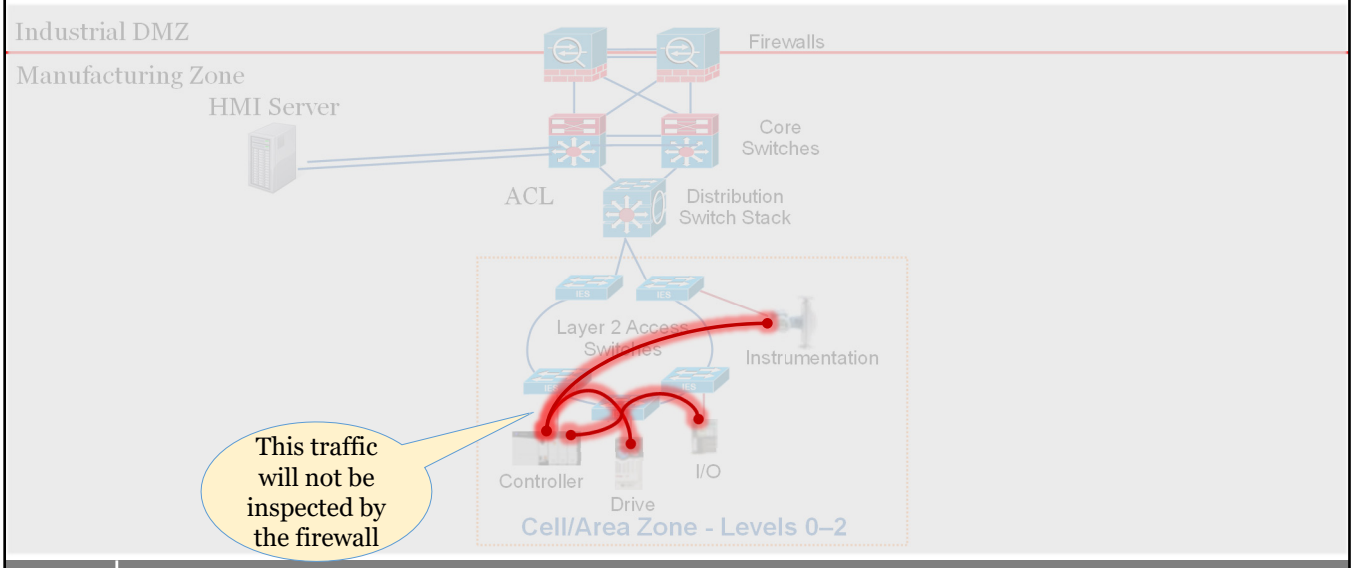


Real-time control systems are designed to minimize the number of network hops. Specifically, the real-time control traffic is never routed nor is it ever run through a firewall. This is an important point; when firewall vendors claim they can inspect control traffic, they mean they can inspect TCP or UDP traffic that is not control I/O but rather traffic that is more like HMI or Data Server traffic.

Stating the obvious, in order for a firewall to inspect traffic, the network has to be architected so the traffic flows into the firewall in either of two ways: Traffic enters one interface and exits another; or traffic is hairpinned into one interface and out the same interface.

This type of architecture limits the size of the security zones because of having to either use switch ACLs or apply more firewalls into the architecture.

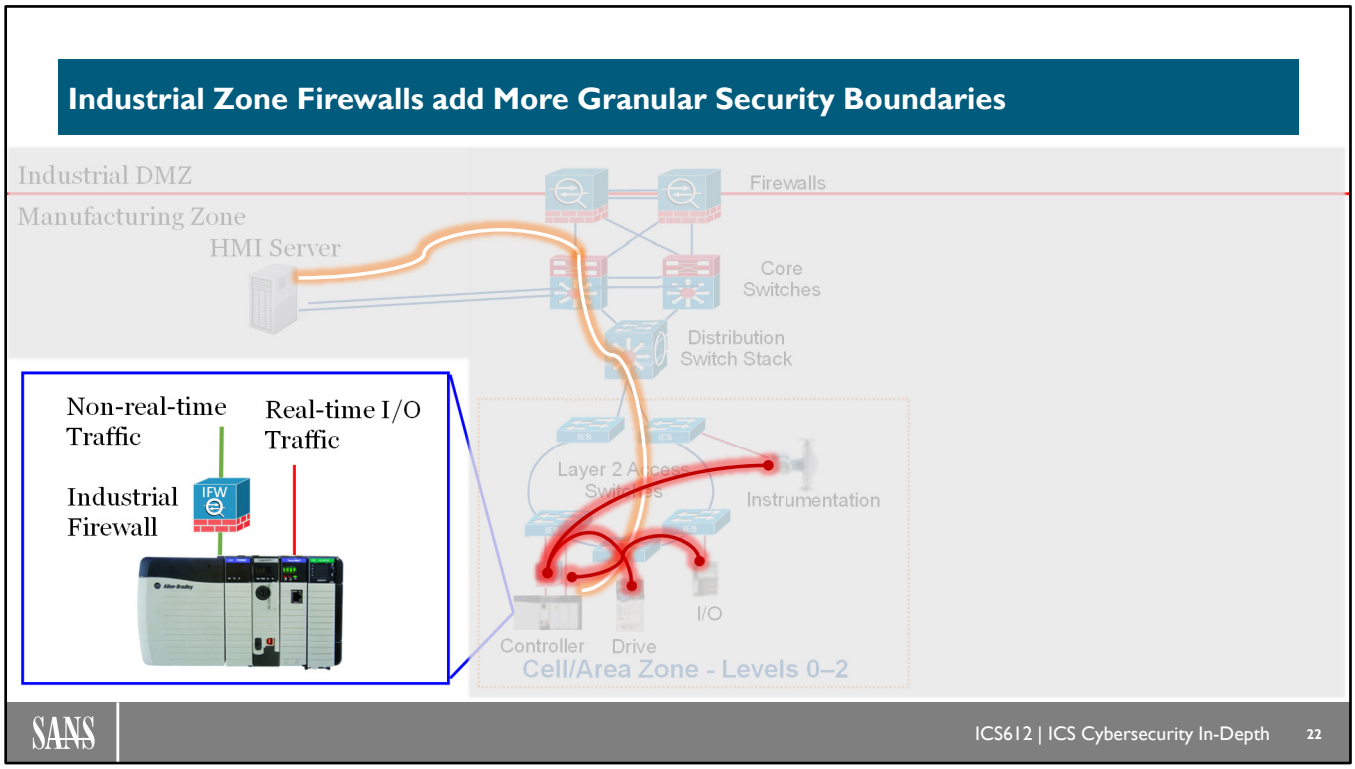
Firewalls Require the Traffic to Pass through Them in Order to Inspect! (2)



Real-time control systems are designed to minimize the number of network hops. Specifically, the real-time control traffic is never routed nor is it ever run through a firewall. This is an important point; when firewall vendors claim they can inspect control traffic, they mean they can inspect TCP or UDP traffic that is not control I/O but rather traffic that is more like HMI or Data Server traffic.

Stating the obvious, in order for a firewall to inspect traffic, the network has to be architected so the traffic flows into the firewall in either of two ways: Traffic enters one interface and exits another; or traffic is hairpinned into one interface and out the same interface.

This type of architecture limits the size of the security zones because of having to either use switch ACLs or apply more firewalls into the architecture.



ICS and infrastructure vendors have created lower-cost and ICS protocol aware firewalls. The advent of these ICS firewalls has allowed network designers to create more granular security zones.

Please note: The commercial off-the-shelf (COTS) firewalls are not meant to be placed in the real-time control I/O stream because of the latency of packet inspection. The ICS firewall is meant to stop compromised computer systems from performing malicious activities on the controller. It is important to remember this fact and architect your control system with separate communication cards and I/O communication network cards.

Lab 3.1: Implementing Local Firewall

Go to the Lab Workbook: Lab 3.1

This page intentionally left blank.

Process Operation and Enforcement Zones Checkpoint 3.1 (1)

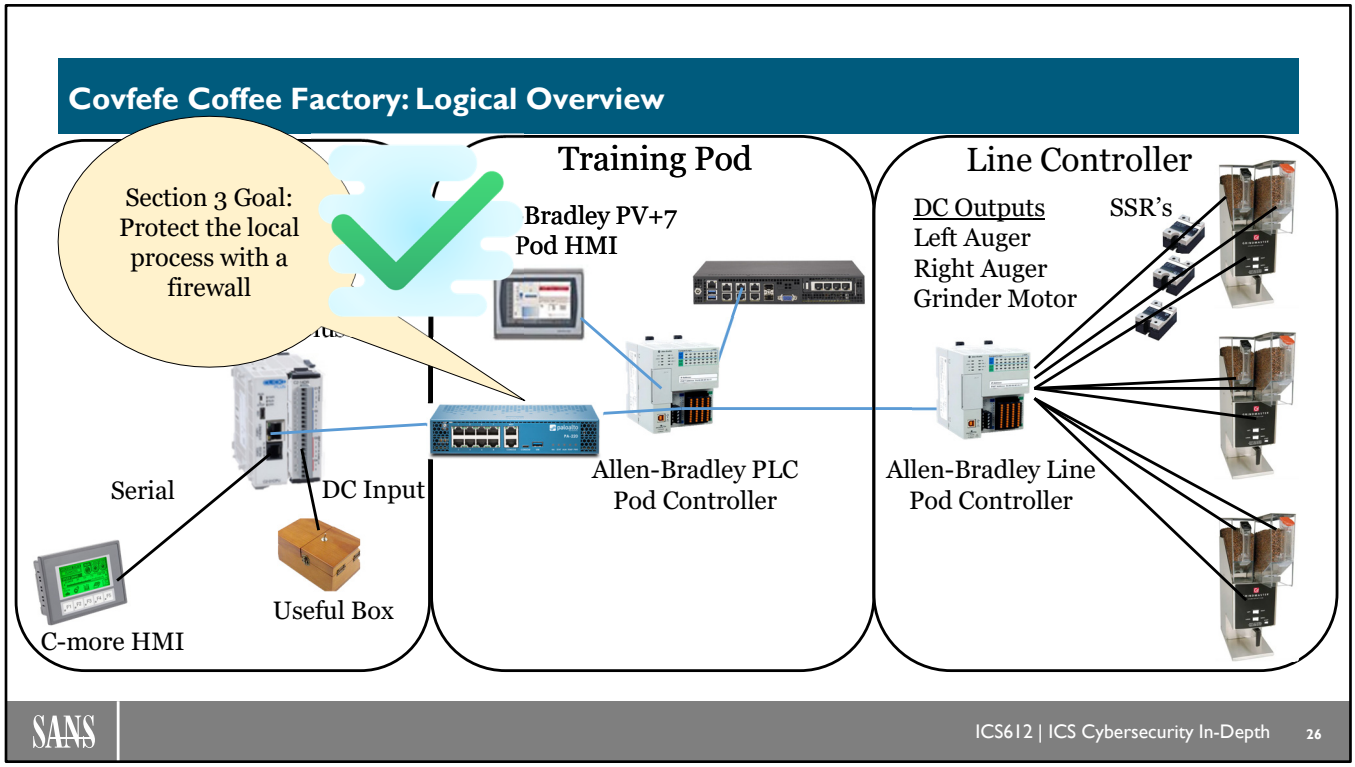
- Demilitarized Zones contain replicated or brokered services in order to hide or buffer an asset in the trusted zone from an untrusted zone
- The Industrial DMZ mimics the design of a corporate DMZ except it is placed between the Enterprise and the Manufacturing Zone.
  - We try to eliminate direct communications between the Enterprise and the Manufacturing Zone; instead, we drive the communications through a replicated service
- Firewalls define network security boundaries because they are capable of inspecting ingress and egress traffic into and out of the security zone

This page intentionally left blank.

Process Operation and Enforcement Zones Checkpoint 3.1 (2)

- Real-time control traffic inspection is not part of the firewall strategy
  - Most popular targeting strategy would come from traffic that could be inspected by a capable firewall that can understand ICS protocols
- ICS and infrastructure vendors are selling lower-cost products that are intended to be placed logically closer to the controller so as to create smaller security zones
- ICS and infrastructure vendors are also creating firewalls that have a deeper knowledge of ICS protocols
  - Inspect beyond the packet header

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.

ICS612 Section 3 Outline (3)

- Process Operation and Enforcement Zones
- Lab 3.1: Implementing Local Firewall
- Process Application Integration
- Lab 3.2: Process Historian
- ICS Environment Remote Access
- Lab 3.3: Configure and Establish Secure Remote Access
- Process Environment Network Protocol Attack Vectors
- Lab 3.4: SMB Attack
- Lab 3.5: RDP Pivot Attack
- Lab 3.6: Stage 2 Attack

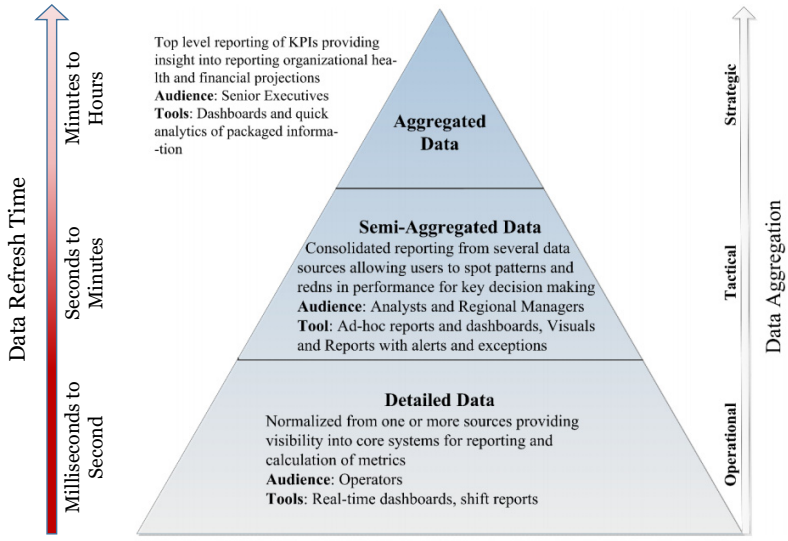
This page intentionally left blank.

Process Application Integration

Process Databases
Historians
Operator Views
Industrial Wireless Use Cases

This page intentionally left blank.

Users and Their Data



Production data has different uses throughout the organization. When we talk about 'real-time' data use we are referring to operational data. Operational data is typically used as produced from the source with minimal aggregation. This data is mostly used by either automation or operations staff to monitor the state of and make direct changes to the operation of the ICS, which requires the most current (real-time) data.

As the aggregation of the data for tactical and strategic use increases, the update (or refresh) time of the data decreases. Also, heavy aggregation of data can pull from many different and disparate sources with varying data creation and refresh capabilities, thereby limiting the overall actual data refresh time requirement for all data sources. The understanding of actual data refresh capabilities and requirements for each user, system, and data consumer can be extremely beneficial when selecting the appropriate method and architecture to use to transact the data. For example, if a cloud analytics system can only process on a 10-minute data refresh, then pulling data directly from a PLC, or its first upstream data store, delivering 100ms of data seems unnecessary. It would also add extra communication burden on the PLC and additional security concerns of having the cloud service communicate directly to the PLC. Instead, the cloud service can communicate to either a broker in a DMZ or preferably a storage in the Enterprise that is able to refresh data for the analytics system in under the 10-minute interval.

Reference:

- http://cdn.osisoft.com/learningcontent/pdfs/PISystemArchitecturePlanningAndImplementationWorkbook.pdf

Data Genesis

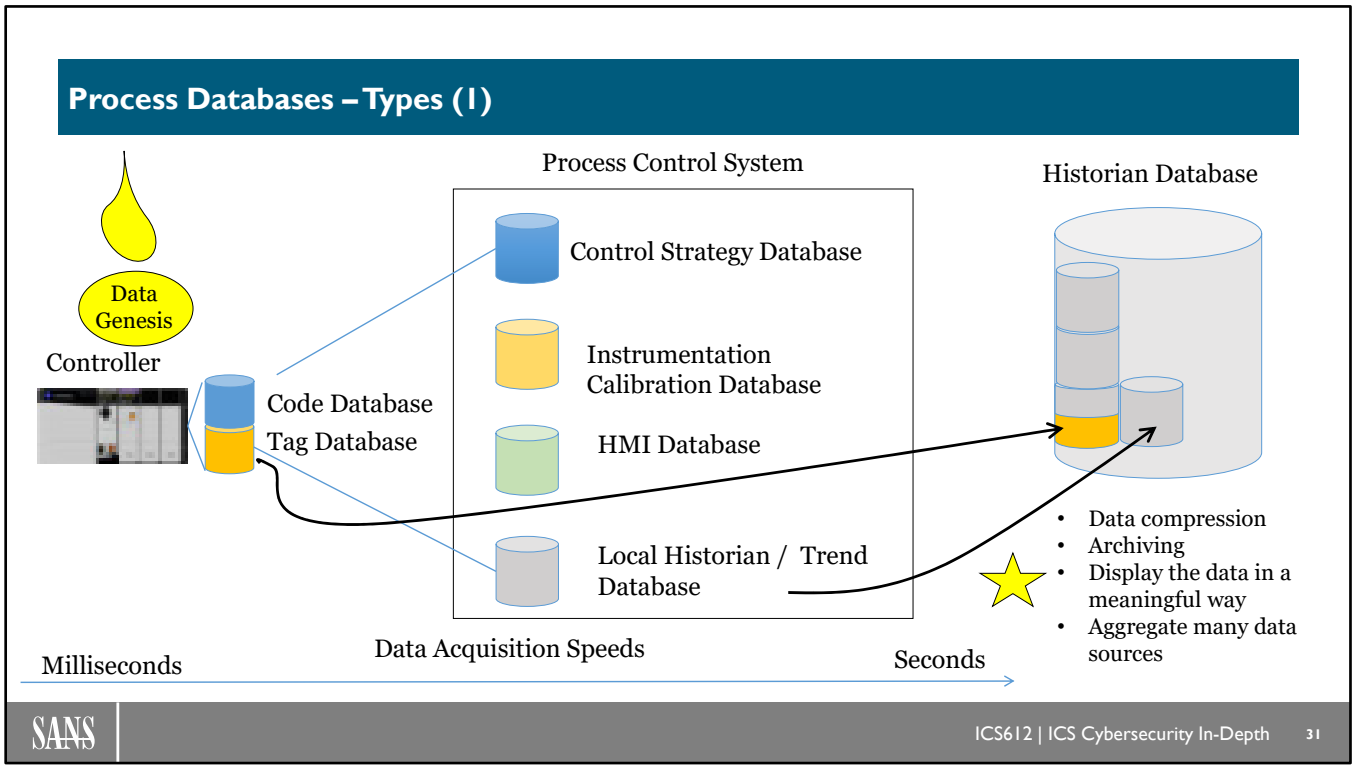
- Understanding data genesis is critical to tracing the data flow through the environment.
- Data genesis can be started on many devices within the ICS
  - A low-level device (i.e., sensors, barcode generators)
  - The first device that can associate time or other data points against a value
  - An operator input panel
- Data genesis can be event-based or time-based

It should be noted that data creation can start at the instrumentation, I/O, and PLC layers. Understanding how the data is created, moved, and stored is paramount to securing an ICS environment.

Computer systems and the associated software applications within the ICS environment certainly comprise the majority of attacks. Why? Computer systems are more commonly studied and understood and often computer programmers are writing their programs to run on COTS operating systems often found on computers, mobile tablets, phones, etc. Understanding and targeting embedded systems like a PLC or I/O subsystem requires specialized knowledge of the platform's OS and compilers, and sometimes requires access to specialized debugging hardware.

All of this illustrates that data coming from the lower levels in the architecture are trusted and consumed by higher level systems. It becomes paramount to protect the lower automation levels where the data is created so the data consumers can act on reliable and trustworthy data.

Real-time control systems rely on being able to read input values and update output values at a very predictable time period. The frequency at which a control system must measure the sensor data and correct the process through a system output is typically measured in milliseconds. Historians rely on the controller hardware to measure the data, store the data, and offload this to the Historian at a much slower rate. The controller's first priority is to read and control the process, store the data, and then offload to a higher-level system.



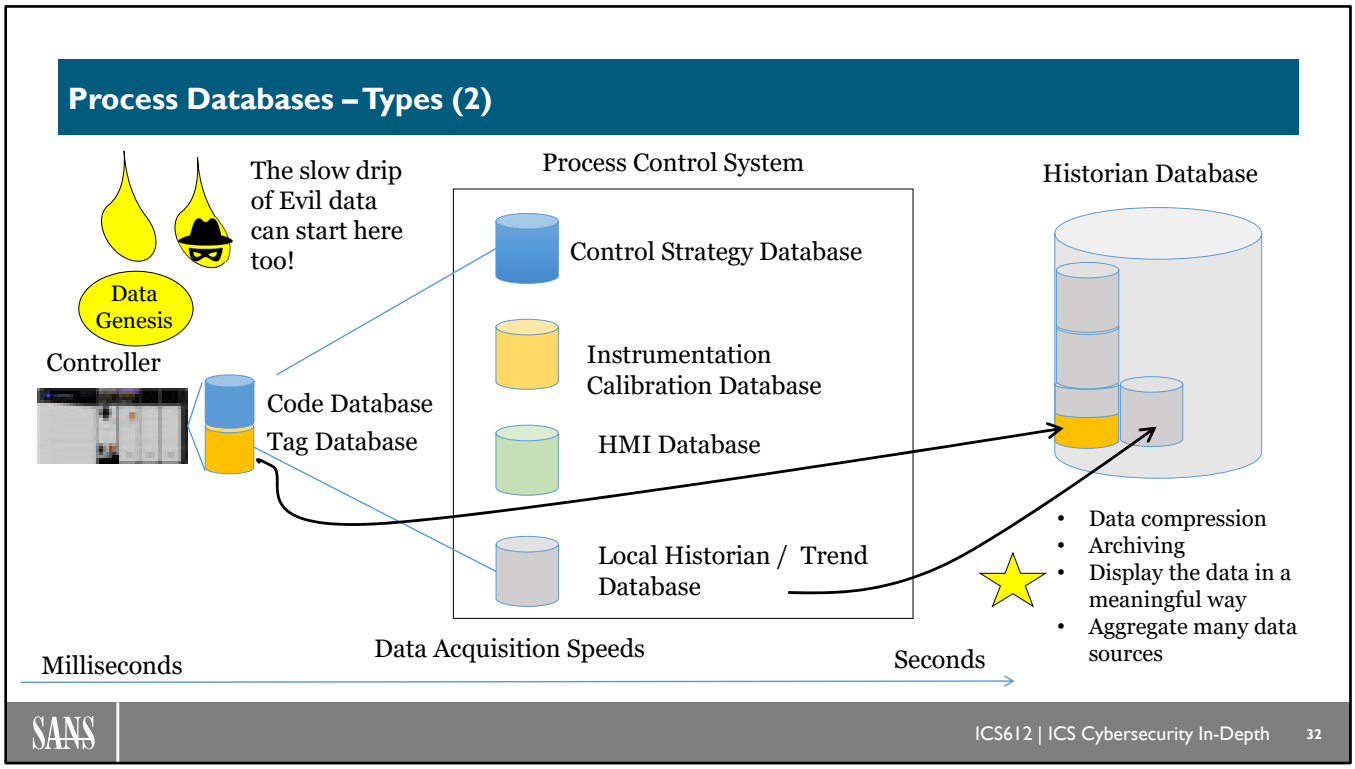
Process systems are comprised of many types of databases. For instance, the control strategy is held in a database, the instrumentation calibration information is stored in a database, and the HMI screen information is stored in a database. Oftentimes when we talk about databases as they relate to ICS or Process Control Systems, we think of capturing live data and storing this information in a database so it can be archived and displayed on a trend chart.

Historian products offer the capability to store and compress data in an effective manner and display the data in a meaningful way to an interested consumer.

In this diagram we see the controller on the left is not only capable of controlling the process but storing the critical values on board with millisecond precision. In motion applications, this would be in the microsecond precision range and most likely not consumed by the Historian.

As we continue to look at this slide and move the Process Control System or the Historian, we are showing that once we are using a computer system to poll the controller for data, the time precision changes to tenths of seconds or maybe even seconds. Network latency, controller responses to communication events, and the computer's ability to process the response are just some of the factors that will affect the jitter associated with receiving data from a controller.

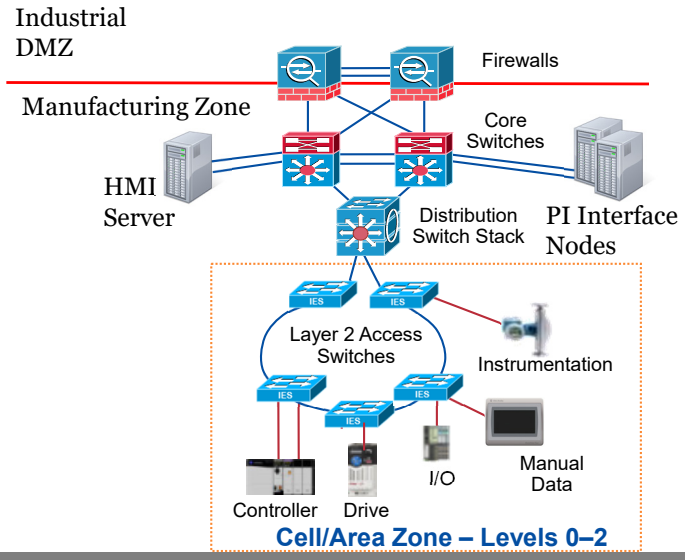
It is important to note that the precision timestamping of an event, especially if the frequency is in micro or milliseconds, will not be stamped within the Historian but rather within the controller platform. This is simply because computer systems are too far removed from the sensor and the time latency is more than a micro or millisecond. While a Historian is capable of reporting when the packet arrived, they are not capable of timestamping the actual event with any accuracy.



We also need to be aware that if we send "inaccurate" or "falsified" data from the lowest levels of our automation, this can lead to storing falsified records within our higher-level systems.

Historians – Collection Architecture

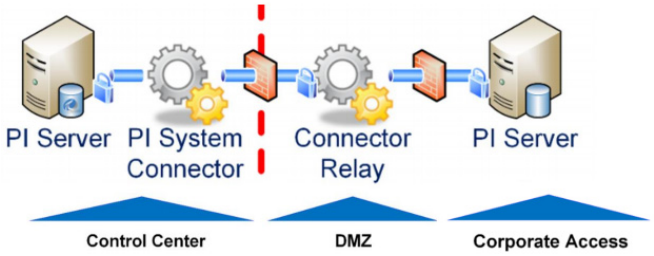
- Sources of data for collection do not always come from the primary devices (PLCs) or computer systems
- Many Historian applications require protocol gateways
  - Some companies only focus on developing gateway products
- The final database repository is usually vendor or system specific



Many people assume the data required is only sourced from the primary controls systems. However, that is not always the case and can be very specific to the organization, sector or industry. Some of the data may be from ancillary systems or even unexpected sources such as a weather station. Historian vendors are focused on collecting, compressing, calculating, storing, and in some cases, visualizing data but do not traditionally support all of the ICS protocols that exist. Instead, these vendors rely on interfacing with a protocol gateway supplied by others including those companies specifically focused on building those products. Repository of the data can include proprietary flat files or commercial off-the-shelf (COTS) databases (e.g., MS SQL).

Historians – IDMZ Architecture

- Ideally, data is transitioned (pushed) out of the protected ICS network into a lower trust zone
- The data can be every data point, selective, compressed, aggregated, or a calculated result
- Time synchronization must be considered
- Data should pass through or be stored temporarily but never processed in the IDMZ



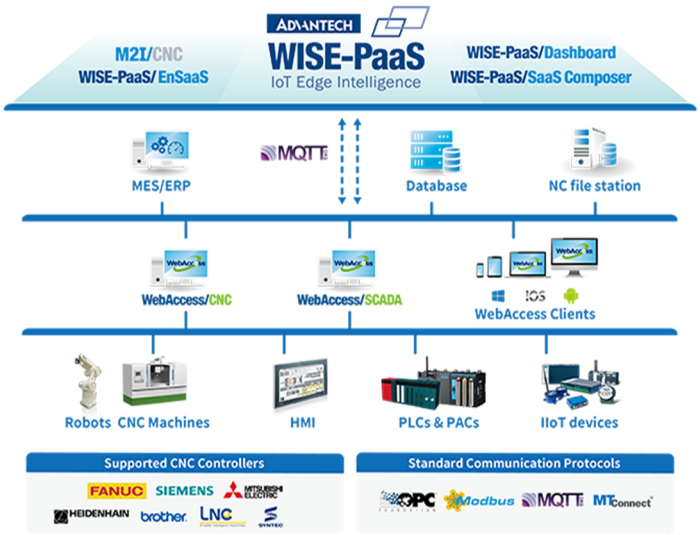
Although there is inherent operational value to Historian data, it typically requires access, or use, outside of the immediate ICS network where it is collected. For most situations, this data is read-only but some ICS implementations have used read-write features of a Historian application to issue commands or data values back to the ICS. Not every Historian application or implementation will be the same as they need to meet the specific needs of the organization. However, when considering a read-only system, pushing data up through the IDMZ architecture to a destination in a lower trust zone is the preferred method. The IDMZ broker should require little, if any, configuration to maintain small data set changes. As with data collection, the integrity of time is crucial for the type of data set being used regardless of the number of systems the data moves through or where the data is stored.

Reference:

- https://cdn.osisoft.com/osi/presentations/2017-uc-emea-london/UC17EU-D3PN05-OSIsoft-Mohan-Whats-New-in-PI-Security.pdf

HMI and Operator Interface Trends

- Traditionally local to panel or monolithic server-client applications and infrastructure
  - Many vendor-specific proprietary applications and protocols, strewn across a mostly Microsoft-based infrastructure
  - Slow to migrate, slow to adopt new technologies and business strategies
- Trend to move to a commonly available web-based architecture
  - Many variations across vendors on how graphic displays and data are served to clients
  - Allow clients to use standard web browsers



The common Human Machine Interfaces (HMI) used today are based on traditional on-prem server-client infrastructure and technologies. These monolithic systems contain many vendor-specific proprietary application protocols forcing the infrastructure requirements to a specific vendor solution. Typically applying from the client workstations, the underlying network infrastructure devices, and the servers. The rapid change of business needs has left these systems difficult and slow to migrate and adapt, resulting in many custom or complex solutions that only barely fit their needs.

Traditional methods of HMI include:

Local HMI

- All-in-one panel display
- Located directly on or near equipment
- Can be connected directly to a PLC or on a local switch

Distributed HMI

- Traditional client-server based
- Located in a control room or control center or spread out to strategic locations throughout the plant

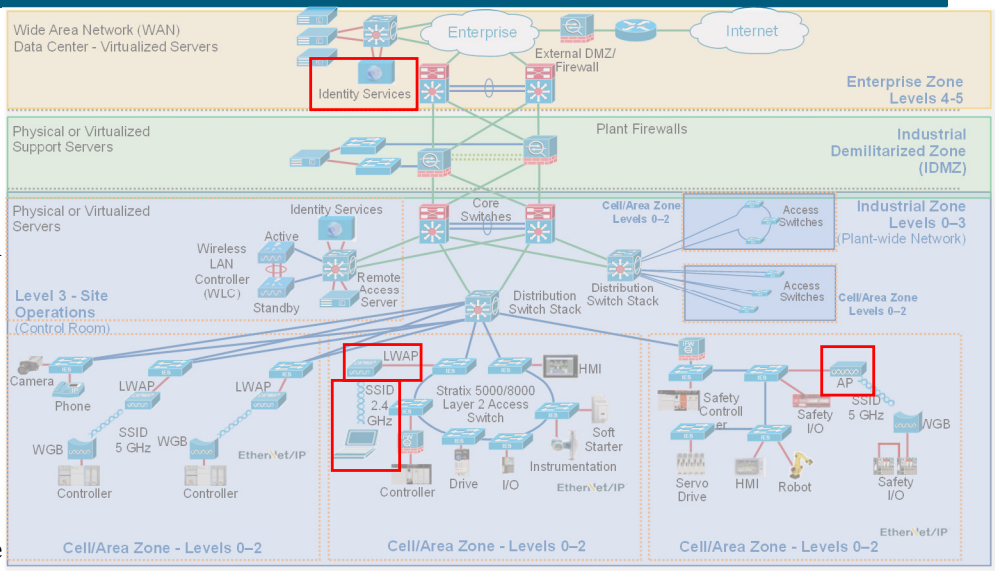
With the advancements of the user experience across a wide array of web enabled applications, new advancements have been made that bring more COTS technologies into the ICS deployments. These advancements have included better support for good security practices, making it easier for owners and operators to meet security objectives.

Reference:

➢ Image source: https://www.advantech.com/industrial-automation/webaccess/webaccesscnc

Wireless Deployments

- Wireless deployments within a manufacturing facility are typically managed by the IT staff
- Challenges include authorizing devices, applications, patch levels, etc. This is typically done in conjunction with a Mobile Device Manager (MDM)
- Most industrial customers want to leverage their existing authentication and authorization controls therefore the Industrial Zone wireless Access Point (AP) sends authentication back to the Enterprise Zone



Most wireless deployments are managed by the IT staff rather than the OT staff.

One of the biggest challenges for deploying wireless in an industrial setting is making sure the wireless coverage is not interfered with by metal structures blocking reception or by a noisy environment. A site survey is required during the wireless planning stage to ensure the coverage is as expected.

Another challenge for wireless management that is typically handled by the IT staff is making sure the devices that connect to the wireless are appropriately patched and are not running applications that are unapproved. Most larger enterprises will deploy two technologies to ensure the device is authorized for network access. First, a company will likely have a Mobile Device Management (MDM) application that ensures the connecting devices are at the appropriate patch levels and are not running unauthorized applications. Secondly, customers will deploy an appliance that enforces media access control such as the IEEE 802.11 standard. An example of such a policy enforcement device would be a Cisco Identity Service Engine (ISE) appliance.

Since the wireless management and AAA is performed within the Enterprise Zone, some organizations treat those devices, even laptops assigned to the ICS department, as untrusted and force all wireless users to use a remote access mechanism as they would for any other outside device. This method is useful for on-site third-party contractors that need to be physically connected in the ICS, have access to the control systems software and have access to internet resources.

Reference:

➢ Cisco and Rockwell Automation (2011), *Converged Plantwide Ethernet (CPwE) Design and Implementation Guide.* Retrieved from https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf

Wireless Use Cases

Wireless Application	Wireless Technology	Network Characteristics	Typical Throughput	Sensitive to Latency & Packet Loss
SCADA Peer-to-Peer Control	802.11a/g/n	Point-to-point topology	Moderate to High	Yes
Mobile HMI	802.11a/g/n	Integrated Wireless Adapters for site-wide roaming	Moderate	No
Long Haul SCADA Remote Site Connectivity	802.11a/g/n Cellular 3G / LTE WiMAX Proprietary FHSS	Outdoor point-to-point or mesh topology; small or moderate number of nodes	Low to Moderate	No
Process Instrumentation Wireless Sensors, Condition Monitoring	ISA-100.11a Wireless HART ZigBee Bluetooth	Mesh topology w/ large number of nodes, self-healing network, auto provisioning, low cost and power consumption	Low	No

Choosing the right applications for wireless media is very important. We see that major adoptions of wireless applications within the manufacturing environment include mobile HMIs, dashboard displays, and other non-real-time communication-constrained applications. There are wireless technologies such as ISA-100 and Wireless HART that have addressed the sensitivity to latency while Bluetooth provides an interface for conveniently managing the device.

Wireless networks that require routed traffic with the ICS network can be enforced at a perimeter firewall to restrict the type of traffic and the communication flow.

- Wireless reference material: Cisco and Rockwell Automation (2014), *Deploying 802.11 Wireless LAN Technology within a Converged Plantwide Ethernet Architecture*. Retrieved from: https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td006_-en-p.pdf

Reconfigure Local Network

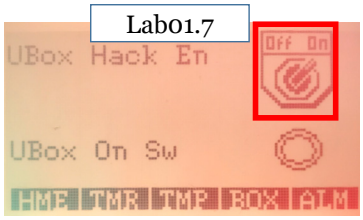
- Throughout the life cycle of an operations environment, there will be changes and modifications. Any changes will need to be reviewed and verified to ensure there are no impacts to operations.
- As cybersecurity enhancements are implemented, you may find that you need to reconfigure devices to support the modified architecture; or install software on ICS devices to work with a newly implemented cybersecurity solution.
- As you implement firewalls or new technology, consider the impacts of those devices within your architecture if they were to fail, degrade, or be misused.

This page intentionally left blank.

Preparing for Lab 3.2: Process Historian

C-more HMI

Lab01.7



C-more HMI

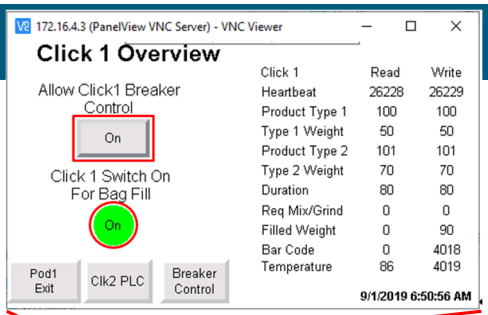
Screen	Setpoint	Value
Prod1 Sel.	Type	100
Prod1 Sel.	Wgt1	.5
Prod2 Sel.	Type	101
Prod2 Sel.	Wgt2	.7
Mix / Grind	Time	8.0

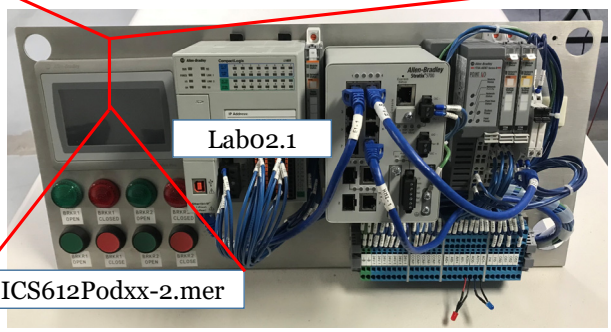
Useless Box Switch "On"

Click Plus PLC

Lab01.7

PanelView HMI





Lab02.1

ICS612Podxx-2.mer

This page intentionally left blank.

Ready to Run?

- C-more HMI
  - Ubox Hack En = On
  - Product 1 Select = 100
  - Product 1 Weight .5 <x > 5.0
  - Product 2 Select = 101
  - Product 2 Weight .5 <x> 5.0
  - Mix / Grind Time 5.0 <y> 15.00
- Click Plus PLC
  - Lab01.7 loaded
- Useless Box
  - Switch “On”
- CompactLogix PLC
  - Lab02.1 loaded
- PanelView
  - ICS612Pod[xx]-2.mer file loaded
  - Allow Breaker Control = On
  - Useless Box / Click Switch Indication = On

This page intentionally left blank.

Lab 3.2: Process Historian

Go to the Lab Workbook: Lab 3.2

This page intentionally left blank.

Process Application Integration Checkpoint 3.2

- A typical Historian software package is comprised of design software, communication configuration software and visualization software
- The Historian tag browser(s) utilize third-party communication software to gain access to the automation asset database(s)
- In critical operations, we find it is not uncommon for an operator to have a "golden" trace up on a display so they can compare how the processes are running
- Some Historian architectures are designed so a Historian server is located in the DMZ, which may require interested clients to "dive" into the DMZ to get the information. This scenario may make it challenging to author granular firewall rules, which may lead to an "any any" rule

This page intentionally left blank.

ICS612 Section 3 Outline (4)

- Process Operation and Enforcement Zones
- Lab 3.1: Implementing Local Firewall
- Process Application Integration
- Lab 3.2: Process Historian
- ICS Environment Remote Access
- Lab 3.3: Configure and Establish Secure Remote Access
- Process Environment Network Protocol Attack Vectors
- Lab 3.4: SMB Attack
- Lab 3.5: RDP Pivot Attack
- Lab 3.6: Stage 2 Attack

This page intentionally left blank.

ICS Environment Remote Access

Network Access
Encryption
Best Practice

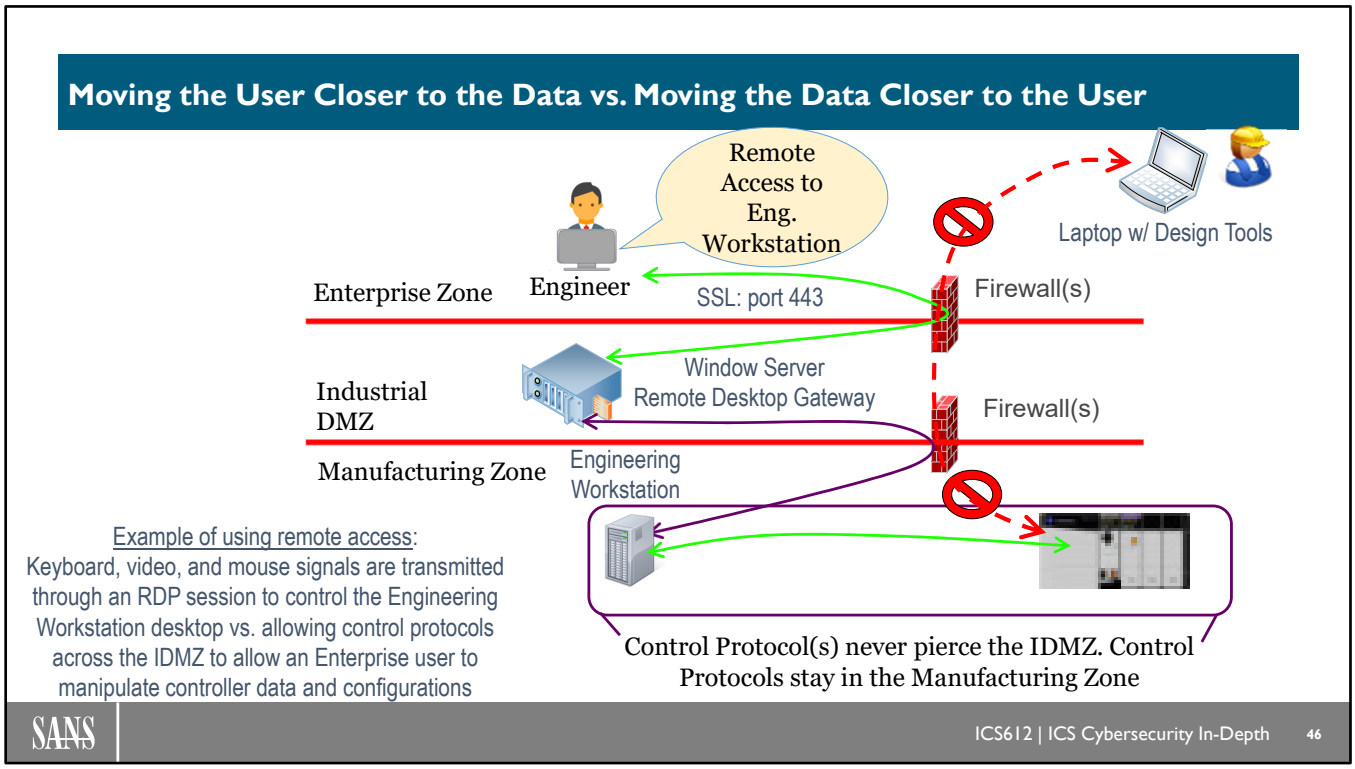
This page intentionally left blank.

ICS Remote Access Fundamentals

Objectives

- Remote access includes ALL entities initiating a connection from outside the destination zone
- This includes third-party personnel, Enterprise personnel and ICS personnel
- All user access must be authenticated, authorized, and audited (AAA)
- AAA must be performed inside the zone
- All individual user communications crossing into the destination zone must be protected by encryption
- Strong protection requires that internet-initiated communications pass Enterprise provided remote access controls before accessing ICS remote access controls

This page intentionally left blank.



Moving data closer to the user is preferred over moving the user closer to data. The idea behind this clever motto is that instead of moving control protocols around many security zones, it makes more sense to use technology like remote desktop protocols to gain access to Manufacturing Zone assets. The control system design goal is to minimize network hops not only for latency and jitter requirements but also to keep the data transactions within the Manufacturing Zone for security purposes. We also want to focus on how our communications to the other support systems like Historians, HMI servers, etc. are configured, maintained, operated, and patched through secured means. We attempt to minimize our methods of configuring, maintaining, operating, and patching our Manufacturing Zone assets, especially if we can minimize the number of ports or services, we use to accomplish our tasks. This often means that we work through remote access strategies instead of allowing design and configuration tools direct access to the Manufacturing assets from the Enterprise Zone.

Jump Host

Objectives

- Provides a common user landing pad and network abstraction for remote access
- Jump hosts provide initial access to other hosts but do not host the ICS tools
- Can be patched, monitored, audited, and disabled without impact to operations
- Multiple jump hosts allow for more complex remote access requirements
- Must be configured with multifactor authentication
- Strong protection includes additional user-level access control and encapsulation (e.g., VPN, SSL, SSH, etc.)

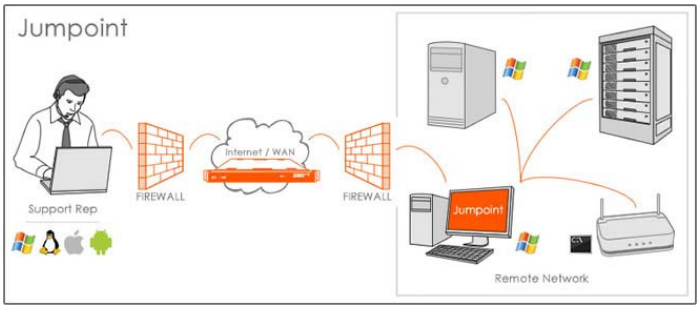
A jump host is a common or a well-known name for a server that allows remote access from an untrusted network to a trusted network. There are multiple technology providers but the qualities to look for in a good jump host are:

- They provide access to remote assets without providing ICS tools or supporting ICS protocols
- They offer scalable and redundant offerings so they can load balance for many users while offering a redundant strategy if one of the jump host boxes fails
- Utilize MFA (multifactor authentication)
- User-level access control is provided, and
- They are capable of cooperative remote access with logging. This is the ability to require an in-security-zone or on-site person to grant access before the remote session is established. This also means the actions of the remote user are logged.

Jump Host Technologies

Some jump host technologies

– Microsoft RDP Gateway, Citrix Desktop, VMware Horizon, BeyondTrust (formerly Bomgar)

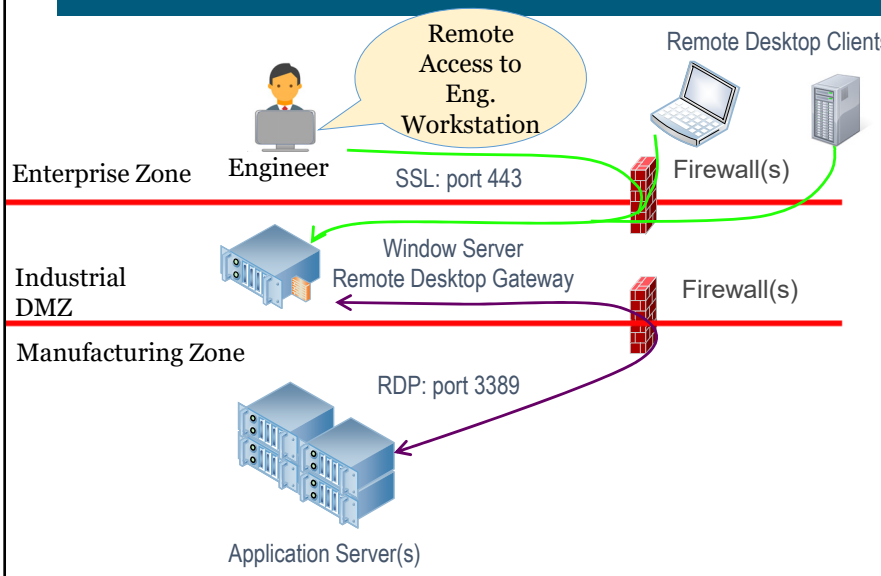


This slide references some of the most commonly found jump host technology providers

References:

- https://www.beyondtrust.com/remote-support/features/jumpoint
- Image source: https://www.beyondtrust.com/remote-support/features/jumpoint

Remote Desktop Gateway inside the IDMZ



- Microsoft Remote Desktop Gateway can be configured for 2FA or MFA
- Firewalls are often configured to allow port 443 through the firewall to the destination
- In IDMZ deployment of an RDG, it is most popular to have the user authenticate to the Enterprise Domain
- In some cases, customers will put a Domain Controller in the IDMZ, so the authentication occurs within the IDMZ zone
- Once the RDG authenticates the user, it uses 3389 to communicate with the desktop of application servers in the Manufacturing Zone

The Microsoft Remote Desktop Gateway (RDG) can be used as a jump host located in the IDMZ. This use case focuses on getting an approved Enterprise Zone asset and authorized user connected through the RDG to gain access to application servers such as an Engineering Workstation.

The RDG allows for configuring "who" can connect through "what" network to host computers through the configuration of Connection Authorization Policies (RD CAPs), computer groups, and Remote Desktop Resource Authorization Policies (RD RAPs).

RD CAPs allow you to specify who can connect to an RD Gateway server while RD RAPs allow you to specify the internal network resources that remote users can connect to through an RD Gateway server.

User-Level and Device-Level

- User-Level Authentication
  - A mechanism used to validate the person behind the keyboard
  - Strong user-level authentication includes multiple factors such as a password and a token (something known and something in possession)
- Device-Level Authentication
  - A mechanism used to validate the device being used (e.g., certificates)
  - Tying a user to a device increases the level of protection from unauthorized devices
  - Difficult to control with staff BYODs and mostly impossible to control with third-party contractors

Support for authentication of a person or a device is important for establishing a secured environment. Sometimes we only consider user-level authentication but as the ICS community moves forward with secured protocols, it's increasingly required that a device also have support for authentication.

Encryption and Certificates

- Encryption within ICS vendor products is rare
- Many uses of encryption within ICS are intended to protect external communications against eavesdropping
  - Many instances exist where encryption devices are poorly configured using weak encryption or improper key protection, even on commonly known vendors (e.g., Cisco)
- Certificate management within an ICS is complex whether using external trusted certificate authorities (CA) or internal public key infrastructure (PKI)
  - The new protocols (i.e., CIP Security) allow use of vendor-provided certificates in an attempt to maintain ease of use for implementation

Encryption is used primary to protect external communications against eavesdropping. Other use cases may include validation of users and devices from other internal networks or on zone-to-zone communications. However, care must be taken to ensure these extra-network security measures are not impactful to the operations of real-time systems or when troubleshooting operations.

Key management is crucial to the strength of the encryption. Many telemetry owners rely on third-party communication vendors (e.g., cellular) to supply encryption and control the keys. Others have attempted to use certificates as a way to protect keys, similar to what is used on the public internet. However, using public certificate authorities within an ICS network requires access to the public internet and trust of the certificate authority (CA). Implementing an in-house public key infrastructure (PKI) is not a simple task and requires a significant amount of planning, implementation, and management to protect the root certificate. This also requires additional communications access to the internal PKI.

As ICS vendors start adding encryption to their products, they struggle with these same issues relating to certificate management. Since they are not always selling to organizations with a good PKI infrastructure, they have taken steps to provide their own PKI, allowing their customers to use vendor-supplied certificates. Additionally, encrypting low-level systems within a trust boundary usually adds an unnecessary level of complexity that increases the difficulty of monitoring and responding to both malicious and non-malicious events or incidents.

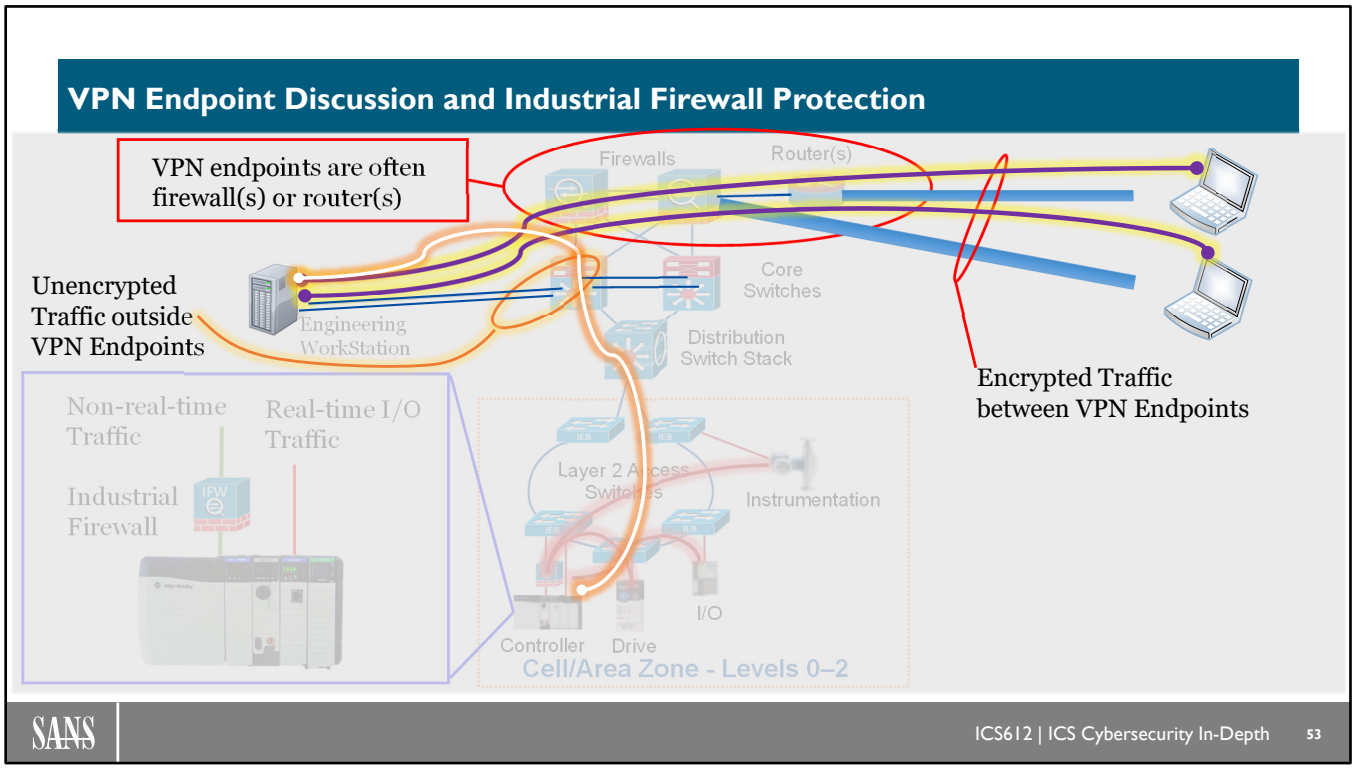
Virtual Private Network (VPN)

A connection between two entities that typically provides the following functionality:

- Protection from eavesdropping through encryption
- Protection from packet tampering through integrity hashing functions
- Protection against Machine-in-the-Middle by using authentication mechanisms
- Protection against replay attacks by using a sequence number
- Defining how data will be encapsulated during transmission between devices
- Defining what traffic should be protected

Virtual Private Networks (VPN) are an established communication connection between two endpoints. There are different parameters that can be negotiated between two VPN endpoints, but in general, VPNs provide the following functionality and benefits:

- Protection from eavesdropping through encryption
- Protection from packet tampering through integrity hashing functions
- Protection against Machine-in-the-Middle by using authentication mechanisms
- Protection against replay attacks by using a sequence number
- Defining how data will be encapsulated during transmission between devices
- Defining what traffic should be protected



The VPN endpoints are typically routers or firewalls that are capable of negotiating the VPN tenets:

- Authentication
- Encapsulation method
- Data encryption
- Packet integrity
- Keys

The traffic between the VPN endpoints is encrypted while the traffic outside the VPN tunnel is not encrypted. In the above example, the VPN tunnel is created between the two laptops and the firewall(s) and the router. The destination for the application on the laptops is to run software on the Engineering Workstation. If the two laptops attempt to do something unauthorized, then the Industrial Firewall can still be effective because the traffic between the Engineering Workstation and the controller is not encrypted.

Lab 3.3: Configure and Establish Secure Remote Access

Go to the Lab Workbook: Lab 3.3

This page intentionally left blank.

ICS Environment Remote Access Checkpoint 3.3 (1)

- The intent of a secure remote access session is to gain access and control of a trusted asset from an untrusted network in an effort to provide a service or support to operations in a fast, efficient, cost-effective, and secure manner
- A recommended remote access design utilizing jump hosts: Allow the secured session establishment to the jump host, but prevent ICS protocols or tools from being used on the jump host directly
- From a jump host architecture into an ICS environment, it is very common to utilize Microsoft's Remote Desktop Gateway service to gain remote access to our Manufacturing Zone servers

This page intentionally left blank.

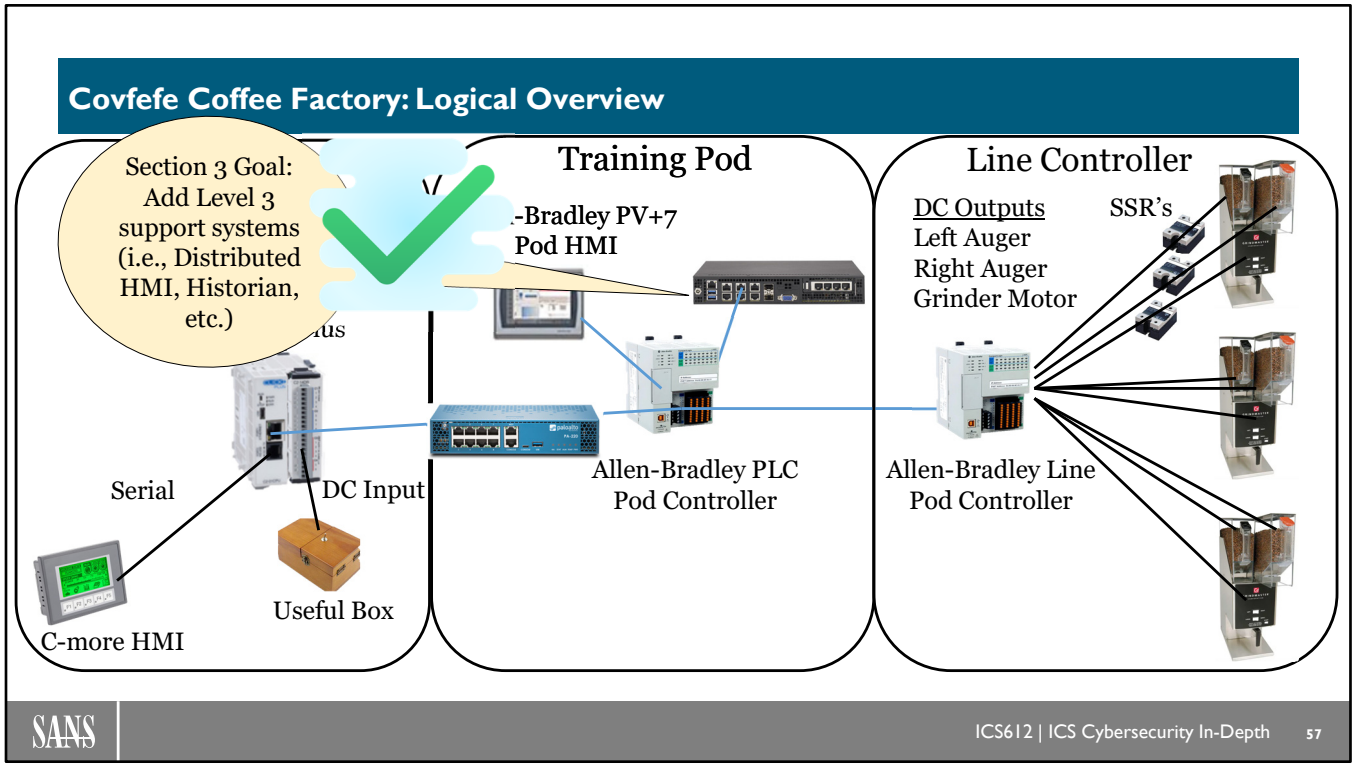
Configure and Establish Secure Remote Access Checkpoint 3.3 (2)

Microsoft Remote Desktop Gateway Pros and Cons

–Pros
- Readily available – simply add the role to a Microsoft Server
- Ability to authenticate user and device
- Ability to define specific user and computer-level authorization

–Cons
- Device authentication less prevalent with third-party devices
- Certificate management process or a PKI infrastructure required

This page intentionally left blank.



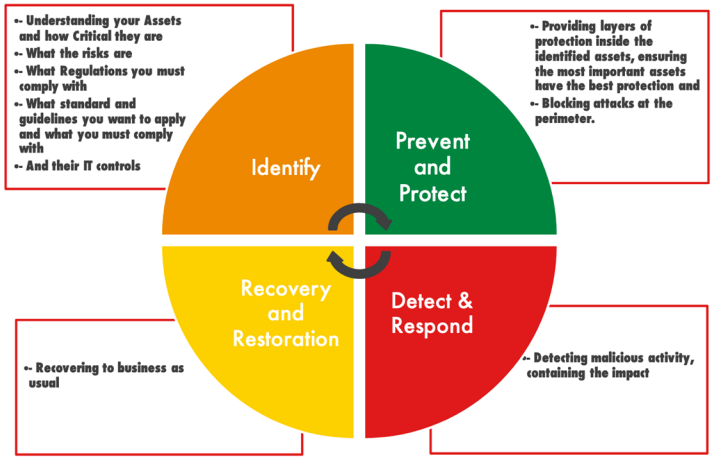
As we look at Levels 0 and 1 hands-on exercises, we will use two systems to achieve the PLC and HMI learning objectives. In the middle of the slide, you will see the training Pod hardware that consists of an Allen-Bradley PanelView HMI and the Allen-Bradley (A-B) CompactLogix PLC. The training Pod also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

Case Study: Shell's Balanced Cybersecurity Program

Balanced Cyber Security Program

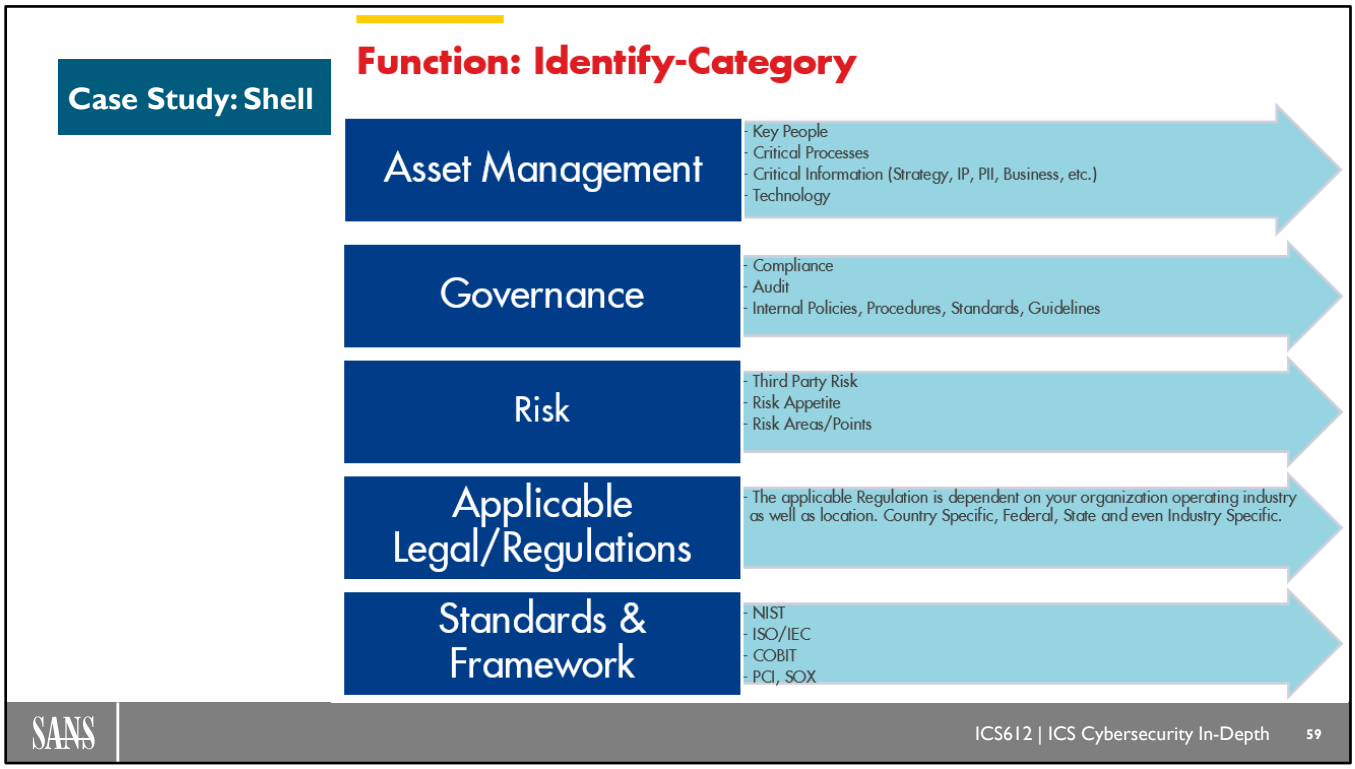
Core Cyber Security Functions



Shell utilizes the NIST Cybersecurity Framework to approach their cybersecurity programs and to communicate their goals to vendors and other third-party service providers. Shell has been actively working with their vendors to assist with architectures, technology selection, deployment, and workforce training.

Reference:

- https://web.archive.org/web/20190819115530/http://www.wwenergyconference.com/wp-content/uploads/2017/03/FINAL-Cyber-Security-Panel-Shell.pdf



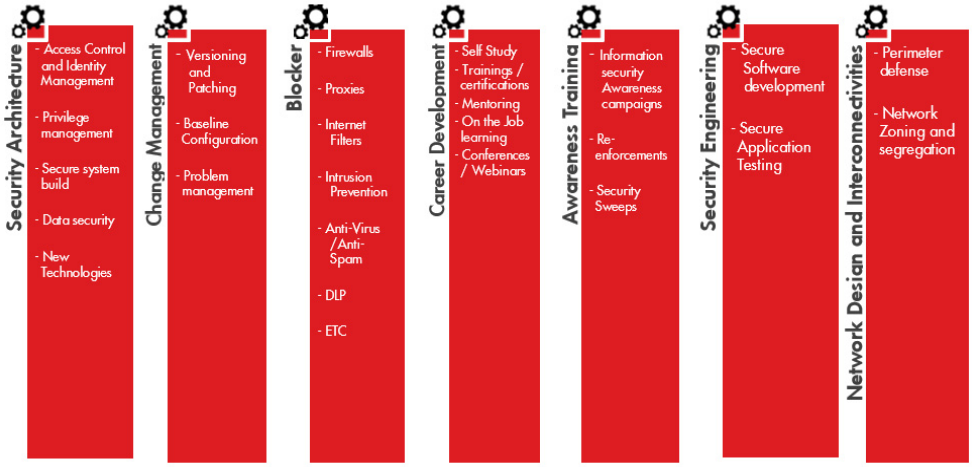
In this table we see how Shell works through their framework. This list satisfies their "Identify" category. It is important to note they follow other standards and frameworks as well.

Reference:

- https://web.archive.org/web/20190819115530/http://www.wwenergyconference.com/wp-content/uploads/2017/03/FINAL-Cyber-Security-Panel-Shell.pdf

Case Study: Shell (1)

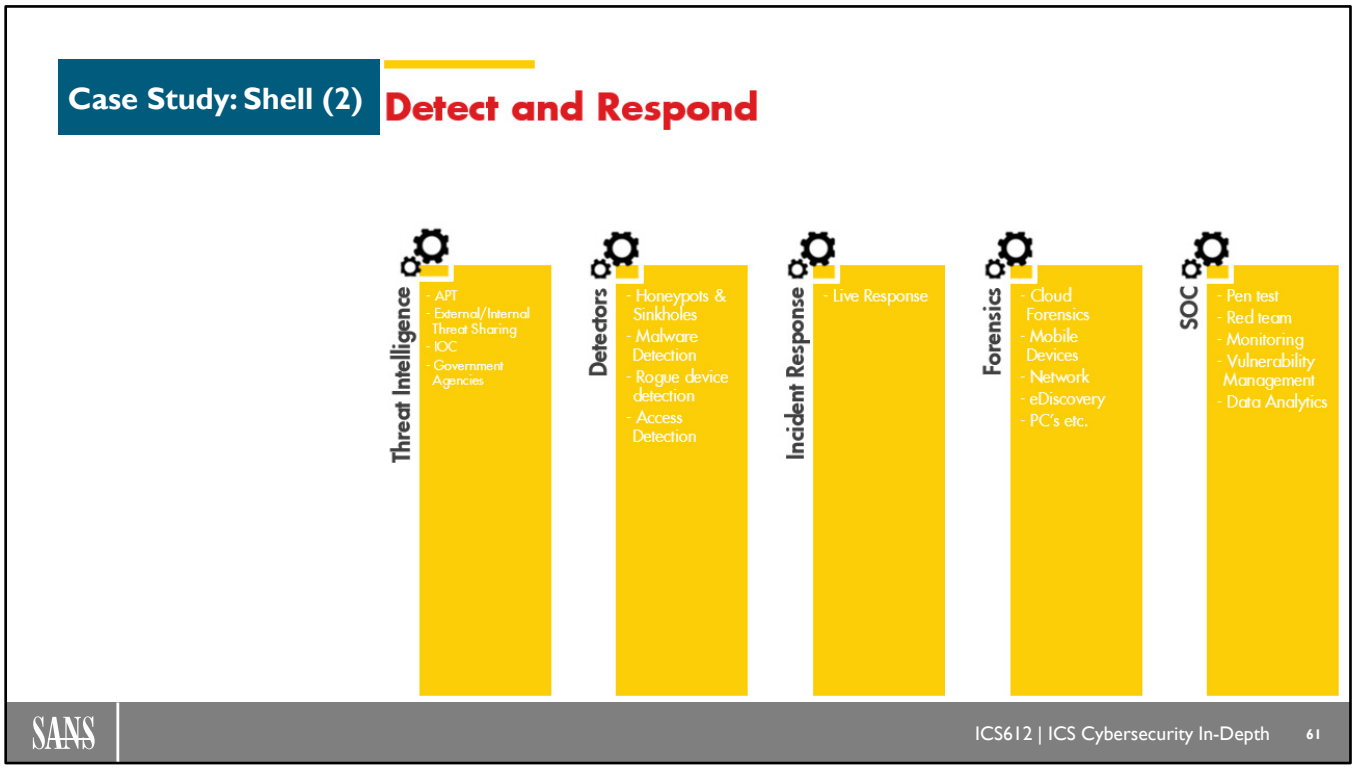
Prevent and Protect



This slide represents how Shell addresses security architectures, change management, technical controls, training, and network monitoring.

Reference:

- https://web.archive.org/web/20190819115530/http://www.wwenergyconference.com/wp-content/uploads/2017/03/FINAL-Cyber-Security-Panel-Shell.pdf

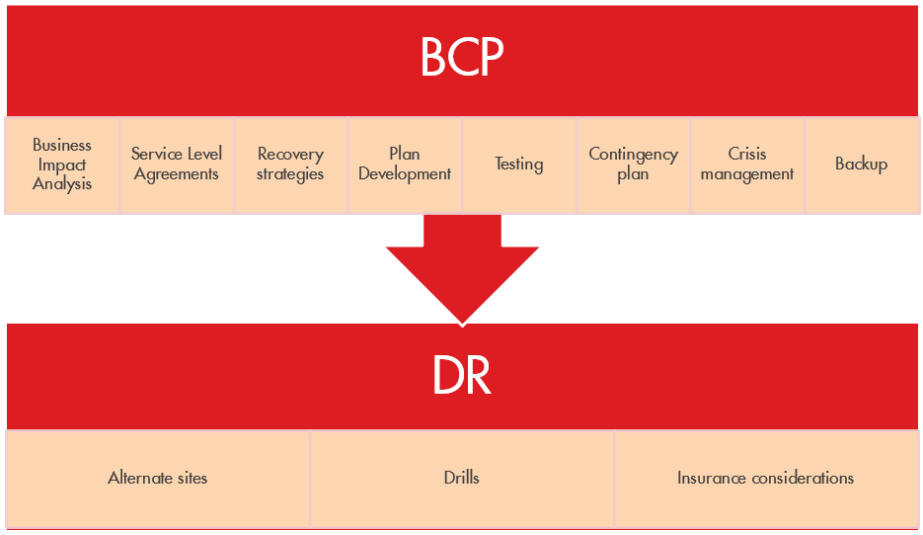


In the Detect and Respond category, we can see the categories and technologies used for detecting an event and how Shell coordinates a response.

Reference:

- https://web.archive.org/web/20190819115530/http://www.wwenergyconference.com/wp-content/uploads/2017/03/FINAL-Cyber-Security-Panel-Shell.pdf

Case Study: Shell (3) Recovery and Restoration



Recovery and Restoration is an important category indicating how Shell will operate after an event has occurred and how Shell trains for such incidents.

Reference:

- https://web.archive.org/web/20190819115530/http://www.wwenergyconference.com/wp-content/uploads/2017/03/FINAL-Cyber-Security-Panel-Shell.pdf

Case Study: Shell, Rockwell Automation, Cisco, Microsoft, and AT&T (1)

"We've been working on cybersecurity since 1993, and we've had a lot more 'uh-oh' moments than 'aha' moments. We understand the value of connectivity, applying analytics, cloud computing and augmented reality, and the challenge with cybersecurity is people want it done today, but it's really a long-term journey."

"Our problem is that everyone is talking about the cloud, but we're still trying to patch Windows 3.1 software in some locations."

"We're trying to do traditional, labor-intensive patching from 30 suppliers, so let's get automation blacklisting protection done before we try to protect against advanced persistent threats."

- Tyler Williams, Global Technology Leader for Industrial Cybersecurity, Shell Global Solutions.

"We appreciate that it's important to invest in new technologies, but many of them don't yet work with how we're operating at our 137 plants"

Shell has been aggressive in partnering with their vendors to help with their ever-challenging cybersecurity solutions and deployments. Executive sponsorship is key to any successful cybersecurity initiative and that was evident in a panel discussion between the leaders of Shell, Rockwell Automation, Cisco, Microsoft, and AT&T. As Shell's Global Technology Leader for Industrial Cybersecurity Tyler Williams has pragmatically realized, throwing new technology at an operational environment is not the answer as their operational business needs cannot withstand a quick technology implementation that doesn't accommodate their operational requirements.

Reference:

- https://www.industryweek.com/connected-enterprise/cybersecurity-makes-connected-enterprise-possible

Case Study: Shell, Rockwell Automation, Cisco, Microsoft, and AT&T (2)

"Williams agreed that the cloud can aid cybersecurity, and reported that Shell will get to it, but he cautioned that it can't be done overnight. 'You can't throw all this onto 55-year-old engineers at once,' added Williams. 'We must be allowed to do basic cybersecurity first, and not be bombarded by sales calls about the latest shiny tools. Right now, there's a chasm between our business model and all the cool tools, but we're going to have cybersecurity solutions in place in five years that will be improved by an order of magnitude.'"

"There's still a lot of fear, uncertainty and doubt about cybersecurity, but that's an ineffective way to motivate people, and doesn't give them the common business model it needs. Cybersecurity is an opportunity, and implementing it can help users reduce costs."

- Tyler Williams, Global Technology Leader for Industrial Cybersecurity, Shell Global Solutions.

"It's just important to appreciate the time it takes to operationalize security before the next bolt-in product arrives, and then show what business benefit it actually has."

Shell realized that a cybersecurity technology rollout required not only a good business case but equally important a workforce trained to support these technologies. Paraphrasing Tyler's comments, as Shell pragmatically chooses the technology they deploy, they will receive benefits in an exponential manner.

Reference:

- https://www.industryweek.com/connected-enterprise/cybersecurity-makes-connected-enterprise-possible

ICS612 Section 3 Outline (5)

- Process Operation and Enforcement Zones
- Lab 3.1: Implementing Local Firewall
- Process Application Integration
- Lab 3.2: Process Historian
- ICS Environment Remote Access
- Lab 3.3: Configure and Establish Secure Remote Access
- Process Environment Network Protocol Attack Vectors
- Lab 3.4: SMB Attack
- Lab 3.5: RDP Pivot Attack
- Lab 3.6: Stage 2 Attack

This page intentionally left blank.

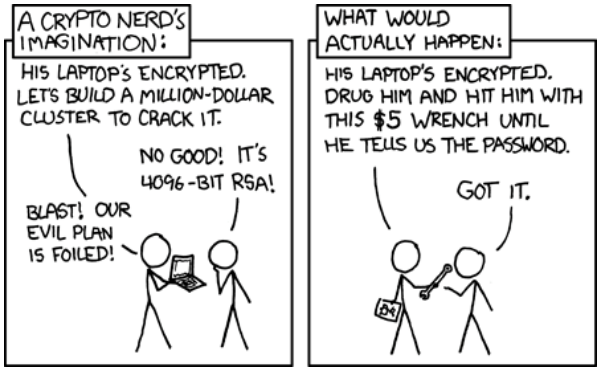
Process Environment Network Protocol Attack Vectors

Host-to-Device Communications
Remote Access Communications
Device-to-Device Communications

This page intentionally left blank.

Common Examples of Insecure IT Protocols

- Insecure IT protocols commonly found in the ICS environments
  - Telnet
  - HTTP
  - SNMPv1/2
  - FTP
- Secure alternative IT protocols
  - SSH
  - HTTPS
  - SNMPv3
  - SFTP



Many insecure IT protocols are widely used throughout the process environment. Some of this is due to legacy equipment that does not support more secure protocols. Some of this is due to compatibility or ease-of-use concerns. However, it is mostly due to vendors, integrators, and operators not understanding the security implications of using these insecure protocols.

Reference:

- Image source: https://imgs.xkcd.com/comics/security.png

Internet Control Message Protocol (ICMP)

- The **Internet Control Message Protocol (ICMP)** is part of the Internet Protocol (IP) suite
  - Operates at Layer 3 of the OSI Model
  - Used by diagnostic tools such as ping and traceroute
- Can be abused by attackers
  - Mapping out the network to aid additional attacks
  - Denial-of-service attack (e.g., Ping of Death, ping flooding)
  - Covert channel (i.e., exfiltrate data in ICMP packets)

The Internet Control Message Protocol (ICMP) is part of the Internet Protocol (IP) suite and because it operates at Layer 3 of the OSI Model, it does not have a TCP or UDP port associated with it.

ICMP is widely used as follows:

- To troubleshoot network connectivity issues (e.g., ping)
- As a type of heartbeat protocol that monitors the availability of systems (e.g., ping)
- To identify a possible route for an IP packet to travel (e.g., traceroute)

Attackers can abuse ICMP in multiple ways.

- ICMP can be used to map out the network, allowing an attacker to get a better understanding of how the network is laid out. The attacker could then use this information to identify systems that are possible pivot points or identify valuable targets.
- ICMP has been used in several different types of denial-of-service attacks. The Ping of Death attack used malformed ping packets that caused systems to crash because these systems were not designed to properly handle the malformed ping packets. A ping flooding attack overwhelms the victim's system with ICMP packets (e.g., Smurf or Fraggle attacks).
- ICMP can also be used as a convert channel. ICMP error messages contain a data section that an attacker can use to exfiltrate data out of an environment.

Simple Network Management Protocol (SNMP)

- The **Simple Network Management Protocol (SNMP)** is used for collecting information from managed devices or making changes to their configurations
- Three main SNMP versions
  - SNMPv1 – Initial implementation of SNMP
  - SNMPv2 – Added improvements to performance and security
  - SNMPv3 – Added security improvements such as authentication and encryption
- Attackers monitoring the network can see the SNMP **community string** in cleartext for SNMPv1 and potentially hashed for SNMPv2

The Simple Network Management Protocol (SNMP) is used for collecting information from managed devices or making changes to their configurations.

SNMP Agent listens on UDP Port 161 for requests from the SNMP Manager
SNMP Manager listens on UDP Port 162 for traps from the SNMP Agent

Three main SNPM versions

- SNMPv1 – Initial implementation of SNMP
- SNMPv2 – Added improvements to performance and security
- SNMPv3 – Added cryptographic security such as authentication and encryption

The SNMP **community string** authenticates access to Management Information Base (MIB) objects, which contain variables that describe the system's status and configuration. There are three different types of community strings: Read-only, read-write, and trap.

Attackers monitoring the network can see the SNMP **community string** in cleartext for SNMPv1 and potentially hashed for SNMPv2, if it is properly configured. SNMPv3 does not use community strings but uses SNMP users, which serve the same purpose.

References:
- https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

Domain Name System (DNS)

- The **Domain Name System (DNS)** is responsible for resolving a request for a network resource by name, typically a computer name, to an IP address
- Can be abused by attackers
  - DNS spoofing (previously discussed)
  - DNS tunneling (i.e., encoding data in DNS queries and responses)

The Domain Name System (DNS) is responsible for resolving a request for a network resource by name, typically a computer name, to an IP address. DNS is a fundamental building block of the internet. Without DNS, SANS students would have to remember that www.google.com is located at 172.217.169.4, instead of just being able to type in the URL.

As previously discussed in Section 2, DNS spoofing and DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record, e.g., an IP address. This results in traffic being diverted to the attacker's computer (or any other computer).

DNS tunneling is a method of cyber attack that encodes the data of other programs or protocols in DNS queries and responses. DNS tunneling can be used to exfiltrate data or even as a Command and Control (C2) channel.

References:
- https://en.wikipedia.org/wiki/Domain_Name_System
- https://en.wikipedia.org/wiki/DNS_spoofing
- https://www.infoblox.com/glossary/dns-tunneling/
- Image source: https://imgs.xkcd.com/comics/google_announcement.png

Server Message Block (SMB) (1)

- The **Server Message Block (SMB)** Protocol is a network file-sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol.
  - Can also be used for printing over a network, network browsing, etc.
  - Unix-like version of SMB is called **Samba**
- Microsoft SMB Protocol is most often used as an application layer or a presentation layer protocol, and it relies on lower-level protocols for transport.
- What account does SMB run as?

Although its main purpose is file sharing, additional Microsoft SMB Protocol functionality includes the following:

- Dialect negotiation
- Determining other Microsoft SMB Protocol servers on the network, or network browsing
- Printing over a network
- File, directory, and share access authentication
- File and record locking
- File and directory change notification
- Extended file attribute handling
- Unicode support
- Opportunistic locks

What account does SMB run as? SMB runs on Windows as "**LocalSystem**".

Reference:

- https://docs.microsoft.com/en-us/windows/win32/fileio/microsoft-smb-protocol-and-cifs-protocol-overview

Server Message Block (SMB) (2)

Since 2001, Microsoft has released 18 Security Bulletins related to SMB	Categorization		
	Critical	Important	Moderate
Remote Code Execution	10	5	
Elevation of Privilege		1	
Denial of Service		1	
Not a Vulnerability			1

Since 2001, Microsoft has released 18 Security Bulletins related to SMB.

10 of the 18 Security Bulletins had a severity rating of "**Critical**".
15 of the 18 Security Bulletins had an impact rating of "**Remote Code Execution**".

Reference:
- Data source: https://www.microsoft.com/en-us/download/details.aspx?id=36982

SMB Vulnerability – EternalBlue

Exploits a vulnerability in Microsoft's implementation of the Server Message Block (SMB) Protocol

- Reportedly Developed by the US National Security Agency (NSA)
- Leaked by *Shadow Brokers* hacking group in 2017
- Used in *WannaCry* and *NotPetya* malware
- Microsoft Security Bulletin MS17-010 (a.k.a. EternalBlue)

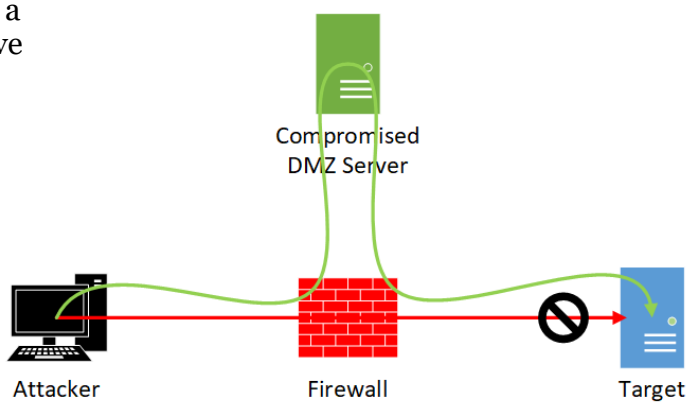
It is typical for ICS system integrators and controls engineers to understand ICS protocols and some basic IT protocols, such as telnet and ftp, that are available or used in the ICS. The backend Microsoft protocols used to communicate between Microsoft hosts are generally less understood. Amongst these protocols is the SMB Protocol. Because of its inherent ease of use, the minimal user understanding required, and its effectiveness in helping to complete tasks (i.e., move files), this protocol has been taken for granted in the ICS. The wide availability of this protocol combined with the mostly misunderstood risk it presents has fueled the success of WannaCry and NotPetya malware to propagate into and throughout the ICS network.

References:

- https://en.wikipedia.org/wiki/EternalBlue
- https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

Pivoting

- **Pivoting** is the unique technique of using an instance (also referred to as a 'plant' or 'foothold') to be able to move around inside a network
  - Basically, use the first compromised system to help compromise other otherwise inaccessible systems
- Examples of pivoting
  - Port Forwarding/Redirection
  - SSH/HTTP Tunneling
  - SOCKS Proxy



Pivoting is the unique technique of using an instance (also referred to as a 'plant' or 'foothold') to be able to move around inside a network. Basically, use the first compromised system to help compromise other otherwise inaccessible systems

Examples of pivoting

- Port Forwarding/Redirection
- SSH/HTTP Tunneling
- SOCKS Proxy

Reference:

➢ https://www.offensive-security.com/metasploit-unleashed/pivoting/

Common Platform and Tools to Perform Attack (1)

- Kali Linux
  - Kali Linux is an open-source penetration testing platform/distro that is maintained and funded by Offensive Security
- Metasploit
  - Metasploit is an open-source project that provides the infrastructure, content, and tools to perform penetration tests and extensive security auditing
- Nmap
  - Nmap ("Network Mapper") is a free and open-source utility for network discovery and security auditing

Most penetration testers will use easily available attack tools like those found on Kali Linux and Metasploit. These are tools we will use in these labs as we aren't expecting our students to create their own attack tools. It should be noted, adversaries will create and share their own tools such as BlackEnergy, BlackEnergy2, and Trisis. As we protect our ICS environments, become familiar with the Kali tools.

References:
- https://www.kali.org/
- https://metasploit.help.rapid7.com/docs
- https://nmap.org/

Common Platform and Tools to Perform Attack (2)

- Cobalt Strike
  - Red team tool used to emulate adversary TTP
- Mimikatz
  - Mimikatz can extract plaintext passwords, hashes, PIN codes, and Kerberos tickets from memory
  - Mimikatz can also perform pass-the-hash and pass-the-ticket, or build Golden Tickets

Attackers commonly use Mimikatz to steal credentials and escalate privileges. In most cases, endpoint protection software and antivirus systems will detect and delete it. Pen testers use Mimikatz to detect and exploit vulnerabilities in your networks so you can fix them.

References:

- https://blogvaronis2.wpengine.com/what-is-mimikatz/
- https://github.com/gentilkiwi/mimikatz
- https://www.cobaltstrike.com/

Lab 3.4: SMB Attack

Go to the Lab Workbook: Lab 3.4

This page intentionally left blank.

Process Environment Network Protocol Attack Vectors Checkpoint 3.5

- It is important to understand the process that adversaries use to assess the environment and leverage it to build an operational understanding from within.
- In their initial efforts to understand the environment, adversaries will commonly use tools and exploits targeting known vulnerabilities.
- Scanning an environment and discovering systems with TCP Port 445 (i.e., SMB) open could be interesting to an adversary as they may then interact with the discovered systems to see if any are vulnerable to a known SMB exploit like EternalBlue.
- After identifying any systems actively communicating on TCP Port 445 and vulnerable to EternalBlue, adversaries can then run additional exploit tools like Mimikatz to dump cleartext credentials.
- Having access and credentials can then enable the next stage of the attack.

This page intentionally left blank.

Lab 3.5: RDP Pivot Attack

Go to the Lab Workbook: Lab 3.5

This page intentionally left blank.

Process Environment Network Protocol Attack Vectors Checkpoint 3.6

- Remote access is used to connect from an untrusted network to a trusted zone asset
- As an adversary leverages capabilities and footholds gained in previous stages of an attack, it is quite likely that an adversary would target remote access and gain entry by leveraging internal footholds and trusted user credentials
- This was the specific approach used in the Ukraine 2015 attack against three different distribution utilities that resulted in power outages for more than a quarter million customers

This page intentionally left blank.

Lab 3.6: Stage 2 Attack

Go to the Lab Workbook: Lab 3.6

This page intentionally left blank.

Process Environment Network Protocol Attack Vectors Checkpoint 3.7

- With a foothold in the target environment and access to trusted user credentials, adversaries can manipulate the network infrastructure and security controls directly
- This capability allows adversary groups to impact access to systems, networks, user groups, remote access, data sets, and anything else of interest that an administrator role would traditionally manage
- Manipulating routing within an environment can truly give a remote adversary the ability to have a long dwell time in the target environment as well as the ability to achieve broad impacts

This page intentionally left blank.

Section 3 Summary (1)

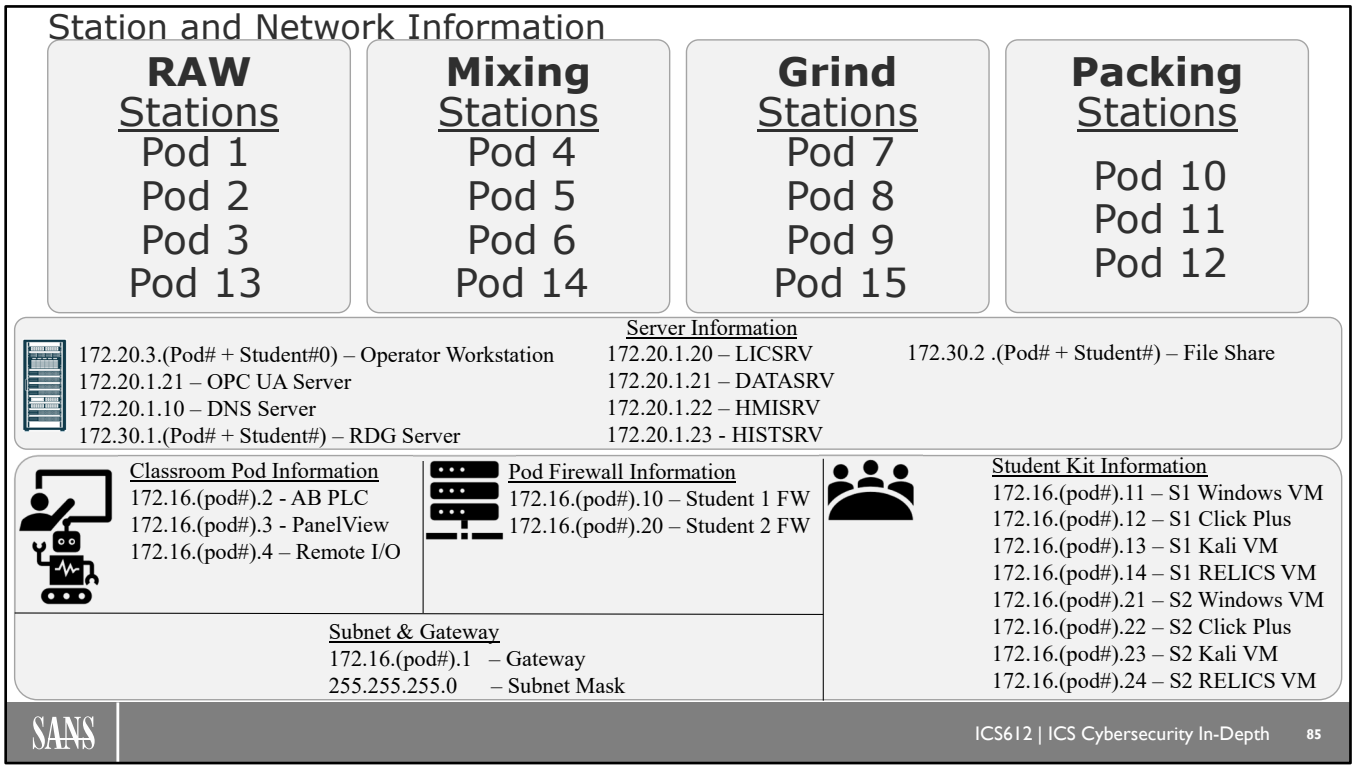
- In this section, we used firewalls to create a security perimeter around our Click Plus PLCs
- We discussed the purpose of the Industrial Demilitarized Zone (IDMZ) to keep our Manufacturing Zone assets running when there is a disruption in the Enterprise Zone
- We identified system and architecture improvements that will help secure the operational environment
- We explored the data connectivity, compression, and archive capabilities of Historians

This page intentionally left blank.

Section 3 Summary (2)

- We used a remote access server to connect from an untrusted network onto a trusted asset
  - We pivoted from the remote access server to an unauthorized asset
- We exploited the SMB vulnerability to steal RDP credentials
- Using the RDP connection we developed and executed an objective-based attack plan

This page intentionally left blank.



This page intentionally left blank.