SIU Southern Illinois University
CARBONDALE

Department of Computer Science
Southern Illinois University Carbondale

CS 491/531
SECURITY IN CYBER-PHYSICAL SYSTEMS

Lecture 18: Implementing Security and Access Controls

DR. ABDULLAH AYDEGER

LOCATION: ENGINEERING A 409F

EMAIL: AYDEGER@CS.SIU.EDU

Outline

Network Segmentation

Implementing Network Security Controls

- Firewall Configuration Guidelines
- Intrusion Detection and Prevention (IDS/IPS) Configuration Guidelines
- Application and Protocol Monitoring in Industrial Networks

Recall: Zones and Conduits

Security zones (or zones) can be either physical or logical

- Based on location
- Based on particular functionality or characteristics

Security conduits are special type of zone

- Communications into a logical arrangement of information flows between various zones
- Can also be arranged physically (network cabling)

Adapted mainly due to the need of more secure environments, if used

- More resilient to negative consequence in the event of threat exploiting particular vulnerability

Zones and Conduits Explained

Asset at particular site are grouped based on their relative security requirements or security level

When multiple layers of protection required, zones can be nested

Allows security controls to be deployed to zones (and assets they contain) based on unique security requirements of each

Info needs to flow into/out of/within given zone via conduits

Recall: Recommended Security Zones

Can be applied at almost any level

- Exact implementation depends on network architecture, operational requirements, identified risks and risk tolerance, etc.

Overlap can occur

- For ex. Physical control subsystem with logically defined zone by protocols

When assessing network and identifying potential zones, include all assets, systems, users, protocols

- If two (i.e., protocol and asset) can be separated without impacting either item's primary function, they belong to two functional groups

Recall: Recommended Security Zones

Network Connectivity

Control Loops

Supervisory Controls

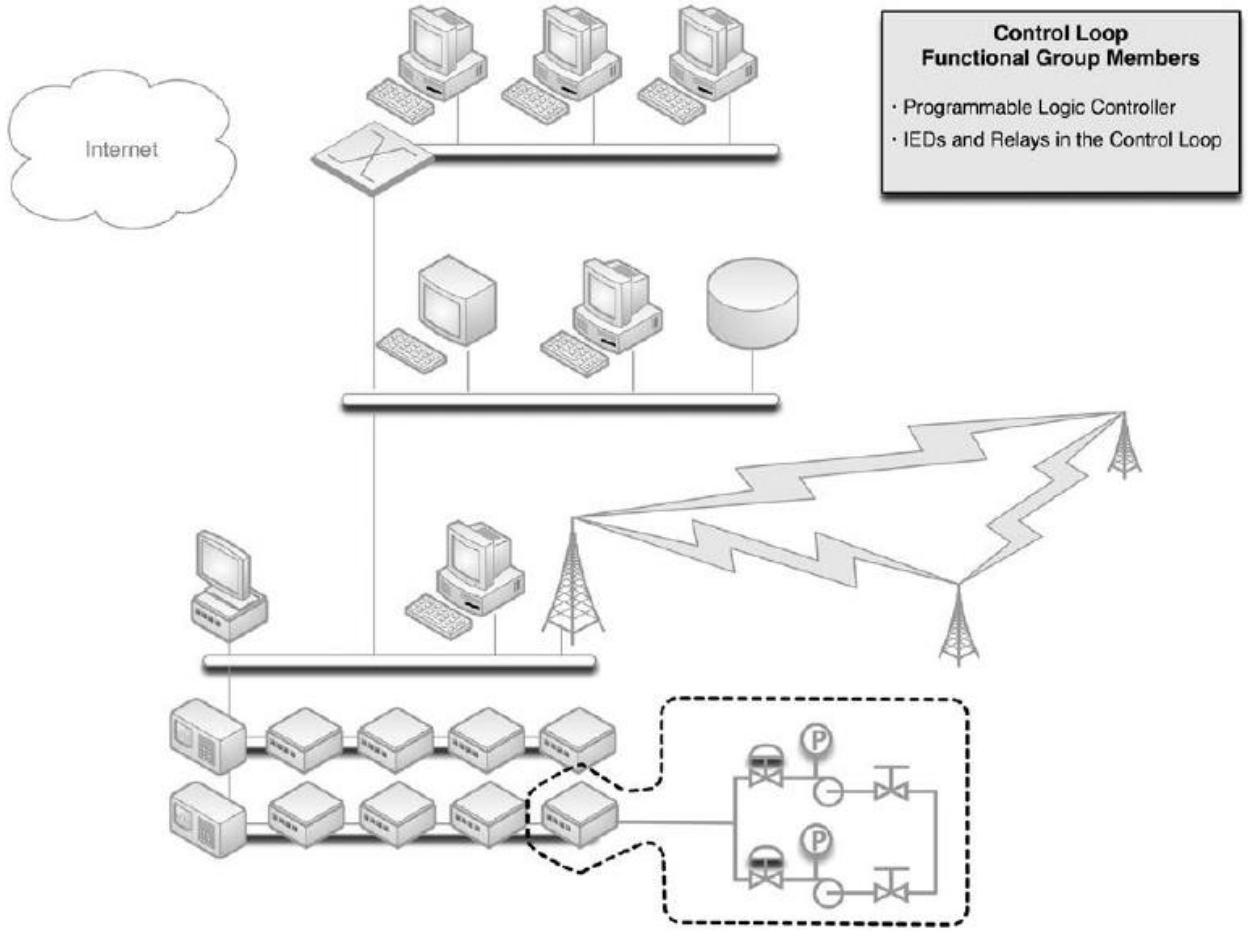
Control Process

Control Data Storage

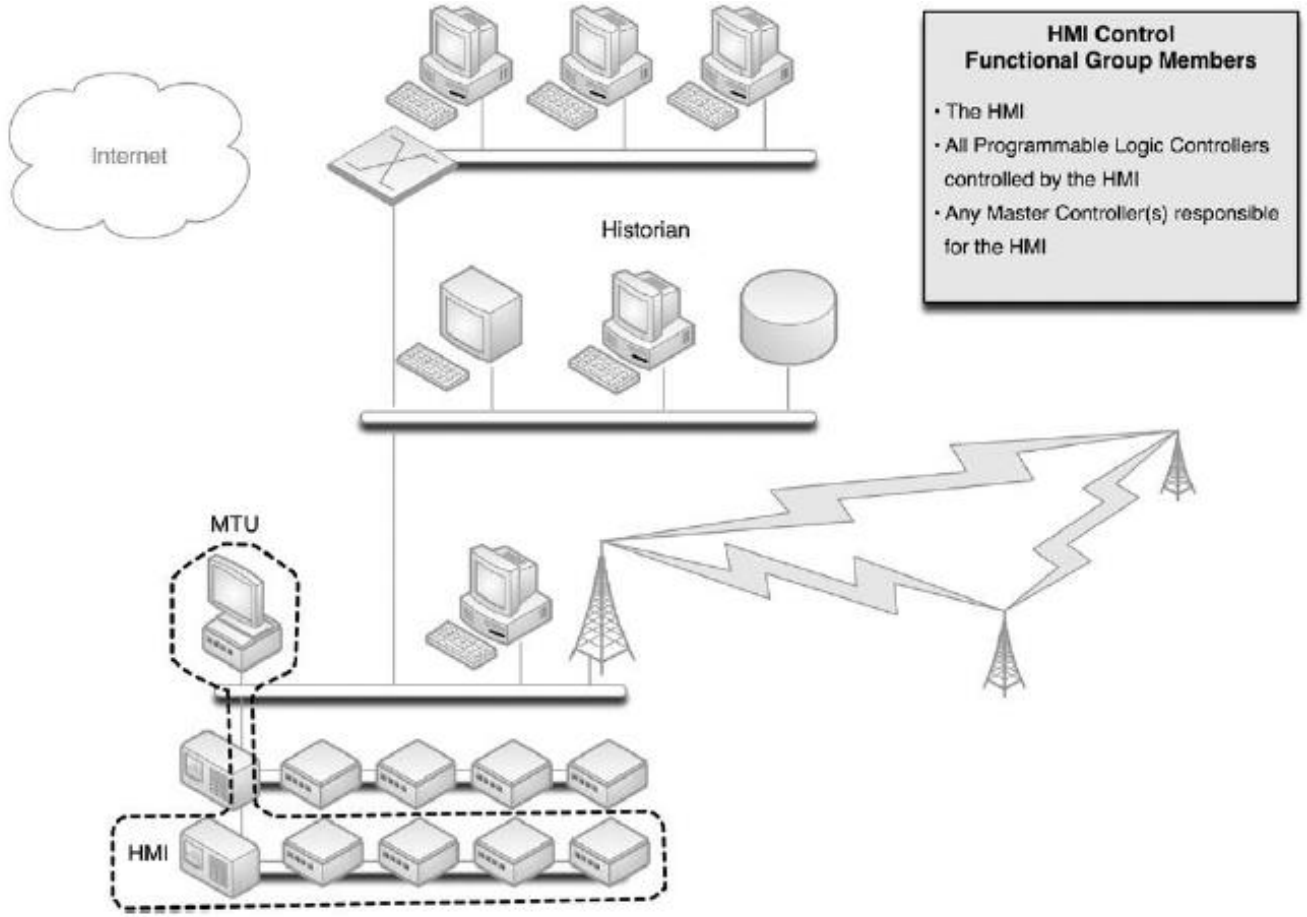
Remote Access

Users and Roles

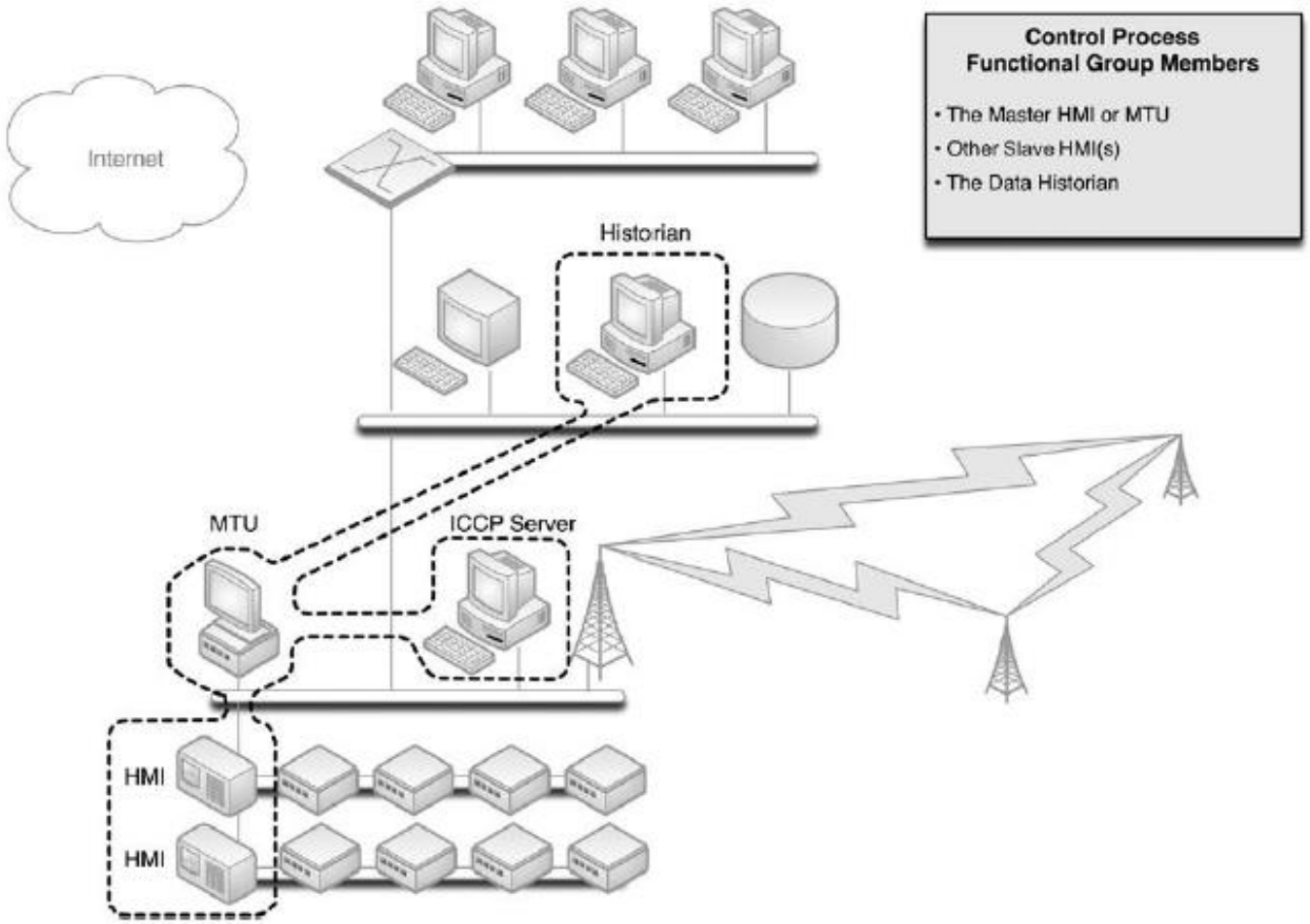
Recall: Control Loops



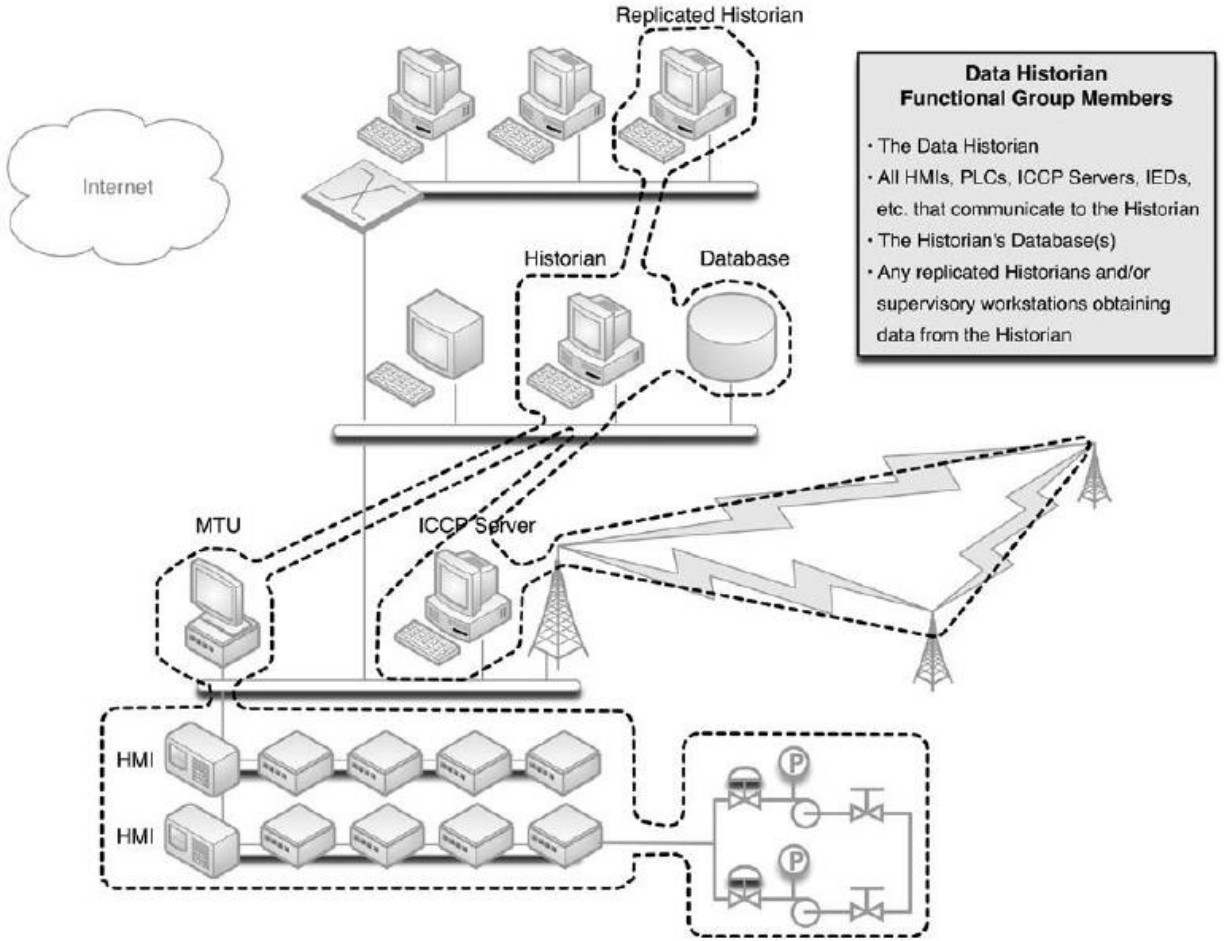
Recall: Supervisory Controls



Recall: Control Processes



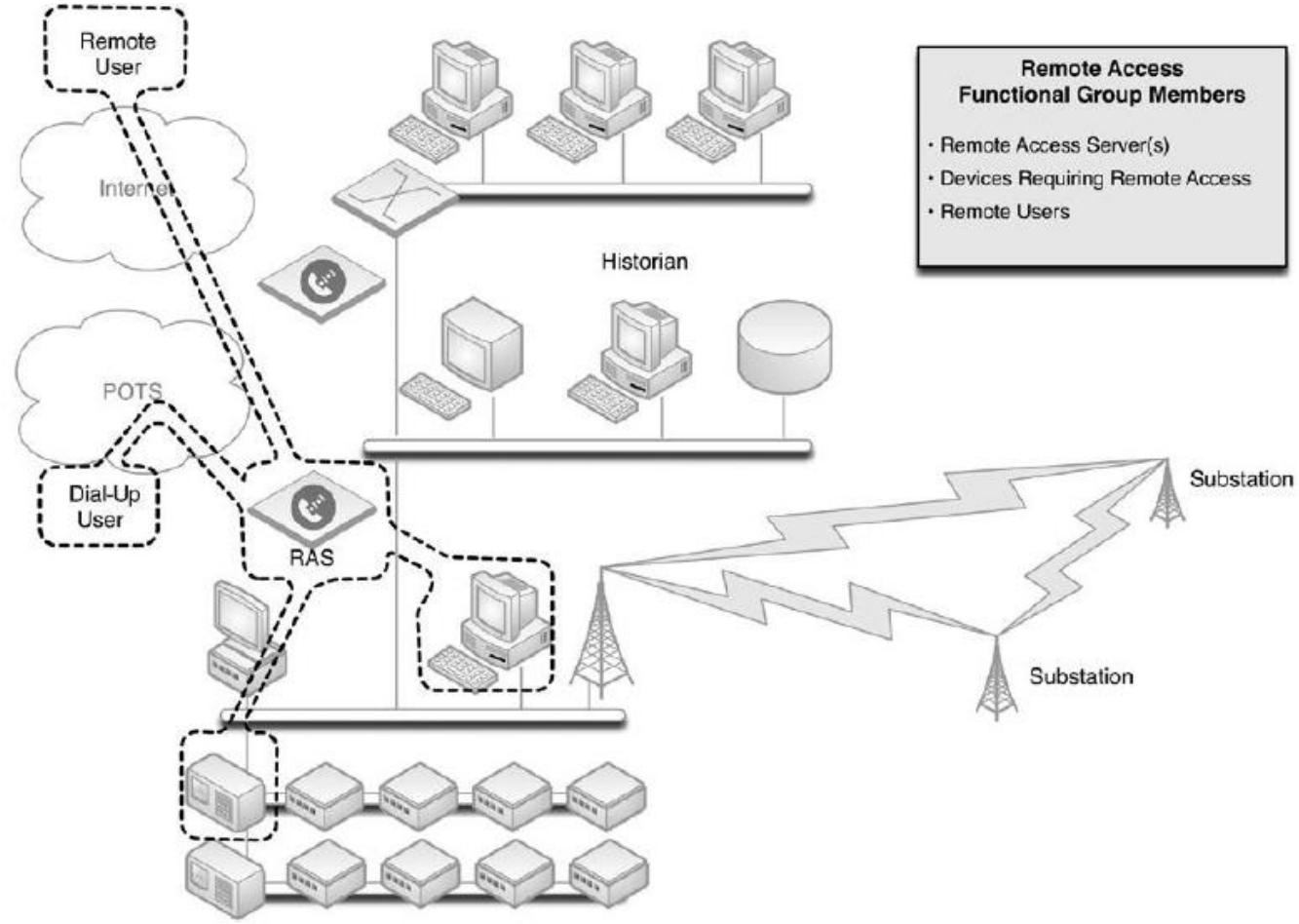
Recall: Control Data Storage



Recall: Remote Access

By functionally isolating remote connections, additional security can be imposed

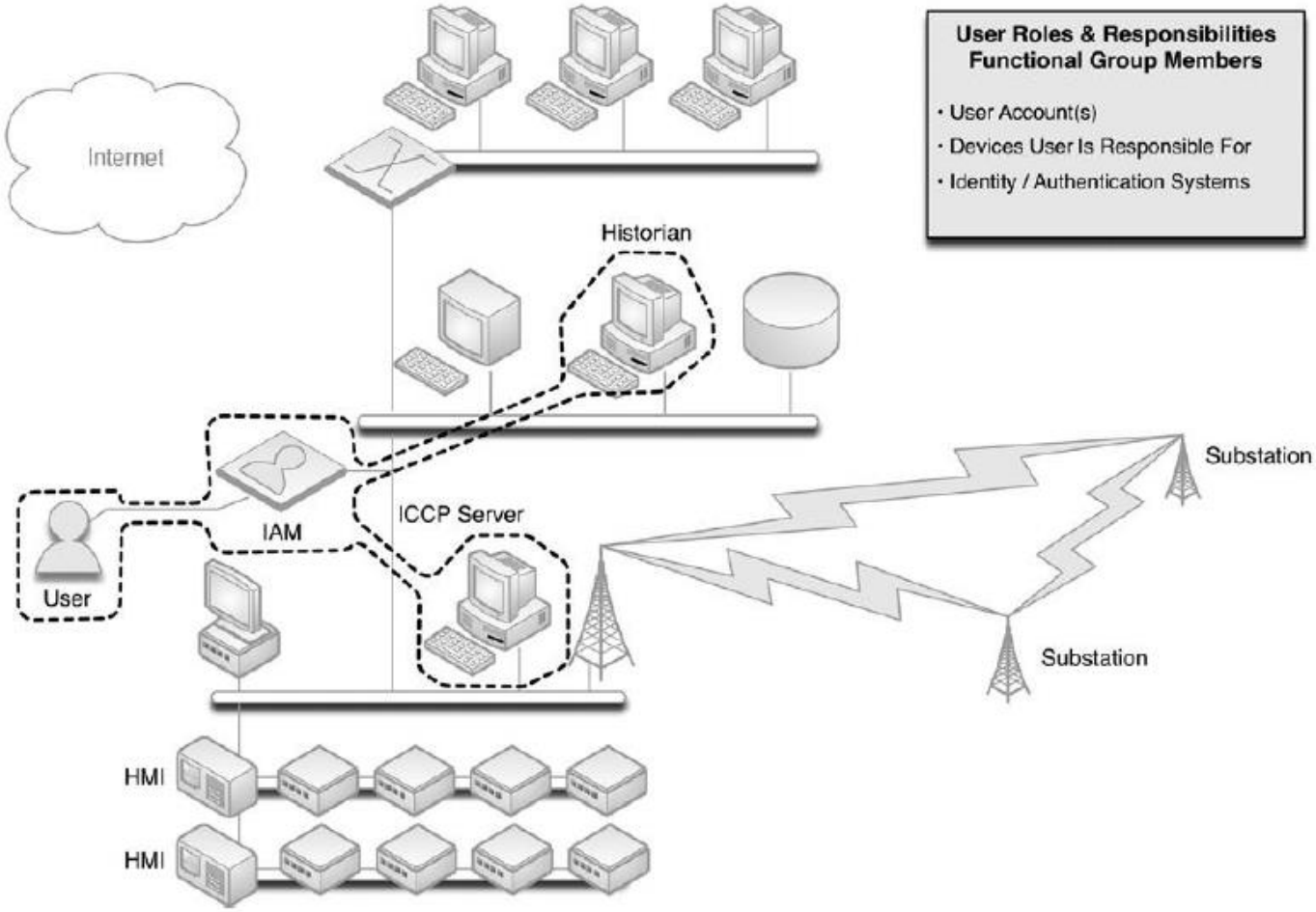
- Important to avoid open and inviting vector to attacker



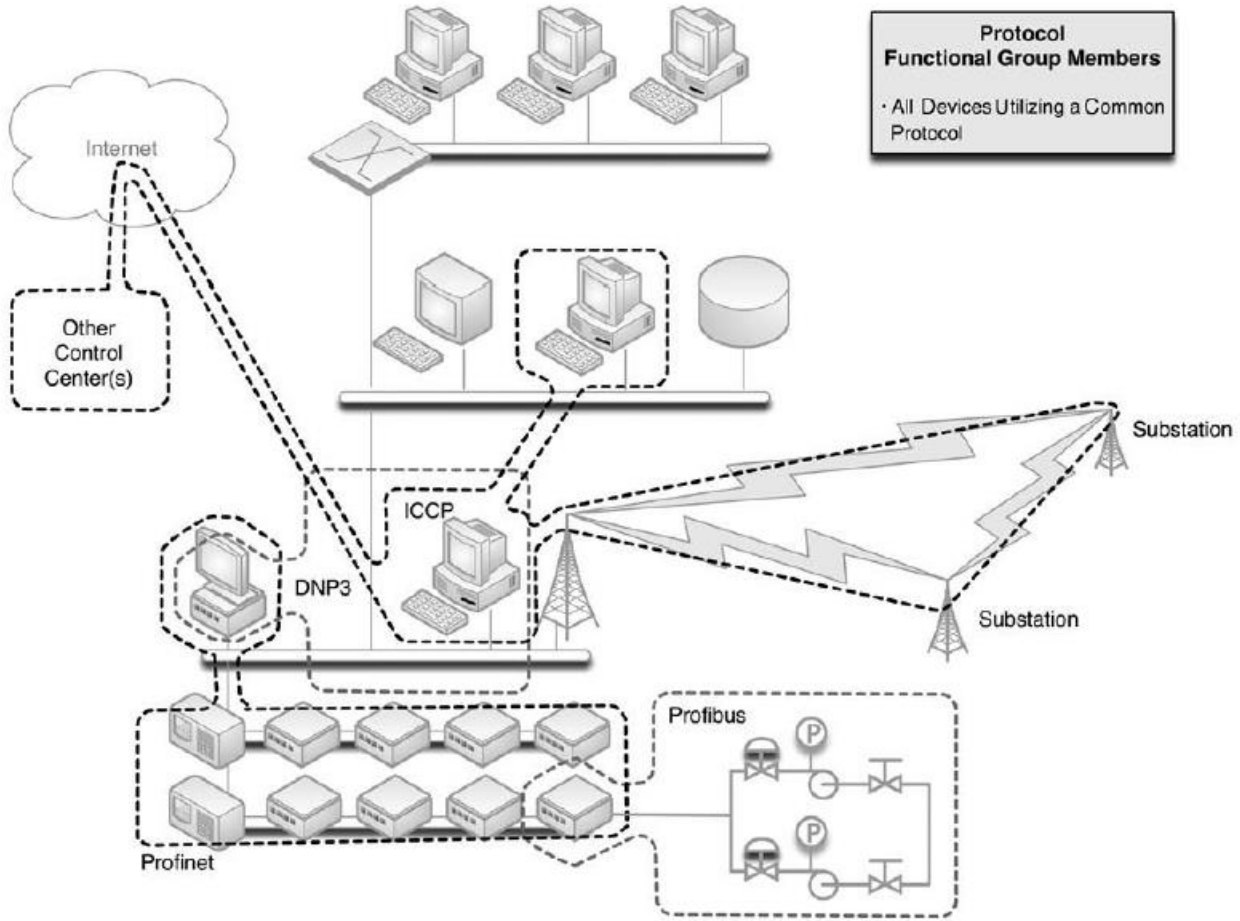
Recall: Users and Roles

Employee with control system access to a certain HMI, upon termination of his or her employment, might decide to tamper with other systems

- By placing a user in a functional group with only those devices he or she should be using, this type of activity could be easily detected and possibly prevented

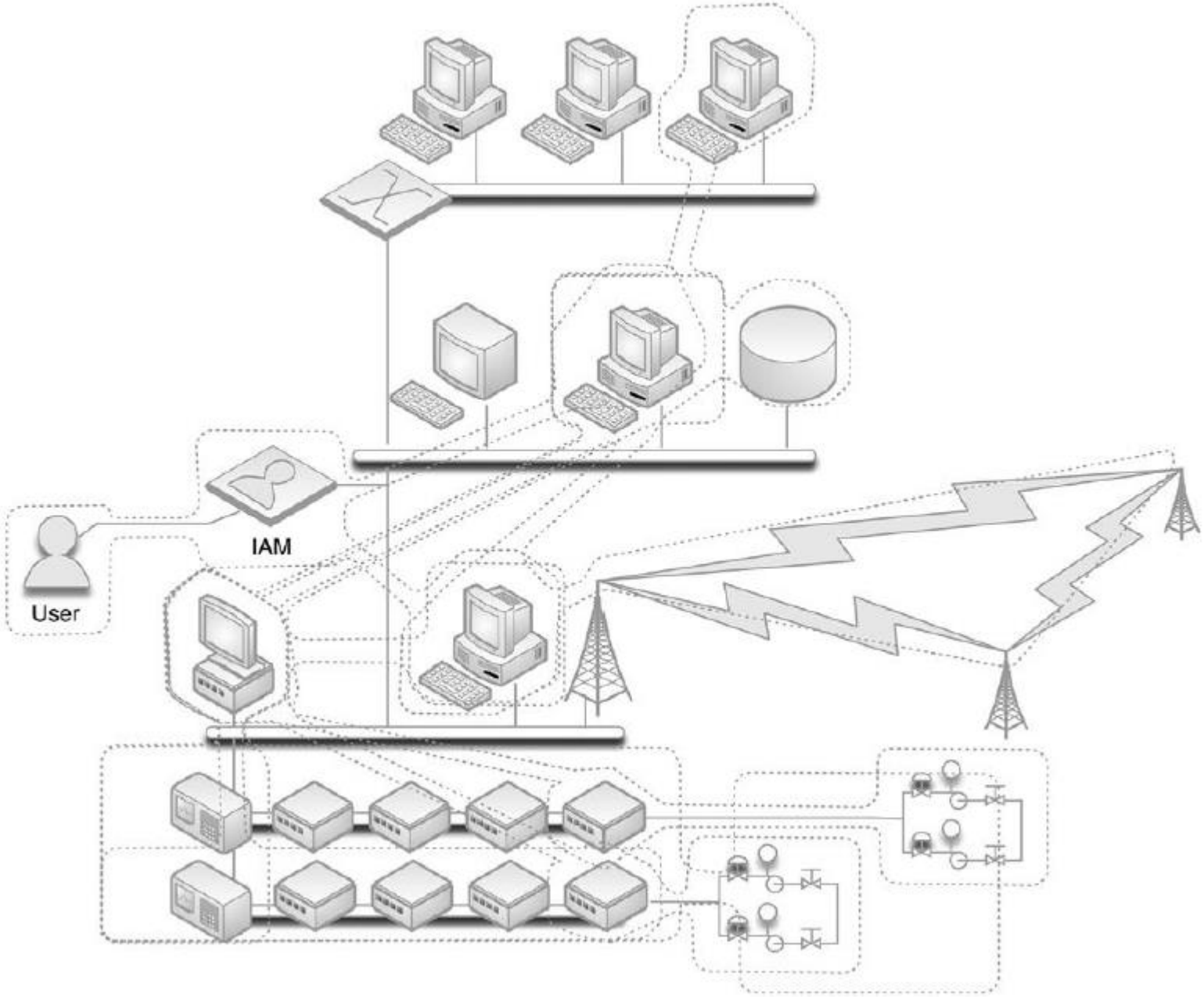


Recall: Protocols



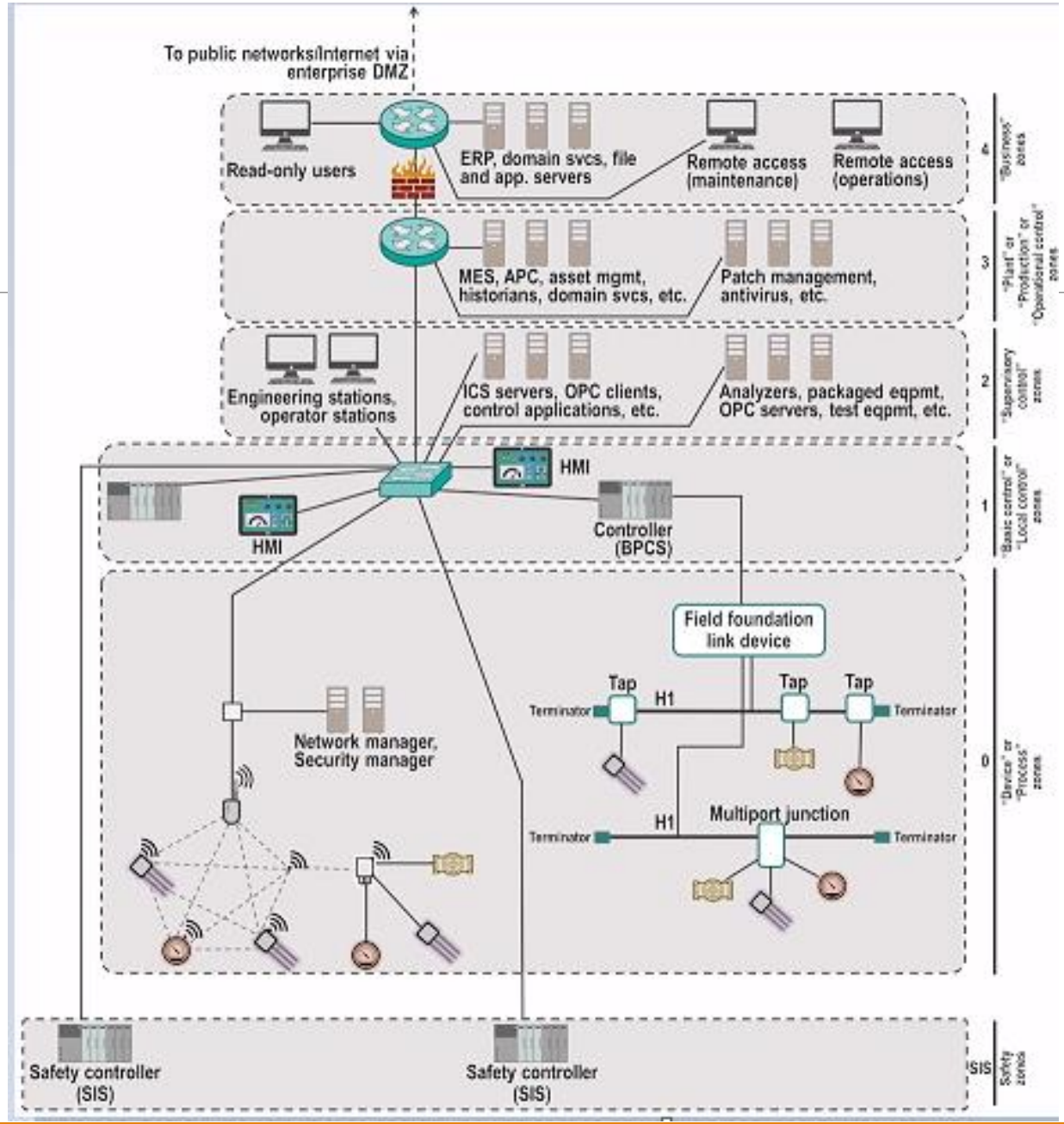
Recall:

Overlapping Function Groups

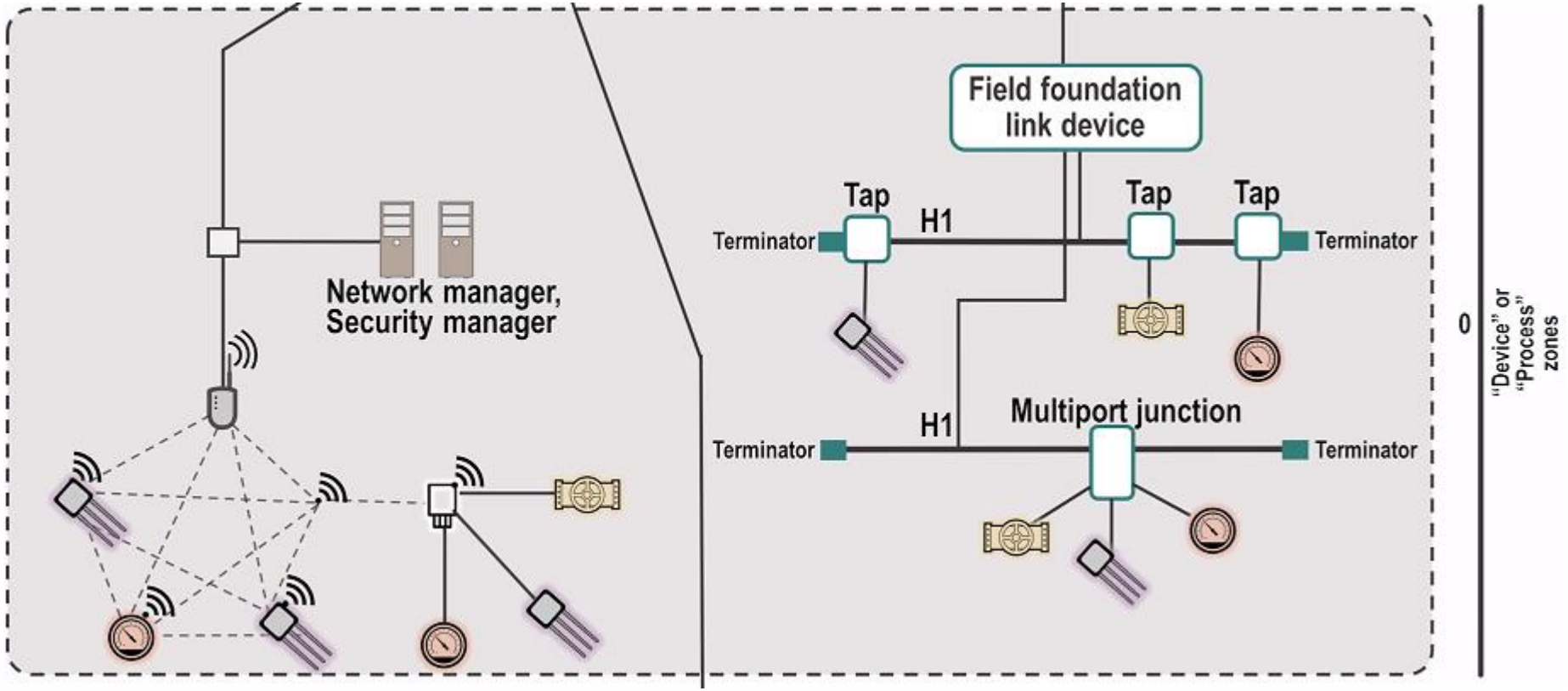


Recall:

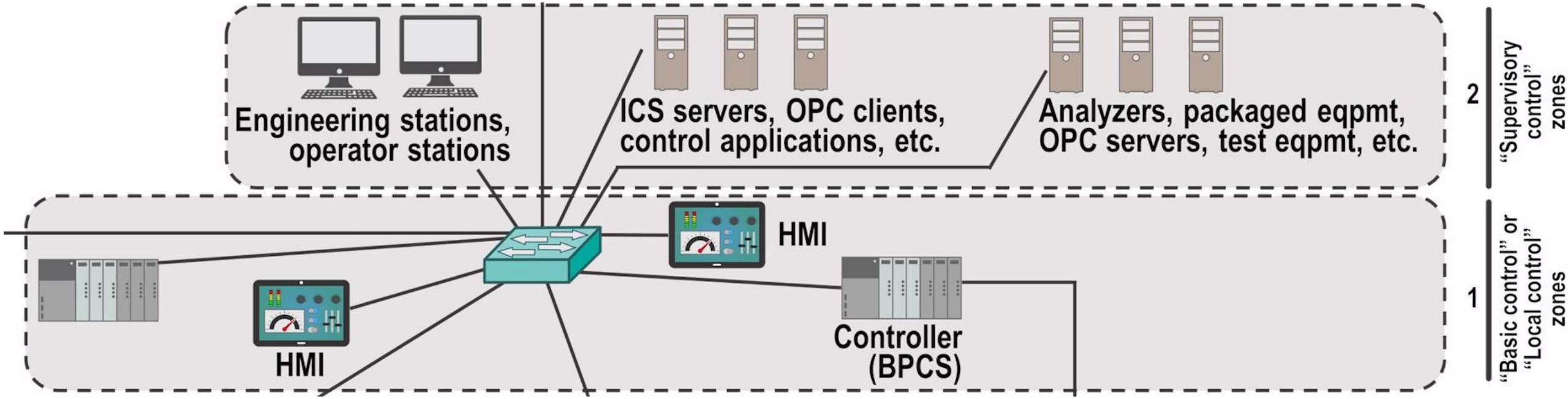
Example of Zones



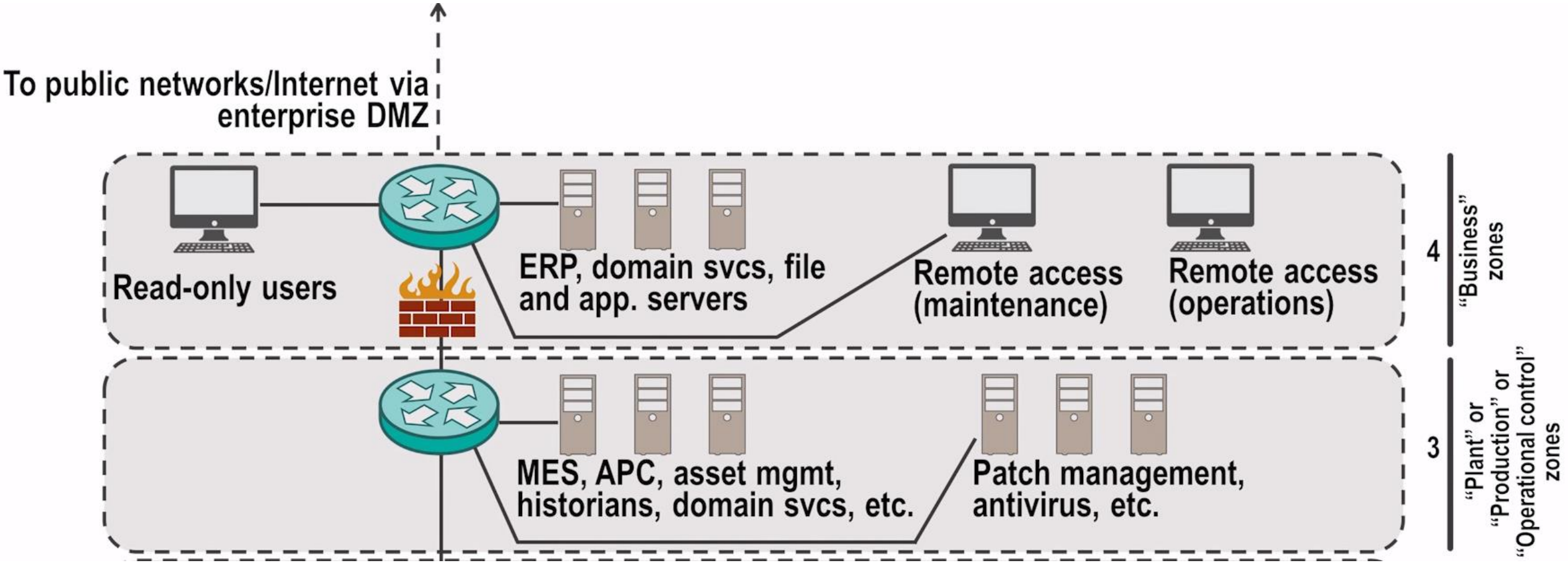
Recall: Process Zone



Recall: Local Control and Supervisory Control Zones



Recall: Plant (Production) and Business Zones



Recall: Characteristics within Zone

Security policies

Access requirements and control

Threats and vulnerabilities

Consequence in the event of breach

Technologies (wifi, Bluetooth, etc.) authorized and not authorized

Connected zones

Implementing Zones

Zone represents logically (sometimes physically) isolated network of systems

- More difficult to breach from outside threat agent
- Better contain incidents in case of breach
  - Only if there is proper network segmentation and access controls in place

If outside communication required, defined and secure access points should be used

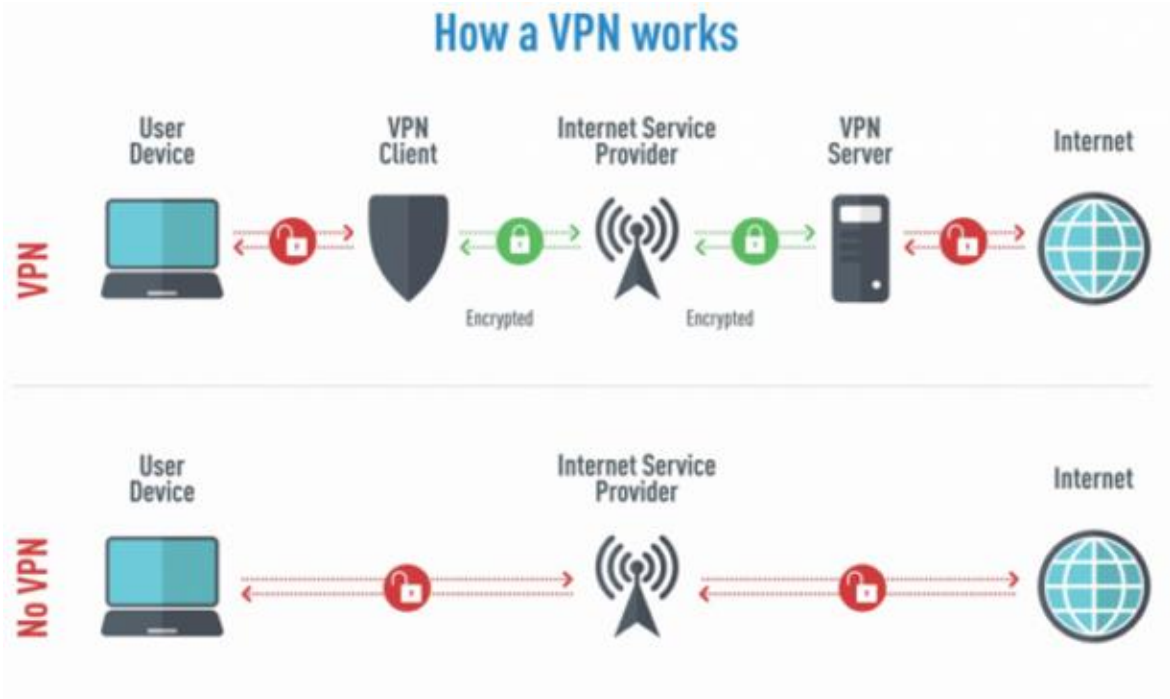
- VPN (Virtual Private Networks) or other encrypted gateways to provide secure point-to-point communication
- Or dedicated network connection (i.e., fiber cable) can be used for extremely critical zones

VPN

VPN connects your PC, smartphone, or tablet to another computer (called a server) somewhere on the internet and allows you to browse the internet using that computer's internet connection

So if that server is in a different country, it will appear as if you are coming from that country, and you can potentially access things that you couldn't normally

- One Example Client: Cisco anyconnect vpn



VPN Benefits

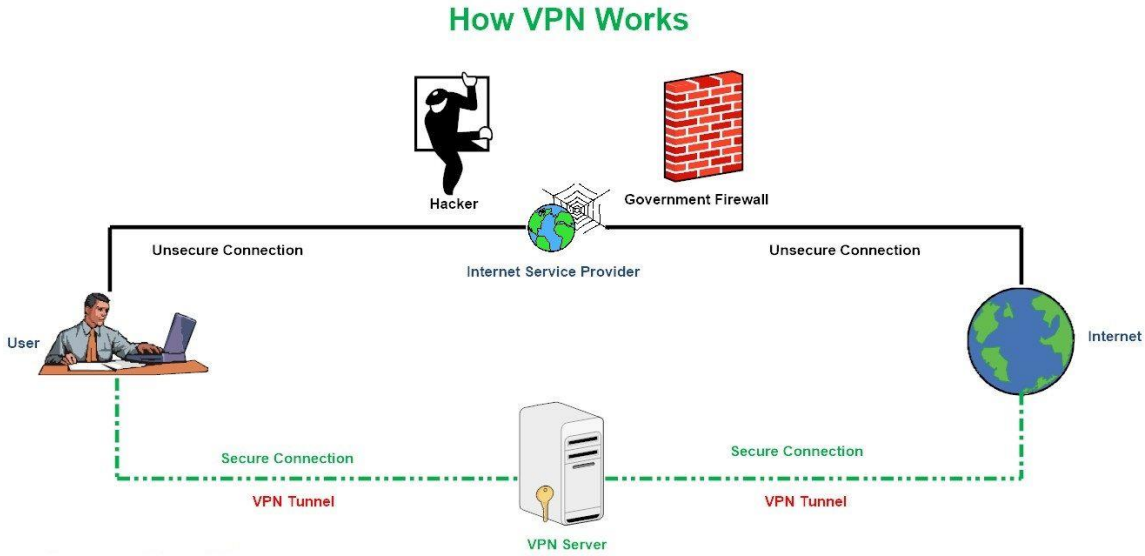
Bypass geographic restrictions on websites or streaming audio and video

Watch streaming media like Netflix and Hulu

Protect yourself from snooping on untrustworthy Wi-Fi hotspots

Gain at least some anonymity online by hiding your true location

Protect yourself from being logged while torrenting



Example Uses for VPNs

Access a Business Network While Traveling

Access Your Home Network While Travelling

Hide Your Browsing Activity From Your Local Network and ISP

Access Geo-Blocked Websites

- Downloading Files
- Bypass Internet Censorship

Process of Securing Zones

Map logical container of zone against network architecture

- Minimal network paths or communication channels into/out of each zone
  - Creates perimeter

Make necessary changes to network to align with defined zones

- For ex., two zones within flat network, segment the network to separate zones

Document zones for policy development & enforcement

- Also for security device configuration and monitoring
- Also for change management

Network Segmentation

In case not possible to clearly identify boundaries of zone;

- VLANs
  - Any broadcast domain that is partitioned and isolated in a computer network at the data link layer
- Next generation firewall for application layer segmentation
- Variable-length subnet masking (VLSM)
  - Enables network layer communication without layer 3 device

Network Segmentation

Effective zone separation:

- Identify all network connections into/out of each zone
- For each conduit
  - Start at layer 1 (physical) to layer 7 (application layer)
  - Investigate if network segmentation is feasible for each layer
  - For critical conduits, aim greater segmentation (combination of each layer)
  - For each layer, implement network security and access control to enforce segmentation
  - Provide monitoring capabilities to assist in potential breach

Using Zone Policies

Lists to maintain:

- Devices belong to zone (by IP or MAC)
- Software inventory for devices
- Users with authority
- Protocol, ports, services in use
- Technologies that are forbidden (i.e., no cloud access)

In IDS/IPS (SNORT example):

```
ipvar ControlSystem_Devices 192.168.1.0/24
alert tcp any any -> $ControlSystem_Devices any
```

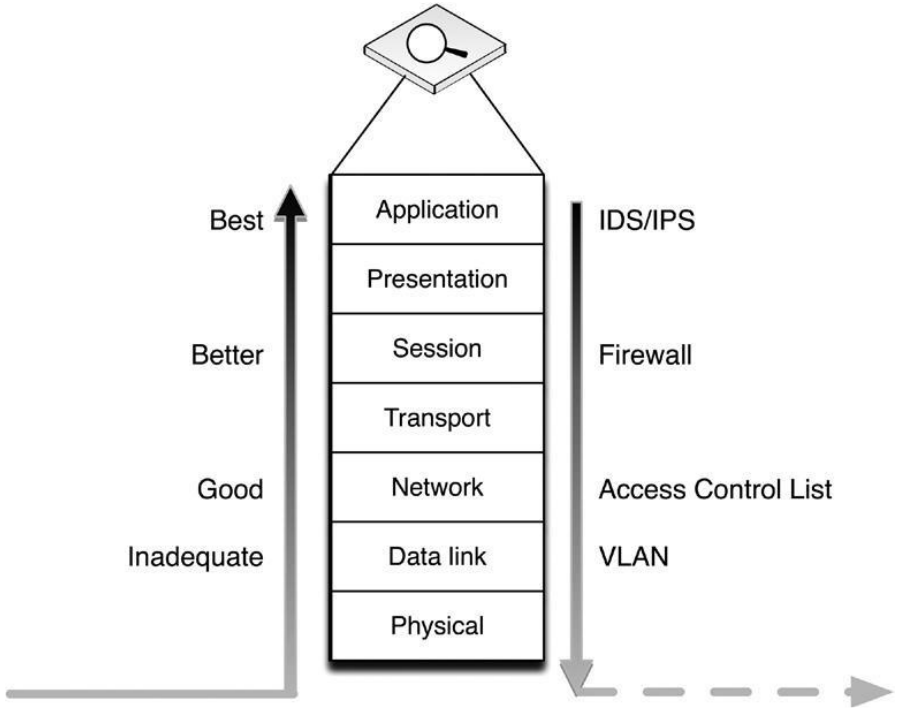
Implementing Network Security Controls

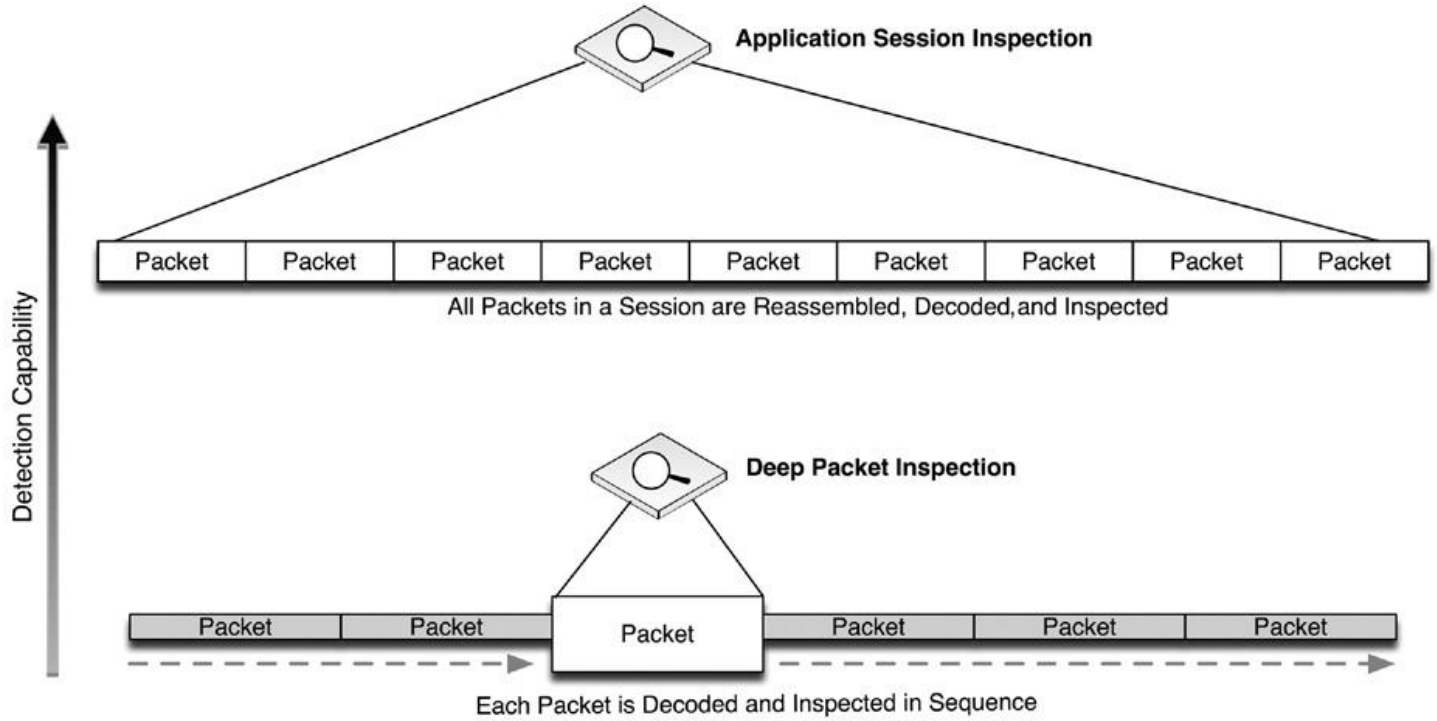
All inbound and outbound traffic must be forced through one or more known network connections that can be monitored and controlled

One or more security devices must be placed in-line at each of these connections

Criticality	Required Security	Recommended Enhancements
4 (highest)	NRC CFR 73.54: Unidirectional Perimeter, NERC CIP 005: Firewall or IDS or IPS	Application layer monitoring, Firewall, IDS and IPS
3	NRC CFR 73.54: Unidirectional Perimeter, NERC CIP 005: Firewall or IDS or IPS	Application layer monitoring, Firewall, IDS and IPS
2	NERC CIP 005: Firewall or IDS or IPS	Firewall and IDS and IPS
1	NERC CIP 005: Firewall or IDS or IPS	Firewall and IPS
0 (lowest)	NERC CIP 005: Firewall or IDS or IPS	Firewall and IPS

Implementing Network Security Controls





Firewall Configuration Guidelines

Using a defined configuration policy

- Typically consisting of Accept (allow) and Drop (deny) statements

Most firewalls will enforce a configuration in sequence, such that starting with a broadly defined policy, such as Deny All, which will drop all inbound traffic by default

- These broad rules can then be overruled by subsequent, more focused rules
- Therefore, the following firewall policy would only allow a single IP address to communicate outside of the firewall on port 80 (HTTP)

```
Deny All
Allow 10.0.0.2 to Any Port 80
```

Firewall Configuration Guidelines

The enclave will by its nature be limited in scope, resulting in concise firewall policies

The method of properly configuring an enclave firewall is as follows:

- Begin with bidirectional Deny All rules
- Configure specific exceptions, using the defined variables $ControlSystem_Enclave01_Devices and $ControlSystem_Enclave01_PortsServices
- Verify that all Allow rules are explicitly defined (i.e., no All rules)

NISCC (National Infrastructure Security Coordination Center) Firewall Configuration Guidelines with Enclave Variables

NISCC Recommendations	Example Rule Using Enclave Variables	Notes
Start with universal exclusion as a default policy	`Deny All / Permit None`	Firewalls should explicitly deny all traffic inbound and outbound as the default policy.
Ports and services between the control system environment and an external network should be enabled and permissions granted on a specific case by case basis	`Allow 10.2.2.120 port 162 to 192.168.1.15 port 162` `#Allow SNMP traps from router ip 10.2.2.120 to network management station ip 192.168.1.15, authorized by John Doe on April 1 2005`	Comments used within the firewall configuration file can be used to document special cases, permissions, and other details.
All "permit" rules should be both IP address and TCP/UDP port specific, and stateful if appropriate, and shall restrict traffic to specific IP address or range of addresses	N/A	This guideline can be enforced by using `$ControlSystem_Enclave01_Devices` and `$ControlSystem_Enclave01_PortsServices` to define rules.
All traffic on the SCADA and DCS network(s) are typically based only on routable IP protocols, either TCP/IP or UDP/IP; thus, any non-IP protocol should be dropped	N/A	By using `$ControlSystem_Enclave01_PortsServices` within all defined rules, only protocols explicitly allowed within that enclave will be accepted by the firewall, and all others will be dropped by the overarching `Deny All` rule.
Prevent traffic from transiting directly from the Process Control / SCADA network to the enterprise network; all traffic should terminate in the DMZ	`Deny [Not $Neighboring Enclave1, Not $Neighboring Enclave2] to $ControlSystem_Enclave01_Devices` `Deny $ControlSystem_Enclave01_Devices to [Not $Neighboring Enclave1, Not $Neighboring Enclave2]`	By configuring a rule on each enclave that explicitly denies all traffic to and from any enclave that is NOT a neighboring enclave will prevent any transitive traffic. All traffic will need to be terminated and reestablished using a device local to that enclave.

Any protocol allowed between the DCS and the SCADA DMZ is explicitly NOT allowed between SCADA DMZ and enterprise networks (and vice versa)	At the demarcation between the enterprise network and SCADA DMZ:
	`Deny $ControlSystem_Enclave01_PortsServices to $EnterpriseNetwork_Enclave01_Devices`
	At the demarcation between the DCS and SCADA DMZ:
	`Deny $EnterpriseNetwork_Enclave01_PortsServices to $ControlSystem_Enclave01_ Devices`
		These rules enforce the concept of "disjointing" protocols, and further prevents transitive communication from occurring across an enclave.

NISCC Firewall Configuration Guidelines with Enclave Variables

Allow outbound packets from the PCN or DMZ only if those packets have a correct source IP address assigned to the PCN or DMZ devices	N/A	Explicitly defined `Deny All` rules combined with explicitly defined known-good IP addresses using `$ControlSystem_Enclave01_Devices` ensures that all outbound packets are from a correct source IP. Firewalls may also be able to detect spoofed IP addresses. In addition, network activity monitoring using a Network Behavior Anomaly Detection (NBAD), Security Information and Event Management (SIEM), or Log Management solution may be able to detect instances of a known-good IP address originating from an unexpected device based on MAC Address or some other identifying factor (see Chapter 9, "Monitoring Enclaves")
Control network devices should not be allowed to access the Internet	At the Internet firewall: `Deny [$ControlSystem_Enclave01_ Devices, $ControlSystem_Enclave02_ Devices, $ControlSystem_Enclave03_ Devices, $ControlSystem_Enclave04_ Devices]`	Because all devices in all enclaves have been identified and mapped into variables, these devices can be explicitly denied at the Internet firewall.
Control system networks shall not be directly connected to the Internet, even if protected via a firewall	N/A	Using the enclave approach, no control system should be directly connected to the Internet (see "Establishing Enclaves").
All firewall management traffic be: 1. Either via a separate, secured management network (e.g., out of band) or over an encrypted network with two-factor authentication 2. Restricted by IP address to specific management stations	N/A	This recommendation supports the establishment of a Firewall Management enclave using the methods described earlier under "Establishing Enclaves." By placing all firewall management interfaces and management stations in an enclave, which is isolated from the rest of the network, the traffic can be kept separate and secured.

Intrusion Detection and Prevention (IDS/IPS) Configuration Guidelines

Rule functions different than firewall, only dropping traffic from the source address in question if the HTTP traffic contains a POST request (used by many web forms or applications attempting to upload a file to a web server over HTTP)

```
drop tcp 10.2.2.1 80 -> any any (msg: "drop http POST"; content:
"POST";)
```

Example usage:

```
[Action] [Protocol] [Source Address] [Source Port] [Direction
Indicator] [Destination Address] [Destination Port] [Rule Options]
```

```
drop tcp 10.2.2.1 80 -> 192.168.1.1 80 (flags: <optional snort
flags>; msg: "<message text>"; content: <this is what the rule is
looking for>; reference: <reference to external threat source>;)
```

Method of properly configuring an IDS/IPS

1. Begin with a more robust signature set, with many active rules

2. If a protocol or service is not allowed in the enclave, replace any specific detection signatures associated with that protocol or service with a broader rule that will block all traffic from that protocol or service (i.e., drop unauthorized ports and services)

3. If a protocol or service is allowed in the enclave, keep all detection signatures associated with that protocol or service active
   - For all active signatures, assess the appropriate action

4. Keep all IDS signatures current and up to date

Determining Appropriate IDS/IPS Actions

Allowed Port or Service?	Source	Destination	Criticality of Service	Severity of Event	Recommended Action	Note
No	Any	Any	Any	Any	`Reject`	Any communication not explicitly allowed within the enclave should be `Rejected` to disrupt unauthorized sessions and deter an attack.
Yes	Inside Enclave	Inside Enclave	High	Any	`Alert`	Active blocking or rejection of traffic that originates and terminates within an enclave could impact operations. For example, a false positive could result in legitimate control system traffic being blocked or rejected.
Yes	Inside Enclave	Inside Enclave	Low	Any	`Alert` or `Pass`	For noncritical services, logging is recommended but not necessary (`Alert` actions will provide valuable event and packet information that could assist in later incident investigations).
Yes	Outside Enclave	Inside Enclave	High	Low (events from obfuscated detection signatures or informational events)	`Alert`	Many detection signatures are broad to detect a wider range of potential threat activity. These signatures should `Alert` only to prevent unintentional interruption of control system operations.

Determining Appropriate IDS/IPS Actions

Allowed Port or Service?	Source	Destination	Criticality of Service	Severity of Event	Recommended Action	Note
Yes	Outside Enclave	Inside Enclave	High	High (explicit malware or exploit detected by a precisely tuned signature)	`Block, Alert`	If inbound traffic to a critical system or asset contains known malicious payload, the traffic should be blocked to prevent outside cyber incidents or sabotage.
Yes	Inside Enclave	Outside Enclave (explicitly allowed destination address)	Any	Any	`Alert`	This traffic is most likely legitimate. However, alerting and logging the event will provide valuable event and packet information that could assist in later incident investigations.
Yes	Inside Enclave	Outside Enclave (unknown destination address)	Any	Any	`Block` or `Reset`	This traffic is most likely illegitimate. Generated alerts should be addressed quickly: if the event is a false positive, necessary traffic could be unintentionally blocked; if the event is a threat, it could indicate that the enclave has been breached.

A few examples

Signature designed to detect a known SCADA buffer overflow attack

```
alert tcp !$ControlSystem_Enclave01_Devices -> $ControlSystem_
Enclave01_Devices 20222 (msg: "SCADA ODBC Overflow Attempt";
content: <long string in the second application packet in a TCP
session>; reference:cve,2008-2639; reference:url, http://www
.digitalbond.com/index.php/research/ids-signatures/m1111601/;
sid:1111601; rev:2; priority:1;)
```

Looks for one of the early delivery mechanisms for the Stuxnet malware: specifically, a shortcut image file delivered via a WebDav connection

```
tcp !$ControlSystem_Enclave01_Devices $HTTP_PORTS ->
$ControlSystem_Enclave01_Devices any (msg: "Possible Stuxnet
Delivery: Microsoft WebDav PIF File Move Detected"; flow:from_
server; content: "MOVE"; offset:0; within:5; content: ".pif";
distance:0; classtype:attempted-user; reference:cve, 2010-
2568; reference:osvdb,66387; reference:bugtraq,41732;
reference:secunia,40647; reference:research,20100720-01;
sid:710072205; rev:1;)
```

Recommended IDS/IPS Rules

Prevent any undefined traffic from crossing enclave boundaries (where the disruption of the communication will not impact the reliability of a legitimate service)

Prevent any defined traffic containing malware or exploitation code from crossing enclave boundaries

Detect and log suspicious or abnormal activity within an enclave

Log normal or legitimate activity within an enclave, which may be useful for compliance reporting

- This is how Machine Learning works!

Rules suitable for use in enclave perimeters

Block any industrial network protocol packets that are the wrong size or length

Block any network traffic that is detected inbound to or outbound from any enclave where that is not expected or allowed

Block any industrial network protocol packets that are detected in any enclave where that protocol is not expected or allowed

Alert any authentication attempts, in order to log both successful and failed logins

Alert any industrial network port scans

Rules suitable for use in enclave perimeters

Alert any industrial network protocol function codes of interest, such as:

- "Write" functions, including codes that write files or that clear, erase, or reset diagnostic counters
- "System" functions, including codes that stop or restart a device
- "System" functions that disable alerting or alarming
- "Read" functions that request sensitive information
- "Alarm" or "Exception" codes and messages

Cautions for IDS/IPS Implementation

A false positive (a rule that triggers in response to unintended traffic, typically due to imprecisions in the detection signature) can block legitimate traffic and in a control system legitimate traffic could represent a necessary operational control

- Only use block IPS rules where absolutely necessary, and only after extensive testing

IDS and IPS signatures are only able to block known threats, meaning that the IDS/IPS policy must be kept current in order to detect more recently identified attacks (virus, exploits, etc.)

- IDS/IPS products must be included within the overall Patch Management Strategy in order for the devices to remain effective

Anomaly based Intrusion Detection

Anomaly detection uses statistical models to detect when something unusual is happening, on the premise that unexpected behavior could be the result of an attack

These systems are able to detect a sudden increase in outbound traffic, an increase in sessions, an increase in total bytes transmitted, an increase in the number of unique destination IP addresses, or other quantifiable metrics

Anomaly rules are often based on thresholds and/or statistical deviations, such as in the following example

```
TotalByteCount from $Control_System_Enclave01_Devices increases by
>20%
```

Anomaly based Intrusion Detection

Anomaly detection is useful because it does not require an explicitly defined signature in order to detect a threat

- This allows anomaly detection systems to identify zero day attacks or other threats for which no detection signature exists
- At the same time, however, anomaly detection trends toward a higher number of false positives, as a benign change in behavior can lead to an alert
  - It is for this reason that anomaly-based threat detection is typically used passively, generating alerts rather than actively blocking suspect traffic

In industrial networks—especially in well-isolated control system enclaves—network behavior tends to be highly predictable, making anomaly detection more reliable

Application and Protocol Monitoring in Industrial Networks

Many industrial operations are controlled using specialized industrial network protocols that issue commands, read and write data, etc. using defined function codes

- Specialized devices can leverage that understanding along with Firewall, IDS, and IPS technology to enforce communications based on the specific operations being performed across the network

In addition to the inspection of industrial protocol contents (e.g., DNP3 function codes), the applications themselves can also be inspected

- Application Monitors provide a very broad and very deep look into how network traffic is being used
- Useful in environments where both control systems and enterprise protocols and applications are in use

A Comparison of Industrial Security Devices

Security Product	Functionality	Strengths	Weaknesses	Rule Example
SCADA Firewall	Traffic policy enforcement	Enables separation of networks, ports and services	Does not block hidden threats or exploits within "allowed" traffic	Allow only TCP port 502 (Modbus TCP)
SCADA IDS/IPS	Detects malware and exploits within traffic	Prevents exploitation of vulnerabilities via authorized ports and services	"Blacklist" methodology can only detect and block known threats	Block Modbus packets containing known malware code
SCADA UTM or hybrid security appliance	Combines firewall, IDS/IPS, VPN, and other security functions	Combination of security functions facilitates "defense in depth" via a single product	Security functions maintain their component weaknesses (i.e., the whole is equal to but not greater than the sum of its parts)	Allow only TCP port 502 with "read only" function codes Allow outbound TCP 502 only via encrypted VPN to other SCADA enclaves
SCADA Content Firewall or Application Firewall	Traffic policy enforcement	Enables content-based traffic separation, based on industrial network protocols	Assesses content of a single packet only (lacks session reassembly or document decode)	Allow only "Read only" Modbus TCP functions
Deep Session Inspection (application content monitoring)	Session Reassembly File/Content Decode File/Content Capture	Functions of a SCADA content firewall, plus visibility into full application session and document contents to detect APT threats and insider data theft; provides strong security in hybrid enterprise/ industrial areas such as SCADA DMZ	Typically limited to TCP/IP inspection, making session inspection less suitable for deployment in pure control system environments	Alert on Modbus TCP traffic on ports other than TCP 502 Alert on any traffic with base64-encoded content
Network Whitelist	Allows only defined "good" traffic	Prevents all malicious traffic by allowing only known, good traffic to pass	Requires proper baselining of correct network behavior	Can make legitimate changes in network operations more difficult