Department of Computer Science
Southern Illinois University Carbondale

CS 491/531
SECURITY IN CYBER-PHYSICAL SYSTEMS

Lecture 15: Security Zones and Conduits

DR. ABDULLAH AYDEGER

LOCATION: ENGINEERING A 409F

EMAIL: AYDEGER@CS.SIU.EDU

Outline

What are Security Zones and Conduits

Recommended Implementation of Security Zones and Conduits

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

Once defined, they will help to pinpoint the areas where security and access control may be required

- Each conduits represents potential network attack vector

One example: Grouping of assets that cannot be protected individually with anti-malware defense or whitelisting

- Logically group these assets into zone
- Anti-malware defense is implemented on conduit into this zone

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

Zones and Conduits Explained

A zone can have sub-zones

A conduit cannot have sub-conduits

A zone can have more than one conduit

- Cyber assets (HOSTs) within a zone use one or more conduits to communicate

A conduit cannot traverse more than one zone

A conduit can be used for two or more zones to communicate with each other

Example of Zones and Conduits in ICS

Broadly defined zones:

- Control system, business zone, and demilitarized zone between the two

Broadly defined conduits

- All communication paths within a single zone
- All communication paths between two zones

Better be more precisely defined

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

Recommended Security Zones

Network Connectivity

Control Loops

Supervisory Controls

Control Process

Control Data Storage

Remote Access

Users and Roles

Network Connectivity

By nature, network connects devices

Physical network boundaries using network map

- For wireless, all can be considered physically connected
- Logical separation can be done by authenticated wireless access

Logical boundaries are defined by use of devices operating network layer

- Layer 3 (routers)
- VLAN at layer 2
  - Not recommended due to possibility of modifying packet header to hop VLANs (bypassing router)

Control Loops

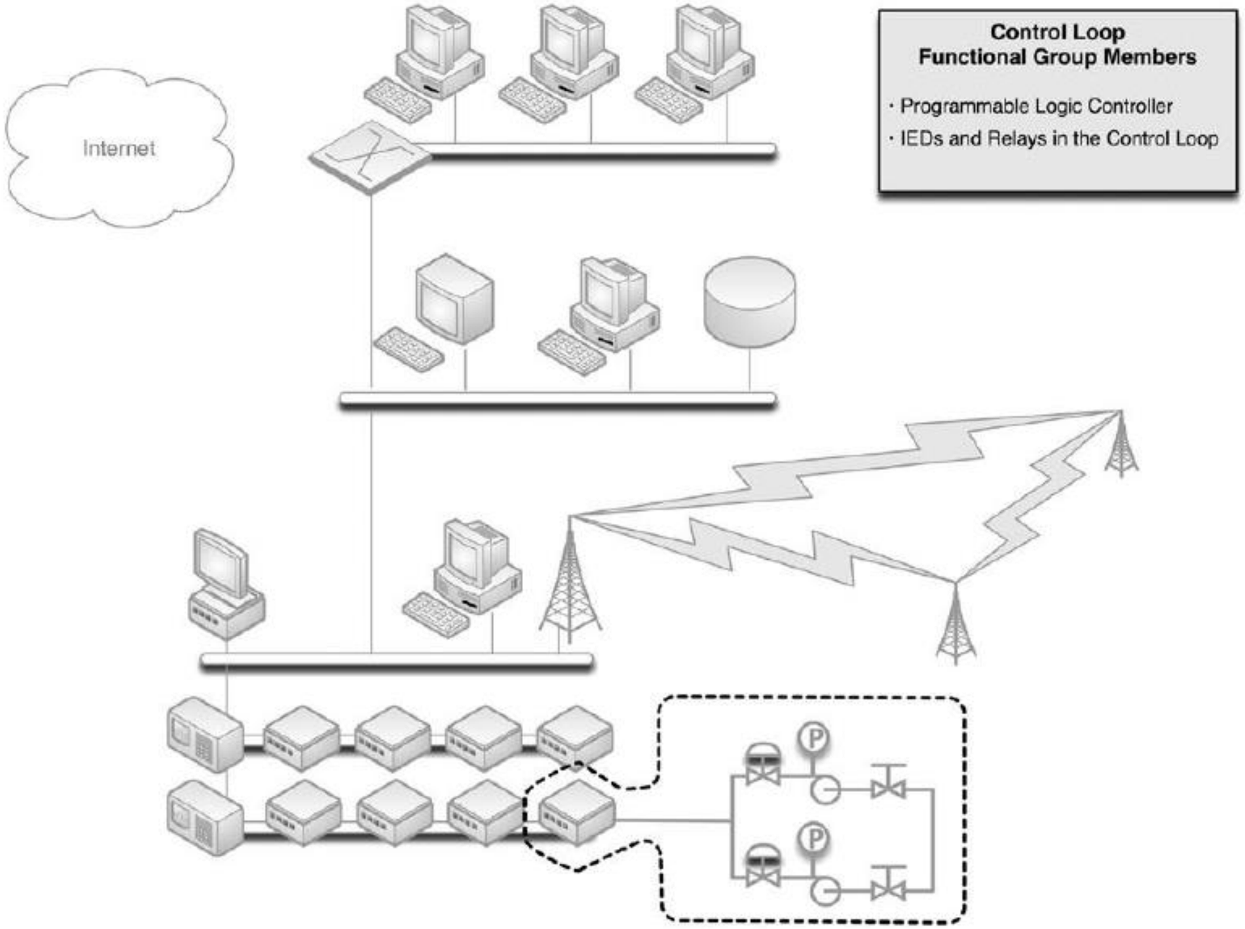
Devices responsible for particular automated process

- Sensor, controller, and actuator

Building a functional group based on a control loop is a very precise example

- The functional groups created will be numerous, and each will contain a relatively small number of devices
  - Specific PLC or RTU, and a collection of relays and IEDs

Control Loops



Control Loop
Functional Group Members

- Programmable Logic Controller
- IEDs and Relays in the Control Loop

Supervisory Controls

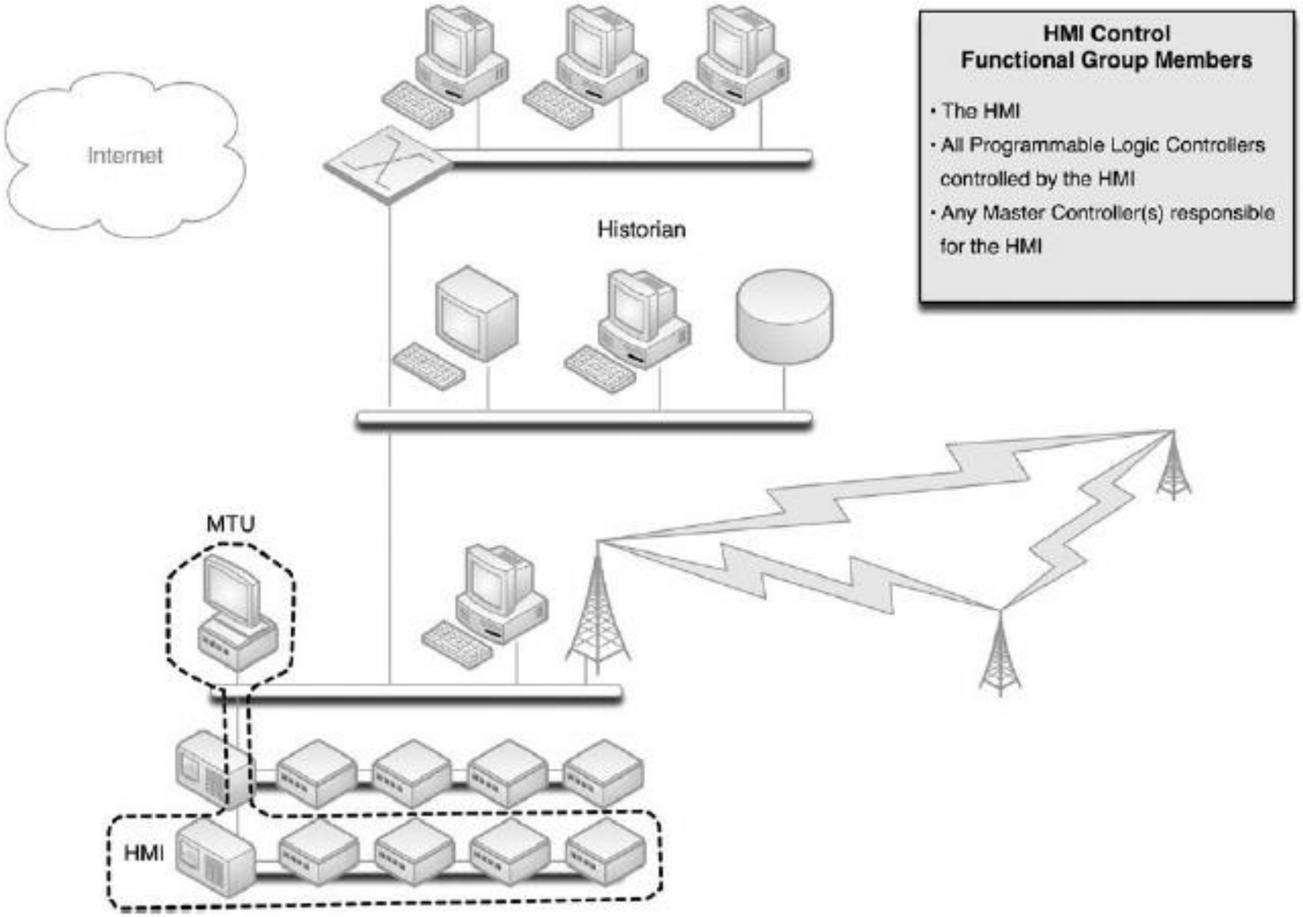
Each control loop is also connected to some sort of supervisory control

- Typically an HMI—that is responsible for the configuration, monitoring, and management of the automated process

Because the HMI is responsible for the PLC, these two devices belong to a common functional group

However, because the HMI is not directly responsible for those IEDs connected to the PLC, these items are not necessarily in a common functional group as the HMI

Supervisory Controls



HMI Control Functional Group Members

- The HMI
- All Programmable Logic Controllers controlled by the HMI
- Any Master Controller(s) responsible for the HMI

Control Processes

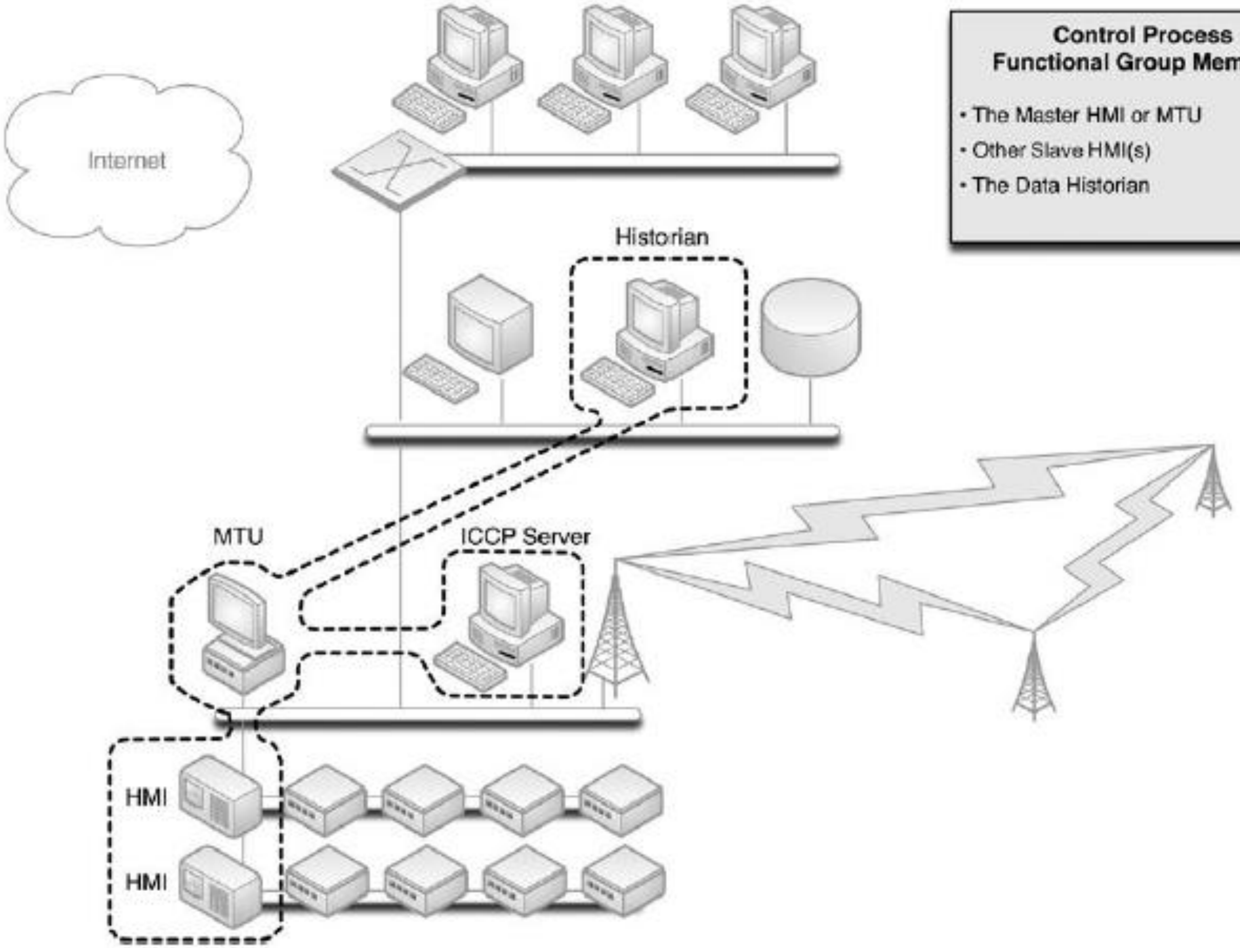
If a Master Controller (MTU) is used to manage multiple HMIs, each responsible for a specific part of a larger control process

This example also introduces the concept of process communication and historization

If MTU interfaces with an ICCP server, the ICCP server should also be included in the MTU's functional group

If the process information from the MTU is fed into a Data Historian, that system should also be included

Control Processes



Control Process Functional Group Members

- The Master HMI or MTU
- Other Slave HMI(s)
- The Data Historian

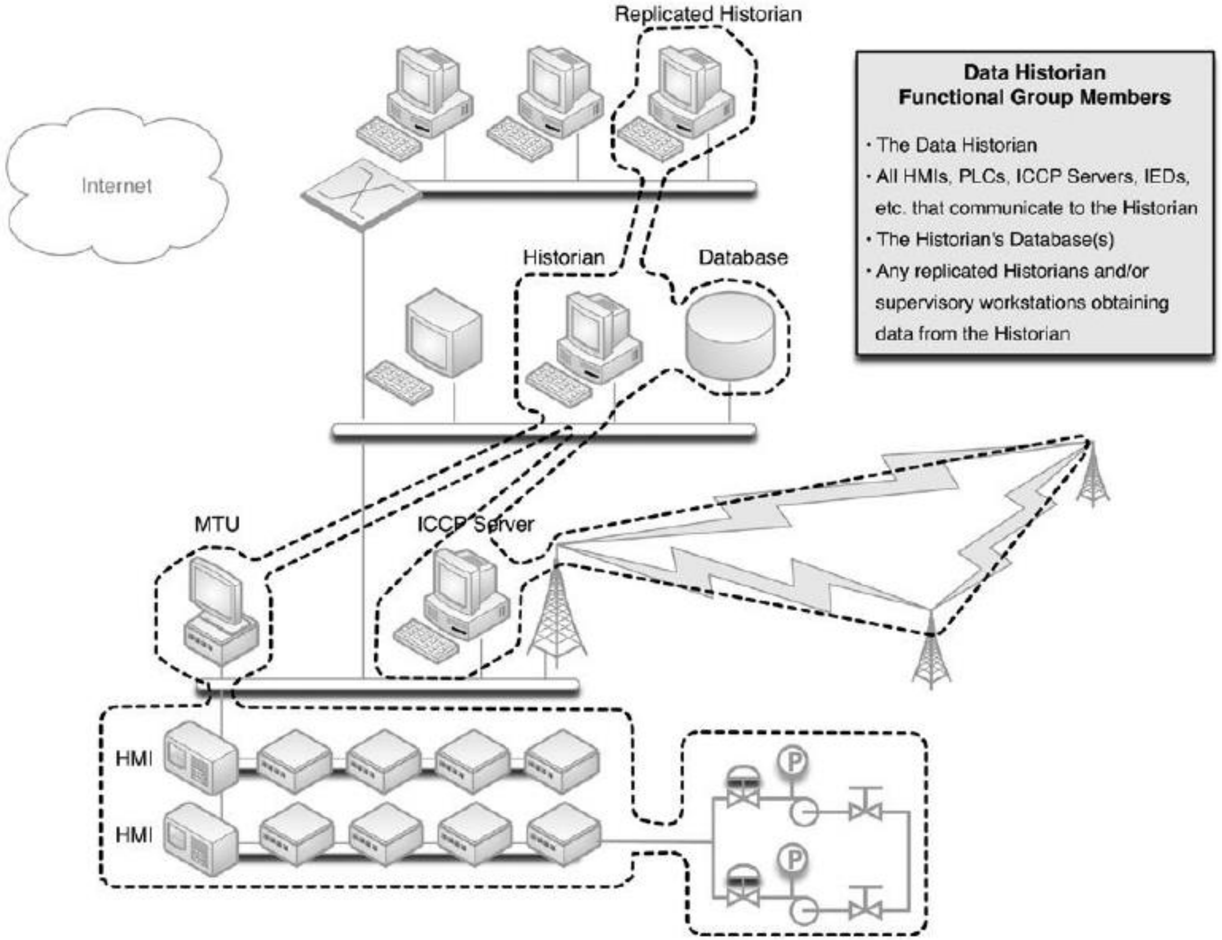
Control Data Storage

Many industrial automation and control system devices generate data, reflecting current configurations, the status of a process, alarms, and other information

- This information is typically collected and “historized” by a Data Historian

The Data Historian system may connect to many—potentially all—devices throughout the control system network, supervisory network, and in some cases the business network

Control Data Storage



Data Historian Functional Group Members

- The Data Historian
- All HMIs, PLCs, ICCP Servers, IEDs, etc. that communicate to the Historian
- The Historian's Database(s)
- Any replicated Historians and/or supervisory workstations obtaining data from the Historian

Remote Access

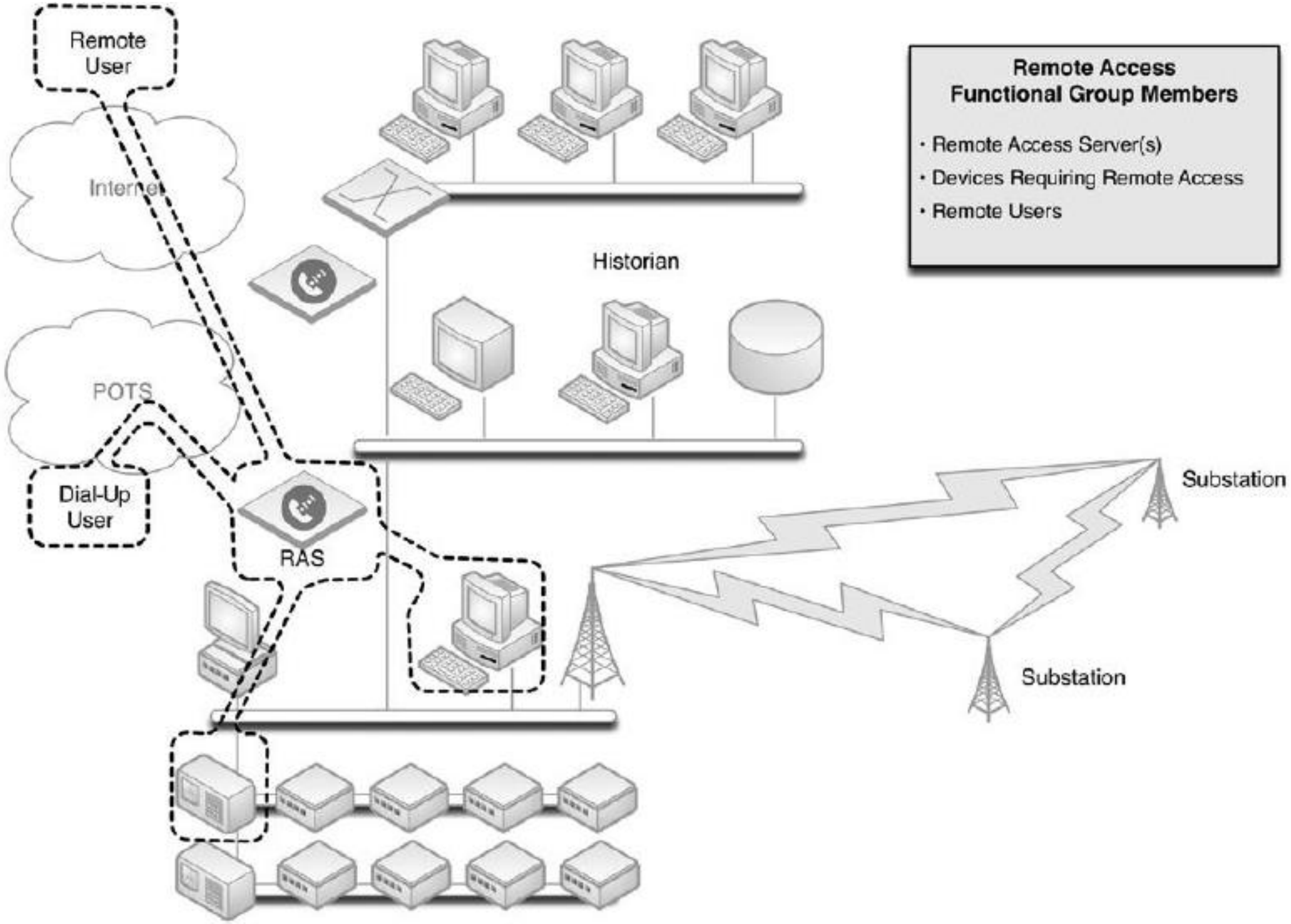
Many control systems and industrial devices—including HMIs, PLCs, RTUs, and even IEDs— allow remote access for technical support and diagnostics

- This access could be via dial-up connection, or via a routable network connection
- Remote access to control system devices should be controlled via specialized virtual private networks (VPNs) or remote access servers (RAS), and should only allow explicitly defined, point-to-point connections from known entities, over secure and encrypted channels
- These explicitly defined users, the devices that they access, and any VPN or RAS systems that are used constitute a remote access functional group

Remote Access

By functionally isolating remote connections, additional security can be imposed

- Important to avoid open and inviting vector to attacker


Remote User
Internet
POTS
Dial-Up User
RAS
Historian
Substation
Substation
Remote Access Functional Group Members
• Remote Access Server(s)
• Devices Requiring Remote Access
• Remote Users

Users and Roles

For human interaction, such as an operator accessing an HMI to adjust a process, it is just as important to define which users should legitimately be communicating with which devices

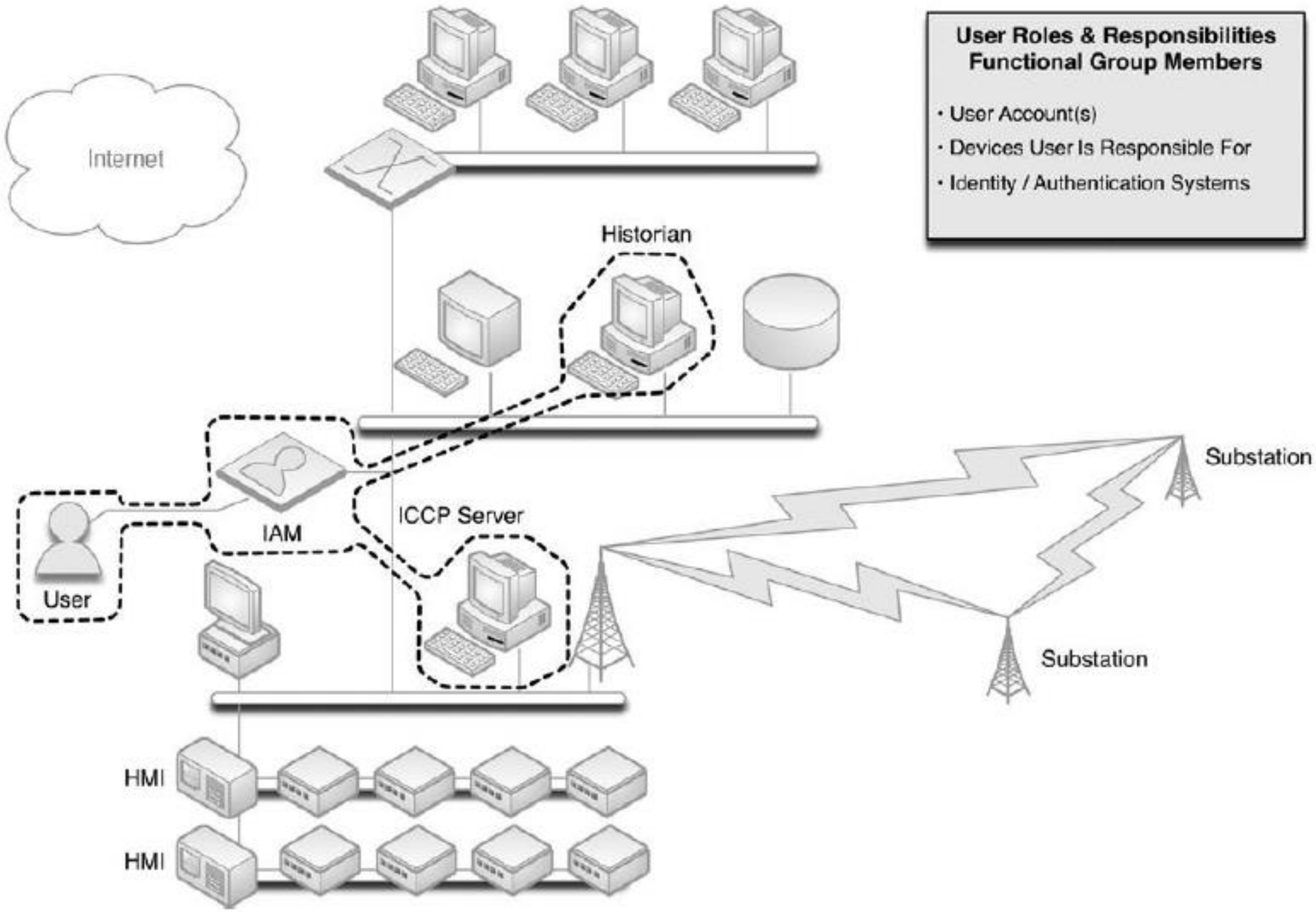
- This requires a degree of Identity and Authentication Management (IAM), which defines users and their roles.
- The most well-known example of an IAM is Microsoft's Active Directory services, although many other commercial IAM systems exist

Functional group can be used to monitor for unauthorized access to a system by an otherwise legitimate user

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

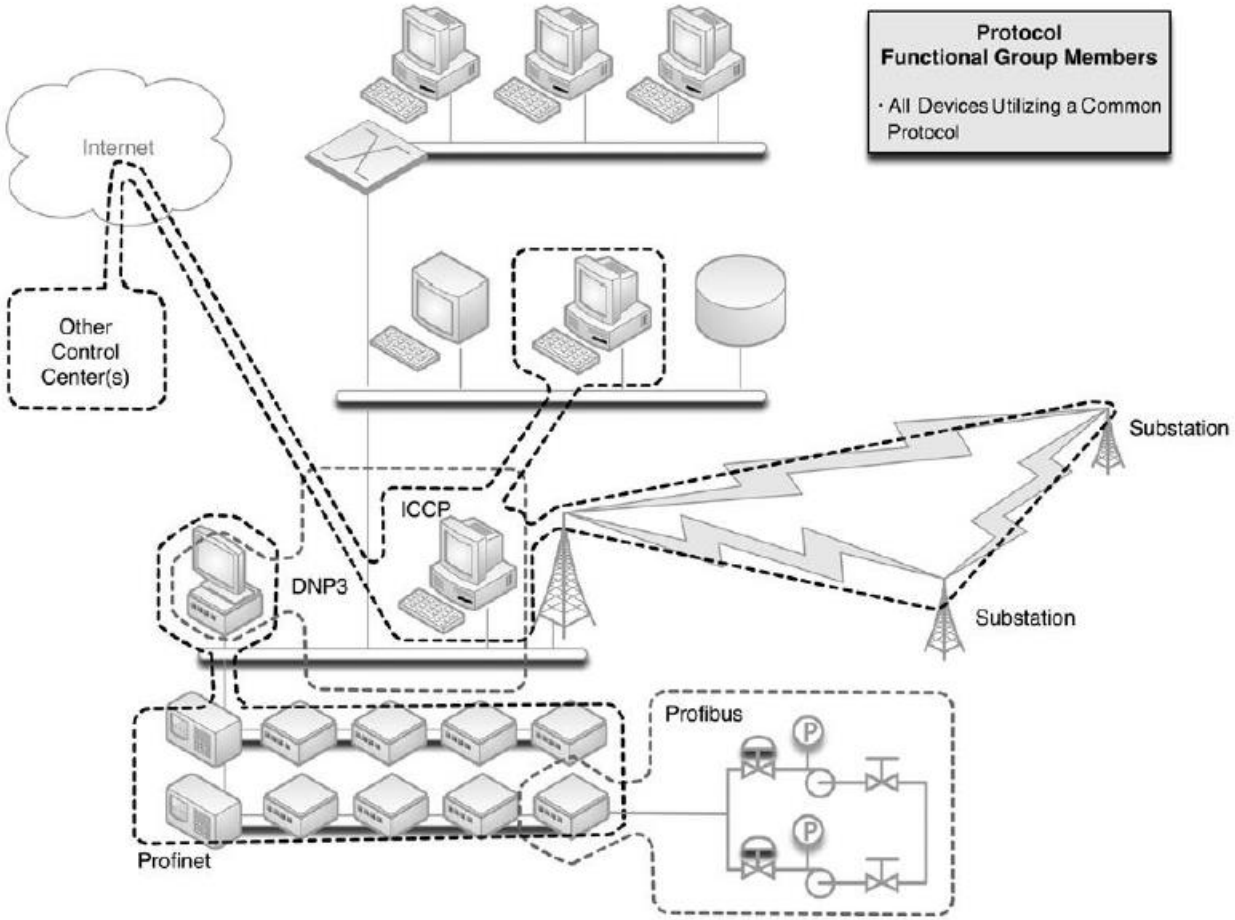


Protocols

The protocols that a device uses in industrial networks can be explicitly defined, and so it should be, in order to create functional groups based on protocols.

- Only devices that are known to use DNP3 should ever use DNP3,
- If any other device uses DNP3, it is a notable exception that should be detected quickly and prevented outright if possible

Protocols


Protocol
Functional Group Members
· All Devices Utilizing a Common Protocol
Internet
Other Control Center(s)
ICCP
DNP3
Substation
Substation
Profibus
Profinet

Criticality

Enclave-based security is about isolating common influencing factors into functional groups so that they can be kept separate and secure from other non-influencing factors

Simply defining functional groups around criticality to identify enclaves will result in very few enclaves

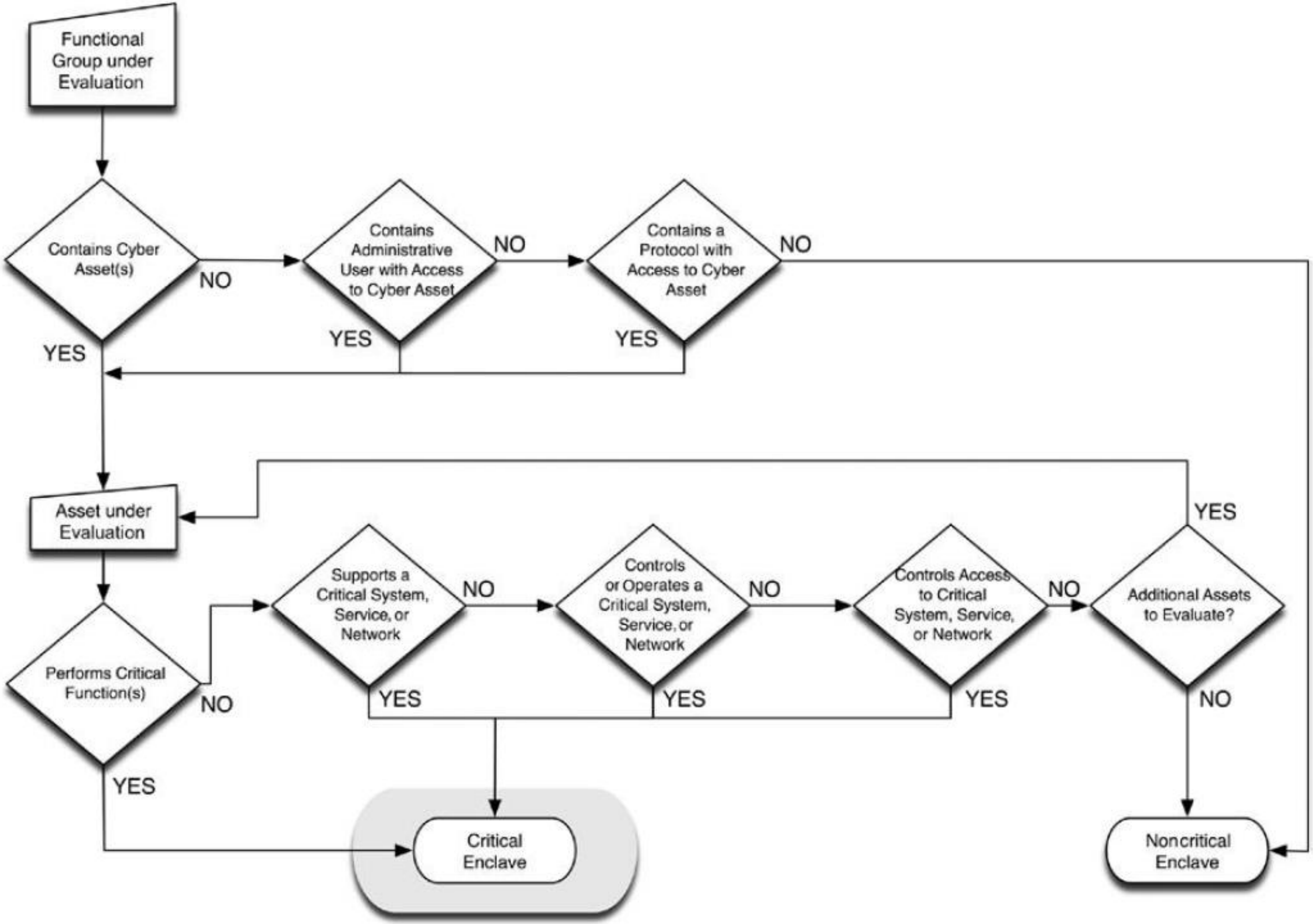
- Functionally defined zones should be assessed within the context of their criticality
- Additional protection within each zone

Criticality

Granular zoning benefits:

- Minimize scope of accident
  - If asset is compromised, only limited number of systems are impacted due to communication via conduits
- Secure critical devices from insider threat
  - Employee has access to physical devices but parent zone (logical access) via conduits
- Prevent lateral attacks from one critical system to the next
  - If all critical systems are grouped as “critical”, successful breach of one puts entire infrastructure at risk

Determining the Criticality of an Enclave


Functional Group under Evaluation
Contains Cyber Asset(s)
NO
Contains Administrative User with Access to Cyber Asset
NO
Contains a Protocol with Access to Cyber Asset
NO
YES
YES
YES
Asset under Evaluation
YES
Performs Critical Function(s)
NO
Supports a Critical System, Service, or Network
NO
Controls or Operates a Critical System, Service, or Network
NO
Controls Access to Critical System, Service, or Network
NO
Additional Assets to Evaluate?
YES
YES
YES
NO
YES
Critical Enclave
Noncritical Enclave

Functional Groups for Zones and Conduits

Excellent way to eliminate unknown, unauthorized devices from a group

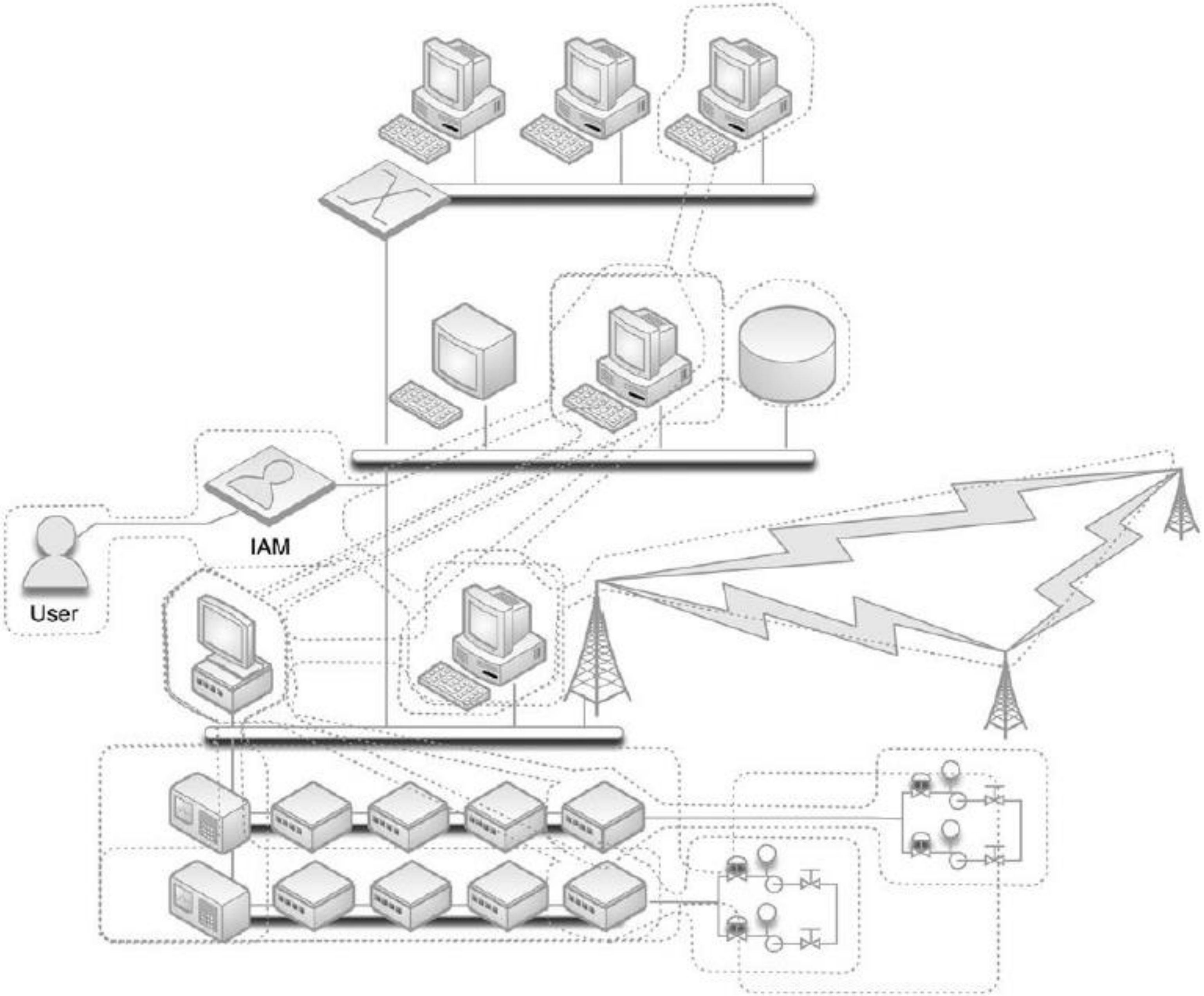
- If two devices do not share a common quality, there is no way for them to communicate

Yet, there are overlapping functional groups

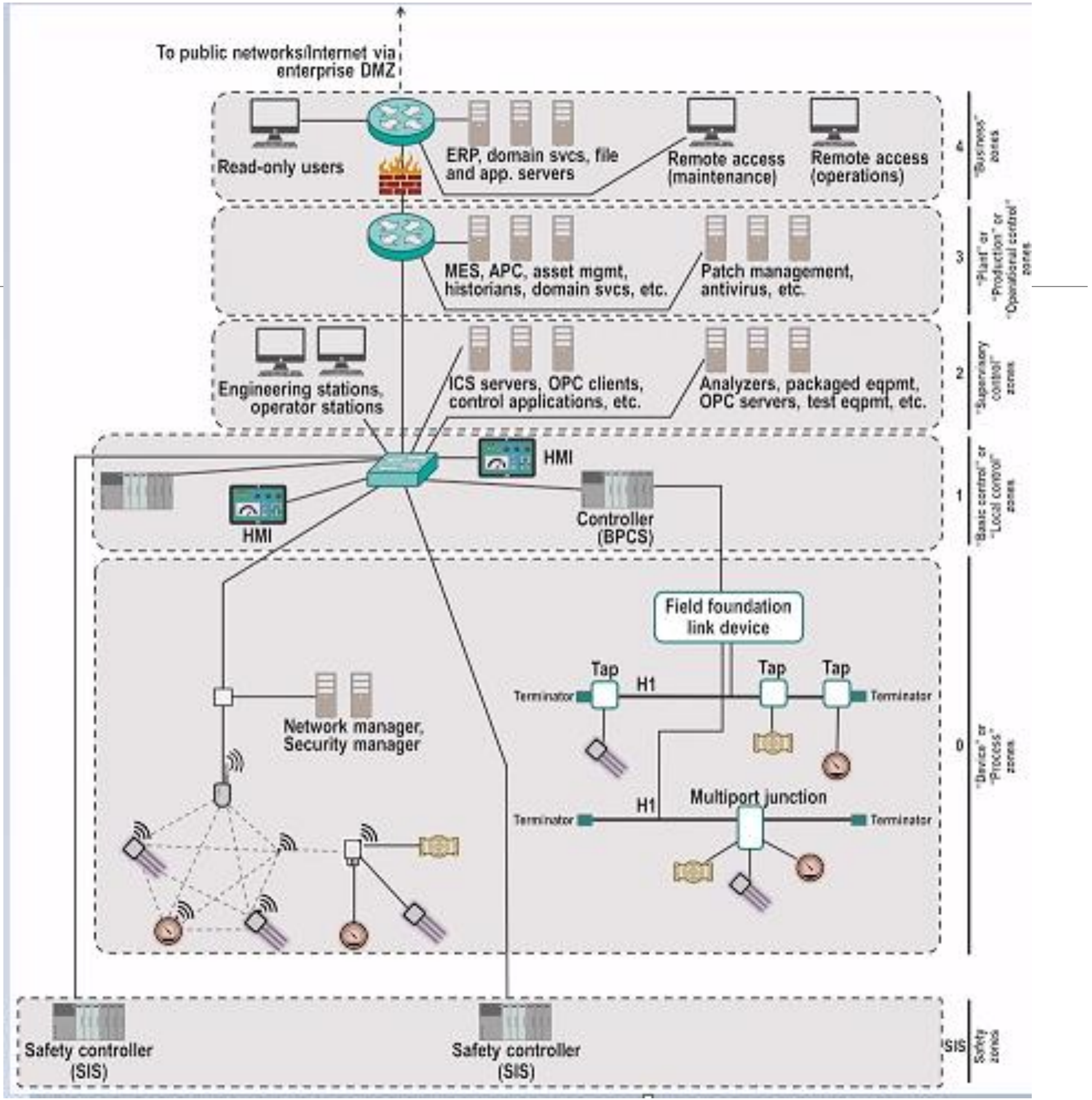
- Any devices support multiple protocols, applications, services, and other qualities
- Difficult defining clear-cut groups when so many variables are in play

Ideally, every functional group would contain a clear demarcation from every other group, and each demarcation would be secured using a unique protective device

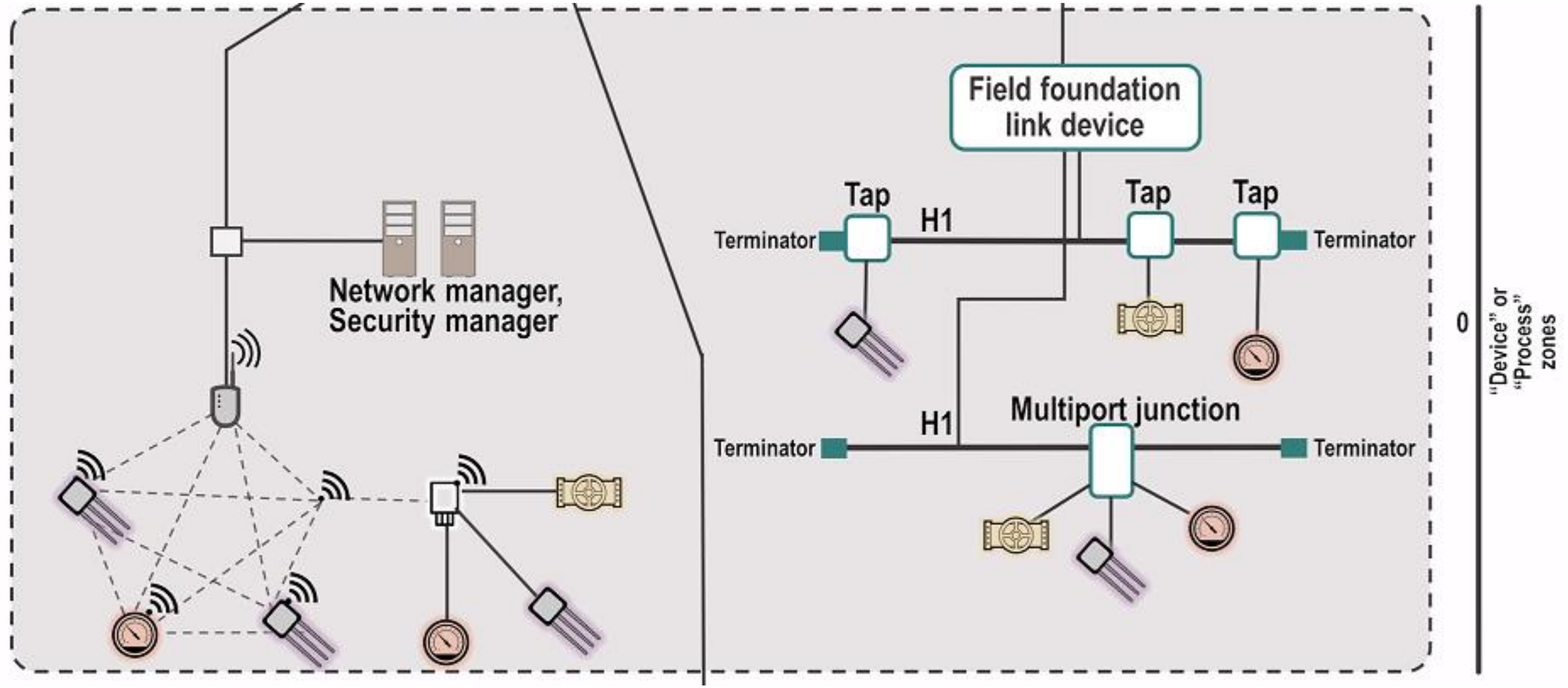
Overlapping Function Groups



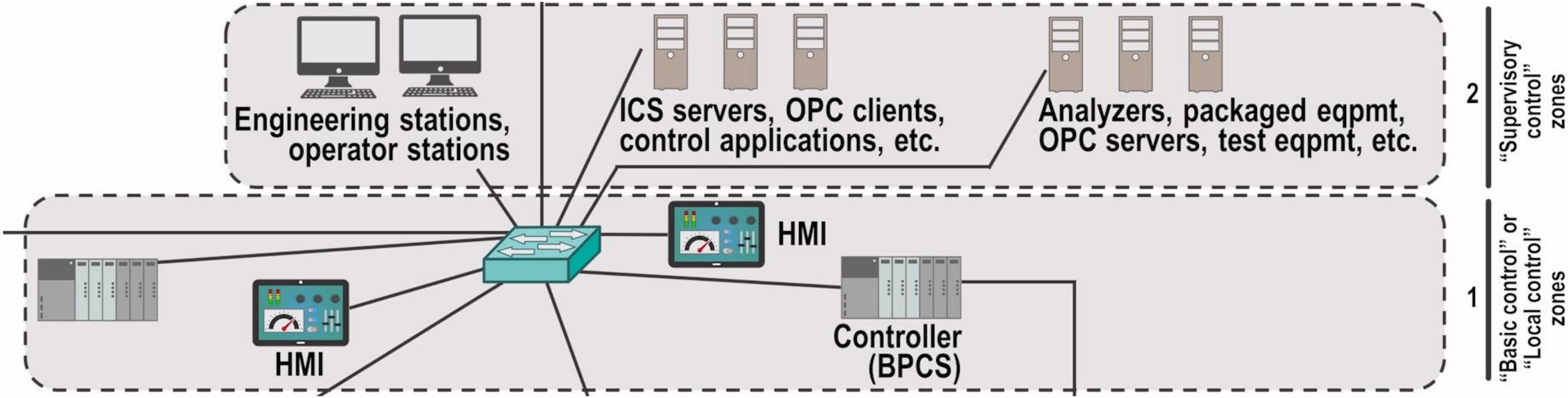
Example of Zones


To public networks/Internet via enterprise DMZ
Read-only users
ERP, domain svcs, file and app. servers
Remote access (maintenance)
Remote access (operations)
4
"Business" zones
MES, APC, asset mgmt, historians, domain svcs, etc.
Patch management, antivirus, etc.
3
"Plant" or "Production" or "Operational control" zones
Engineering stations, operator stations
ICS servers, OPC clients, control applications, etc.
Analyzers, packaged eqpmt, OPC servers, test eqpmt, etc.
2
"Supervisory control" zones
HMI
HMI
Controller (BPCS)
1
"Basic control" or "Local control" zones
Field foundation link device
Tap
Tap
Tap
H1
Terminator
Terminator
Network manager, Security manager
Multiport junction
H1
Terminator
Terminator
0
"Device" or "Process" zones
Safety controller (SIS)
Safety controller (SIS)
SIS
Safety zones

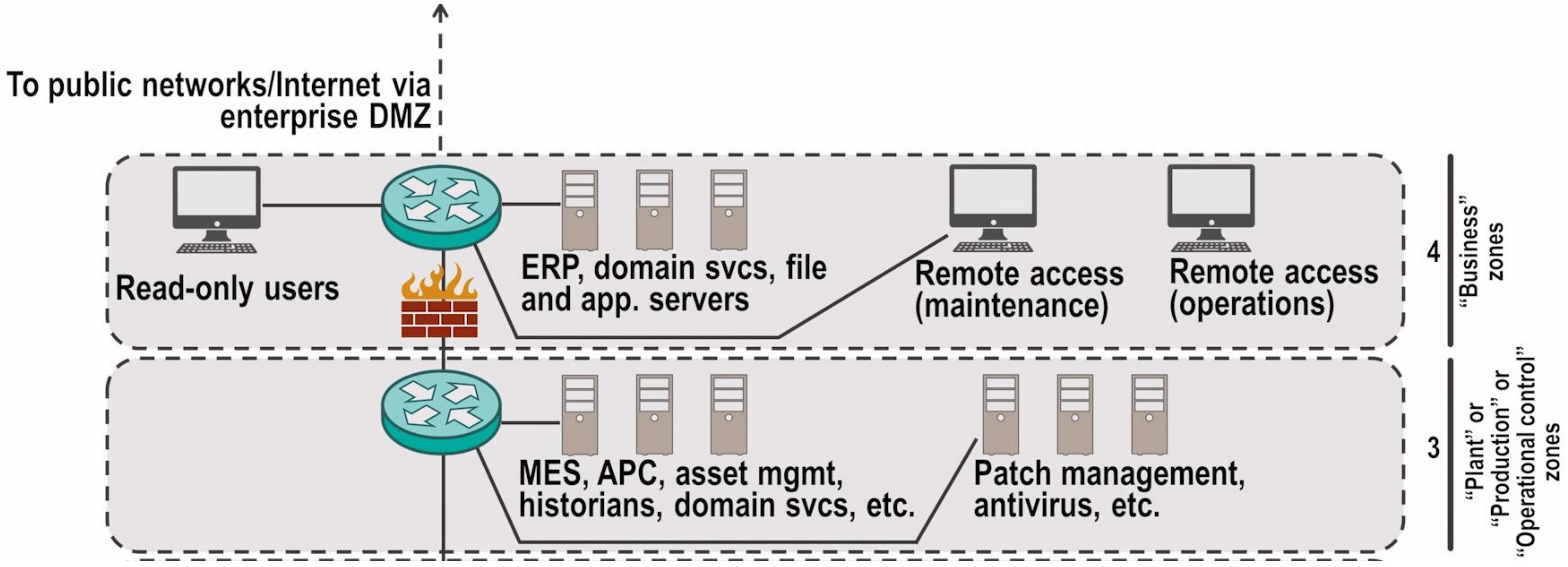
Process Zone



Local Control and Supervisory Control Zones


Engineering stations,
operator stations
ICS servers, OPC clients,
control applications, etc.
Analyzers, packaged eqpmt,
OPC servers, test eqpmt, etc.
2
"Supervisory control" zones
HMI
HMI
Controller
(BPCS)
1
"Basic control" or "Local control" zones

Plant (Production) and Business Zones


To public networks/Internet via enterprise DMZ
Read-only users
ERP, domain svcs, file and app. servers
Remote access (maintenance)
Remote access (operations)
4
“Business” zones
MES, APC, asset mgmt, historians, domain svcs, etc.
Patch management, antivirus, etc.
3
“Plant” or “Production” or “Operational control” zones

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

Establishing Zones and Conduits

Establishing an enclave is <u>mapping those functional groups that need to be isolated</u> to the network architecture, policies, <u>and</u> configurations that are necessary to <u>enforce that isolation</u>

- Identifying the boundaries of each enclave so that perimeter defenses can be deployed in the correct location
- Making any necessary changes to the network so that the network architecture aligns with the defined enclaves
- Documenting the enclave for purposes of policy development and enforcement
- Documenting the enclave for purposes of security device configuration