Component/Device/Application/System/ Network Architecture Levels

Note: This was borrowed from DoD **UFC 4-010-06 10 October 2023** but can be used universally to categorize all ICS OT IoT devices, components, applications, systems, and network levels based on how assets are being used, interfaced, configured etcetera. This is very helpful when tagging types of assets during threat modeling, security testing, security assessments, and when building and maintaining asset inventories, etcetera.

Architecture Diagrams

Figure 2-1 5-Level Control System Architecture

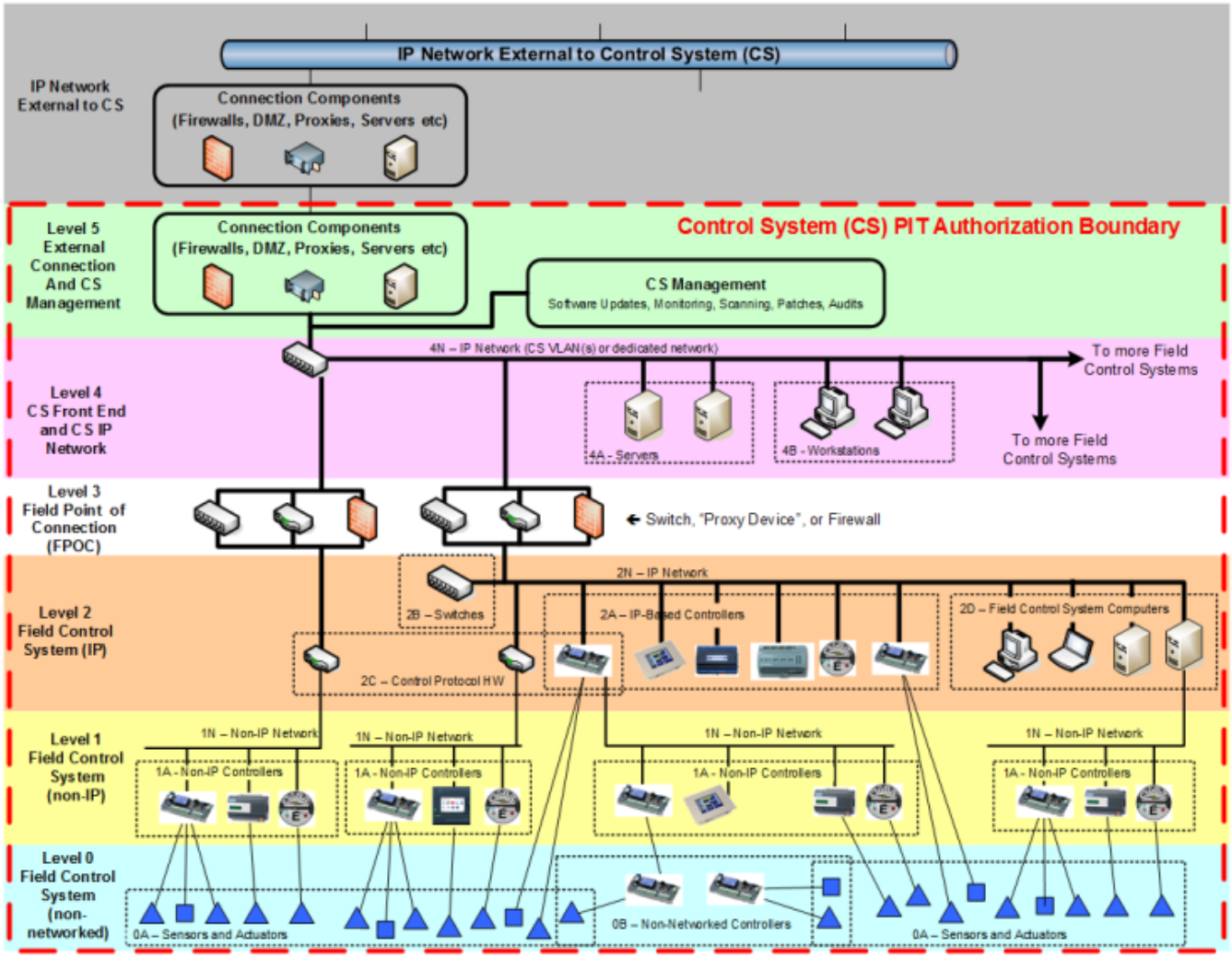
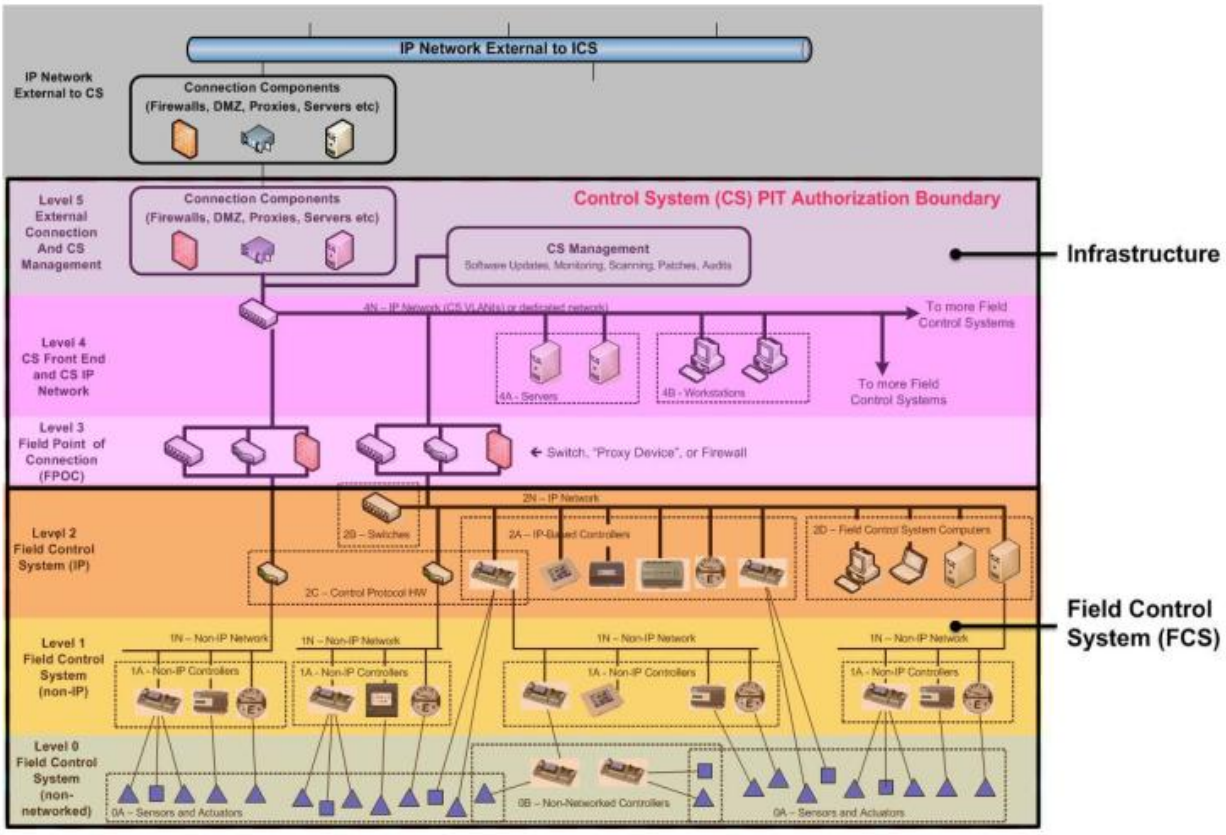


Figure 2-2 Control System Architecture



Component Architecture High Level Descriptions

- **Level 0:** Non-networked devices which communicate using analog and binary signals. These include (“dumb”) sensors and actuators as well as nonnetworked controllers (including their dedicated sensors and actuators). These communicate with Level 1 via hardware I/O (analog and binary signals).
- **Level 1:** Networked controllers not on an IP network (such as BACnet MS/TP, RS-485 (DNP, Modbus), LonWorks TP/FT-10). Can be fieldbus, RF and or ethernet physical/data link/application layer conduits.
- **Level 2:** Networked controllers on an IP network. Can be fiber, ethernet, RF conduits.
- **Level 3:** The Field Point of Connection (FPOC), which is a connection between the field control system IP network at Level 2 and the Level 4 IP network.
- **Level 4:** The site-wide IP network used for the control system, along with front end servers and workstations (desktops and laptops).

- **Level 5:** Interfaces to “external” networks (IP networks other than the control system network). In many cases this level will not be a requirement of the project and will be provided by others. When it is part of the project it must be specified separately than the control system using IT specifications and standards. Can be Cloud components.

Note: that some levels contain sub-levels. Some assets can also have the features and functionality to operate at more than one level within the same component. In those cases, assigned the component level based on the components configuration and usage within the system under consideration in the boundary/enclave/zone scope. Terms like base, installation in the military can be understood to be equivalent to an entire plant or campus or compound in the commercial and civilian sectors. FCS/FRCS = facility related control systems. These component architecture levels can be used to map out all types of ICS OT IIoT IoT and Cyber-Physical Systems. The referenced UFC was written by the FRCS community within DoD.

Component Architecture Level Details

Example detailed explanations for each level.

Level 0: SENSORS AND ACTUATORS

Level 0 consists of non-networked devices which communicate using analog and binary signals. These include (“dumb”) sensors and actuators, as well as non-networked controllers. These communicate with Level 1 or Level 2 via hardware I/O (analog and binary signals).

Definition:

Level 0 devices lack a network and therefore cannot be attacked over a network. Level 0 devices, if they communicate at all, use only simple analog and binary signals, they do not use any form of digital protocol for communication. A sensor or actuator that uses a communications protocol (such as Zigbee, Bluetooth) is a Level 1 (non-IP) or Level 2 (IP) device.

Functional Description:

The interface between the control system and the underlying controlled process / equipment where electrical signals in the control system get converted to/from physical values and actions in the underlying controlled system. Level 0A consists of Sensors and actuators Level 0B consists of non-networked controllers and their integral sensors and actuators. Level 0B devices may have some intelligence and may even have an internal network, but the device does not expose any internal network to other devices. These devices are typically packaged units with factory-installed integral controllers. Note that a “stand-alone” built-up unit with multiple field installed controllers which communicate over a network specific to that unit is NOT a Level 0 component, but rather a stand-alone field control system of its own.

Implemented Via:

Devices which:

- Convert physical properties (temperature, pressure, etc.)to a binary or analog electrical signal
- Take a binary or analog electrical signal and produce a physical action (open / close a valve or damper, etc.)

These electrical signals are purely binary or analog – there are no exposed digital signals or networks at this level. Also note that "smart" sensors or “smart” actuators which include a controller and network connection are Level1 or Level 2 devices.

Example Components:

Many of these devices are very simple (“dumb”) sensors or actuators, but more complex equipment may be at level 0 – if it lacks a network connection. Some examples are:

- A thermistor temperature sensor which simply provides a changing resistance as an indication of temperature is a Level 0A device.
- An electric actuator which takes a 4-20 mA signal and produces a proportional physical response is a Level 0A device.
- An occupancy sensor which uses BACnet to communicate occupancy values is a Level 1 (or Level 2) device, ***not*** a Level 0 device.
- A variable frequency drive controlling an air handler fan and using only binary and analog signals to communicate with the air handler controller is a Level 0B device.
- A flow sensor using HART over an analog wire is using a digital protocol (HART) and is a Level 1 device, ***not*** a Level 0 device.
- A packaged diesel generator operating in a stand-alone configuration – again with no network connection to other devices - is a Level 0B device, even if it has binary or analog connections to other devices.
- A relay panel acting as a Level 0 hardware interface between a building fire protection system and a sitewide radio network to a sitewide fire department.

The last three examples illustrate that the defining characteristic for Level 0 is not the complexity of the device, but rather whether the device communicates with other devices using a network.

Security Considerations:

In general, management and operational controls such as physical security and access control may still apply to this level. These devices are physically attached to the mechanical/electrical system and physical security is dictated and implemented based on the physical access to the

equipment. Utility vaults, Mechanical, Electrical, Plumbing rooms, Pump Stations, etc. should be secure and only authorized personnel should have access. These devices, while they do not have network communication, can cause physical damage, for example a valve left in the “Open” position.

Level 1: FIELD CONTROL SYSTEM (NON-IP)

Level 1 contains networked controllers not on an IP network (such as BACnet MS/TP, RS-485 (DNP, Modbus), LonWorks TP/FT-10). Details for Level 1 are shown in Table C-2.

Definition:

That portion of the controls network which does not use the IP protocol. This includes both the controllers themselves (Level 1A) and the network (Level 1N).

Functional Description:

(Level 1A) This is where the control logic resides and gets converted to or from binary and analog electrical signals, as well as the portion of the control system where:

- Analog and binary electrical signals (from sensors) get converted to digital signals via analog-to-digital (A-D)converters.
- Digital information is converted to analog and binary electrical signals (to actuators) via digital-to-analog (D-A)converters.
- Digital information is transmitted and received over a network.
- Digital information is processed according to a user defined sequence to generate new digital information.
- Devices may incorporate integral Level 0 sensors and actuators, for example, many variable air volume (VAV)box controllers incorporate an electric actuator.

Not all controllers will have hardware inputs. While there is exchange of data over the network, good design practice dictates that most of the data processing occurs using local (integral or via analog or binary signals) sensor data and local actuator outputs; the system is designed to minimize dependence on networked data.(Level 1N) The Level 1 network (media and hardware) does not use IP. It uses a variety of media at OSI Layers 1 and 2 (some standard, some not) and it uses Layer 3 protocols other than IP. Some examples are:

- BACnet over MS/TP, or BACnet over ARCnet
- LonTalk over TP/FT-10 or LonTalk over TP/XF-1250
- Modbus over RS-485For this reason, it is generally very specific to the control application and cannot be used for "standard" IT protocols and applications.

Implemented Via:

(Level 1A) Controllers, typically equipped with multiple analog and binary inputs and outputs and corresponding A-D and D-A converters. These devices are driven by cost to have the minimal functionality for the application and are very constrained in random access memory (RAM), processing power, and network input/output (I/O). In addition, these devices come in a vast variety of architectures, processors, vendors, and firmware.(Level 1N) The network media and hardware are similarly dedicated to that specific control protocol and are made by a variety of vendors.

Example Components:

- VAV box controllers
- Networked (non-IP) electric meter
- Intelligent (networked) thermostat
- LonWorks TP/XF-1250 (media) to TP/FT-10 (media) router. (This is not an IP router but routes the control system protocol at Open Systems Interconnection layer 3.)

Security Considerations:

Since devices (controllers) in this tier tend to be simpler devices, often few security controls can be applied, particularly after the system has been designed and installed. Since they do not use IP, network attacks must be very protocol specific. Some basic controls/measures that can be applied at this tier include:

- Disabling (or at a minimum prohibiting) secondary network connections (connections other than to the Level 1network)
- The use of passwords on devices such as displays (to the capability supported by the device – many of which do not permit 14 character passwords, for example)
- The application of physical security measures – which will be dictated and implemented by the underlying equipment

Level 2: FIELD CONTROL SYSTEM (IP)

Level 2 consists of networked controllers on an IP network.

Definition:

The portion of the control system which uses IP but is not shared with any other system. “Shared” in this context primarily refers to physical equipment and media. Note the Level 2 IP network is typically contained within a single building but may span multiple buildings in support of a control system for a single (linear) facility.

Functional Description:

2A	This Level (along with Level 1) is where the control logic resides and where it gets converted to/and from electrical signals and can have the first IP connections. This is the portion of the control system where: • Analog and binary electrical signals (from sensors)get converted to digital signals via A-D converters • (although not all controllers will have hardware inputs). • Digital information is converted to analog and binary electrical signals (to actuators) via D-A converters(although not all controllers will have hardware outputs). • Digital information is transmitted and received over a network. • Digital information is processed according to a user defined sequence to generate new digitalin formation. • These devices may incorporate integral Level 0sensors and actuators, for example, many Variable Air Volume (VAV) box controllers incorporate an electric actuator. Note this functional description is identical to that of Level 1. From a controls perspective, there is little difference between Level 1 and Level 2.
2N/2B	The IP network (media and hardware) dedicated to the control network and carrying the control protocol (such as Distributed Network Protocol (DNP), IEC-

	61850, BACnet/IP, or Lon/IP)). Generally, IP over Ethernet.
2C	Control Protocol Routers and Gateways. Control Protocol Routers route the control protocol – that is, they selectively forward control protocol packets based on destination address. They are not IP routers. Control Protocol Gateways translate between Control Protocols.
2D	Where the local control system has an elevated C-I-A requirement (due for example to a reliability requirement, an operator response time, or a need for local operators which cannot be met by the remote site-wide front end), the facility control system may contain a local operator interface similar to what is normally found at Level 4 but dedicated to this specific control system. In other cases, for either legacy or stand-alone systems (not necessarily isolated but stand alone in that they do not rely on another system such as a control system), the front-end operator interface may be physically local to that system. In this case, the operator interface is part of Level 2 since it is dedicated to that building or facility and traffic between it and the Level 1 and Level 2 devices does not pass through the Level 3 FPOC.

Implemented Via:

2A	Controllers, typically equipped with multiple analog inputs and outputs and corresponding A-D and D-A converters. These devices are driven by cost to have the minimal functionality for the application and are very constrained in RAM, processing power, and network I/O. In addition, these devices come

	in a vast variety of architectures, processors, vendors, and firmware. Aside from the fact that they use IP and are more powerful than Level 1A devices, they are otherwise identical to Level 1A devices. Many devices are available as either Level 1A or 2A devices, where the hardware is identical except for the transceiver; some can even be field configured for one or the other.
2N/2B	The Level 2N IP network is Ethernet, and the Level 2B network hardware is standard IT network hardware, though sometimes with reduced functionality. For example, there may not be any requirement for remotely managed switches. Similarly, there is seldom a need for an IP router, since field control systems reside within a single (private) IP subnet.
2C	Controllers are very similar in hardware characteristics to Level 2A devices except that these devices typically have multiple network interfaces.
2D	Computers (as for Level 4)Computers for legacy systems Custom or modified computers with a touch screen interface.

Example Components:

2A	Air Handler Controller Chiller Controller Boiler Controller Terminal Unit Controller Hydronic System Controller Supervisory Controller System Scheduler Electric Meter Local Display Panels Electrical Protective Relay Voltage Regulator Controller

2N/2B	Ethernet Switch
2C	BACnet MS/TP to BACnet/IP Router LonWorks TP/FT-10 to LonWorks IP Router
2D	Control system at a central plant where the nature and criticality of the system requires a local operator interface.

Security Considerations:

2A	Controllers residing on the dedicated IP network vary from devices residing on a typical IP network. • They use a single fixed protocol (or a small number of fixed protocols) • They often do not support “log in” functionality • There is often no “session” capability • They usually do not include a user interface, and if they do it is extremely limited. • They have very limited hardware capabilities (RAM,CPU, storage, etc.) • They do not use Windows and seldom use Linux. They are some version of a real time operating system (RTOS). Many of the controllers will have the same limitations as the controllers in Level 1, where most security controls cannot/or will not apply to them. Some controllers will have significantly more capability, however, and additional controls will be applicable. In either case, the controllers should disable any network connections or services not required for operation of the control system.

2N/2B	This network is dedicated to the control system and is installed by the control system contractor, not the IT organization. This does not reduce the need for securing this network, but does affect the way in which this network is secured, and the risks and vulnerabilities that need to be addressed Some key differentiators between the Level 2 network and a standard IP network are: • The network structure and connected devices remain more static throughout the life of the system. Components are not added and removed on a regular basis. • The protocol(s) used are fixed, and in many cases only a single protocol is used. The protocols also differ from “regular” IP networks in that they are control system protocols rather than standard IT protocols. This allows for the implementation of very simple (a few very broad rules) firewalls to limit traffic. • Bandwidth usage is lower. Because the network configuration is more static, the bandwidth usage is also more fixed. • The devices residing on the network have fewer capabilities and do not support network security standards such as IEEE 802.1X. • The control system does not require the level of functionality that Approved Product List (APL)network infrastructure devices provide. The Navy, however, does require APL products for all IP Network Hardware.

	• Standard IT devices typically do not meet the UL Listing requirements for fire and life safety systems, so specialized network hardware may be required to meet the control system needs.
2C	These devices are not manufactured by traditional IT companies and do not run standard IT software. Their functionality is often included as part of a Level 2A device. They do not route IP.
2D	While functionally, Level 2D components act similarly to computers at Level 4, the fact that they are local to (and dedicated to) a specific control system means that from a security controls perspective, they are better addressed as Level 2 components. There are two main reasons for computers at Level 2D: • Legacy systems that cannot be patched. The computers at Level 2D may be running an older operating system and may not support some of the security controls. In this case, the controls which can be applied without negatively affecting the availability of the system should be applied, and mitigating controls and measures should be taken when otherwise needed. Systems containing these computers should not be connected to other systems (i.e., should be operated stand-alone) until they can be properly addressed, with the computers replaced or otherwise upgraded to Level 4standards. • Where a new system requires a local front end that, for whatever reason, cannot be installed on the base-wide shared IP network (Level 4). This is

	typically due to a C-I-A requirement. When installing a new system with a Level 2 front end, it is important to note that the Level 2 front end should be subject to the same controls as a Level 4 front end. While implementation and inheritance of security controls at this level may differ from the Level 4 front end, computers at this Level should be subject to the same controls as a "normal" Level 4 front end of equivalent criticality.

Level 3: FIELD POINT OF CONNECTION (FPOC)

Level 3 is the Field Point of Connection (FPOC), which is a connection between the field control system IP network at Level 2 and the Level 4 IP network.

Note: that there may be devices which resemble an FPOC in the sense that they are a security device providing a managed interface between different networks but are not located between a dedicated IP network and a base-wide shared IP network. While these devices act as a security barrier, the term FPOC is reserved for a security device between Level 2 and Level 4.

Definition:

The device which connects the dedicated Level 2 IP network with the Level 4 IP network.

Functional Description:

For each field control system, the FPOC is the specific single demarcation point in the control system between that field control system and the front-end system. The FPOC is a standard IT device, usually an Ethernet Switch. The FPOC has security controls in that it restricts access (by user, protocol, or specific commands) between levels above and levels below. Note that a large system (consisting of hundreds of FCS) will have hundreds of these FPOC devices, one at each connection of a field control system to the local network.

Implemented Via:

Almost always an Ethernet switch or IP router.

Example Components:

Standard IT managed Ethernet switch or IP router.

Security Considerations:

This device is critical from a security controls perspective as it is where the dedicated local field control network connects to the installation-wide IP network. Normally, securing this device protects the installation-wide network from the local field systems (which often have a difficult time meeting security controls). Occasionally, where there is a critical field control system, this device can protect the more critical field control system from the less-secure local system (i.e., where there are 99 non-critical systems and 1 critical one, isolate the 1 from the 99 rather than try and secure the 99).This device should, in effect, have a "deny all / permit by exception" policy applied. The FPOC should be set up with the most restrictive set of access control list (ACL) possible.

Level 4: CONTROL SYSTEM FRONT END AND CONTROL SYSTEM IP NETWORK

Level 4 is the IP network used to connect multiple Level 2 networks, along with front end servers and workstations (desktops and laptops).

Definition:

Front End computers and the IP network which connects multiple Level 2 Field Control Networks and is (generally) not dedicated to a specific FCS. The IP network may be shared with other applications, a dedicated physical network, or a Virtual Local Area Network (VLAN) or a Virtual Private Network (VPN) riding on top of another network.

Functional Description:

(Level 4A and 4B) The multi-facility operator interface for the system. This is typically a web-based client-server system with the servers (Level 4A) running vendor-specific software on standard server PCs and the clients (Level 4B) accessing the servers via standard web browser software. Some functions of the control system are:

- Providing graphical screens for monitoring and control of the system
- Allowing operators to schedule systems, set up historical trends, and respond to alarm conditions
- Provide for and support global control and optimization strategies that are impractical to implement within the control systems
- Perform real-time analytical analysis and take appropriate real-time actions through supervisory commands to devices at levels 1 or 2.

This level usually also includes Engineering Tool Software which provides tools for creating and modifying the control system. The Level 4N network is the network that connects multiple facility networks into a common base-wide network. (Note that this network is referred to as base wide as that is the normal use case, but it could be entirely contained within a single building).

Implemented Via:

Either a dedicated physical network, or a Virtual Local Area Network (VLAN) or a Virtual Private Network (VPN) riding on top of another network, or some combination of these options. Personal Computers, servers, and network devices.

Example Components:

Servers and racks, computers, Laptops, operator interfaces, and network devices. The control system racks, hardware and software will be in an Energy Operations Center, Campus Wide Operations Center, Facility Operations Center, Facility and Energy Operations Center, Security Operations Center, or Regional Operations Center.

Security Considerations:

Level 4 is where the control systems (ICS OT IIoT IoT Cyber-Physical Systems) most closely resemble a “standard” information system, and most security controls can be applied at this layer. It is critical to remember that control system is NOT a standard IS, however, and that controls must be applied in such a way as to not hamper the availability of the system. For example, some control systems require software updates from the manufacturer prior to the implementation of a Java patch, and controls relating to the application of patches must not be implemented in a manner that requires automatic or immediate patching without ensuring that this will not cause the system to go offline. Unlike standard IT applications (such as virus software or office automation tools), control system applications are a niche product and while standard guidance may cover some aspects of securing these applications, it will be insufficient to fully secure them.

Level 5: EXTERNAL CONNECTION AND CONTROL SYSTEM MANAGEMENT

Level 5 contains interfaces to “external” networks (IP networks other than the control system network).

Definition:

Additional hardware, software, and networking used to manage the control system, provide security functionality, user management, and external access. These are IT management and IT security functions, and do not provide control system functionality. (e.g., email, HR, finance, Cloud infrastructure etcetera)

Functional Description:

In many architectures, this level provides the enclave boundary defense between the control system (at Level 4 and below) and IP networks external to the control system. (In other architectures, this boundary defense occurs in the external network). In many cases, there is a component within the control system which would reside in Level 5.This level may be absent for a variety of reasons: there may not be an external connection, or the connection may be handled in the external network. Additional functionality allowed through external connections may include:

- Sending alarm notification using outbound access to a SMTP email server.
- Upload of historical data and meter data to an enterprise server using outbound HTTP/HTTPS access for uploading.

In some cases, inbound HTTP/HTTPS may be allowed from web clients on the external network to the Level 4A server, but this is not required and is often prohibited for security reasons. The Navy prohibits this functionality.

Implemented Via:

Firewalls
DMZ/Perimeter Networking
Proxy Servers
Domain Controller, etc.

Example Components:

Wide Area Networks

Metropolitan Area Networks

Local Area Networks

Campus Area Networks

Virtual Private Networks

Point of Presence

Demarcation Point or Main Point of Presence

Security Considerations:

If the control system can function in a completely isolated configuration, it should, and external connection should be absent. This Level should implement a "deny all / permit exception" policy to protect the control system from the external network and the external network from the control system.

Summary

When conducting Threat Models, Security Assessments, Asset Inventories etcetera, remember to reference the 5 level ICS OT IIoT IoT Cyber-Physical Systems architecture. Always describe which level the components in scope each are being used and configured as for the systems, components, zones, enclaves etcetera under consideration/in scope. This enables a common lexicon when discussing ICS OT IoT IIoT Cyber-Physical Assets from a security and operational perspective.