CHAPTER 2

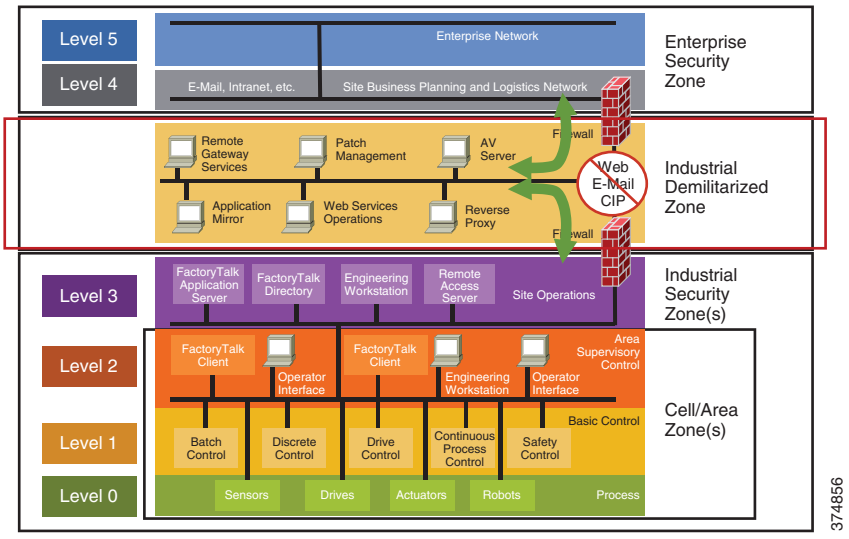
CPwE Network Security Solution Considerations

This chapter covers the CPwE Network Security Solution and its various solutions, components, and their relation to each other. CPwE Network Security Solution is an architecture that provides visibility, profiling, segmentation, network flow detection, malware detection, and OT influenced remote access services to the devices, equipment, and applications found in an Industrial Automation and Control Systems (IACS). The CPwE Network Security Solution architecture overview provides the background and description of an IACS network model.

CPwE Reference Architecture

The CPwE logical model employs commonly used industry standards such as Purdue Model for Control Hierarchy (reference ISBN 1-55617-265-6) to organize the plant functions into Levels and IEC-62443 (formerly ISA99) to organize the Levels into functional and security Zones, as shown in Figure 2-1.

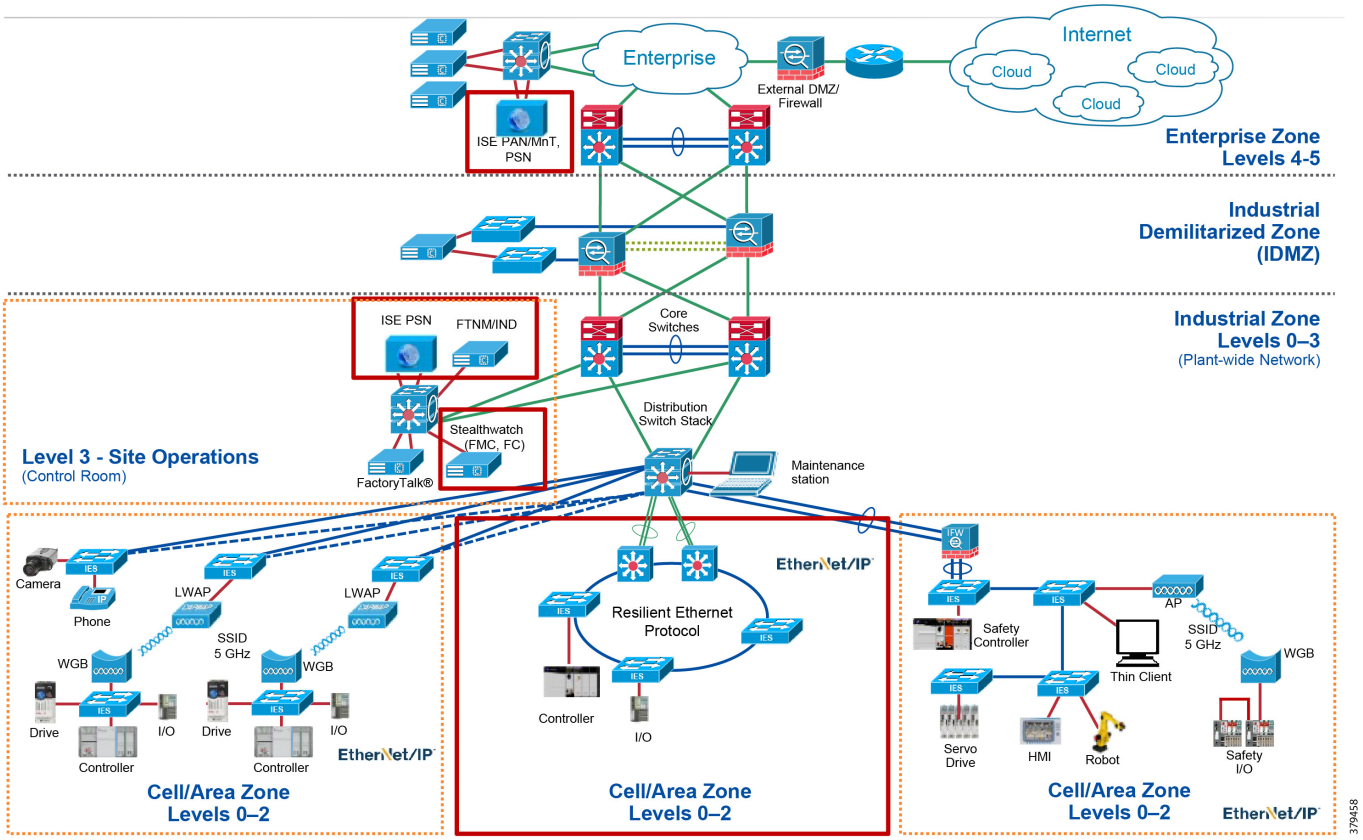
Figure 2-1 CPwE Logical Zoning Based on Purdue Model and IEC-62443



Cell/Area Zone

The Cell/Area Zone is a functional zone where the IACS assets interact with each other. The industrial network is a critical factor for the Cell/Area Zone because all the IACS assets must communicate to ensure that requirements for industrial operations are met. A plant-wide architecture may have one or multiple Cell/Area Zones. Each Cell/Area Zone can have the same or different network topologies. There could be different network topologies present throughout the entire plant-wide architecture. For the purpose of this CPwE Network Security CVD DIG, a ring topology was chosen for design, testing and validation because the ring topology design provides resiliency. Figure 2-2 depicts what Cisco and Rockwell Automation have validated as part of CPwE Network Security CVD.

Figure 2-2 CPwE Network Security Scope



Industrial Zone

The Industrial Zone comprises the Cell/Area Zone(s) (Levels 0 to 2) and Site Operations (Level 3) activities. The Industrial Zone is important because all the IACS applications, assets, and controllers critical to monitoring and controlling the plant-wide architecture industrial operations are in this zone. To preserve smooth industrial operations and functioning of the IACS applications and IACS network, this zone requires clear logical segmentation and protection from Levels 4 and 5 of the enterprise operations.

System Components

Table 2-1 lists all the Cisco and Rockwell Automation components that are involved in this design.

Table 2-1 Cisco and Rockwell Automation Components

Role	Model	Software Release	Comments
Layer 2 Industrial Ethernet Switch	Cisco IE 4000/5000 Allen-Bradley Stratix 5400/5410	15.2(6)E2	Provides connectivity to IACS assets at Levels 0-2
Distribution Switch	Cisco Catalyst 3850	16.3.5B	Distribution/Aggregation switch connecting the Cell/Area Zones
Cisco Identity Service Engine		2.4	Policy Access Control
Industry Network Director/Factory Talk Network Manager		1.5	Network Monitoring Tool (NMT)
Stealthwatch Flow Collector		6.10.2	Flow anomaly detection
Stealthwatch Management Console		6.10.2	Dashboard
Core Switch	Cisco Catalyst 6880	15.2(1)SY1a	Provides core functionality to the design.

Cisco Industrial Ethernet 4000 and Allen-Bradley Stratix 5400 Series IES

These platforms have been selected for the CPwE Network Security Solution for the following reasons:

- Support for in-line tagging.
- Full NetFlow support.
- Bandwidth and capacity to grow with your networking requirements, including 20 Gbps nonblocking switching capacity with up to 20 Gigabit Ethernet ports per switch.
- Cisco IOS software features for smooth IT integration and policy consistency.
- Robust resiliency enabled by 4x Gigabit Ethernet uplink ports, Resilient Ethernet Protocol (REP) for ring topology, EtherChannel and Flex Links for redundant start topology, and redundant power input.
- True zero-touch replacement for middle-of-the-night or middle-of-nowhere situations.
- Simplified software upgrade path with universal images.
- Industrial environmental compliance and certifications.
- Industrial protocol support: e.g., EtherNet/IP and PROFINET.

Cisco Identity Service Engine

Cisco Identity Service Engine (ISE) brings awareness to all the devices that are accessing the network. It allows an OT-IT security team to design and implement a consistent security access policy in the IACS network. The users and device details are presented in a simple, flexible interface. ISE shares user, device, and network details through the Cisco Platform Exchange Grid (pxGrid) with NMT to enhance the security access policy. Cisco ISE can reduce risks and contain threats by dynamically controlling network access. More details about Cisco ISE can be found in the Cisco ISE Overview (https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html#~stickynav=1).

Cisco Industry Network Director and Rockwell Automation FactoryTalk Network Manager

A purpose-built platform for managing IACS networks, the Cisco Industrial Network Director and FactoryTalk Network Manager network monitoring tool (NMT) is designed to help operations teams gain full visibility of network devices and IACS assets in the context of industrial operations and provides improved architecture availability and performance, leading to increased overall equipment effectiveness (OEE).

NMT can also discover IACS assets such as PAC, I/O, RTU devices, etc. by communicating in their native communication protocol. NMT supports discovery of IACS assets that utilize the following industrial protocols:

- Common Industrial Protocol (CIP) for EtherNet/IP
- Profinet
- BACnet™
- Modbus®
- OPC-UA

NMT collects a set of attributes from IACS assets to provide visibility into IACS assets, as shown in Figure 1-3. NMT is able to show IACS asset information such as Vendor, Communication, Protocol, Product Name, Serial Number, and Device types.

Cisco Stealthwatch

Cisco Stealthwatch turns the network into a sensor (Network as a Sensor [NaaS]) and provides deeper visibility in your network by leveraging NetFlow and sFlow on switches, routers, and IPFIX on firewalls. With pxGrid integration to ISE Stealthwatch can help to quarantine security incidents, depending on the industrial security policy, and thereby protect potentially vulnerable IACS assets.

Cisco Stealthwatch provides real-time metadata into what each device is doing on the network, all of its network connections, interface utilization, and overall network performance. Also shown is various levels of machine-to-machine communication; if any IACS asset is infected, then Cisco Stealthwatch can detect IoT peer-to-peer malware. Malicious P2P traffic is hard to detect and block using traditional approaches that rely on lists of known IP addresses and hosts associated with command-and-control servers. Defense-in-depth security is required, but the capability to analyze and understand the information shown by combining different information points and vectors provides unequaled visibility for making operational decisions.

For example, Distributed Denial of Service (DDoS) attacks attempt to exhaust device resources, including network bandwidth, computing power, and operating system data structures. To launch a DDoS attack, malicious users first build a network of devices that will be used to produce the volume of traffic needed to deny services to users.

To create this attack network, attackers discover vulnerable devices on the network. Vulnerable devices are usually those that are not running antivirus software, running out-of-date software, or those that have not been properly patched. Vulnerable devices are then exploited by attackers to gain access to these devices. The next step for the attacker is to install attack tools on the compromised devices of the attack network. The devices that are running these attack tools are known as zombies and they can carry out any attack under the control of the attacker. Many zombies together form what is referred to as a botnet army. WAN saturation, an increase in host counts, and an increase in UDP packets are all common for a compromised organization.

An alternative approach to detect network attacks is to capture all traffic using RSPAN and observe the behavior of the packets to detect if there is any malicious attack occurring in the network. To capture all traffic, every switch needs to be configured with a port for redirecting the traffic to a central location, which often increases the cost of deployment. Moreover, if an attack is occurring in the network, then the IT security architect needs to use multiple programs to parse several captured files to detect the attack. With Cisco Stealthwatch, there is no need to invest in additional ports for capturing the traffic. Instead, the router or switch as a sensor captures the key pieces of the flow such as source IP address, destination IP address, source port, destination port, and other important fields that are part of a flow by using NetFlow which is built into the IES. Observing flows in a network can be used to quickly pinpoint where an attack is occurring in the network. In addition, to investigate how long a malicious behavior is occurring in the network, Cisco Stealthwatch can provide historical data for the flows that are interesting to obtain a detailed view on how long a particular attack has been occurring in a network.

Cisco Stealthwatch can detect and remediate a threat with over 94 different analytic algorithms on the contextual and flow information it receives which are used for anomaly detection. Events feed into high level alarm categories, which can generate an alarm. Some security events can alarm on their own. An alarm can have an associated response such as notify in the alarm table or generate a syslog message to a Security Information and Event Management (SIEM). Cisco Stealthwatch was deployed using the Network as a Sensor Cisco Validated Design guide and pxGrid was configured to communicate with ISE using self-signed based certificates.

- *Network as a Sensor with Stealthwatch and Stealthwatch Learning Networks for Threat Visibility and Defense Deployment Guide:*
  https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Feb2017/CVD-NaaS-Stealthwatch-SLN-Threat-Visibility-Defense-Dep-Feb17.pdf
- *Stealthwatch® Management Console VE and Flow Collector VE Installation and Configuration Guide (for Stealthwatch System v6.9.0):*
  https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management_console/virtual/installation/guide/SW_6_9_0_SMC_VE_and_Flow_Collector_VE_Installation_and_Configuration_DV_1_4.pdf

Cisco Catalyst 6880-X Product Details

The Cisco Catalyst 6880-X provides flexibility to build desired port density through two versions of base chassis (C6880-X-LE with standard FIB/ACL/NetFlow tables and C6880-X with larger FIB/ACL/NetFlow tables) along with optional port cards. The base chassis comes with 16 10G/1G ports and each port card supports 16 additional 10G/1G ports. Each system can be built up to 80 ports in 16-port increments. The port interface on the base module and the port cards support both 10 Gigabit Ethernet and 1 Gigabit Ethernet speeds, allowing customers to use their investment in 1 Gigabit Ethernet SFP and upgrade to 10 Gigabit Ethernet SFP+ when business demands change without having to do a comprehensive upgrade of the existing deployment. The port cards are hot swappable. For further information, visit the following page http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6880-x-switch/data_sheet_c78-728228.html

Note CPwE Network Security CVD was tested and validated with the Catalyst 6880. Taking into account TrustSec technology, a Catalyst 9500 could be used.

Cisco Catalyst 3850 Switch

The Cisco Catalyst 3850 Series multigigabit and 10-Gbps network switches provide both wired and wireless to support the scalability of a large network. These switches support stacking and are ideal for distribution in the CPwE network architecture. They offer different models for aggregation; details can be found at: https://www.cisco.com/c/en/us/products/switches/catalyst-3850-series-switches/index.html#~stickynav=1

Note CPwE Network Security CVD was tested and validated with the Catalyst 3850. Taking into account TrustSec technology, a Catalyst 9300 could be used.