CHAPTER 1

CPwE IDMZ Overview

This chapter includes the following major topics:

CPwE IDMZ Introduction

The prevailing trend in Industrial Automation and Control System (IACS) networking is the convergence of technology, specifically IACS operational technology (OT) with information technology (IT). Converged Plantwide Ethernet (CPwE) helps to enable IACS network and security technology convergence, including OT-IT persona convergence, by using standard Ethernet, Internet Protocol (IP), network services, security services, and EtherNet/IP. A reliable and secure converged plant-wide or site-wide IACS architecture helps to enable the Industrial Internet of Things (IIoT).

IIoT helps offer the promise of business benefits by using innovative technology such as mobility, collaboration, analytics and cloud-based services. The challenge for industrial operations is to develop a balanced security stance to take advantage of IIoT innovation while maintaining the integrity of industrial security best practices. Business practices, corporate standards, security policies and procedures, application requirements, industry security standards, regulatory compliance, risk management policies, and overall tolerance to risk are all key factors in determining the appropriate security stance.

Many organizations and standards bodies recommend segmenting business system networks from plant-wide and site-wide networks by using an Industrial Demilitarized Zone (IDMZ). The IDMZ exists as a separate network in a level between the Industrial and Enterprise Zones, commonly referred to as Level 3.5. An IDMZ environment consists of numerous infrastructure devices, including firewalls, virtual private network (VPN) servers, IACS application mirrors, remote gateway services and reverse proxy servers, in addition to network infrastructure devices such as routers, switches and virtualized services. CPwE IDMZ details considerations to help with the successful design and implementation of an IDMZ to securely share IACS data between the business systems within the Enterprise Zone and industrial operations within the Industrial Zone.

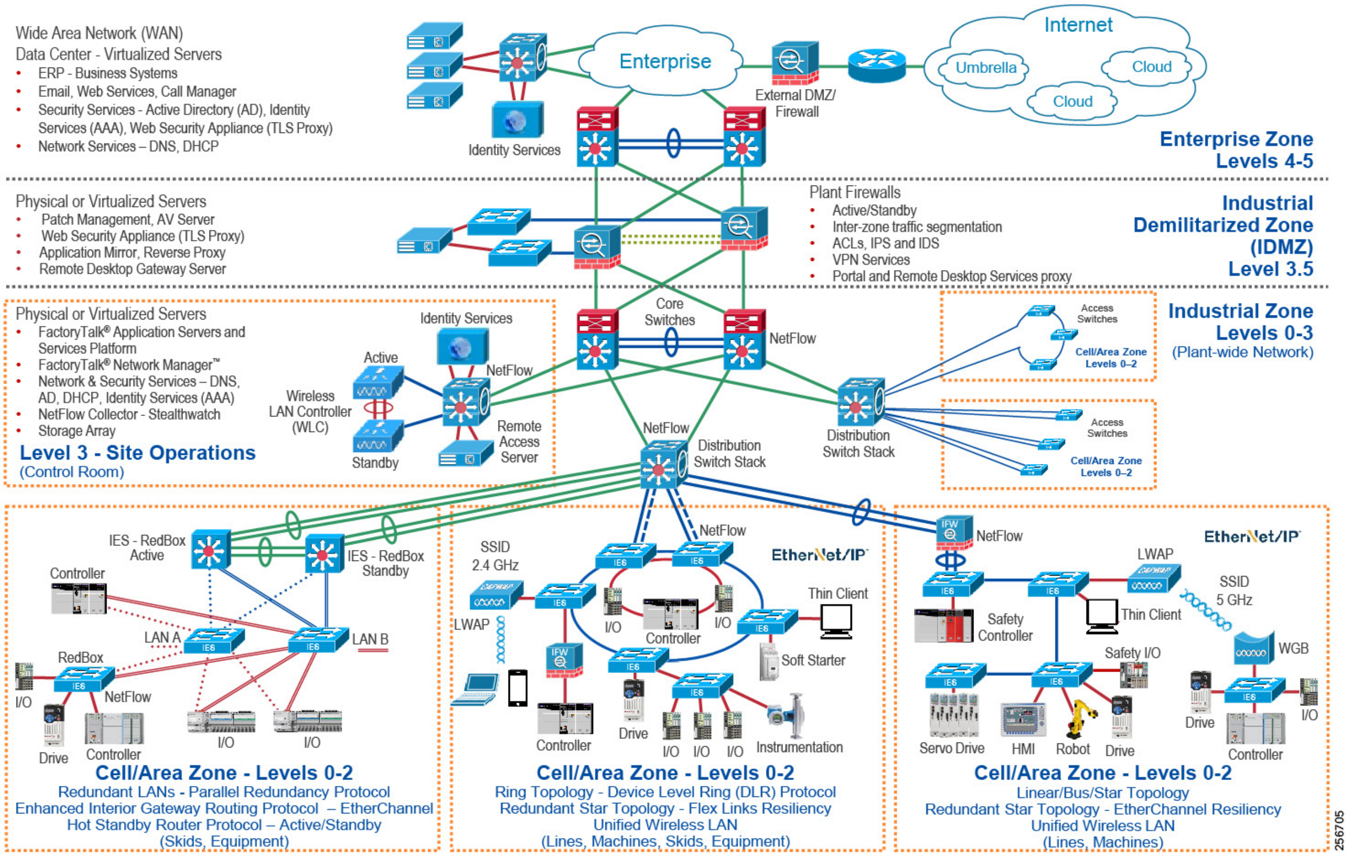
CPwE Overview

CPwE is the underlying architecture that provides standard network and security services for control and information disciplines, devices, and equipment found in modern IACS applications. The CPwE architectures (Figure 1-1) were architected, tested, and validated to provide design and implementation guidance, test results, and documented configuration settings. This can help to achieve the real-time communication, reliability, scalability, security, and resiliency requirements of modern IACS applications. The content and key tenets of CPwE are relevant to both OT and IT disciplines.

CPwE key tenets include:

- Smart IIoT devices-Controllers, I/O, drives, instrumentation, actuators, analytics, and a single IIoT network technology (EtherNet/IP), facilitating both technology coexistence and IACS device interoperability, which helps to enable the choice of best-in-class IACS devices
- Zoning (segmentation)-Smaller connected LANs, functional areas, and security groups
- Managed infrastructure-Managed Allen-Bradley® Stratix® industrial Ethernet switches (IES), Cisco Catalyst® distribution/core switches, FactoryTalk® Network Manager™ software, and Stratix® industrial firewalls
- Resiliency-Robust physical layer and resilient or redundant topologies with resiliency protocols
- Time-critical data-Data prioritization and time synchronization via CIP Sync® and IEEE-1588 Precision Time Protocol (PTP)
- Wireless-Unified wireless LAN (WLAN) to enable mobility for personnel and equipment
- Holistic defense-in-depth security-Multiple layers of diverse technologies for threat detection and prevention, implemented by different persona (for example, OT and IT) and applied at different levels of the plant-wide or site-wide IACS architecture
- Convergence-ready-Seamless plant-wide or site-wide integration by trusted partner application

Figure 1-1 CPwE Architectures


Wide Area Network (WAN)
Data Center - Virtualized Servers
ERP - Business Systems
Email, Web Services, Call Manager
Security Services - Active Directory (AD), Identity Services (AAA), Web Security Appliance (TLS Proxy)
Network Services – DNS, DHCP
Identity Services
Enterprise
External DMZ/ Firewall
Internet
Umbrella
Cloud
Cloud
Enterprise Zone
Levels 4-5
Physical or Virtualized Servers
Patch Management, AV Server
Web Security Appliance (TLS Proxy)
Application Mirror, Reverse Proxy
Remote Desktop Gateway Server
Plant Firewalls
Active/Standby
Inter-zone traffic segmentation
ACLs, IPS and IDS
VPN Services
Portal and Remote Desktop Services proxy
Industrial Demilitarized Zone (IDMZ)
Level 3.5
Physical or Virtualized Servers
FactoryTalk® Application Servers and Services Platform
FactoryTalk® Network Manager™
Network & Security Services – DNS, AD, DHCP, Identity Services (AAA)
NetFlow Collector - Stealthwatch
Storage Array
Level 3 - Site Operations
(Control Room)
Identity Services
Active
Wireless LAN Controller (WLC)
Standby
NetFlow
Remote Access Server
Core Switches
NetFlow
NetFlow
Distribution Switch Stack
Distribution Switch Stack
Access Switches
Cell/Area Zone Levels 0–2
Access Switches
Cell/Area Zone Levels 0–2
Industrial Zone
Levels 0-3
(Plant-wide Network)
IES - RedBox Active
IES - RedBox Standby
Controller
LAN A
LAN B
RedBox
NetFlow
I/O
Drive
Controller
I/O
I/O
IES
Cell/Area Zone - Levels 0-2
Redundant LANs - Parallel Redundancy Protocol
Enhanced Interior Gateway Routing Protocol – EtherChannel
Hot Standby Router Protocol – Active/Standby
(Skids, Equipment)
SSID 2.4 GHz
LWAP
NetFlow
EtherNet/IP
I/O
Controller
I/O
Thin Client
IFW
Soft Starter
Controller
Drive
I/O
I/O
I/O
Instrumentation
Cell/Area Zone - Levels 0-2
Ring Topology - Device Level Ring (DLR) Protocol
Redundant Star Topology - Flex Links Resiliency
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)
IFW
NetFlow
EtherNet/IP
LWAP
SSID 5 GHz
Safety Controller
Thin Client
WGB
Safety I/O
Drive
I/O
Servo Drive
HMI
Robot
Drive
Controller
Cell/Area Zone - Levels 0-2
Linear/Bus/Star Topology
Redundant Star Topology - EtherChannel Resiliency
Unified Wireless LAN
(Lines, Machines)
256705

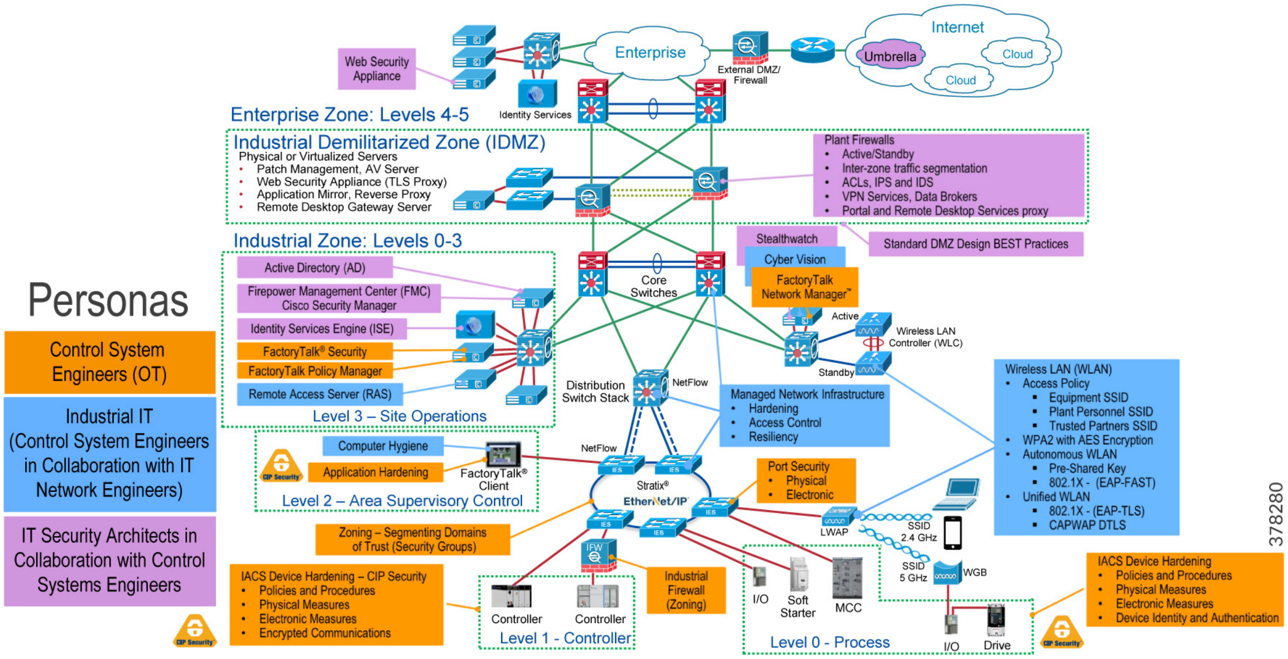
CPwE Industrial Security Framework Overview

No single product, technology, methodology or strategy can fully secure plant-wide or site-wide architectures. Protecting IACS assets requires a holistic defense-in-depth security approach that addresses internal and external security threats. This approach uses multiple layers of defense (administrative, technical, and physical) using diverse technologies for threat detection and prevention, implemented by different personas, and applied at separate levels of the IACS architecture (Figure 1-2).

- Control System Engineers (highlighted in tan) - IACS asset hardening (for example, physical and electronic), IACS application hardening (for example, CIP Security^{TM} with FactoryTalk® Policy Manager), infrastructure device hardening (for example, port security), network monitoring and change management (for example, FactoryTalk Network Manager), cybersecurity visibility and threat detection (for example, Cyber Vision), network segmentation (trust zoning), industrial firewalls (with deep packet inspection) at the IACS application edge, and IACS policy-based application authentication, authorization, and accounting (AAA).
- Control System Engineers in collaboration with IT Network Engineers (highlighted in blue) - Computer hardening (OS patching), network device hardening (for example, access control, and resiliency), network monitoring and inspection, and wired and wireless LAN access policies.

- IT Security Architects in collaboration with Control Systems Engineers (highlighted in purple) - Identity and Mobility Services (wired and wireless), network monitoring with anomaly detection, Active Directory (AD), Remote Access Servers, plant/site firewalls, Industrial Demilitarized Zone (IDMZ) design best practices, data brokers (for example, Web Security Appliance), and OpenDNS (for example, Umbrella).

Figure 1-2 CPwE Industrial Cybersecurity Framework


Web Security Appliance
Enterprise
External DMZ/ Firewall
Internet
Umbrella
Cloud
Cloud
Identity Services
Enterprise Zone: Levels 4-5
Industrial Demilitarized Zone (IDMZ)
Physical or Virtualized Servers
• Patch Management, AV Server
• Web Security Appliance (TLS Proxy)
• Application Mirror, Reverse Proxy
• Remote Desktop Gateway Server
Plant Firewalls
• Active/Standby
• Inter-zone traffic segmentation
• ACLs, IPS and IDS
• VPN Services, Data Brokers
• Portal and Remote Desktop Services proxy
Industrial Zone: Levels 0-3
Stealthwatch
Cyber Vision
FactoryTalk Network Manager™
Standard DMZ Design BEST Practices
Personas
Control System Engineers (OT)
Industrial IT (Control System Engineers in Collaboration with IT Network Engineers)
IT Security Architects in Collaboration with Control Systems Engineers
Active Directory (AD)
Firepower Management Center (FMC) Cisco Security Manager
Identity Services Engine (ISE)
FactoryTalk® Security
FactoryTalk Policy Manager
Remote Access Server (RAS)
Level 3 – Site Operations
Core Switches
Active
Wireless LAN Controller (WLC)
Standby
Distribution Switch Stack
NetFlow
Managed Network Infrastructure
• Hardening
• Access Control
• Resiliency
Wireless LAN (WLAN)
• Access Policy
▪ Equipment SSID
▪ Plant Personnel SSID
▪ Trusted Partners SSID
• WPA2 with AES Encryption
• Autonomous WLAN
▪ Pre-Shared Key
▪ 802.1X - (EAP-FAST)
• Unified WLAN
▪ 802.1X - (EAP-TLS)
▪ CAPWAP DTLS
Computer Hygiene
Application Hardening
CIP Security
FactoryTalk® Client
NetFlow
Level 2 – Area Supervisory Control
IES
Stratix®
EtherNet/IP
Port Security
• Physical
• Electronic
LWAP
SSID 2.4 GHz
SSID 5 GHz
WGB
Zoning – Segmenting Domains of Trust (Security Groups)
IFW
IACS Device Hardening – CIP Security
• Policies and Procedures
• Physical Measures
• Electronic Measures
• Encrypted Communications
Controller
Controller
Level 1 - Controller
Industrial Firewall (Zoning)
I/O
Soft Starter
MCC
Level 0 - Process
I/O
Drive
IACS Device Hardening
• Policies and Procedures
• Physical Measures
• Electronic Measures
• Device Identity and Authentication
CIP Security
378280

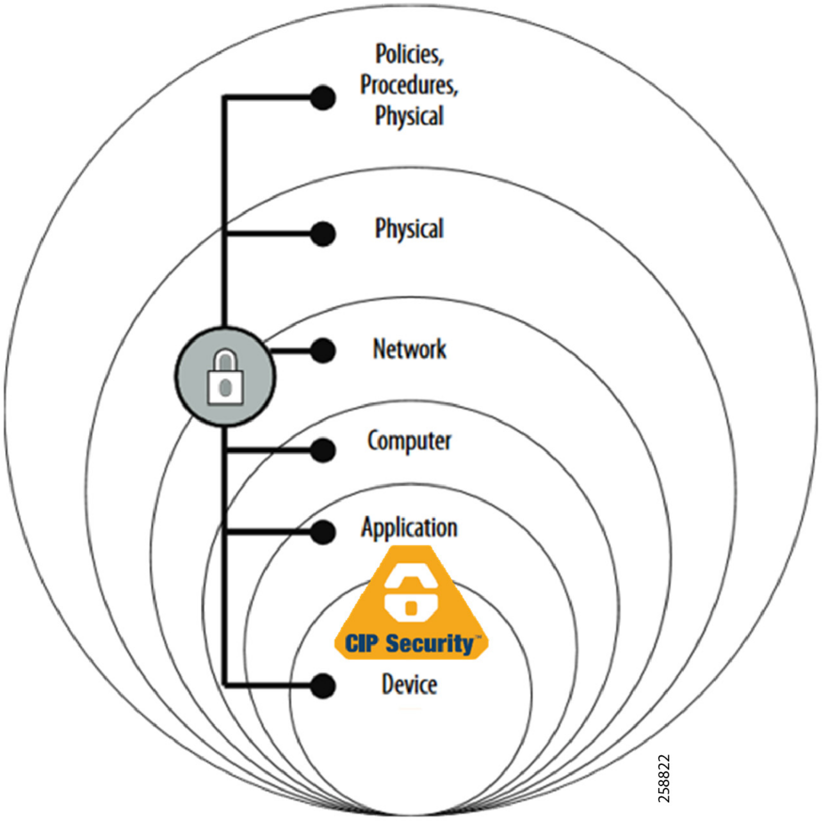
The CPwE Industrial Security Framework (Figure 1-2), using a defense-in-depth approach (Figure 1-3), is aligned to industrial security standards such as ISA/IEC-62443 Industrial Automation and Control Systems (IACS) Security and NIST 800-82 Industrial Control System (ICS) Security.

Defense-in-depth applies policies and procedures that address many different types of threats.

To achieve a defense-in-depth approach, an operational process is required to establish and maintain the security capability. A security-operational process includes the following actions:

1. Identify IACS asset device types and locations within the plant-wide or site-wide network infrastructure.
2. Identify potential internal and external vulnerabilities and threats to those IACS assets and assess the associated risks.
3. Understand the application and functional requirements of the IACS assets including 24x7 operations, communication patterns, topology, required resiliency, and traffic types.
4. Understand the associated risks of balancing the application and functional requirements of IACS assets with the need to help protect the availability, integrity, and confidentiality of IACS asset data.

Figure 1-3 Defense-in-Depth Security



In a defense-in-depth security approach (Figure 1-3), different solutions are needed to address various network and security requirements for a plant-wide or site-wide architecture. This section summarizes the existing Cisco, Panduit, and Rockwell Automation CPwE security CVDs and CRDs that address different aspects of the CPwE Industrial Security Framework (Figure 1-2).

- Deploying Network Security within a Converged Plantwide Ethernet Architecture Design and Implementation Guide outlines several industrial security architecture use cases, with Cisco ISE, for designing with visibility, segmentation, and anomaly detection throughout a plant-wide IACS network infrastructure.
  - Rockwell Automation site: https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td019_-en-p.pdf
  - Cisco site: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/Network_Security/DIG/CPwE-5-1-NetworkSecurity-DIG.html
- Deploying Identity and Mobility Services within a Converged Plantwide Ethernet Architecture Design and Implementation Guide outlines several industrial security and mobility architecture use cases, with Cisco ISE, for designing and deploying mobile devices, with FactoryTalk® applications, throughout a plant-wide or site-wide IACS network infrastructure.
  - Rockwell Automation site: http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td008_-en-p.pdf

  - Cisco site:
    http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/ISE/DIG/CPwE_ISE_CVD.html
- Cloud Connectivity to a Converged Plantwide Ethernet Architecture Design Guide outlines several industrial security architecture use cases for designing and deploying restricted end-to-end outbound connectivity from FactoryTalk applications to the Rockwell Automation cloud within a CPwE architecture.
  - Rockwell Automation site:
    https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td017_-en-p.pdf
  - Cisco site:
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/Cloud/DIG/CPwE_Cloud_Connect_CVD.html
- Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture Design and Implementation Guide outlines several use cases for designing, deploying, and managing industrial firewalls throughout a plant-wide IACS network. The Industrial Firewall is ideal for IACS applications that need trusted zone segmentation.
  - Rockwell Automation site:
    http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td002_-en-p.pdf
  - Cisco site:
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-0/Firewalls/DIG/CPwE-5-IFS-%20DIG.html
- Deploying CIP Security within a Converged Plantwide Ethernet Architecture Design Guide outlines a comprehensive explanation of the CIP Security application design. It includes information about key requirements, possible deployment models, potential challenges, technology considerations, and guidelines for implementation and configuration of these specific use security cases within the CPwE framework.
  - Rockwell Automation site:
    https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td022_-en-p.pdf
  - Cisco site:
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-0/Firewalls/DIG/CPwE-5-IFS-%20DIG.html

Industrial Demilitarized Zone

Sometimes referred to as a perimeter network, the IDMZ (see Figure 1-4) is a buffer that enforces data security policies between a trusted network (Industrial Zone) and an untrusted network (Enterprise Zone). The IDMZ is an additional layer of defense-in-depth to securely share IACS data and network services between the Industrial and Enterprise Zones. The demilitarized zone concept is commonplace to traditional IT networks and adoption for IACS applications.

For secure IACS data sharing, the IDMZ contains assets that act as brokers between the zones. Multiple methods to broker IACS data across the IDMZ exist:

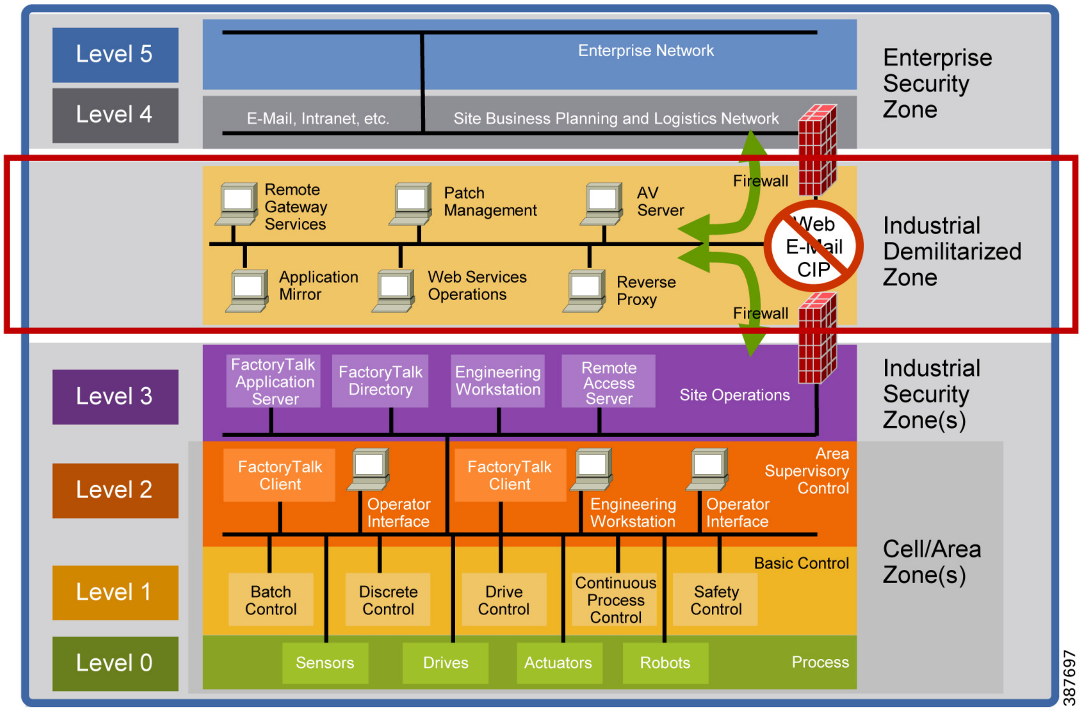
- Use application mirrors or proxies, such as:
  - PI-to-PI interface for FactoryTalk Historian
  - Secure File Transfer Gateway
  - Cisco Telemetry Broker

- Windows Server Update Services (WSUS)

- Use Microsoft® Remote Desktop (RD) Gateway services for secure remote access via Remote Desktop Connection client and ThinManager.

These broker methods, which help to hide and protect the existence and characteristics of the Industrial Zone servers from clients and servers in the Enterprise Zone, are highlighted in Figure 1-4 and are covered in CPwE IDMZ.

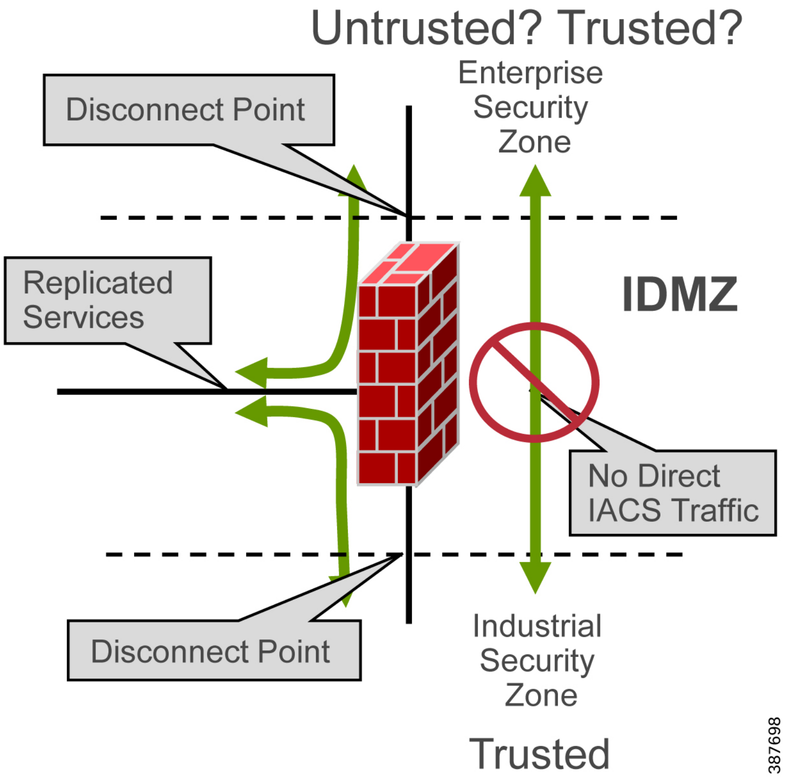
Figure 1-4 CPwE Logical Model



High-level IDMZ design principles (see Figure 1-5) include:

- All IACS network traffic from either side of the IDMZ terminates in the IDMZ; no IACS traffic directly traverses the IDMZ
- EtherNet/IP IACS traffic does not enter the IDMZ; it remains within the Industrial Zone
- Primary services are not permanently stored in the IDMZ
- All data is transient; the IDMZ does not permanently store data
- Functional sub-zones within the IDMZ are configured to segment access to IACS data and network services (for example, IT, Operations and Trusted Partner zones)
- A properly designed IDMZ will support the capability of being unplugged if compromised, while still allowing the Industrial Zone to operate without disruption

Figure 1-5 IDMZ High Level Concepts



CPwE IDMZ Solution Use Cases

CPwE IDMZ outlines key requirements and design considerations to help with successfully designing and deploying an IDMZ and implementing IACS data and network services between the Industrial and Enterprise Zones:

- An IDMZ overview and key design considerations
- A Resilient CPwE Architectural Framework:
  - Redundant IDMZ firewalls
  - Redundant distribution/aggregation Ethernet switches
  - Redundant core switches
- Methodologies to securely traverse IACS data across the IDMZ:
  - PI-to-PI interface for FactoryTalk Historian
  - Secure File Transfer Gateway
  - Cisco Telemetry Broker
  - Use Microsoft Remote Desktop (RD) Gateway services for secure remote access via Remote Desktop Connection client and ThinManager
  - WSUS Server
- Methodologies to securely traverse network services across the IDMZ

- CPwE IDMZ use cases:
  - IACS applications-for example, Secure File Transfer, FactoryTalk applications (FactoryTalk Historian, FactoryTalk® VantagePoint®, FactoryTalk View Site Edition, FactoryTalk ViewPoint, FactoryTalk AssetCentre, Studio 5000 Logix Designer®)
  - Network services-for example, AD, Cisco Identity Services Engine (ISE), Network Time Protocol (NTP), licensing management via Cisco Smart Software Manager On-Prem, and Windows Updates
  - Secure Remote Access
  - ThinManager access via Remote Desktop Gateway to IACS assets
  - Data Brokering via Cisco Telemetry Broker
- Important steps and design considerations for IDMZ implementation and configuration