CHAPTER 1

# CPwE Cloud Connectivity Overview

This chapter includes the following major topics:


- Cloud Connectivity Architecture Introduction, page 1-1
- CPwE Overview, page 1-2
- CPwE Cloud Connectivity, page 1-4
- Security Architecture Use Cases, page 1-5
- CPwE Industrial Security Overview, page 1-9


## Cloud Connectivity Architecture 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 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.

Cloud-based services help to enable data collaboration and remote monitoring of dashboards by industrial operations and/or trusted industry partners (for example, system integrator, OEM or IACS vendor) for IACS applications within the CPwE architecture (Figure 1-1). A holistic industrial security stance is necessary to help protect the integrity of safety and security best practices while also helping to enable restricted cloud-based services. No single product, technology or methodology can fully secure plant-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), utilizing diverse technologies for threat detection and prevention, implemented by different personas, and applied at separate levels of the IACS architecture.

Defense-in-depth applies policies and procedures that address many different types of threats. The CPwE Industrial Security Framework (Figure 1-2), using a defense-in-depth approach, is aligned to industrial security standards such as IEC-62443 (formerly ISA99), Industrial Automation and Control Systems (IACS) Security, and NIST 800-82 Industrial Control System (ICS) Cybersecurity Framework (CSF).

CPwE Cloud Connectivity outlines several security architecture use cases for designing and deploying restricted end-to-end outbound connectivity with FactoryTalk applications from industrial operations to the Rockwell Automation cloud within a CPwE architecture (Figure 1-1).

**Note** This design guide helps with meeting the following IEC-62443 3-3 Functional Requirements:
- FR3 SR 3.2 RE1: Malicious code protection on entry and exit points
- FR5 SR 5.2: Zone boundary protection
- FR5 SR 5.3: General purpose person-to-person communication restrictions

# 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)
- **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 (e.g., 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 applications

Figure 1-1 CPwE Architectures

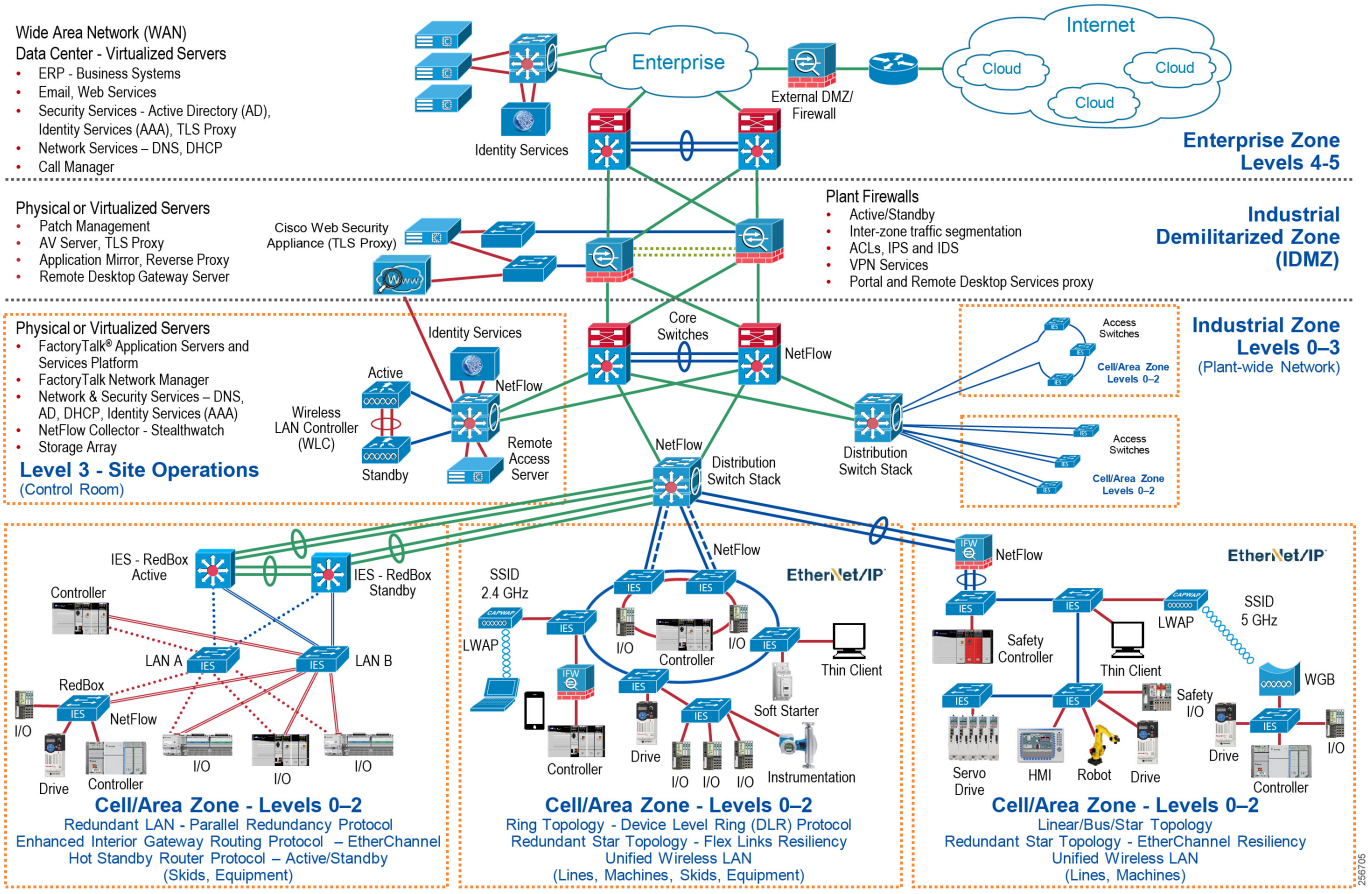
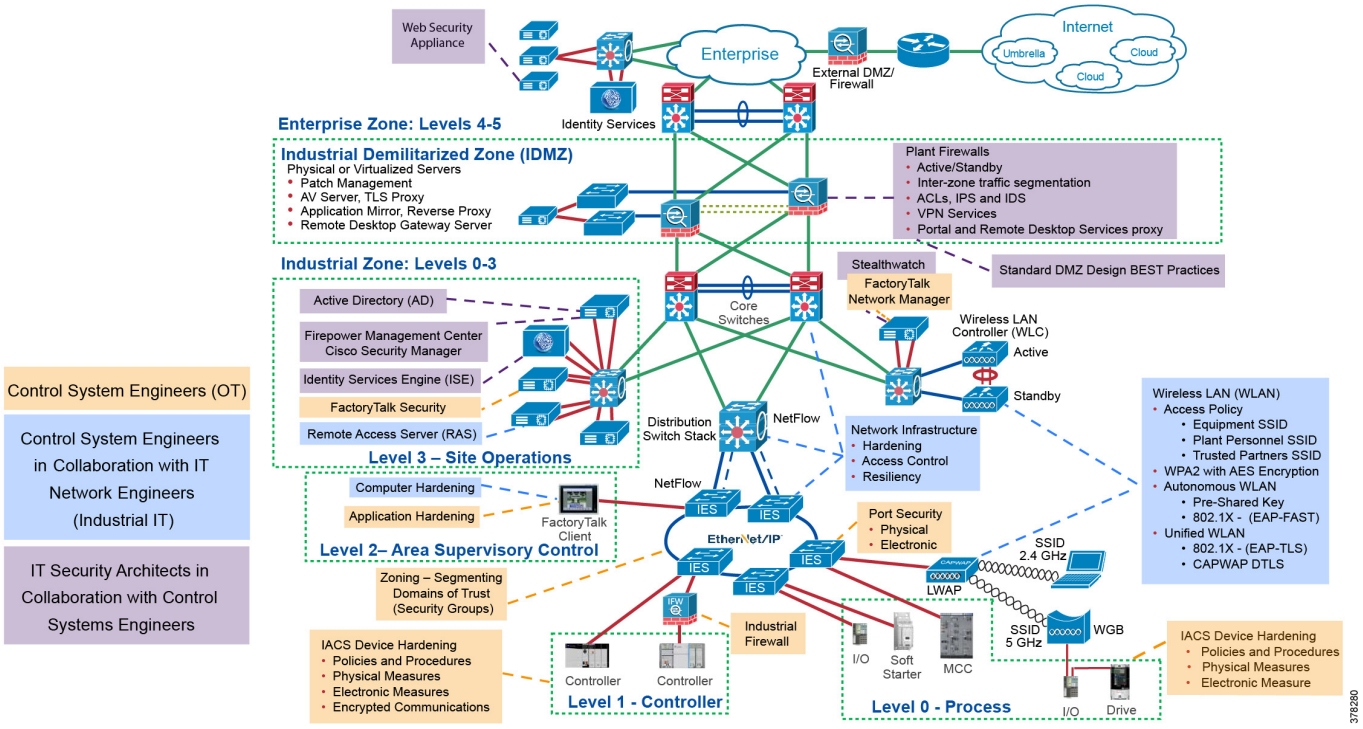


Figure 1-2 CPwE Industrial Security Framework




# CPwE Cloud Connectivity

An IACS is deployed in a wide variety of industries such as automotive, pharmaceuticals, consumer packaged goods, distribution, pulp and paper, oil and gas, mining and energy. IACS applications are composed of multiple control and information disciplines such as continuous process, batch, discrete and hybrid combinations. One of the challenges facing industrial operations and OEMs is the need to establish and secure connectivity from IACS applications to cloud-based services to take advantage of the business benefits associated with the IIoT.

CPwE Cloud Connectivity describes several security architecture use cases that are addressed using diverse security solutions and technologies, managed by different persona, at different levels of the plant-wide security architecture as shown in Figure 1-2.

- Control System Engineers (highlighted in tan)—IACS asset hardening (for example, physical and electronic), IACS application hardening (for example, CIP Security), infrastructure device hardening (for example, port security), network monitoring and change management (for example, FactoryTalk Network Manager), network segmentation (trust zoning), industrial firewalls (with inspection) at the IACS application edge, and IACS application authentication, authorization, and accounting (AAA).
- Control System Engineers in collaboration with IT Network Engineer (highlighted in blue)—Computer hardening (OS patching, application whitelisting), network device hardening (for example, access control, 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, and Industrial Demilitarized Zone (IDMZ) design best practices.

CPwE Cloud Connectivity outlines the concepts, requirements and technology solutions for reference designs developed around a specific set of security architecture use cases. These use cases were tested for solution functional validation by Cisco Systems and Rockwell Automation with assistance by Panduit. The following is a synopsis for this release of CPwE Cloud Connectivity:

- End-to-end outbound cloud connectivity
  - Tested and verified as part of this design guide—End-to-end FactoryTalk solution use cases—Platinum, Gold, Silver, and Bronze
  - Referenced only—Cisco Kinetic, Cisco IoT Gateway, any public cloud service
- Security Stance Overview
  - Risk management—Risk assessment considerations, risk tolerance, and risk mitigation
  - One size does not fit all
  - Trusted versus untrusted security zones
  - Policies and procedures to balance business benefits (such as innovation) with risk management
- End-to-end FactoryTalk Solutions Capabilities Overview
  - FactoryTalk AssetCentre
  - ControlFLASH Plus
  - FactoryTalk Activation Manager
  - Rockwell Automation Cloud API—Currently this API is used to ascertain product life cycle status and acts as the cloud endpoint.
- Design and Deployment Considerations for End-to-End FactoryTalk Solution
  - Establishing the restricted outbound path from the Industrial Zone to the Rockwell Automation cloud
  - Securing the restricted outbound path from the Industrial Zone to the Rockwell Automation cloud
  - Securing the plant-wide IACS network from the Industrial Zone ingress/egress point
  - Securing access to the Rockwell Automation cloud
  - Securing access to the Industrial Demilitarized Zone (IDMZ) Cisco Web Security Appliance acting as the Transport Layer Security (TLS) proxy

# Security Architecture Use Cases

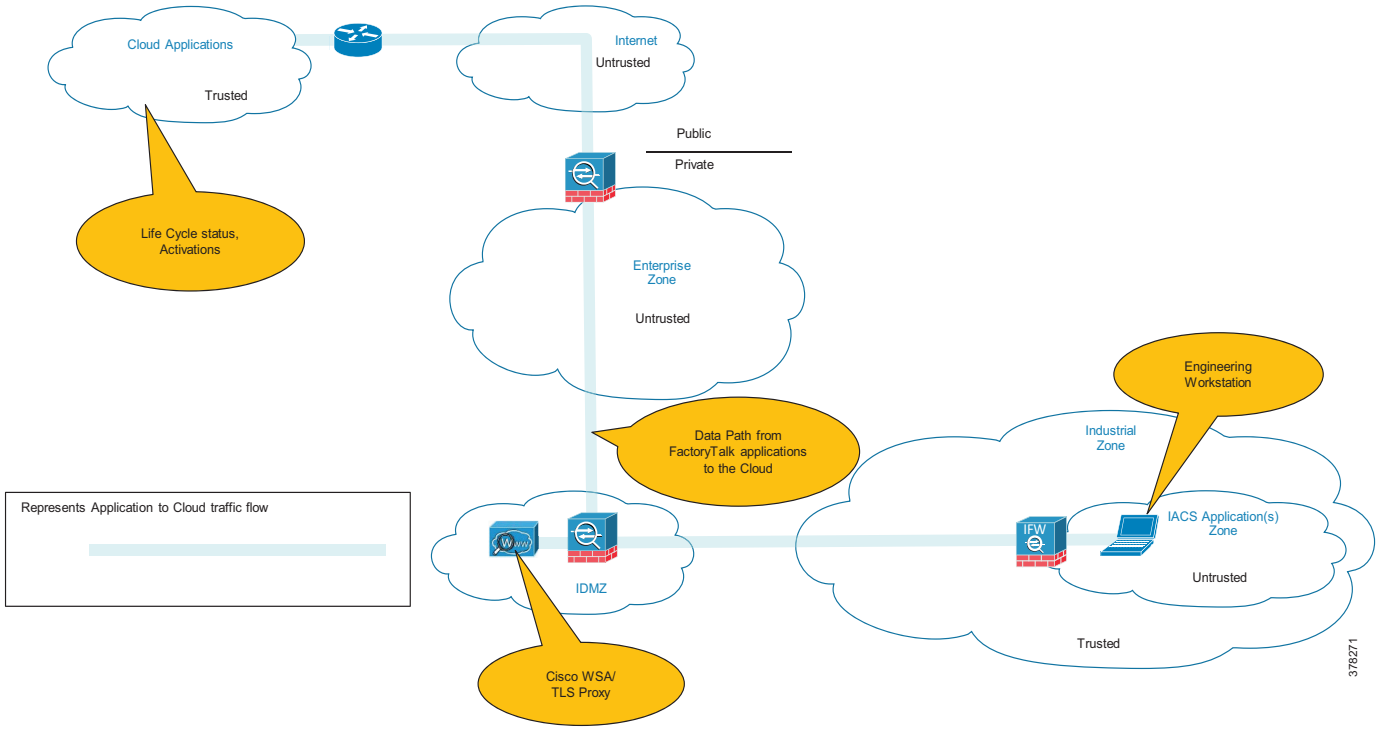
One size does not fit all when it comes to risk tolerance. What's acceptable by one industrial operator may be unacceptable to another and vice versa. The CPwE architecture supports scalability, which includes the degree of holistic and diverse industrial security technologies (Figure 1-2) applied to a plant-wide security architecture. Scalable security comes in many forms. Based on risk mitigation requirements, several diverse technology options are available for threat detection and prevention to help industrial operations meet their tolerance to risk. Industrial operators should also ensure that the cloud provider and internet service provider (ISP) are trusted. They are required to help protect connectivity and data per the industrial operator's security policies.

- **Platinum Security Architecture**—The Industrial Zone communicates with the Rockwell Automation Cloud via Transport Layer Security (TLS). In keeping with the Industrial Demilitarized Zone (IDMZ) concept of brokered services, a TLS proxy is located in the IDMZ (Figure 1-3). For testing and verification purposes, the TLS proxy that was used is the Cisco Web Security Appliance (Cisco WSA). This security architecture uses the IDMZ with Firewall(s) and replicated services to buffer the Industrial

Zone from the Enterprise Zone. Industrial Firewall(s) are also implemented to enforce security policies within a Cell/Area Zone to help protect the Industrial Zone from the ingress/egress point of the TLS traffic.

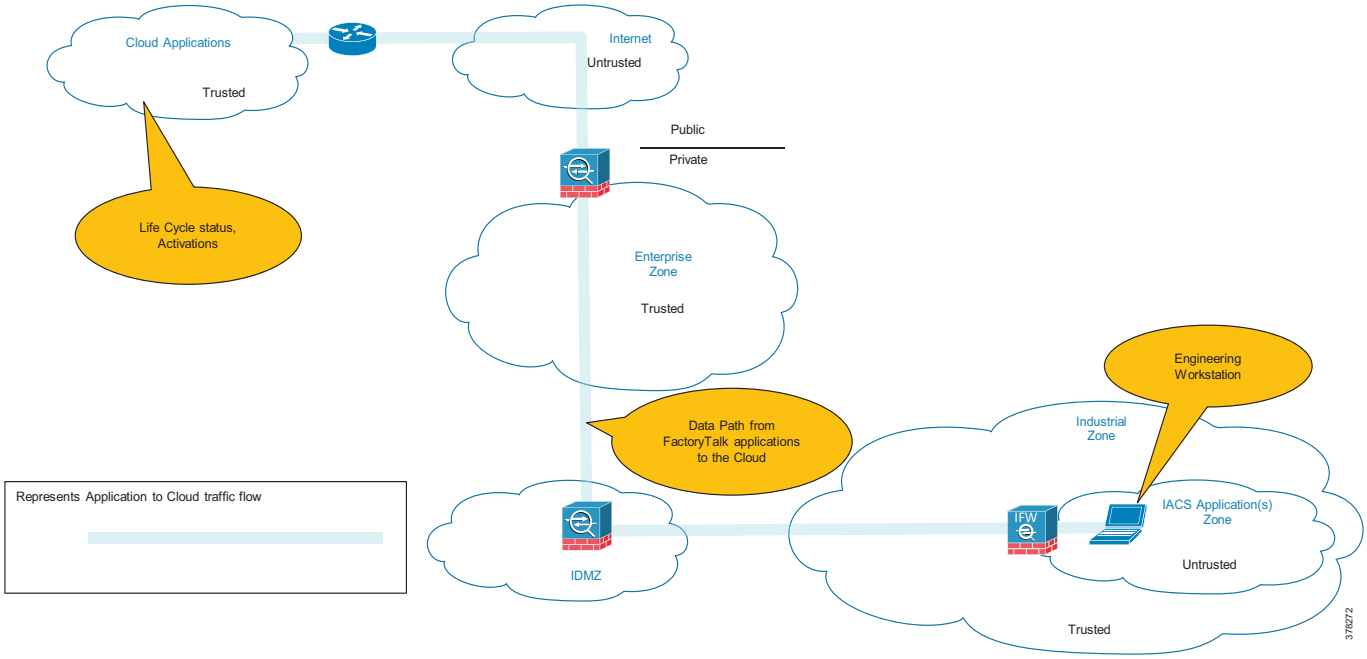
This is the security architecture recommended by Cisco, Panduit, and Rockwell Automation for industrial operations that require cloud-based connectivity yet have a lower tolerance to risk. Some industrial operators may already have a TLS proxy located in their Enterprise DMZ that buffers their Enterprise Zone from the Internet. This security architecture could be implemented to leverage that existing TLS proxy. A third option is to have a TLS Proxy located in the cloud like the Cisco Umbrella Intelligent Proxy. This solution only proxies the traffic that is destined for domains that are proven to be harmful.

Figure 1-3 Platinum Security CPwE Cloud Connectivity Use Case



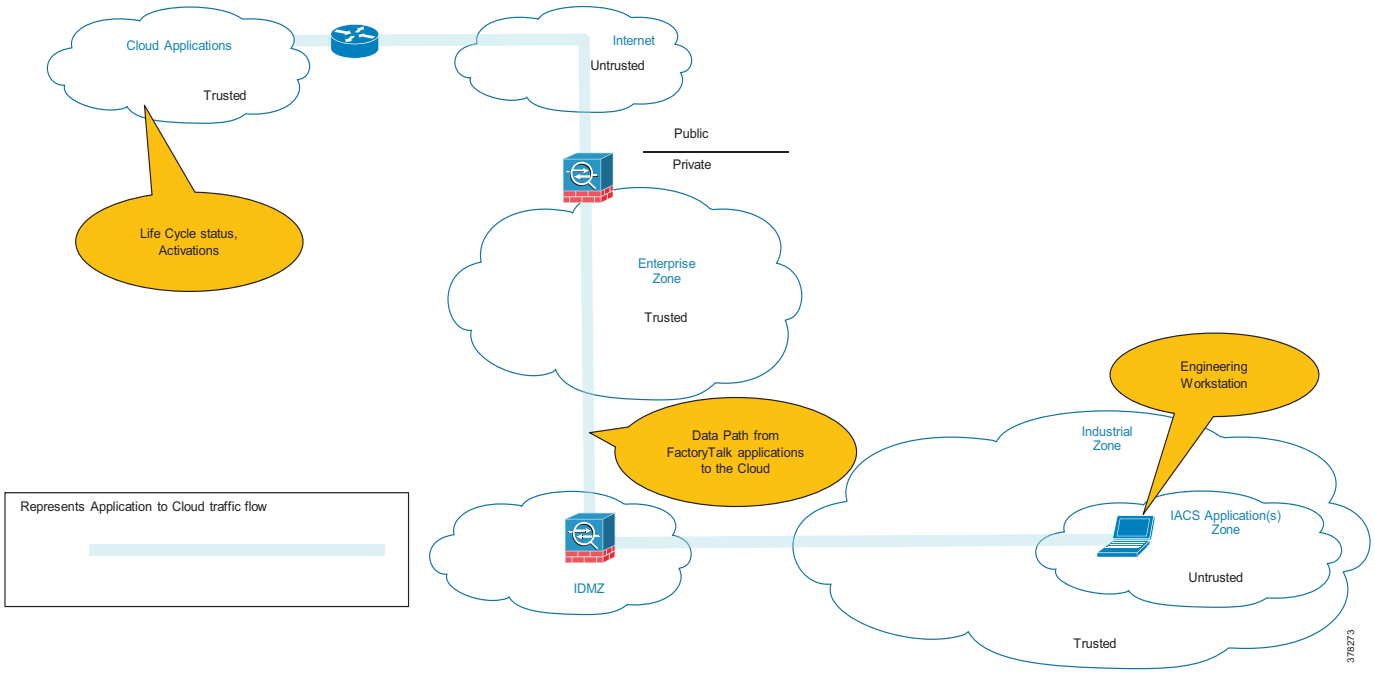
- **Gold Security Architecture**—This security architecture could be deployed when a TLS proxy is not present and when multiple layers of diverse industrial security best practices (Figure 1-2) have been followed. This security architecture uses the IDMZ with Firewall(s) and replicated services to buffer the Industrial Zone from the Enterprise Zone. Industrial Firewall(s) are also implemented to enforce security policies within a Cell/Area Zone to help protect the Industrial Zone from the ingress/egress point (Figure 1-4).

Figure 1-4 Gold Security CPwE Cloud Connectivity Use Case



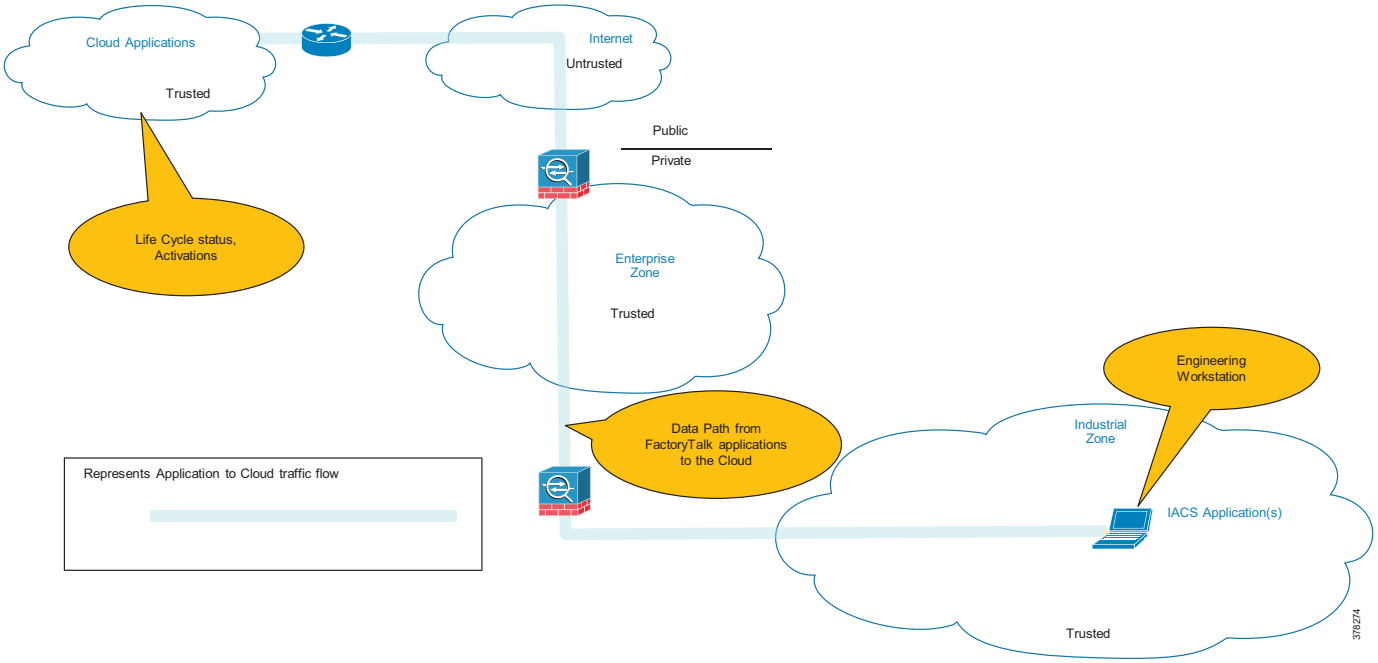
- **Silver Security Architecture**—This security architecture has an IDMZ with Firewall(s) and replicated services to buffer the Industrial Zone from the Enterprise Zone. No additional Industrial Firewall(s) exist that enforce security policies to help protect the Industrial Zone from the ingress/egress point (Figure 1-5).

Figure 1-5 Silver Security CPwE Cloud Connectivity Use Case



- **Bronze Security Architecture**—This security architecture has the fewest defensive layers of diverse industrial security best practices for threat protection and detection. A Firewall is the only buffer between the Enterprise and Industrial Zone. No additional Industrial Firewall(s) exist to enforce security policies to help protect the Industrial Zone from the ingress/egress point. Only industrial operations with a higher tolerance to risk should consider this security architecture for cloud-based connectivity (Figure 1-6).

Figure 1-6 Bronze Security CPwE Cloud Connectivity Use Case




# CPwE Industrial Security Overview

Protecting IACS assets requires a defense-in-depth security approach (Figure 1-2) where different solutions are needed to address various network and security requirements for a plant-wide architecture. This section summarizes the existing Cisco, Panduit, and Rockwell Automation CPwE security CVDs and CRDs that address different aspects of industrial security.

- *Deploying Network Security within a Converged Plantwide Ethernet Architecture Design and Implementation Guide* outlines several network security use cases for plant-wide IACS network infrastructure to help enable IIoT innovation within the CPwE framework.
  - 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 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

- *Securely Traversing IACS Data Across the Industrial Demilitarized Zone Design and Implementation Guide* details design considerations to help with the successful design and implementation of an IDMZ to securely share IACS data across the IDMZ.
  - Rockwell Automation site: http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td009_-en-p.pdf
  - Cisco site: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/IDMZ/DIG/CPwE_IDMZ_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-DIG.html