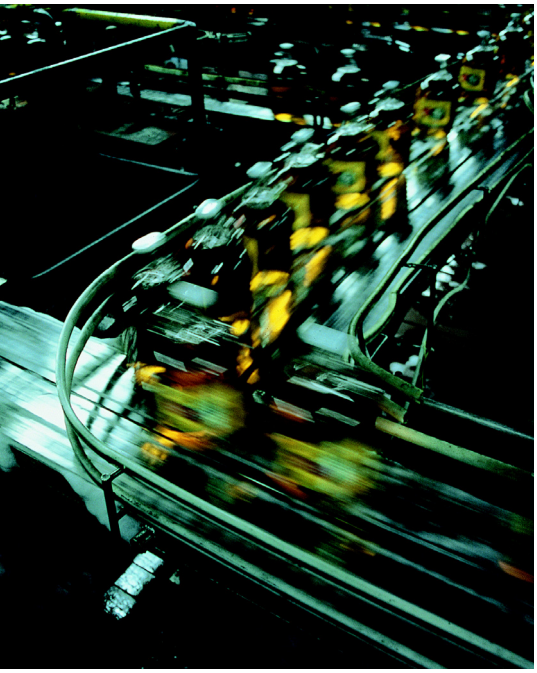


Cloud Connectivity to a Converged Plantwide Ethernet Architecture

White Paper

May 2018

Rockwell Automation and Cisco Four Key Initiatives:

- Common Technology View:
  A single scalable architecture, using open EtherNet/IP™ standard networking technologies, is paramount to enable the Industrial Internet of Things for achieving the flexibility, visibility and efficiency required in a competitive manufacturing environment.
- Converged Plantwide Ethernet Architectures:
  Collection of tested and validated architectures developed by subject matter authorities at Cisco and Rockwell Automation. The content of CPwE is relevant to both Operational Technology (OT) and Information Technology (IT) disciplines and consists of documented architectures, best practices, guidance and configuration settings to help manufacturers with design and deployment of a scalable, robust, secure and future-ready plant-wide industrial network infrastructure.
- Joint Product Collaboration:
  Stratix® 5950 Industrial Firewall, Stratix 5100 Wireless Access Point/Workgroup Bridge, and Stratix 5700, Stratix 5400 and Stratix 5410 Industrial Ethernet Switches, incorporating the best of Cisco and the best of Rockwell Automation.
- People and Process Optimization:
  Education and services to facilitate Operational Technology (OT) and Information Technology (IT) convergence, assist with successful architecture deployment, and enable efficient operations that allow critical resources to focus on increasing innovation and productivity.

Document Reference Number: ENET-WP019B-EN-P

Cloud Connectivity to a Converged Plantwide Ethernet Architecture

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 technology convergence through the use of standard Ethernet, Internet Protocol (IP), network services, security services and EtherNet/IP. A reliable and secure converged IACS network technology helps to enable the Industrial Internet of Things (IIoT).

IIoT helps offer the promise of business benefits through the use of innovative technology such as mobility, collaboration, analytics and cloud-based services. The challenge for manufacturers 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 plant personnel and/or trusted industry partners (for example, system integrator, OEM or contractor) for IACS applications within the CPwE architecture (Figure 1). A holistic industrial security stance is necessary in order 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), using diverse technologies for threat detection and prevention at separate IACS levels, by applying policies and procedures that address different types of threats. The CPwE Industrial Security Framework (Figure 2), which applies a holistic 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) Security.

This release of Cloud Connectivity to a Converged Plantwide Ethernet Architecture (CPwE Cloud Connectivity), which is documented in the *Cloud Connectivity to a Converged Plantwide Ethernet Architecture Application Guide*, outlines several security architecture use cases for designing and deploying restricted end-to-end outbound connectivity with FactoryTalk® software from the machine to the enterprise, to the cloud within a CPwE architecture (Figure 3). CPwE Cloud Connectivity is brought to market through a strategic alliance between Cisco Systems and Rockwell Automation.

Figure 1 CPwE Architectures

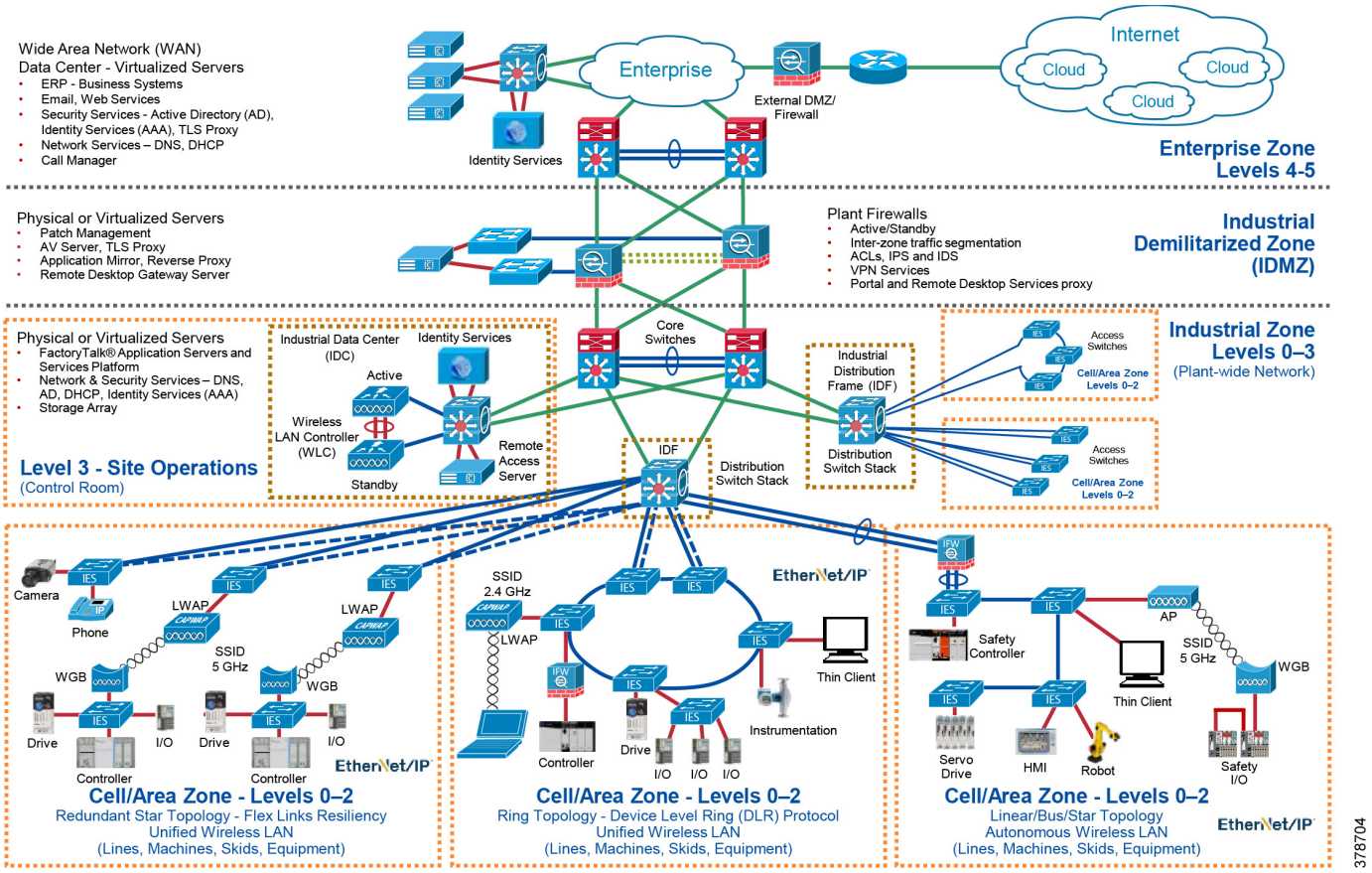
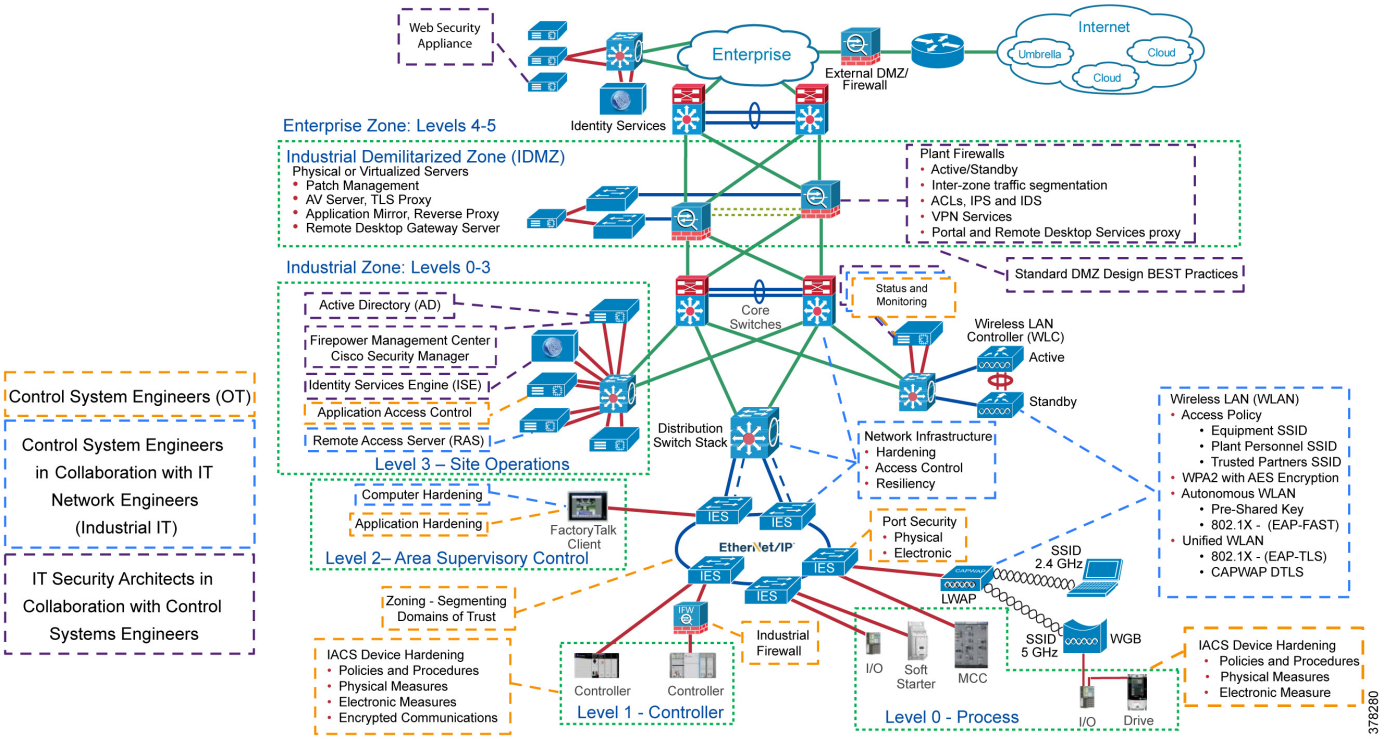


Figure 2 CPwE Industrial Security Framework



Note This release of the CPwE architecture focuses on EtherNet/IP, which uses the ODVA Common Industrial Protocol (CIP™) and is ready for the Industrial Internet of Things (IIoT). For more information on EtherNet/IP, see odva.org at the following URL:

- http://www.odva.org/Technology-Standards/EtherNet-IP/Overview

CPwE Cloud Connectivity

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

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 architecture (Figure 1), through testing and validation by Cisco and Rockwell Automation, provides design and implementation guidance, test results and documented configuration settings that can help to achieve the real-time communication, reliability, scalability, security and resiliency requirements of modern IACS applications for manufacturers and OEMs.

This release of CPwE Cloud Connectivity outlines the concepts, requirements and technology solutions for several security architecture use cases that were proof of concept (PoC) tested and documented by Cisco and Rockwell Automation. The following is a synopsis for this release of CPwE Cloud Connectivity:

- End-to-end outbound cloud connectivity
  - Proof of Concept tested and verified as part of this application 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 Cloud Gateway—Collects information from EtherNet/IP end devices
  - FactoryTalk Cloud—Microsoft Azure public cloud service
  - FactoryTalk Analytics for Machines
- Design and Deployment Considerations for End-to-End FactoryTalk Solution
  - Establishing the restricted outbound path from the FactoryTalk Cloud Gateway to the FactoryTalk Cloud
  - Securing the restricted outbound path from the FactoryTalk Cloud Gateway to the FactoryTalk Cloud
  - Securing the plant-wide IACS network from the FactoryTalk Cloud Gateway ingress/egress point
  - Securing access to the FactoryTalk Cloud Gateway
  - Securing access to the Industrial Demilitarized Zone (IDMZ) Transport Layer Security (TLS) proxy

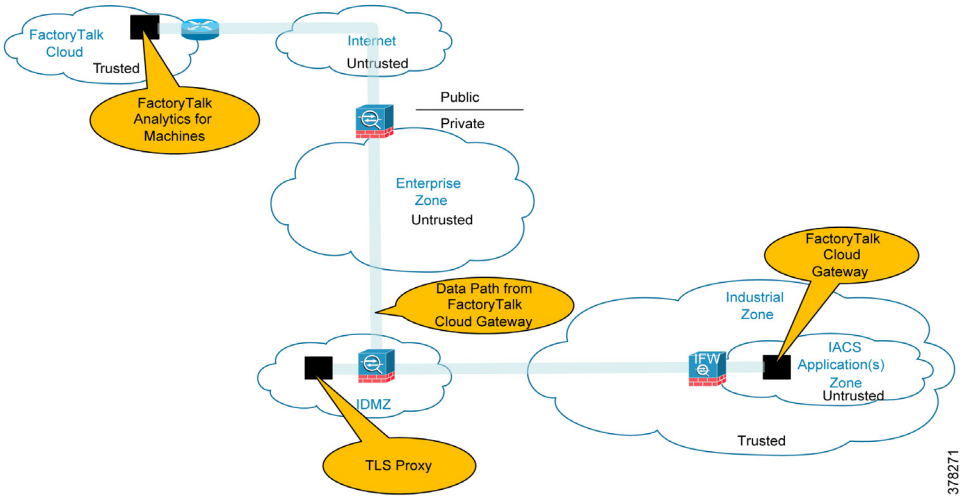
Security Architecture Use Cases

One size does not fit all when it comes to risk tolerance. What's acceptable by one manufacturer 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 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 manufacturers meet their tolerance to risk. The manufacturer should also ensure that the cloud provider and internet service provider (ISP) are trusted. They are required to protect connectivity and data per the manufacturer's security policies.

- **Platinum Security Architecture**—The FactoryTalk Cloud Gateway communicates with the FactoryTalk 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 3). 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 protect the Industrial Zone from the FactoryTalk Cloud Gateway ingress/egress point.

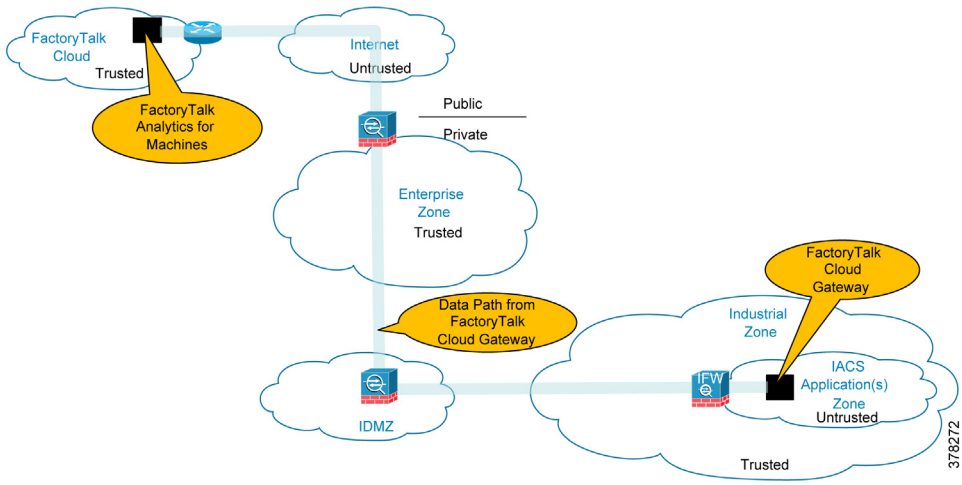
This is the security architecture recommended by Cisco and Rockwell Automation for manufacturers that require cloud-based connectivity yet have a lower tolerance to risk. Some manufacturers may already have a TLS proxy located in their Enterprise DMZ that buffers their Enterprise Zone from the Internet. 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.

Figure 3 Platinum Security CPwE Cloud Connectivity Use Case



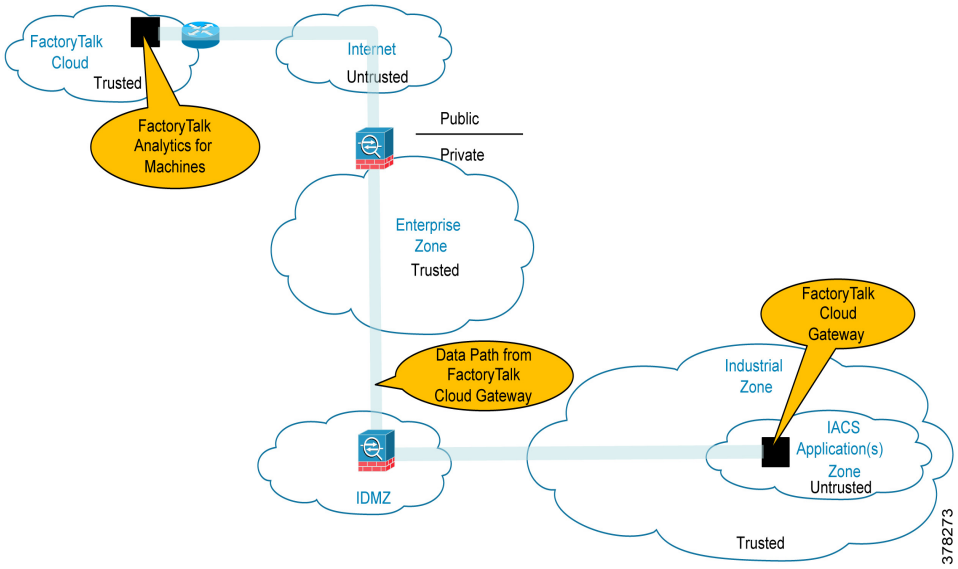
- **Gold Security Architecture**—This security architecture could be deployed when a TLS proxy is not present and when multiple layers of diverse industrial security best practices (Figure 2) have been followed. This security architecture uses the IDMZ with Firewall(s) and replicated services to buffer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

Figure 4 Gold Security CPwE Cloud Connectivity Use Case



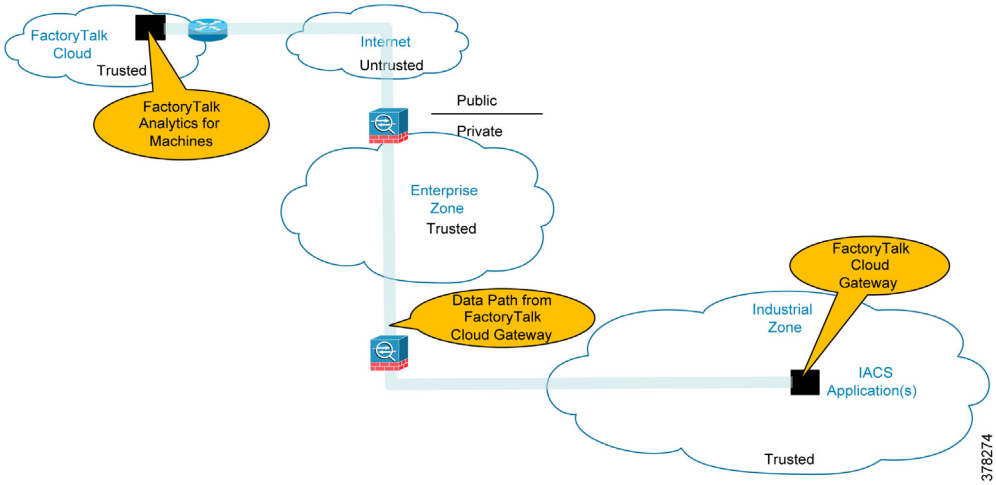
- **Silver Security Architecture**—This security architecture has an IDMZ with Firewall(s) and replicated services to buffer the Industrial Zone from the Enterprise Zone. No additional Industrial Firewall(s) exist to enforce security policies to help protect the Industrial Zone from the FactoryTalk Cloud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

Figure 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 FactoryTalk Cloud Gateway ingress/egress point. Only manufacturers with a higher tolerance to risk should consider this security architecture for cloud-based connectivity (Figure 6).

Figure 6 Bronze Security CPwE Cloud Connectivity Use Case



Summary

CPwE is a collection of tested and validated architectures that are developed by subject matter authorities at Cisco and Rockwell Automation. The testing and validation follow the Cisco Validated Design (CVD) and Cisco Reference Design (CRD) methodologies.

The content of CPwE, which is relevant to both OT and IT disciplines, consists of documented architectures, best practices, guidance and configuration settings to help manufacturers and OEMs with design and deployment of a scalable, reliable, secure and future-ready plant-wide industrial network infrastructure. CPwE also helps manufacturers and OEMs achieve the benefits of minimizing costs using proven designs that can help lead to quicker deployment and reduced risk in deploying new technology. CPwE is brought to market through a strategic alliance between Cisco Systems and Rockwell Automation.

The *Cloud Connectivity to a Converged Plantwide Ethernet Architecture Application Guide* outlines several security architecture use cases for designing and deploying restricted end-to-end outbound connectivity with FactoryTalk® software from the machine to the enterprise, to the cloud within a CPwE architecture. CPwE Cloud Connectivity was architected, PoC tested, and documented by Cisco and Rockwell Automation. The Application Guide highlights the key IACS application requirements, technology, and supporting design considerations to help with the successful design and deployment of these specific security architecture use cases within the framework of CPwE.

More information on CPwE Design and Implementation Guides can be found at the following URLs:

- Rockwell Automation site:
  - http://www.rockwellautomation.com/global/products-technologies/network-technology/architectures.page?
- Cisco site:
  - http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html

Publication ENET-WP019B-EN-P May 2018