Securely Traversing IACS Data Across the Industrial Demilitarized Zone

White Paper

January 2017

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:**

- **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.
Securely Traversing IACS Data Across the Industrial Demilitarized Zone

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 network technology convergence through the use of standard Ethernet and Internet Protocol (IP) technology, which helps to enable the Industrial Internet of Things (IIoT).

A converged IACS network is generally open by default. Openness facilitates both technology coexistence and IACS device interoperability, which helps to enable the choice of best-in-class IACS products. This openness also requires that IACS networks be secured and hardened through configuration and architecture. The degree of hardening depends upon the required security stance. Business practices, corporate standards, security policies, application requirements, industry security standards, regulatory compliance, risk management policies and overall tolerance to risk are key factors in determining the appropriate security stance.

Many organizations and standards bodies recommend segmenting business system networks from plant-wide networks by using an Industrial Demilitarized Zone (IDMZ). The IDMZ exists as a separate network located at 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, VPN servers, IACS application mirrors and reverse proxy servers, in addition to network infrastructure devices such as switches, routers and virtualized services.

CPwE is the underlying architecture that provides standard network services for control and information disciplines, devices and equipment found in modern IACS applications. The CPwE architectures, through testing and validation by Cisco and Rockwell Automation, provide 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.

The Securely Traversing IACS Data across the Industrial Demilitarized Zone CVD (Cisco and Rockwell Automation Validated Design), which is documented in the Securely Traversing IACS Data across the Industrial Demilitarized Zone Design and Implementation Guide (DIG), outlines several use case design considerations to help with the successful design and implementation of an IDMZ to securely share IACS data across the IDMZ. The CPwE IDMZ CVD is brought to market through a strategic alliance between Cisco Systems® and Rockwell Automation®.
Securely Traversing IACS Data across the Industrial Demilitarized Zone

Holistic Industrial Security

No single product, technology or methodology can fully secure IACS applications. Protecting IACS assets requires a defense-in-depth security approach, which addresses internal and external security threats. This approach uses multiple layers of defense (administrative, technical and physical) at separate IACS levels that address different types of threats.

Note

Security requirements for a physical IDMZ must recognize IACS application needs since data must securely pass from the Industrial Zone to the Enterprise Zone. Separately, Network Address Translation (NAT) and Identity Services are part of CPwE's overall security architecture. Each is available separately, completing CPwE's holistic industrial security approach.

The CPwE Industrial Network Security Framework (Figure 1), which uses a defense-in-depth approach, is aligned to industrial security standards such as IEC-62443 (formerly ISA-99) Industrial Automation and Control Systems (IACS) Security and NIST 800-82 Industrial Control System (ICS) Security.

Designing and implementing a comprehensive IACS network security framework should serve as a natural extension to the IACS. Network security should not be implemented as an afterthought. The industrial network security framework should be pervasive and core to the IACS. However, for existing IACS deployments, the same defense-in-depth layers can be applied incrementally to help improve the security stance of the IACS.

CPwE defense-in-depth layers (Figure 1) include:

- **Control System Engineers** (highlighted in tan)—IACS device hardening (for example, physical and electronic), infrastructure device hardening (for example, port security), network segmentation (trust zoning), industrial firewalls (with inspection) at the IACS application edge, IACS application authentication, authorization and accounting (AAA)

- **Control System Engineers in collaboration with IT Network Engineers** (highlighted in blue)—Computer hardening (OS patching, application white listing), network device hardening (for example, access control, resiliency), wireless LAN access policies

- **IT Security Architects in collaboration with Control Systems Engineers** (highlighted in purple)—Identity Services (wired and wireless), Active Directory (AD), Remote Access Servers, plant firewalls, Industrial Demilitarized Zone (IDMZ) design best practices
Industrial Demilitarized Zone

Sometimes referred to as a perimeter network, the IDMZ (Figure 2) is a buffer that enforces data security policies between a trusted network (Industrial Zone) to 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 in traditional IT networks, but is still in early 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 an application mirror, such as a PI-to-PI interface for FactoryTalk® Historian
- Use Microsoft® Remote Desktop Gateway (RD Gateway) services
- Use a reverse proxy server

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 2 and are covered in CPwE IDMZ.
High-level IDMZ design principles (Figure 3) include:

- All IACS network traffic from either side of the IDMZ terminates in the IDMZ; no IACS traffic directly traverses the IDMZ:
  - No direct path between the Industrial and Enterprise Zones
  - No common protocols in each logical firewall
- 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 will not permanently store data
- Set-up functional sub-zones within the IDMZ to segment access to IACS data and network services (for example, IT, Operations and Trusted Partner zone)
- A properly designed IDMZ will support the capability of being unplugged if compromised, while still allowing the Industrial Zone to operate without disruption

Figure 3  Industrial Demilitarized Zone High-level Concepts
Converged Plantwide Ethernet IDMZ

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

- An IDMZ overview and key design considerations
- A resilient CPwE Architectural Framework:
  - Redundant IDMZ Firewalls
  - Redundant Distribution/Aggregation Ethernet Switches
- Methodologies to securely traverse IACS data across the IDMZ:
  - Application mirror
  - Reverse proxy
  - Remote Desktop Gateway Services
- 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 (SE), FactoryTalk® ViewPoint, FactoryTalk® AssetCentre, Studio 5000 Logix Designer®)
  - Network services—for example, Active Directory (AD), Identity Services Engine (ISE), wireless LAN controller (WLC) control and provisioning of wireless access points (CAPWAP), Network Time Protocol
  - Secure Remote Access
- Important steps and design considerations for IDMZ implementation and configuration

**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:


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

**Rockwell Automation site:**


**Cisco site:**

Securely Traversing IACS Data across the Industrial Demilitarized Zone

Cisco is the worldwide leader in networking that transforms how people connect, communicate and collaborate. Information about Cisco can be found at www.cisco.com. For ongoing news, please go to http://newsroom.cisco.com. Cisco equipment in Europe is supplied by Cisco Systems International BV, a wholly owned subsidiary of Cisco Systems, Inc.

www.cisco.com

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Rockwell Automation is a leading provider of power, control and information solutions that enable customers to get products to market faster, reduce their total cost of ownership, better utilize plant assets, and minimize risks in their manufacturing environments.

www.rockwellautomation.com

Americas:
Rockwell Automation
1201 South Second Street
Milwaukee, WI 53204-2496 USA
Tel: (1) 414.382.2000, Fax: (1) 414.382.4444

Asia Pacific:
Rockwell Automation
Level 14, Core F, Cyberport 3
100 Cyberport Road, Hong Kong
Tel: (852) 2887 4788, Fax: (852) 2508 1846

Europe/Middle East/Africa:
Rockwell Automation
NV, Pegasus Park, De Kleelaan 12a
1831 Diegem, Belgium
Tel: (32) 2 663 0600, Fax: (32) 2 663 0640

Integrated Architecture®, FactoryTalk®, Stratix® 5700, Stratix® 8000 and Studio 5000 Logix Designer® are trademarks of Rockwell Automation, Inc. EtherNet/IP is a trademark of the ODVA.

© 2017 Cisco Systems, Inc. and Rockwell Automation, Inc. All rights reserved.