Securely Traversing IACS Data Across the Industrial Demilitarized Zone

Rockwell Automation and Cisco Four Key Initiatives:

- **Common Technology View:** A single system architecture, using open, industry standard networking technologies, such as Ethernet and IP, is paramount for achieving the flexibility, visibility and efficiency required in a competitive manufacturing environment.

- **Converged Plantwide Ethernet Architectures:** These manufacturing focused reference architectures, comprised of the Rockwell Automation Integrated Architecture® and Cisco's Ethernet to the Factory, provide users with the foundation for success to deploy the latest technology by addressing topics relevant to both engineering and IT professionals.

- **Joint Product and Solution Collaboration:** Stratix 5700™ and Stratix 8000™ 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 and allow successful architecture deployment and efficient operations allowing critical resources to focus on increasing innovation and productivity.

White Paper

May 2015

Document Reference Number: ENET-WP038A-EN-P
Securely Traversing IACS Data Across the Industrial Demilitarized Zone

Industrial Automation and Control System (IACS) networks are generally open by default; openness facilitates both technology coexistence and IACS device interoperability. Openness also requires that IACS networks be secured by configuration and architecture—that is, defend the edge. 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.

Converged Plantwide Ethernet (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 architecture provides design and implementation guidance to achieve the real-time communication, reliability, scalability, security and resiliency requirements of the IACS.

CPwE IDMZ for IACS applications is brought to market through a strategic alliance between Cisco Systems® and Rockwell Automation. The CPwE IDMZ details design considerations to help with the successful design and implementation of an IDMZ to securely share IACS data across the IDMZ.

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 (physical, procedural and electronic) 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 ISA/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, IACS application authentication, authorization and accounting (AAA)

- **Control System Engineers in collaboration with IT Network Engineers** (highlighted in blue)—zone-based policy firewall at the IACS application, operating system hardening, 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

![Figure 1 CPwE Industrial Network Security Framework](image-url)
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
Securely Traversing IACS Data across the Industrial Demilitarized Zone

Converged Plantwide Ethernet IDMZ

The CPwE IDMZ Cisco Validated Design (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®)
  - 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 is driven by the ODVA Common Industrial Protocol (CIP). Refer to the IACS Communication Protocols section of the CPwE Design and Implementation Guide.
Rockwell Automation site:

Cisco site: