Industrial Firewalls within a Converged Plantwide Ethernet Architecture

White Paper

December 2016

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:**
  A 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.

Document Reference Number: ENET-WP011B-EN-P
Industrial Firewalls within 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 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.

Plant-wide deployment of Industrial Firewalls (IFW), which is part of a holistic defense-in-depth industrial security stance, helps to harden the IACS network infrastructure and creates smaller zones of trust. Industrial firewalls have the ability to restrict and inspect traffic flow throughout the plant-wide IACS network. It is common for OT personnel to apply industrial firewalls to protect their legacy IACS applications - equipment, machines or skids. It is becoming more common for Original Equipment Manufacturers (OEMs) to include an industrial firewall as part of their offering. To support this convergence of OT and IT, modern industrial firewalls support the capability of being deployed and managed using several different methodologies that are either locally or centrally managed. Locally managed is common for OT plant personnel and OEM applications. Centrally managed is common for IT.

The Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture CVD (Cisco and Rockwell Automation Validated Design), which is documented in the Deploying Industrial Firewalls within a CPwE Architecture Design and Implementation Guide (DIG), outlines several use cases for designing, deploying and managing industrial firewalls throughout a plant-wide IACS network. The CPwE Industrial Firewalls CVD is brought to market through a strategic alliance between Cisco Systems® and Rockwell Automation.

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 (Figure 1), 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.
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. The CPwE Industrial Network Security Framework (Figure 2), 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 be a natural extension to the IACS application. 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 2) 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)

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
Industrial Firewall Use Cases

An IACS is deployed in a wide variety of discrete and process manufacturing industries such as automotive, pharmaceuticals, consumer 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 is the industrial hardening of standard Ethernet and IP-converged IACS networking technologies to take advantage of the business benefits associated with the Industrial Internet of Things (IIoT).

The Deploying Industrial Firewalls within a CPwE Architecture DIG outlines the concepts, requirements and technology solutions for application use cases that were tested, validated and documented by Cisco and Rockwell Automation to help support a hardened and converged plant-wide EtherNet/IP™ IACS architecture. The following is a summary of the CPwE IFW CVD use cases:

- **Industrial Firewall Technology Overview:**
  - Modes of operation:
    - Inline Transparent mode
    - Inline Routed mode
    - Passive Monitor-only mode
  - Network Protection (Cisco Adaptive Security Appliance)
  - Intrusion Prevention and Detection (Cisco FireSIGHT® Management System), Deep Packet Inspection (DPI) of the Common Industrial Protocol (CIP)
Summary

- Industrial Firewall (IFW):
  - The Allen-Bradley® Stratix 5950™ Industrial Network Security Appliance
  - The Cisco Industrial Security Appliance 3000

- Application Use Cases (Figure 3):
  - Equipment/Machine/Skid Protection
  - Cell/Area Zone Protection:
    - Redundant Star Topology, Ring Topology
  - Cell/Area Zone Monitoring

- Management Use Cases:
  - Local Management:
    - Command Line Interface (CLI), Adaptive Security Device Manager
  - Centralized Management:
    - Cisco FireSIGHT Management Center, Cisco Security Manager
  - Migration from local to centralized management of industrial firewalls

Figure 3  Plant-wide Industrial Firewall Deployments

Summary

CPwE is a collection of tested and validated architectures that are developed by subject matter authorities at Cisco and Rockwell Automation and that follow the Cisco Validated Design (CVD) program. The content of CPwE, which is relevant to both Operational Technology (OT) and Informational Technology (IT) disciplines, consists of documented architectures, best practices, guidance and configuration settings to help manufacturers with design and deployment of a scalable, reliable, secure and future-ready plant-wide industrial network infrastructure. CPwE also helps manufacturers achieve the benefits of cost reductions using proven designs that can help lead to quicker deployment and reduced risk in deploying new technology.
The Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture Design and Implementation Guide (DIG) outlines several use cases for designing, deploying and managing industrial firewalls throughout a plant-wide Industrial Automation and Control System (IACS) network infrastructure. This DIG highlights the key IACS application requirements, technology, and supporting design considerations to help with the successful design and deployment of these specific 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:
- Cisco site:

Note

This document references FireSIGHT Management Center as the centralized management software for the IFW FirePOWER™ modules. Starting with version 6.0, the software was renamed Firepower Management Center. Either version is capable of managing IFW FirePOWER modules that are performing CIP inspection. For more information on this terminology change, please see the Cisco Firepower Compatibility Guide at the following URL: