T84 – Develop a Secure Architecture for the Connected Enterprise

Scalable, Reliable, Safe, Secure and Future-Ready Architectures
Abstract

- New innovative technologies like cloud, and new service models like remote monitoring are helping to improve operational efficiency. Learn about the architectural security framework and solutions to help improve the availability, integrity and confidentiality of the architecture.
Agenda

- What's Driving This?
- Industrial Security Trends
- Defense-in-Depth
- Holistic Plant-wide Security
- Additional Material
- Training Resources
What’s Driving This?
What’s Driving This?
Reliable, Safe and Secure Architectures for The Connected Enterprise

A reliable, secure architecture is critical to building a connected enterprise

- Application
- Software
- Network
What’s Driving This?

Industrial IoT / Industrial IT (Bridging OT-IT)

Physical or Virtualized Servers
- Patch Management
- AV Server
- Application Mirror
- Remote Desktop Gateway Server

Wide Area Network (WAN)
- Data Center - Virtualized Servers
  - ERP - Business Systems
  - Email, Web Services
  - Security Services - Active Directory (AD), Identity Services (AAA)
- IT Network Services – DNS, DHCP

Enterprise Zone
- Levels 4–5
- Enterprise Demilitarized Zone (IDMZ)
- Enterprise Identity Services
- Levels 4–5
- Enterprise Zone
- Enterprise Firewalls
  - Active/Standby
  - Inter-zone traffic segmentation
  - ACLs, IPS and IDS
  - VPN Services
  - Portal and Remote Desktop Services proxy

Industrial Zone
- Levels 0–3
- Remote Access Server
- Physical or Virtualized Servers
  - FactoryTalk® Application Servers and Services Platform
  - Network Security Services – DNS, AD, DHCP, Identity Services (AAA)
  - Storage Array

Level 3 - Site Operations
- (Control Room)
- Active/Standby AP
- 5 GHz WGB
- LWAP SSID
- 2.4 GHz WGB

Level 2 - Cellular Zone
- Levels 0–2
- Redundant Star Topology - Flex Links Resiliency
- Unified Wireless LAN (Lines, Machines, Skids, Equipment)
- Ring Topology - Device Level Ring (DLR) Protocol
- Unified Wireless LAN (Lines, Machines, Skids, Equipment)

Drive
- I/O
- Robot
- Servo Drive
- HMI
- Safety Controller
- IFW
- LWAP

Operational Technology
- Industrial IoT
- Rockwell Automation
- Public
What’s Driving This?
Business Outcomes – Industrial IoT / Industrial IT (Bridging OT-IT)

- Smart Devices, Smart Machines, Smart Manufacturing
- Standard Network and Security Services; Standard Network Tools
- Customer choice of best-in-class products through Industrial IoT device coexistence and interoperability
- Pervasive Asset Optimization and Utilization
  - Common infrastructure devices and tools
  - Human assets: knowledge, experience, training
- Better Analytics
  - Device/Machine, System/Plant, Enterprise
- Enables Innovative Technologies
  - Mobility – Personnel and Equipment
  - Cloud –On Premise and Off Premise
### What’s Driving This?

**Technology and Cultural Convergence - Similarities and Differences**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Industrial OT Network</th>
<th>Enterprise IT Network</th>
</tr>
</thead>
</table>
| **Environment** | Plant-floor  
Control Room  
Control Panel, Industrial Distribution Frame (IDF) | Carpeted Space, Data Center  
Data Communication or Wiring Closet, Intermediate Distribution Frame (IDF) |
| **Switches** | Managed and unmanaged  
Layer 2 is predominant  
DIN rail or panel mount is predominant | Managed  
Layer 2 and Layer 3  
Rack mount |
| **Wireless** | Autonomous (locally managed) – point solutions  
Mobile equipment (emerging) and personnel (prevalent) | Unified (centrally managed) solutions  
Mobile personnel – corporate provided or BYOD  
Guest access |
| **Computing** | Industrial Hardened Panel Mount Computers and Monitors  
Desktop, Notebook  
19” Rack Server  
Virtualization - becoming prevalent  
Hardening – Sporadic patching and white listing | Desktop, Notebook  
Tablets  
19” Rack Server and Blade Server  
Unified Computing Systems (UCS)  
Virtualization – widespread  
Hardening - Patching and white listing |
## What’s Driving This?
Technology and Cultural Convergence - Similarities and Differences

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Industrial OT Network</th>
<th>Enterprise IT Network</th>
</tr>
</thead>
</table>
| **Network Technology** | • Standard IEEE 802.3 Ethernet and proprietary (non-standard) versions  
• Standard IETF Internet Protocol (IPv4) and proprietary (non-standard) alternatives  
• Sporadic use of standard network and security services  | • Standard IEEE 802.3 Ethernet  
• Standard IETF Internet Protocol (IPv4 and IPv6)  
• Pervasive use of standard network and security services |
| **Network Availability** | • Switch-Level and Device-Level topologies  
• Ring topology is predominant for both, Redundant Star for switch topologies is emerging  
• Standard IEEE, IEC and vendor-specific Layer 2 resiliency protocols | • Switch-Level topologies  
• Redundant Star topology is predominant  
• Standard IEEE, IETF, and vendor-specific Layer 2 and Layer 3 resiliency protocols |
| **Service Level Agreement (SLA)** | • Mean time to recovery (MTTR) - Minutes, Hours | • Mean time to recovery (MTTR) - Hours, Days |
| **IP Addressing**      | • Mostly Static                                           | • Mostly Dynamic                                                                       |
## What’s Driving This?
Technology and Cultural Convergence - Similarities and Differences

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Industrial OT Network</th>
<th>Enterprise IT Network</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Traffic Type</strong></td>
<td>• Primarily local – traffic between local assets</td>
<td>• Primarily non-local – traffic to remote assets</td>
</tr>
<tr>
<td></td>
<td>• Information, control, safety, motion, time synchronization, energy management</td>
<td>• Voice, Video, Data</td>
</tr>
<tr>
<td></td>
<td>• Smaller frames for control traffic</td>
<td>• Larger packets and frames</td>
</tr>
<tr>
<td></td>
<td>• Industrial application layer protocols: CIP™, Profinet, IEC 61850, Modbus TCP, and so on.</td>
<td>• Standard application layer protocols: Http, SNMP, DNS, RTP, SSH, and so on.</td>
</tr>
<tr>
<td><strong>Performance</strong></td>
<td>• Low Latency, Low Jitter</td>
<td>• Low Latency, Low Jitter</td>
</tr>
<tr>
<td></td>
<td>• Data Prioritization – QoS – Layer 2 &amp; 3</td>
<td>• Data Prioritization – QoS – Layer 3</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>• Open by default, must secure by configuration and architecture</td>
<td>• Pervasive</td>
</tr>
<tr>
<td></td>
<td>• Industrial security standards – for example, IEC, NIST</td>
<td>• Enterprise security best practices</td>
</tr>
<tr>
<td></td>
<td>• Inconsistent deployment of security policies</td>
<td>• Strong security policies</td>
</tr>
<tr>
<td></td>
<td>• No line-of-sight to the Enterprise or to the Internet</td>
<td>• Line-of-sight across the Enterprise and to the Internet</td>
</tr>
</tbody>
</table>
### What’s Driving This?

Security Policies - Similarities and Differences

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Industrial OT Network</th>
<th>Enterprise IT Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Focus</td>
<td>24/7 operations, high OEE</td>
<td>Helping to protect intellectual property and company assets</td>
</tr>
<tr>
<td>Precedence of Priorities</td>
<td>Availability, Integrity, Confidentiality</td>
<td>Confidentiality, Integrity, Availability</td>
</tr>
<tr>
<td>Types of Data Traffic</td>
<td>Converged network of data, control, information, safety and motion</td>
<td>Converged network of data, voice and video</td>
</tr>
<tr>
<td>Access Control</td>
<td>Strict physical access, Simple network device access</td>
<td>Strict network authentication and access policies</td>
</tr>
<tr>
<td>Implications of a Device Failure</td>
<td>Production is down ($$’s/hour … or worse)</td>
<td>Workaround or wait</td>
</tr>
<tr>
<td>Threat Protection</td>
<td>Isolate threat but keep operating</td>
<td>Shut down access to detected threat</td>
</tr>
<tr>
<td>Upgrades</td>
<td>Scheduled during downtime</td>
<td>Automatically pushed during uptime</td>
</tr>
</tbody>
</table>
Industrial Security Trends
"Good enough" security now, is better than "perfect" security ... never (Tom West, Data General)

Security ultimately relies - and fails - on the degree to which you are thorough. People don't like to be thorough. It gets in the way of being done (Dave Piscitello)

Your absolute security is only as strong as your weakest link

Concentrate on known, probable threats

Security is not a static end state, it is an interactive process
Industrial Security Trends
End-User Stance on Cost and Risk Reduction - Availability, Safety, Security

- Risk management policies and overall tolerance to risk
  - Business practices
  - Corporate / local standards
  - Application requirements
  - Applicable industry standards – for example, NERC CIP™
  - Government regulations and compliance

- Enterprise and industrial policies (safety and security), procedures, access control (avoidance of back doors) and network ownership
  - Alignment with industrial safety standards such as IEC 61508 – SIL 3 and EN 954-1 - Cat 4
  - Alignment with industrial security standards such as IEC-62443 (formerly ISA99), NIST 800-82 and ICS-CERT

Early, open and two-way OT-IT dialogue is critical!

“one-size-fits-all”
Industry Security Trends
Established Industrial Security Standards

- International Electrotechnical Commission
  - IEC-62443 (Formerly ISA99), Industrial Automation and Control Systems (IACS) Security
  - Zones and Conduits
    - Defense-in-Depth
    - Segmentation, IDMZ

- National Institute of Standards and Technology
  - NIST 800-82, Industrial Control System (ICS) Security
  - Cyber security Framework: Help Identify, Protect, Detect, Respond, Recover
    - Defense-in-Depth
    - Segmentation, IDMZ

- Department of Homeland Security / The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
  - Recommended Practices, Secure Network Architecture
    - Defense-in-Depth
    - Segmentation, IDMZ

- Department of Homeland Security / Idaho National Lab
  - DHS INL/EXT-06-11478
  - Control Systems cyber security: Defense-in-Depth Strategies
    - Defense-in-Depth
    - Segmentation, IDMZ
Industrial Security Trends
Established Industrial Security Standards

IEC 62443
Industrial Automation and Control System Security

- Series of Standards
- Zones & Conduits
- Availability, Integrity, Confidentiality

NIST 800-82 Cybersecurity Framework
BEFORE
Discover
Enforce
Harden

DURING
Detect
Block
Defend

AFTER
Scope
Contain
Remediate

Identify
Protect
Detect
Respond
Recover
Defense-in-Depth
Defense-in-Depth
Industrial Automation and Control System (IACS) Application

- No single product, technology or methodology can fully secure Industrial Automation and Control System (IACS) applications

- Helping protect IACS assets requires a defense-in-depth security approach, which addresses internal and external security threats

- Uses multiple layers of defense, uses diverse technologies at separate IACS levels, by applying policies and procedures that address different types of threats
Defense-in-Depth
Industrial Automation and Control System (IACS) Application

- Open by default to allow both technology coexistence and device interoperability for IACS Networks, choice of best-in-class products

- Secure by configuration and architecture:
  - Configuration
    - Harden the infrastructure through holistic defense-in-depth - multiple layers of security
  - Architecture
    - Structure the infrastructure to defend the edge - Logical Zoning
Defense-in-Depth
Critical Elements to Industrial Security

- A balanced Industrial Security Program must address both Technical and Non-Technical Elements
  - Non-technical controls - rules for environments: e.g., business practices, standards, policies, procedures, risk management, education and awareness programs
  - Technical controls – technology to provide restrictive measures for non-technical controls: for example, Firewalls, Group Policy Objects, Layer 3 access control lists (ACLs)
- Security is only as strong as the weakest link
- Vigilance and attention to detail are KEY to the long-term security success

"one-size-fits-all"
Defense-in-Depth
Industrial Security Policies Drive Technical Controls

- **Education and awareness programs** - Training of OT personnel on industrial security policies and procedures including how to respond to a security incident
- **Physical** – Limit physical access to authorized personnel: control room, cells/areas, control panels, IACS devices…. locks, gates, biometrics
- **Network** – Restrictive access, hardening, traffic inspection
- **Computer Hardening** – Patch management, anti-x software, white listing, removal of unused applications/protocols/services, closing unnecessary logical ports, help protect physical ports
- **Application** – Restrictive access, hardening, monitoring
- **Device Hardening** – Trusted communications, change management, data encryption, restrictive access
## OSI 7-Layer Reference Model

### Open Systems Interconnection

<table>
<thead>
<tr>
<th>Layer No.</th>
<th>Layer Name</th>
<th>Function</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 7</td>
<td>Application</td>
<td>Network Services to User App</td>
<td>CIP™ - IEC 61158</td>
</tr>
<tr>
<td>Layer 6</td>
<td>Presentation</td>
<td>Encryption/Other processing</td>
<td></td>
</tr>
<tr>
<td>Layer 5</td>
<td>Session</td>
<td>Manage Multiple Applications</td>
<td></td>
</tr>
<tr>
<td>Layer 4</td>
<td>Transport</td>
<td>Reliable End-to-End Delivery Error Correction</td>
<td></td>
</tr>
<tr>
<td>Layer 3</td>
<td>Network</td>
<td>Packet Delivery, Routing</td>
<td>IETF TCP/UDP</td>
</tr>
<tr>
<td>Layer 2</td>
<td>Data Link</td>
<td>Framing of Data, Error Checking</td>
<td>IETF IP</td>
</tr>
<tr>
<td>Layer 1</td>
<td>Physical</td>
<td>Signal type to transmit bits, pinouts, cable type</td>
<td>IEEE 802.3/802.1/802.11</td>
</tr>
</tbody>
</table>

---

*Copyright © 2018 Rockwell Automation, Inc. All Rights Reserved.*
## Open Systems Interconnection

<table>
<thead>
<tr>
<th>Layer No.</th>
<th>Layer Name</th>
<th>Function</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 7</td>
<td>Application</td>
<td>Network Services to User App</td>
<td>FactoryTalk® Security</td>
</tr>
<tr>
<td>Layer 6</td>
<td>Presentation</td>
<td>Encryption/Other processing</td>
<td>CIP Security</td>
</tr>
<tr>
<td>Layer 5</td>
<td>Session</td>
<td>Manage Multiple Applications</td>
<td>TLS / DTLS</td>
</tr>
<tr>
<td>Layer 4</td>
<td>Transport</td>
<td>Reliable End-to-End Delivery Error Correction</td>
<td>IPsec / ACLs</td>
</tr>
<tr>
<td>Layer 3</td>
<td>Network</td>
<td>Packet Delivery, Routing</td>
<td>MACsec / Port Security</td>
</tr>
<tr>
<td>Layer 2</td>
<td>Data Link</td>
<td>Framing of Data, Error Checking</td>
<td>Blockouts / Lock-ins</td>
</tr>
<tr>
<td>Layer 1</td>
<td>Physical</td>
<td>Signal type to transmit bits, pinouts, cable type</td>
<td></td>
</tr>
</tbody>
</table>
Holistic Plant-wide Security

Defense-in-Depth Security
<table>
<thead>
<tr>
<th>Business Enterprise</th>
<th>Sales &amp; Solutions</th>
<th>Products &amp; Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Strategic Alliances – develop seamless joint solutions</td>
<td>• Distributors – local delivery, expertise and support</td>
<td>• Encompass™ Product Reference – products with additional functionality that enhance and extend Rockwell Automation® solutions</td>
</tr>
<tr>
<td></td>
<td>• Solution Partners – extensive experience in design, implementation, project management and maintenance</td>
<td>• Technology Licensing – Embed Rockwell Automation technologies into their own products</td>
</tr>
</tbody>
</table>

**Holistic Plant-wide Security**  
**PartnerNetwork™ program - Collaboration of Partners**

**Reduce Risk**  
**Simplify Design**  
**Speed Deployment**
# Holistic Plant-wide Security

**PartnerNetwork™ program - Collaboration of Partners**

- **Rockwell Automation**
  - Products with security features
  - Security products
  - Security services

- **Strategic Alliances**
  - Products with security features
  - Security products
  - Security services

- **Encompass™ Product Reference**
  - Products with security features
  - Security products

- **Distributor**
  - Products with security features
  - Security products
  - Security services

- **Solution Partner**
  - Industrial IT and Information Software Disciplines
  - Industry leader and knowledge
  - Security solutions

- **OEM**
  - Convergence-ready solutions
Industrials IT & Industrial IoT
Cisco and Rockwell Automation Strategic Alliance (Bridging OT-IT)

Common Technology View:
A single scalable architecture, using open and standard Ethernet and IP networking technologies, such as EtherNet/IP, enabling the Industrial Internet of Things to help achieve the flexibility, visibility and efficiency required in a competitive manufacturing environment.

Converged Plantwide Ethernet (CPwE) 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, reliable, safe, secure and future-ready plant-wide industrial network infrastructure.

Joint Product Collaboration:
Stratix® 5900 Services Router, Stratix 5950 Industrial Firewall, Stratix 5100 Wireless Access Point/Workgroup Bridge, and Stratix 2500 / Stratix 5000 / Stratix 8000 families of managed industrial Ethernet switches, combine the best of both Rockwell Automation® and Cisco.

People and Process Optimization:
Education and services to facilitate OT and IT convergence, assist with successful architecture deployment, and enable efficient operations that allow critical resources to focus on increasing innovation and productivity.
Converged Plantwide Ethernet (CPwE)
Industrial IT & Industrial IoT (Bridging OT-IT)

- Tested, validated and documented reference architectures
  - Comprised of a collection of Cisco and Rockwell Automation® validated architectures, following the Cisco Validated Design (CVD) program
  - Developed from application and technology use cases
  - Industry neutral, one-to-many approach, customers adapt to meet their application needs
  - Tested for performance, availability, repeatability, scalability and security by subject matter authorities at Cisco and Rockwell Automation® CPwE test labs
- Built on technology and industry standards (IEC, IEEE, IETF)
  - “Future-ready” network design
- Content relevant to both OT and IT Engineers
- Deliverables
  - White Papers, Design & Implementation Guides
    recommendations, best practices, documented test results and configuration settings
- Proven architectures:
  - Helps customers to reduce their costs by simplifying their designs, accelerating their deployments, and reducing their risk in deploying new technology
Holistic Plant-wide Security
Built on CPwE Industrial Security Framework

Enterprise Zone: Levels 4–5
- Industrial Demilitarized Zone (IDMZ)
  - Physical or Virtualized Servers
    - Patch Management
    - AV Server
    - Application Mirror
    - Remote Desktop Gateway Server

Industrial Demilitarized Zone (IDMZ)
- Plant Firewalls
  - Active/Standby
  - Inter-zone traffic segmentation
- ACLs, IPS and IDS
- VPN Services
- Portal and Remote Desktop Services proxy

Industrial Zone: Levels 0–3
- Active Directory (AD)
- Plant-wide Firewall Management
- Network Access Control
- Application Access Control
- Remote Access Server (RAS)

Level 3 – Site Operations
- Computer Hardening
- Application Hardening
- FactoryTalk

Level 2 – Area Supervisory Control
- Segmentation – Zones
- Domains of Trust

Level 1 - Controller
- IACS Device Hardening
- Policies and Procedures
- Physical Measures
- Electronic Measures
- Encrypted Communications

Level 0 - Process
- Industrial Firewall
- I/O Soft Starter
- MCC
- Drive

Enterprise Identity Services
External DMZ Firewall

Cloud

Defense-in-Depth
- Architecture Best Practices
  - IEC 62443
  - Zones & Conduits
  - Availability, Integrity, Confidentiality
- NIST 800-82
  - Cyber security Framework
  - Identify, Protect, Detect, Respond, Recover
- ICS-CERT
  - Recommended Practices

Control System Engineers (OT)
Control System Engineers in Collaboration with IT Network Engineers (Industrial IT)
IT Security Architects in Collaboration with Control Systems Engineers

IPSec Firewalls
- I/O
- LWAP

SSID 2.4 GHz
SSID 5 GHz WGB

Wireless LAN Controller (WLC)
Active
Standby

Core Switches
Distribution Switch Stack

Network Infrastructure
- Hardening
- Access Control Resiliency
- Port Security
- Physical Electronic

Wireless LAN (WLAN)
- Access Policy
  - Equipment SSD
  - Plant Personnel SSD
  - Trusted Partners SSD
- WPA2 with AES Encryption
- Autonomous WLAN
  - Pre-shared key
  - 802.1X - (EAP-FAST)
- Unified WLAN
  - 802.1X - (EAP-TLS)
- CAPWAP DTLS

IACS Device Hardening
- Policies and Procedures
- Physical Measures
- Electronic Measures

Engineers (OT)
in Collaboration with IT
Network Engineers (Industrial IT)
IT Security Architects in Collaboration with Control Systems Engineers

Copyright © 2018 Rockwell Automation, Inc. All Rights Reserved.
Holistic Plant-wide Security
Built on CPwE Industrial Security Framework

Enterprise Zone: Levels 4–5
Industrial Demilitarized Zone (IDMZ)
- Physical or Virtualized Servers
  - Patch Management
  - AV Server
  - Application Mirror
  - Remote Desktop Gateway Server

Industrial Zone: Levels 0–3
- Application Access Control
- Application Hardening
- Segregating - Zoning Domains of Trust

Level 3 – Site Operations
- Industrial Demilitarized Zone (IDMZ)
- Communication Gateway

Level 2 – Area Supervisory Control
- Active Wireless LAN Controller (WLC)
- Standby Core Switches
- Distribution Switch Stack

Level 1 - Controller
- Industrial Firewall
- IACS Device Hardening
  - Policies and Procedures
  - Physical Measures
  - Electronic Measures
  - Encrypted Communications

Level 0 - Process
- LWAP
- Switch Stack
- Enterprise I/O

Defense-in-Depth
- Architecture Best Practices
- IEC 62443
- Zones & Conduits
- Availability, Integrity, Confidentiality
- NIST 800-82
- Cyber Security Framework
- Help identify, Protect, Detect, Respond, Recover
- ICS-CERT
- Recommended Practices

Control System Engineers (OT)
Control System Engineers (OT)
Holistic Plant-wide Security

- IACS Device Hardening
  - Policies and Procedures
  - Product Hardening
- Physical Measures
  - Locked Enclosures, Data Ports
- Electronic Measures
  - Application Security
  - CIP Security (CY18)
- Encrypted Communications
- Port Security
  - Physical
  - Electronic
- Application Authentication, Authorization and Accounting (AAA)
- Industrial Firewall
- Logical Zoning
Logical Zoning

Holistic Plant-wide Security - CPwE Logical Model

OT Standards

- Operational Levels
  - ISA 95, Purdue – Levels 0–5
  - Level 0 Sensor/Actuators, Level 1 Controller, Level 2 Local Supervisor, Level 3 Site Operations, Level 4–5 Enterprise

- Functional / Security Zones
  - IEC-62443, NIST 800-82, ICS-CERT
  - Enterprise, Industrial, IDMZ

IT Standards

- Network Technology
  - OSI Reference Model – 7 Layers
  - IEEE 802.1, 802.3, 802.11
  - IETF TCP, UDP, UP

- Network Switch Hierarchy
  - Campus Network Model
    - Layer 2 Access
    - Layer 3
Logical Zoning
Holistic Plant-wide Security - CPwE Logical Model

- Levels – ISA 95, Purdue Reference Model
- Zones – IEC 62443, NIST 800-82, ICS-CERT Recommended Practices
Logical Zoning
Holistic Plant-wide Security - CPwE Logical Model

Plant-wide Zoning

- Functional / Security Areas
- Smaller Connected LANs
  - Smaller Broadcast Domains
  - Smaller Fault Domains
  - Smaller Domains of Trust
- Industrial IoT Technology
- Building Block Approach for Scalability
Logical Zoning
Holistic Plant-wide Security – Data Diode

- Owl Cyber Defense
  - Owl Perimeter Defense Solution (OPDS)
    - DualDiode Technology
    - Tested with certain Rockwell Automation software solutions – for example, FactoryTalk® Historian
    - Aligned to IEC 62443-3-3
      - Security Zones, Secure Conduits
  - Multiple Industries - Critical Infrastructure
Logical Zoning
Holistic Plant-wide Security – Encryption / Zoning

- Tempered Networks
  - Identity-Defined Networking (IDN)
    - Host Identity Protocol (HIP) Technology
      - HIP separates endpoint locator (IP) from identifier role (IP)
      - Cloaks (hides) equipment and endpoints that are IP-enabled - cryptographic host identifiers (HI)
      - IETF RFC 4423 - Host Identity Protocol (HIP) Architecture
    - HIPswitch Series and HIPswitch Conductor
  - Multiple Industries - Critical Infrastructure
Logical Zoning
Holistic Plant-wide Security – Port Security / Zoning

- Panduit Corp.
  - Port Security - Physical
    - Lock-in / Blockout
      - Copper Ethernet
      - Fiber Ethernet
      - USB
  - Physical Zoning
    - Physical Network Zone System
  - Multiple Industries - Critical Infrastructure
IACS Device Hardening - Encryption
Holistic Plant-wide Security
IACS Device Hardening - Encryption
Holistic Plant-wide Security

- Physical or Virtualized Servers
- Application Servers & Services Platform
- Network Services – for example, DNS, AD, DHCP, AAA
- Remote Access Server (RAS)
- Storage Array

- Enterprise-wide Business Systems

- Plant-wide / Site-wide Operation Systems

2 b) IPsec tunnel from Controller to Firewall
IPsec tunnel from Firewall to Windows Server 2012

2a) IPsec tunnel from Controller to Windows Server 2012

1) IPsec tunnel between two Controllers

- Levels 4–5 – Data Center Enterprise Zone
- Level 3.5 - IDMZ
- Industrial Zone Levels 0–3
- Level 3 - Site Operations
  - Physical or Virtualized Servers
    - Application Servers & Services Platform
    - Network Services – for example, DNS, AD, DHCP, AAA
    - Remote Access Server (RAS)
  - Storage Array

- Workstation

- Local Cell/Area Zone #1
- Local Cell/Area Zone #2
- Local Cell/Area Zone #3
Industrial Firewall

Holistic Plant-wide Security – CPwE Industrial Firewall

- Stratix® 5950 Security Appliance
  - Collaboration with Cisco Systems
  - IACS focused industrial firewall
    - Deep Packet Inspection for IACS protocols
    - DIN rail-mounted network security device
- Transparent Mode, Routed Mode, Monitor Mode
- Leverage industry-leading security technologies:
  - Adaptive Security Appliance for Firewall and VPN

Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture
Industrial Firewall - Policy Enforcement
Holistic Plant-wide Security – CPwE Industrial Firewall

- CIP™ Class 3
- CIP™ Class 1
- ICMP - ping
- Http
- SNMP Sweep
- Ping Sweep
- CIP™ DPI

Industrial Zone

Industrial Firewall

Skid / Machine
Holistic Plant-wide Security
Built on CPwE Industrial Security Framework

Enterprise Zone: Levels 4–5
Industrial Demilitarized Zone (IDMZ)
Physical or Virtualized Servers
- Patch Management
- AV Server
- Application Mirror
- Remote Desktop Gateway Server

Industrial Zone: Levels 0–3
Remote Access Server (RAS)
Level 3 – Site Operations
Computer Hardening
Level 2 – Area Supervisory Control
FactoryTalk Control
Level 1 – Controller
Controller
Controller

Network Infrastructure
- Hardening
- Access Control
- Resiliency

Wireless LAN (WLAN)
- Access Policy
  - Equipment SSID
  - Plant Personnel SSID
  - Trusted Partners SSID
  - WPA2 with AES Encryption
  - Autonomous WLAN
  - Pre-shared key
    - 802.1X - (EAP-FAST)
  - Unified WLAN
    - 802.1X - (EAP-TLS)
    - CAPWAP DTLS

Control System Engineers
in Collaboration with IT
Network Engineers
(Industrial IT)

Defense-in-Depth
- Architecture Best Practices
  IEC 62443
- Zones & Conduits
- Availability, Integrity,
  Confidentiality
  NIST 800-82
- Cyber security Framework
- Help Identify, Protect, Detect,
  Respond, Recover
  ICS-CERT
- Recommended Practices
Industrial IT (OT-IT)  
Holistic Plant-wide Security

- Computer Hardening
  - Windows Best Practices
  - OS Patch Management
  - Hard disk drive Encryption, Anti-X
  - Application White Listing
- Remote Access Server (RAS)
  - Remote Desktop Services
- Wireless LAN
  - Unified WLAN Architectures
  - Autonomous WLAN Architectures
- Network Infrastructure
  - Hardening
    - Port Security – physical, electronic
    - Cryptographic Image
  - Access Control
    - Access Control – local, centralized
  - Resiliency
    - Redundant Path Topology
    - Resiliency Protocol
    - Active / Standby Layer 3 Switches
- Monitoring and Status
  - Application
  - Network
Computer Hardening
Holistic Plant-wide Security

- Symantec Corporation
  - Symantec Embedded Security: Critical System Protection (SES:CSP)
    - Application sandboxing & whitelisting
    - Memory control policies
    - Real-time integrity monitoring
    - Firewall and intrusion prevention
  - Interoperability testing with certain Rockwell Automation software solutions – for example, FactoryTalk® Applications
  - Multiple Industries - Critical Infrastructure
Monitoring and Status
Holistic Plant-wide Security - Application

- Tripwire
  - Configuration Compliance Manager (CCM) for Industrial Automation
    - Integration with FactoryTalk® AssetCentre
    - Security monitoring for authorized and unauthorized network changes
    - ICS-CERT security advisories and alerts
      - FactoryTalk® Applications
      - Stratix® industrial Ethernet switches
      - Cisco Catalyst switches
      - Logix Controllers
    - Project file integrity monitoring
  - Multiple Industries - Critical Infrastructure
- Aligned to IEC 62443 and NIST 800

Encompass Product Partner
Complementary Products
Product Referencing Program
Monitoring and Status
Holistic Plant-wide Security - Network

- Claroty
  - Claroty Platform
    - Network visibility/topology/asset discovery
    - Passive, deep packet inspection (DPI) to examine, analyze and monitor OT networks across Purdue Model layers
    - Creates a high-fidelity baseline model and leverages advanced algorithms to alert customers to anomalous behavior
    - System generates well-crafted, descriptive alerts, not a stream of anomalous events and provides the deep contextual data
  - Aligned to IEC 62443-2-4
    - Totally passive operation
  - Multiple Industries - Critical Infrastructure
  - https://locator.rockwellautomation.com/Encompass/ProductDetails/006895
Holistic Plant-wide Security
Built on CPwE Industrial Security Framework

Enterprise Zone: Levels 4–5
- Physical or Virtualized Servers
- Patch Management
- AV Server
- Application Mirror
- Remote Desktop Gateway Server

Industrial Demilitarized Zone (IDMZ)
- Active/Standby
- Inter-zone traffic segmentation
- ACLs, IPS and IDS
- VPN Services
- Portal and Remote Desktop Services proxy

Industrial Zone: Levels 0–3
- Active Directory (AD)
- Plant-wide Firewall Management
- Network Access Control

Level 3 – Site Operations
- IT Security Architects in Collaboration with Control Systems Engineers

Defense-in-Depth
- Architecture Best Practices
- IEC 62443
- Zones & Conduits
- Availability, Integrity, Confidentiality
- NIST 800-82
- Cyber security Framework
- Help Identify, Protect, Detect, Respond, Recover
- ICS-CERT
- Recommended Practices
IT Security
Holistic Plant-wide Security

- Active Directory
  - Identity Source
- Network Authentication, Authorization and Accounting
  - Authentication – wired, wireless
  - Authorization – downloadable access control lists (dACL)
- Plant-wide Firewall Management
- Status and Monitoring

- IDMZ
  - Data Brokers
    - Remote Desktop Gateway Services
    - Reverse Proxy
    - PI-to-PI Interface
  - IDMZ Firewalls
Cisco Identity Services Engine
- Combines authentication, authorization, profiling and posturing into one appliance
- Uses network access control to manage what resources users and guests are allowed to access
- Determines what kind of mobile device users are using, and whether it complies with hardware and software policies
- Manages wired and wireless access with 802.1X

Deploying Identity and Mobility Services within a Converged Plantwide Ethernet Architecture
Plant-wide Network Access Control
Holistic Plant-wide Security – CPwE Identity Services

Enterprise Zone: Levels 4–5

Industrial Demilitarized Zone (IDMZ)

Industrial Zone
Levels 0–3
(Plant-wide Network)

Cell/Area Zones - Levels 0–2
(Lines, Machines, Skids, Equipment)
Plant-wide Network Access Control
Holistic Plant-wide Security – CPwE Identity Services

Enterprise Zone: Levels 4–5
Enterprise WAN
External DMZ / Firewall
WLC (Enterprise)
ISE PAN/PSN
ISE MnT
Cloud

Industrial Demilitarized Zone (IDMZ)

Industrial Zone Levels 0–3
(Plant-wide Network)

Industrial Zone
Levels 0–3
(Plant-wide Network)

Level 3
Site Operations

Cell/Area Zones - Levels 0–2
(Lines, Machines, Skids, Equipment)

Controller
I/O
Drive
Controller
Controller
FactoryTalk®

LWAP
WLC (Active)
WLC (Standby)

Core switches

ISE PSN

Core switches

ISE MnT

ISE PAN/PSN

Firewalls (Active/Standby)
Plant-wide Firewall Management

Holistic Plant-wide Security – CPwE IDMZ and IFW

- Cisco ASA (adaptive security appliance)
  - Provides firewall capabilities to logically segment the plant floor from the enterprise, tracks and inspects traffic flows
  - Provides up to 8 integrated and up to 14 Gigabit ports with service modules for flexibility in network design
  - Provides up to 700 Mbps of VPN throughput, and up to 5000 concurrent VPN sessions
  - Newly added FirePOWER module from Sourcefire adds next generation IPS for threat detection, and Advanced Malware Protection (AMP)
- Securely Traversing IACS Data Across the Industrial Demilitarized Zone
- Allen-Bradley® Stratix® 5950 (security appliance)
  - Industrial Firewalls within a Converged Plantwide Ethernet Architecture
Holistic Plant-wide Security
Built on CPwE Industrial Security Framework

Enterprise Zone: Levels 4–5
Industrial Demilitarized Zone (IDMZ)
- Physical or Virtualized Servers
  - Patch Management
  - AV Server
  - Application Mirror
  - Remote Desktop Gateway Server

Industrial Zone: Levels 0–3
- Active Directory (AD)
- Plant-wide Firewall Management
- Application Access Control
- Remote Access Server (RAS)
- Level 3 – Site Operations
  - Computer Hardening
  - Application Hardening
  - FactoryTalk
- Level 2 – Area Supervisory Control
  - Segregating - Zoning
  - Domains of Trust
- Control System Engineers (OT)
- Control System Engineers in Collaboration with IT Network Engineers (Industrial IT)
- IT Security Architects in Collaboration with Control Systems Engineers

Defense-in-Depth
- Architecture Best Practices
- IEC 62443
- Zones & Conduits
- Availability, Integrity, Confidentiality
- NIST 800-82
- Cyber security Framework
- ICS-CERT
- Recommended Practices

Level 0 - Process
- Control System
- Engineers (OT)
- Network Engineers (Industrial IT)
- IT Security Architects in Collaboration with Control Systems Engineers

Defense-in-Depth
- Architecture Best Practices
- IEC 62443
- Zones & Conduits
- Availability, Integrity, Confidentiality
- NIST 800-82
- Cyber security Framework
- ICS-CERT
- Recommended Practices
Key Takeaways

- Education and awareness - within your organization, for your customers or trusted partners
- Establish an open dialog between Industrial Automation and IT groups
- Establish an Industrial security policy, unique from and the Enterprise security policy
- Holistic Defense-in-Depth approach: no single product, methodology, nor technology fully secures IACS networks
- Be aware of Industrial Automation and Control System Security (IACS) Standards
  - IEC-62443 (Formerly ISA99), NIST 800-82, ICS-CERT Recommended Practices
- Use standards, reference models, tested and validated reference architectures (simplified design, quicker deployment, reduced risk in deploying new technology)
- Work with trusted partners knowledgeable in industrial automation and security
- "Good enough" security now, is better than "perfect" security ... never
  (Tom West, Data General)
Additional Material
Additional Material
Network Architecture Icon Key

- Layer 2 Access Switch, Catalyst 2960
- Layer 2 Access, Industrial Ethernet Switch (IES), Stratix® 2500, Stratix® 5700, Stratix® 5400, Stratix® 8000
- Layer 2 IES with NAT, Stratix® 5700, Stratix® 5400
- Layer 2 IES with NAT and Connected Routing, Stratix® 5700, Stratix® 5400
- Multi-Layer Switch - Layer 2 and Layer 3, Stratix® 8300, Stratix® 5700, Stratix® 5400, Stratix® 5410
- Layer 3 Distribution Switch Stack, Catalyst 3750-X, Catalyst 3850
- Layer 3 Core Switch, Catalyst 4500, 4500-X, 6500, 6800
- Layer 3 Core Switch with Virtual Switching System (VSS), Catalyst 4500-X, 6500, 6800
- Layer 3 Router, Stratix® 5900
- Layer 3 Router with Zone-based Firewall, Stratix® 5900
- Firewall, Adaptive Security Appliance (ASA) 55xx
- Industrial Firewall, Stratix® 5950
- Autonomous Wireless Access Point (AP), Stratix® 5100 as Autonomous AP
- Wireless workgroup bridge (WGB), Stratix® 5100 as workgroup bridge (WGB)
- Unified Wireless Lightweight Access Point (LWAP), Catalyst 3602E LWAP
- Unified Wireless LAN Controller (WLC), Cisco 5508 WLC
- Unified Computing System (UCS), UCS-C series
- Identity Services Engine (ISE) for Authentication, ISE - PAN/PSN/MnT
- Layer 2 Access Link (EtherNet/IP Device Connectivity)
- Layer 2 Interswitch Link/802.1Q Trunk
- Layer 3 Link
Additional Material
Rockwell Automation Industrial Security Website

http://rockwellautomation.com/security
Additional Material
CPwE Architectures - Cisco and Rockwell Automation®

- CPwE website
- Overview Documents
  - Alliance Profile
  - Top 10 Recommendations for Plant-wide EtherNet/IP Deployments
  - Design Considerations for Securing Industrial Automation and Control System Networks

---

Wide-Area Network (WAN)
Data Center - Virtualized Servers
  - ERP - Business Systems
  - Email/FTP Services
  - Security Services - Active Directory (AD), Identity Services (AAI)
  - Network Services - DNS, DHCP, CA Manager

Physical or Virtualized Servers
  - Task Management
  - AV Server
  - Application Marketplace
  - Parent/Child Server

Plant Firewalls
  - AD/AAI
  - Ethernet/Segmentation
  - Remote Access
  - VPN Services
  - Traffic and Device Table, Services proxy

Enterprise Zone
Levels 4-6

Industrial Demilitarized Zone (IDMZ)

Level 3 - Site Operations (Control Room)

Industrial Zone
Levels 0-3
(Plant-wide Network)

Cell/Area Zone - Levels 0-2
Reduced Star Topology - Flex Links Resiliency
Unified Wireless LAN
(Lines, Machines, Solds, Equipment)

Cell/Area Zone - Levels 0-2
Ring Topology - Camera Level Ring (DLR) Protocol
Unified Wireless LAN
(Lines, Machines, Solds, Equipment)

Cell/Area Zone - Levels 0-2
Linear/Bus/Star Topology
Autonomous Wireless LAN
(Lines, Machines, Solds, Equipment)

---

Rockwell Automation
Cisco
<table>
<thead>
<tr>
<th>Topic</th>
<th>Design Guide</th>
<th>Whitepaper</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design Considerations for Securing IACS Networks</td>
<td></td>
<td>ENET-WP031A-EN-P</td>
</tr>
<tr>
<td>Converged Plantwide Ethernet – Baseline Document</td>
<td>ENET-TD001E-EN-P</td>
<td>—</td>
</tr>
<tr>
<td>Deploying 802.11 Wireless LAN Technology within a CPwE Architecture</td>
<td>ENET-TD006A-EN-P</td>
<td>ENET-WP034A-EN-P</td>
</tr>
<tr>
<td>Deploying Identity and Mobility Services within a CPwE Architecture</td>
<td>ENET-TD008B-EN-P</td>
<td>ENET-WP037B-EN-P</td>
</tr>
<tr>
<td>Securely Traversing IACS Data Across the Industrial Demilitarized Zone (IDMZ)</td>
<td>ENET-TD009B-EN-P</td>
<td>ENET-WP038B-EN-P</td>
</tr>
<tr>
<td>Deploying Network Address Translation within a CPwE Architecture</td>
<td>ENET-TD007A-EN-P</td>
<td>ENET-WP036A-EN-P</td>
</tr>
<tr>
<td>Migrating Legacy IACS Networks to a CPwE Architecture</td>
<td>ENET-TD011A-EN-P</td>
<td>ENET-WP040A-EN-P</td>
</tr>
<tr>
<td>Deploying A Resilient Converged Plantwide Ethernet Architecture</td>
<td>ENET-TD010B-EN-P</td>
<td>ENET-WP039D-EN-P</td>
</tr>
<tr>
<td>Site-to-site VPN to a CPwE Architecture</td>
<td>ENET-TD012A-EN-P</td>
<td>—</td>
</tr>
<tr>
<td>Deploying Industrial Firewalls within a CPwE Architecture</td>
<td>ENET-TD002A-EN-P</td>
<td>ENET-WP011B-EN-P</td>
</tr>
<tr>
<td>Deploying Device Level Ring within a CPwE Architecture</td>
<td>ENET-TD015A-EN-P</td>
<td>ENET-WP016B-EN-P</td>
</tr>
<tr>
<td>OEM Networking within a CPwE Architecture</td>
<td>ENET-TD018A-EN-P</td>
<td>ENET-WP018A-EN-P</td>
</tr>
<tr>
<td>Cloud Connectivity to a Converged Plantwide Ethernet Architecture</td>
<td>ENET-TD017A-EN-P</td>
<td>ENET-WP019A-EN-P</td>
</tr>
</tbody>
</table>
**Additional Material**

**Rockwell Automation Reference Documents**

- **Ethernet Design Considerations Reference Manual**
  - ENET-RM002C-EN-P
  - EtherNet/IP Overview, Ethernet Infrastructure Components, EtherNet/IP Protocol, Predict System Performance
- **EtherNet/IP IntelliCENTER® Reference Manual** (MCC-RM001)
- **The OEM Guide to Networking**
  - ENET-RM001A-EN-P
  - This guide is intended to help OEMs understand relevant technologies, networking capabilities and other considerations that could impact them as they develop EtherNet/IP solutions for the machines, skids or equipment they build
- **Segmentation Methods Within the Cell/Area Zone** ENET-AT004B-EN-E
Additional Material
Rockwell Automation Tools

- Integrated Architecture® Builder (IAB)
  - Updates and additions to better-reflect CPwE structure, hierarchy and best practices
  - Improved Switch Wizard for distribution (for example, Stratix® 5410) and access (for example, Stratix® 5700)
  - Easier to create a large EtherNet/IP network with many topologies
  - CIP™ traffic is measured per segment, not just controller scanner and adapter centric

- EtherNet/IP Capacity Tool
- Popular Configuration Drawings (PCDs)
  - Updates and additions to better reflect CPwE recent enhancements
Additional Material

ODVA

- Website:
  - http://www.odva.org/
- EtherNet/IP
  - https://www.odva.org/Technology-Standards/EtherNet-IP/OverviewSecuring EtherNet/IP Networks
- EtherNet/IP Network Infrastructure Guide
  - https://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00035R0_Infrastructure_Guide.pdf

- Common Industrial Protocol (CIP™)
- The Family of CIP™ Networks
- CIP Security
Training Resources
Training Resources
Education - Industrial IoT / Industrial IT (Bridging OT-IT)

- A ‘go-to’ resource for training and educational information on standard Internet Protocol (IP), security, wireless and other emerging technologies for industrial applications
- Led by Cisco, Panduit, and Rockwell Automation
- Receive monthly e-newsletters with articles and videos on the latest trends
- Scenario-based training on topics such as: logical topologies, protocols, switching, routing, wireless and physical cabling

Network Design eLearning course available at promotional price for Attendees!
Earn PDHs by signing up today at www.industrial-ip.org with code “EVENTS2017”
Four eLearning courses cover key aspects of implementing networked, industrial control systems. 20-30 minutes interactive, scenario-based courses cover automation controls and physical infrastructure considerations.
Training Resources
Education - Industrial IoT / Industrial IT (Bridging OT-IT)

- **Courses 1 and 2: Designing for the Cell/Area Zone**
  - Design secure, robust, future-ready networks for cells, machines, skids and other functional units by implementing reference architectures and standard IP.

- **Course 3: Designing for the Industrial Zone**
  - Learn design principles on line integration, high-availability networks and wireless architectures to optimize plant networks.

- **Course 4: IT/OT Integration**
  - Understand how to effectively converge a smart manufacturing facility with IT and OT stakeholders.
Training Resources
Training and Certification – Industrial IoT / Industrial IT (Bridging OT-IT)

• Cisco Industrial Networking Specialist Training and Certification
  – Classroom training
    • Managing Industrial Networks with Cisco Networking Technologies (IMINS)
  – Exam: 200–401 IMINS
  – CPwE Design Considerations and Best Practices

• CCNA Industrial Training and Certification
  – Classroom training
    • Managing Industrial Networks for Manufacturing with Cisco Technologies (IMINS2)
  – Exam: 200–601 IMINS2
  – CPwE Design Considerations and Best Practices
<table>
<thead>
<tr>
<th>Module 1</th>
<th>Industrial Networking Solutions and Products</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module 2</td>
<td>Industrial Network Documentation and Deployment Considerations</td>
</tr>
<tr>
<td>Module 3</td>
<td>Installing Industrial Network Switches, Routers, and Cabling</td>
</tr>
<tr>
<td>Module 4</td>
<td>Deploying Industrial Ethernet Devices</td>
</tr>
<tr>
<td>Module 5</td>
<td>Maintaining Industrial Ethernet Networks</td>
</tr>
<tr>
<td>Module 6</td>
<td>Troubleshooting Industrial Ethernet Networks</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Module 1</th>
<th>Industrial Networking Concepts and Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module 2</td>
<td>General Troubleshooting Issues</td>
</tr>
<tr>
<td>Module 3</td>
<td>EtherNet/IP</td>
</tr>
<tr>
<td>Module 4</td>
<td>Troubleshooting EtherNet/IP</td>
</tr>
<tr>
<td>Module 5</td>
<td>PROFINET</td>
</tr>
<tr>
<td>Module 6</td>
<td>Configuring PROFINET</td>
</tr>
<tr>
<td>Module 7</td>
<td>Troubleshooting PROFINET</td>
</tr>
<tr>
<td>Module 8</td>
<td>Exploring Security Concerns</td>
</tr>
<tr>
<td>Module 9</td>
<td>802.11 Industrial Ethernet Wireless Networking</td>
</tr>
</tbody>
</table>
Training Resources
Rockwell Automation - Webinars

- **Industrial Automation Webinars**
- **On-Demand Webinars**
  - Introduction to Building a Robust, Secure and Future-ready Network Infrastructure
  - Increase Business Agility by Converging Manufacturing and Business Systems
  - The Power of Building a Secure Network Infrastructure
  - Design Considerations for Building a Secure Network Infrastructure
# Training Resources

## Cisco Training & Certifications

<table>
<thead>
<tr>
<th>Entry</th>
<th>Associate</th>
<th>Professional</th>
<th>Expert</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Architect</strong></td>
<td></td>
<td></td>
<td>CCAr Architect</td>
</tr>
<tr>
<td><strong>Cloud</strong></td>
<td>CCNA Cloud</td>
<td>CCNP Cloud</td>
<td></td>
</tr>
<tr>
<td><strong>Collaboration</strong></td>
<td>CCNA Collaboration</td>
<td>CCNP Collaboration</td>
<td>CCIE Collaboration</td>
</tr>
<tr>
<td><strong>Cybersecurity Operations</strong></td>
<td>CCNA CyberOps</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Data Center</strong></td>
<td>CCNA Data Center</td>
<td>CCNP Data Center</td>
<td>CCIE Data Center</td>
</tr>
<tr>
<td><strong>Design</strong></td>
<td>CCENT</td>
<td>CCDA</td>
<td>CCDP</td>
</tr>
<tr>
<td><strong>Industrial/IoT</strong></td>
<td></td>
<td>CCNA Industrial</td>
<td></td>
</tr>
<tr>
<td><strong>Routing &amp; Switching</strong></td>
<td>CCENT</td>
<td>CCNA Routing and Switching</td>
<td>CCIE Routing and Switching</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>CCENT</td>
<td>CCNA Security</td>
<td>CCIE Security</td>
</tr>
<tr>
<td><strong>Service Provider</strong></td>
<td>CCNA SP</td>
<td>CCNP SP</td>
<td>CCIE SP</td>
</tr>
<tr>
<td><strong>Wireless</strong></td>
<td>CCENT</td>
<td>CCNA Wireless</td>
<td>CCIE Wireless</td>
</tr>
<tr>
<td><strong>Other Certifications</strong></td>
<td>Certified Technician</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Specialist</strong></td>
<td>Business</td>
<td>Data Center</td>
<td>Internet of Things</td>
</tr>
<tr>
<td></td>
<td>Security</td>
<td>Operating System Software</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Cisco Certification Track**

- ICND1
- ICND2