Questions?
Use Cisco Spark to communicate with the speaker after the session

How
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space

cs.co/ciscolivebot#BRKIOT-2108
Agenda

• Connected Factory Architecture
  • Cisco Reference Architecture
  • Factory Network
  • Factory Wireless
  • Factory Security
  • Cisco Kinetic

• Connected Factory in Practice
  • Introduction
  • Factory Security Case Study
  • Enabling Analytics
  • Factory Wireless – AGV Roaming
  • Conclusion

• Recommended Resources
Connected Factory Reference Architectures
Connected Factory Reference Architectures
Converged Plantwide Ethernet (CPwE)

- Tested, validated and documented reference architectures
  - Developed from use cases - customer and application
  - Tested for performance, availability, repeatability, scalability and security
  - Comprised of Cisco® and Rockwell Automation® Validated Designs

- Built on technology and industry standards
  - “Future-ready” network design

- Content relevant to both OT and IT Engineers

- Deliverables
  - Recommendations, best practices, design and implementation guidance, documented test results and configuration settings
  - Simplified design, quicker deployment, reduced risk in deploying new technology
Built on Industry Standards cont.

Purdue Reference Model

Level 5
Level 4
Level 3
Level 2
Level 1
Level 0

Enterprise Network

<table>
<thead>
<tr>
<th>Level 5</th>
<th>Level 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-Mail, Intranet, etc.</td>
<td>Site Business Planning and Logistics Network</td>
</tr>
</tbody>
</table>

Remote Gateway Services
Patch Management
AV Server
Firewall
Application Mirror
Web Services Operations
Application Server
Firewall

Level 3

FactoryTalk Application Server
FactoryTalk Directory
Engineering Workstation
Remote Access Server
Site Operations and Control

Level 2

FactoryTalk Client
Operator Interface
Engineering Workstation
Operator Interface

Level 1

Batch Control
Discrete Control
Drive Control
Continuous Process Control
Safety Control

Level 0

Sensors
Drives
Actuators
Robots

Enterprise Security Zone
Industrial DMZ
Industrial Zone
Cell/Area Zone
Process

BRKIOT-2108 © 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Connected Factory - Designed for Digital Manufacturing
Factory Network
Cell/Area Zone Overview

Cell/Area Zone - Functional Area of a Production Facility. Considerations Include:

- Environmental constraints
- Range of device intelligence
- Time-sensitive applications
Industrial Network Topologies

Cell/Area Zone Topology Options

<table>
<thead>
<tr>
<th>Topology</th>
<th>Linear</th>
<th>Ring</th>
<th>Redundant Star</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cabling Requirements</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>Ease of Configuration</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>Implementation Costs</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>Redundancy and Convergence</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>Disruption During Network Upgrade</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>Readiness for Network Convergence</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>Overall in Network TCO and Performance</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
</tbody>
</table>

- Worst
- OK
- Best
# Performance Requirements

## Industrial Automation & Control System Applications

<table>
<thead>
<tr>
<th>Function</th>
<th>Process Automation</th>
<th>Discrete Automation</th>
<th>Loss Critical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comm. Technology</td>
<td>Information Integration, Slower Process Automation</td>
<td>Industrial Protocols, CIP, Profinet</td>
<td>Multi-axis Motion Control</td>
</tr>
<tr>
<td>Period</td>
<td>1 second or longer</td>
<td>1 ms to 100 ms</td>
<td>100 µs to 10 ms</td>
</tr>
<tr>
<td>Industries</td>
<td>Oil &amp; Gas, chemicals, energy, water</td>
<td>Auto, food and bev, electrical assembly, semiconductor, metals, pharmaceutical</td>
<td>Utilities Subset of Discrete automation</td>
</tr>
<tr>
<td>Applications</td>
<td>Pumps, compressors, mixers; monitoring of temperature, pressure, flow</td>
<td>Material handling, filling, labeling, palletizing, packaging; welding, stamping, cutting, metal forming, soldering, sorting</td>
<td>Life/equipment safety, Synchronization of multiple axes: printing presses, wire drawing, web making, picking and placing</td>
</tr>
</tbody>
</table>

Source: ARC Advisory Group
## Network Resiliency Protocols

Selection is Application Driven

<table>
<thead>
<tr>
<th>Resiliency Protocol</th>
<th>Mixed Vendor</th>
<th>Ring</th>
<th>Redundant Star</th>
<th>Net Conv &gt;250 ms</th>
<th>Net Conv 50-100 ms</th>
<th>Net Conv &lt; 0~10 ms</th>
<th>Layer 3</th>
<th>Layer 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>STP (802.1D)</td>
<td>☑</td>
<td>☑</td>
<td></td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>RSTP (802.1w)</td>
<td>☑</td>
<td>☑</td>
<td></td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>MSTP (802.1s)</td>
<td>☑</td>
<td>☑</td>
<td></td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>PVST+</td>
<td>☑</td>
<td>☑</td>
<td></td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>REP</td>
<td>☑</td>
<td>☑</td>
<td></td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>EtherChannel</td>
<td>☑</td>
<td>☑</td>
<td></td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>(LACP 802.3ad)</td>
<td>☑</td>
<td>☑</td>
<td></td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>MRP (IEC 62439-2)*</td>
<td>☑</td>
<td>☑</td>
<td></td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>Flex Links</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PRP/HSR (IEC 62439)*</td>
<td>☑</td>
<td>☑</td>
<td></td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>DLR (IEC &amp; ODVA)</td>
<td>☑</td>
<td>☑</td>
<td></td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>StackWise</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HSRP</td>
<td>☑</td>
<td>☑</td>
<td></td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>VRRP (IETF RFC 3768)</td>
<td>☑</td>
<td>☑</td>
<td></td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td></td>
</tr>
</tbody>
</table>

* Not part of CPwE

---

**Process and Information**

**Time Critical**

**Loss Critical**
Factory Network
Layer 2 NAT
Challenge - Ethernet Growing Pains

- Ethernet networks continue to grow:
  - Each machine adds another 5 - 50 EtherNet/IP enabled devices
  - Every line adds another 250 - 1,000 EtherNet/IP enabled devices

*How do I connect all these machines into a plant network to gain the advantages?*
Solution - Layer 2 Network Address Translation (NAT)

One to One (1:1) NAT

Outside Subnet (ex. 10.0.0.x)

Many Outside IP addresses
(One per device wishing to be accessible from the Outside Subnet)

NAT Enabled Device

Many Inside IP addresses
(One per connected device)

Inside Subnet (ex. 192.168.1.x)
Layer 3 vs Layer 2 NAT

**Layer 3**
- Typically a software implementation
- NAT device acts as the default gateway (router) for the devices on the inside network
- NAT device will intercept traffic, perform translation, and route traffic
- Translations are handled by the NAT CPU
- Performance of translation directly tied to the loading of the NAT CPU

**Layer 2**
- Hardware based implementation
- NAT device does not act as a router and utilizes 2 translations tables – inside to outside & outside to inside
- Performance is at wire speed throughout switch loading
- Supports multiple VLANs through NAT boundary enhancing segmentation flexibility (Communication between VLANs requires a separate layer 3 device)
Layer 2 NAT Design Scenario #1
Single-Cell, Single VLAN per Switch

<table>
<thead>
<tr>
<th>Inside to Outside NAT Table</th>
<th>Inside</th>
<th>Outside</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.10</td>
<td>10.10.10.10</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Outside to inside NAT Table</th>
<th>Outside</th>
<th>Inside</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.30</td>
<td>192.168.1.30</td>
<td></td>
</tr>
</tbody>
</table>
Layer 2 NAT Design Scenario #3
Multi-Cell, Single Switch, Multi-VLAN

OUTSIDE
IP Address: 10.10.40.X

LINE CONTROLLER
10.10.40.12

VLAN 10
IP Address: 192.168.1.X

VLAN 20
IP Address: 192.168.1.X

VLAN 30
IP Address: 192.168.1.X

INSIDE
IP Address: 192.168.1.X

WORKSTATION
10.10.40.10

NAT
1.4.7.3

Aggregation switch

IES
IES
Aggregation switch

IES
IES
Layer 2 NAT Design Scenario #3
Multi-Cell, Single Switch, Multi-VLAN

Machine 1
NAT Table
192.168.1.3 10.10.10.3
192.168.1.4 10.10.10.4
192.168.1.7 10.10.10.7

Machine 2
NAT Table
192.168.1.3 10.10.20.3
192.168.1.4 10.10.20.4
192.168.1.7 10.10.20.7

Machine 3
NAT Table
192.168.1.3 10.10.30.3
192.168.1.4 10.10.30.4
192.168.1.7 10.10.30.7

NAT Table
Inside Outside
192.168.1.3 10.10.10.3
192.168.1.4 10.10.10.4
192.168.1.7 10.10.10.7
Multiple Instance of NAT per VLAN
Layer 2 NAT Design Scenario #3

Multi-Cell, Single Switch, Multi-VLAN

Multiple Instance of NAT per VLAN

NAT Table
Inside | Outside
--- | ---
Machine 1 | 192.168.1.3 | 10.10.10.3
| 192.168.1.4 | 10.10.10.4
| 192.168.1.7 | 10.10.10.7
Machine 2 | 192.168.1.3 | 10.10.20.3
| 192.168.1.4 | 10.10.20.4
| 192.168.1.7 | 10.10.20.7
Machine 3 | 192.168.1.3 | 10.10.30.3
| 192.168.1.4 | 10.10.30.4
| 192.168.1.7 | 10.10.30.7
Factory Network
Network Management for OT
## Current Challenges

<table>
<thead>
<tr>
<th><strong>IT</strong></th>
<th><strong>Operations</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IT Staff Supporting OT</strong></td>
<td><strong>Line Operator/Technician</strong></td>
</tr>
<tr>
<td>IT or a person with hybrid IT and OT talents</td>
<td>Day to day operations of control system</td>
</tr>
<tr>
<td><strong>Network experts</strong></td>
<td><strong>Control Systems/Design Engineer</strong></td>
</tr>
<tr>
<td></td>
<td>Designs and maintains the automation and control system</td>
</tr>
<tr>
<td><strong>Lack tools that provide network visibility in an operations context</strong></td>
<td><strong>Plant/Facility Manager</strong></td>
</tr>
<tr>
<td></td>
<td>Plant/Facility uptime is top of mind</td>
</tr>
</tbody>
</table>
Current Challenges

**IT**

**IT Staff Supporting OT**

IT or a person with hybrid IT and OT talents

**Network experts**

**Operations ↔ IND Target Users**

**Line Operator/Technician**

Day to day operations of control system

**Control Systems/Design Engineer**

Designs and maintains the automation and control system

**Plant/Facility Manager**

Plant/Facility uptime is top of mind

Lack tools that provide network visibility in an operations context
Cisco Industrial Network Director
Network Management, Simplified & Automated

Dashboard for monitoring system health, metrics, and traffic statistics

Alarm management with real-time alerts of network events

Native industrial protocol support

Plug-and-Play Day-0 configuration

Plug-and-Play for Zero-Touch Switch Commissioning

Improved Industrial Asset Visibility

Network Troubleshooting with Automation Context

APIs for Integration with Automation Systems

Native industrial protocol support

Plug-and-Play Day-0 configuration

Plug-and-Play for Zero-Touch Switch Commissioning

Improved Industrial Asset Visibility

Network Troubleshooting with Automation Context

APIs for Integration with Automation Systems
Cisco Plug and Play

Zero-Touch Commissioning and Replacement

- Pre-provision configuration and software for automated network commissioning
- Help ensure consistent network design and security policy
- Swap hardware when switch fails and recover with automated configuration and software image replacement

Open protocol based on XMPP and HTTP with publically available schema
Simplify and Automate with Plug and Play

- Lightweight – Can run on a laptop
- Workflow tailored for industrial use cases such as machine builders
- Profiles can be exported across instances for multi-party provisioning scenarios
- Technicians commissioning switches do not need to understand networking
Factory Wireless
Wireless Overview
Benefits of industrial wireless network

• Connection to **hard-to-reach** and **restricted areas**
• Integration of machines / skids
  • Remote diagnostics
  • Intelligent assets
• **Lower installation and operational costs**
  • Cabling reduction, elimination of cable failures
• **Equipment mobility**
  • New and more efficient machine designs
Wireless Overview

Benefits of industrial wireless network

- **Workforce mobility** improves effectiveness
  - **Operators** can trend/write back from a mobile device when they step away from machine

- **Engineering and Maintenance** can see and react to system alarming and production data from anywhere, anytime

- **Industrial IT** provide secure infrastructure and multi-platform support

- **Equipment wireless**
  - IEEE 802.11 Wireless connectivity for critical Industrial Automation and Control System (IACS) applications

- **Asset Tracking**
  - Track assets to optimize cost and for safety
Wireless Overview
Challenges of wireless communication

- **Half-duplex shared medium:**
  - Only one radio can transmit on a particular wireless channel
  - A radio cannot transmit and receive at the same time on the same channel

- **Higher latency, jitter and packet loss** compared to wired Ethernet
  - Media contention, collisions and interference
  - Can be minimized but not eliminated
Wireless Overview

Challenges of wireless communication

• Wireless coverage area cannot be precisely defined
  • Site survey is required
  • Spectrum sharing and security concerns

• Signal quality may change over time
  • Interference sources and obstructions
  • Unauthorized transmissions

Wireless advantages > challenges when
• WLAN is designed and maintained properly
• Used for appropriate applications
Factory Wireless Equipment to Equipment
Equipment to Equipment – Use Cases

Wireless Mobility Types

- **Static equipment**
  - Permanent location
  - Wire replacement for hard-to-reach places
  - Examples: process control, condition monitoring, standalone OEM machines
Equipment to Equipment – Use Cases

Wireless Mobility Types

- **Nomadic equipment**
  - Stays in place while operating
  - Moves to a new location in the shutdown state
  - Examples: process skids, storage tanks, reactors, portable manufacturing equipment
Equipment to Equipment – Use Cases

Wireless Mobility Types

- **Mobile equipment (no roaming)**
  - Changes position while operating
  - Remains connected to the same AP
  - Examples: rotary platforms, manufacturing machines with tracks, overhead cranes with small spans
Equipment to Equipment – Use Cases

Wireless Mobility Types

• **Mobile equipment (fast roaming)**
  • Connects to multiple APs while operating
  • Does not drop application connections
  • Examples: AGVs, ASRS, overhead cranes, train cars, entertainment ride vehicles

*Site survey and architecture selection are critical*
Unified WLAN Architecture

Overview

- Identity Services Engine (ISE)
- Connected Mobile Experiences (CMX)
- Cisco Prime® Infrastructure

SSID1 5 GHz
SSID2 5 GHz
SSID3 2.4 GHz

WGB
LWAP
WLC
ETH/Net
IP
LWAP
LWAP
WGB
(5 GHz)
(2.4 GHz)
(Roaming)
Wireless Access
Asset Tracking
Real Time Location Services (RTLS) Architecture

- Single Pane of Glass for Cockpit Dashboard
- Open Ecosystem
- Scalable Infrastructure
- Leverage Common Wireless Infrastructure
- Track Any Wi-Fi Device or Tag
- Chokepoint Integration
Factory Security
IDMZ
Controlling Access to the Industrial Zone

Continued Trend - Industrial Network Security

Logical Model – Industrial Automation and Control System (IACS)
Converged Multi-discipline Industrial Network
No Direct Traffic Flow between Enterprise and Industrial Zone
Industrial Demilitarized Zone (IDMZ)

Best practices

• All network traffic from either side of the IDMZ terminates in the IDMZ; network traffic does not directly traverse the IDMZ
  • Only path between zones
  • No common protocols in each logical firewall

• No control traffic into the IDMZ, CIP stays home

• No primary services are permanently housed in the IDMZ

• IDMZ shall not permanently house data

• Application data mirror to move data into and out of the Industrial Zone

• Limit outbound connections from the IDMZ

• Be prepared to “turn-off” access via the firewall
IDMZ – Replicated Data and Services

Wide Area Network (WAN)
Physical or Virtualized Servers
• ERP, Email
• Active Directory (AD), AAA – Radius
• Call Manager

Firewall (Inspect Traffic)
Physical or Virtualized Servers
• Patch Management
• AV Server
• Application Mirror
• Remote Desktop
Gateway Server

Enterprise Zone
Levels 4-5

Industrial Demilitarized Zone (IDMZ)

Industrial Zone
Levels 0-3

Physical or Virtualized Servers & Services
• Network Services – e.g., DNS, AD, DHCP, AAA
• Call Manager
• Storage Array

Remote Access Server

Enterprise Zone
Levels 4-5

Industrial Demilitarized Zone (IDMZ)

Levels 0-2
Cell/Area Zone

Physical or Virtualized Servers
• FactoryTalk Application Servers & Services
• Network Services – e.g., DNS, AD, DHCP, AAA
• Call Manager
• Storage Array

Remote Desktop

Enterprise Zone
Levels 4-5

Industrial Demilitarized Zone (IDMZ)

Levels 0-2
Cell/Area Zone

Physical or Virtualized Servers
• FactoryTalk Application Servers & Services
• Network Services – e.g., DNS, AD, DHCP, AAA
• Call Manager
• Storage Array

Remote Desktop

Enterprise Zone
Levels 4-5

Industrial Demilitarized Zone (IDMZ)

Levels 0-2
Cell/Area Zone

Physical or Virtualized Servers
• FactoryTalk Application Servers & Services
• Network Services – e.g., DNS, AD, DHCP, AAA
• Call Manager
• Storage Array

Remote Desktop

Enterprise Zone
Levels 4-5

Industrial Demilitarized Zone (IDMZ)

Levels 0-2
Cell/Area Zone

Physical or Virtualized Servers
• FactoryTalk Application Servers & Services
• Network Services – e.g., DNS, AD, DHCP, AAA
• Call Manager
• Storage Array

Remote Desktop

Enterprise Zone
Levels 4-5

Industrial Demilitarized Zone (IDMZ)

Levels 0-2
Cell/Area Zone

Physical or Virtualized Servers
• FactoryTalk Application Servers & Services
• Network Services – e.g., DNS, AD, DHCP, AAA
• Call Manager
• Storage Array

Remote Desktop

Enterprise Zone
Levels 4-5

Industrial Demilitarized Zone (IDMZ)

Levels 0-2
Cell/Area Zone

Physical or Virtualized Servers
• FactoryTalk Application Servers & Services
• Network Services – e.g., DNS, AD, DHCP, AAA
• Call Manager
• Storage Array

Remote Desktop

Enterprise Zone
Levels 4-5

Industrial Demilitarized Zone (IDMZ)

Levels 0-2
Cell/Area Zone

Physical or Virtualized Servers
• FactoryTalk Application Servers & Services
• Network Services – e.g., DNS, AD, DHCP, AAA
• Call Manager
• Storage Array

Remote Desktop

Enterprise Zone
Levels 4-5

Industrial Demilitarized Zone (IDMZ)

Levels 0-2
Cell/Area Zone

Physical or Virtualized Servers
• FactoryTalk Application Servers & Services
• Network Services – e.g., DNS, AD, DHCP, AAA
• Call Manager
• Storage Array

Remote Desktop

Enterprise Zone
Levels 4-5

Industrial Demilitarized Zone (IDMZ)

Levels 0-2
Cell/Area Zone

Physical or Virtualized Servers
• FactoryTalk Application Servers & Services
• Network Services – e.g., DNS, AD, DHCP, AAA
• Call Manager
• Storage Array

Remote Desktop

Enterprise Zone
Levels 4-5

Industrial Demilitarized Zone (IDMZ)

Levels 0-2
Cell/Area Zone

Physical or Virtualized Servers
• FactoryTalk Application Servers & Services
• Network Services – e.g., DNS, AD, DHCP, AAA
• Call Manager
• Storage Array

Remote Desktop

Enterprise Zone
Levels 4-5

Industrial Demilitarized Zone (IDMZ)

Levels 0-2
Cell/Area Zone

Physical or Virtualized Servers
• FactoryTalk Application Servers & Services
• Network Services – e.g., DNS, AD, DHCP, AAA
• Call Manager
• Storage Array

Remote Desktop

Enterprise Zone
Levels 4-5

Industrial Demilitarized Zone (IDMZ)

Levels 0-2
Cell/Area Zone

Physical or Virtualized Servers
• FactoryTalk Application Servers & Services
• Network Services – e.g., DNS, AD, DHCP, AAA
• Call Manager
• Storage Array

Remote Desktop

Enterprise Zone
Levels 4-5

Industrial Demilitarized Zone (IDMZ)

Levels 0-2
Cell/Area Zone

Physical or Virtualized Servers
• FactoryTalk Application Servers & Services
• Network Services – e.g., DNS, AD, DHCP, AAA
• Call Manager
• Storage Array

Remote Desktop

Enterprise Zone
Levels 4-5

Industrial Demilitarized Zone (IDMZ)

Levels 0-2
Cell/Area Zone

Physical or Virtualized Servers
• FactoryTalk Application Servers & Services
• Network Services – e.g., DNS, AD, DHCP, AAA
• Call Manager
• Storage Array

Remote Desktop

Enterprise Zone
Levels 4-5

Industrial Demilitarized Zone (IDMZ)

Levels 0-2
Cell/Area Zone
IDMZ – Replicated Data and Services

**Permit Secure Remote Access to Industrial Assets**

- **Wide Area Network (WAN)**
  - Physical or Virtualized Servers
  - ERP, Email
  - Active Directory (AD), AAA – Radius
  - Call Manager

- **Firewall (Inspect Traffic)**
  - Remote Access

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

- **Remote Access**
  - VantagePoint
  - Network Services – e.g. DNS, AD, DHCP, AAA
  - Call Manager
  - Storage Array

- **Remote Desktop Gateway Server**
  - **Web Proxy**
  - **Firewall (Active/Standby)**

- **Core Switches**
  - **ISE (Enterprise)**
  - **WLC (Enterprise)**

**Enterprise Zone Levels 4-5**

**Industrial Demilitarized Zone (IDMZ)**

**Industrial Zone Levels 0-3**

**Levels 0-2 Cell/Area Zone**

- **Physical or Virtualized Servers**
  - FactoryTalk Application Servers & Services
  - Network Services – e.g. DNS, AD, DHCP, AAA
  - Call Manager
  - Storage Array

**Levels 3 Site Operations**

- **Physical or Virtualized Servers**
  - Access Server
  - VantagePoint
  - **Level 3 Site Operations**

- **Core Switches**
  - **ISE**

- **Remote Access Server**
  - **VantagePoint**
  - **Remote Desktop Gateway Server**

- **Remote Desktop Gateway Server**
  - **Web Proxy**

- **Firewall (Inspect Traffic)**
  - **Firewalls (Active/Standby)**

**Physical or Virtualized Servers**

- **Patch Management**
- **AV Server**
- **Application Mirror**
- **Remote Desktop Gateway Server**

**Remote Access**

- **Web Proxy**
- **Firewall (Active/Standby)**

**Core Switches**

- **ISE (Enterprise)**
- **WLC (Enterprise)**

**Enterprise Zone Levels 4-5**

**Industrial Demilitarized Zone (IDMZ)**

**Industrial Zone Levels 0-3**

**Levels 0-2 Cell/Area Zone**

- **Physical or Virtualized Servers**
  - Access Server
  - VantagePoint
  - **Level 3 Site Operations**

- **Core Switches**
  - **ISE**

- **Remote Access Server**
  - **VantagePoint**
  - **Remote Desktop Gateway Server**

- **Remote Desktop Gateway Server**
  - **Web Proxy**

**Firewall (Inspect Traffic)**

- **Firewalls (Active/Standby)**

**Enterprise Zone Levels 4-5**

**Industrial Demilitarized Zone (IDMZ)**

**Industrial Zone Levels 0-3**
IDMZ – Replicated Data and Services

Permit Secure Remote Access to Industrial Assets

Permit Data from the Industrial Zone to Enterprise Stakeholders

Wide Area Network (WAN) Physical or Virtualized Servers
- ERP, Email
- Active Directory (AD)
- Call Manager

Firewall (Inspect Traffic)

Enterprise Zone Levels 4-5

Industrial Demilitarized Zone (IDMZ)

Industrial Zone Levels 0-3

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

Firewall (Inspect Traffic)

Enterprise Zone

WLC (Enterprise)
ISE (Enterprise)

Web Proxy

Remote Access

Engineer

Plant Manager

Firewall (Active/Standby)

Physical or Virtualized Servers
- FactoryTalk Application Servers & Services
- Network Services – e.g. DNS, AD, DHCP, AAA
- Call Manager
- Storage Array

VantagePoint

Level 3 Site Operations

Remote Access

FactoryTalk Client

Drive

MCC

PAC

PAC

LWAP

WGB
IDMZ – Replicated Data and Services

Permit Secure Remote Access to Industrial Assets
Permit Data from the Industrial Zone to Enterprise Stakeholders

Wide Area Network (WAN)
Physical or Virtualized Servers
- ERP, Email
- Active Directory (AD), AAA – Radius
- Call Manager
Firewall (Inspect Traffic)

Web Proxy
Engineer
Remote Access
Plant Manager
Untrusted

Core switches
WLC (Enterprise)
ISE (Enterprise)
Enterprise Zone Levels 4-5

Firewalls (Active/Standby)

Industrial Demilitarized Zone (IDMZ)

Industrial Zone Levels 0-3

Physical or Virtualized Servers
- Patch Management
- AV Server
- Application Mirror
- Remote Desktop
- Gateway Server
Firewall (Inspect Traffic)

Remote Access Server
VantagePoint
Level 3 Site Operations

Distribution switch

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

Remote Desktop Gateway Server

Remote Desktop Gateway

Web Proxy

FactoryTalk Application Servers & Services
- Network Services – e.g. DNS, AD, DHCP, AAA
- Call Manager
- Storage Array

Levels 0-2 Cell/Area Zone

Firewall (Inspect Traffic)

Permit

Permit Secure Remote Access

Untrusted Access to Industrial Zone

Permit Data from the Industrial Zone to Enterprise Stakeholders

Physical or Virtualized Servers
- ERP, Email
- Active Directory (AD), AAA – Radius
- Call Manager

Network Services – e.g. DNS, AD, DHCP, AAA

Untrusted Access to Industrial Zone

Indicate Engineer, Plant Manager, and Untrusted

Firewall (Inspect Traffic)

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

Remote Desktop Gateway Server

Remote Desktop Gateway

Web Proxy

FactoryTalk Application Servers & Services
- Network Services – e.g. DNS, AD, DHCP, AAA
- Call Manager
- Storage Array

Levels 0-2 Cell/Area Zone

Firewall (Inspect Traffic)

Permit

Permit Secure Remote Access

Untrusted Access to Industrial Zone

Permit Data from the Industrial Zone to Enterprise Stakeholders

Physical or Virtualized Servers
- ERP, Email
- Active Directory (AD), AAA – Radius
- Call Manager

Network Services – e.g. DNS, AD, DHCP, AAA

Untrusted Access to Industrial Zone

Indicate Engineer, Plant Manager, and Untrusted
Factory Security
OT Intent-based Security for Industrial Networks
Cisco Identity Services Engine (ISE)
Delivering Visibility, Context, and Control to Secure Network Access

NETWORK / USER CONTEXT
- Who
- What
- When
- Where
- How

DEVICE PROFILING FEED SERVICE

REDUCE NETWORK UNKNOWNS AND APPLY THE RIGHT LEVEL OF SECURE ACCESS CONSISTENTLY ACROSS WIRED, WIRELESS and VPN

Guest Access
Contractor Vendor (e.g. RBAC)
Employee Access

BRKIOT-2108 © 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Secure Access
Consolidating access for employee/contractors/vendors

Who?
- Employee
- Attacker
- Guest

What?
- Personal Device
- Company Asset

How?
- Wired
- Wireless
- VPN

Where?
- @ plant 1, zone 2
- Headquarters

When?
- Weekends
- (8:00am – 5:00pm) PST
Defining security policies without visibility is complex

Enterprise Assets

Industrial Assets
Operational challenges due to IT-OT dependency

- Centralized IT team
- OT engineers to make adds, moves, and changes to the control system for day-to-day operations
- Dependency on a centralized IT team to modify security policies
## Operational challenges due to IT-OT dependency

### VISIBILITY

Enforcing security in the process network requires Security systems to have visibility to plant floor Assets with the Context of observed behaviors.

### INTENT

Maintaining it effectively, requires dynamic security policy application triggered by OT intent without dependency on IT for day to day operations.
IoT Threat Defense
Visibility in Industrial Networks

Security starts with Visibility

Discover Industrial Assets using CIP, PROFINET, Modbus, BACNet Protocols

Visualize connectivity between automation and networking assets

Industrial Network Director

Context Enhances Security

Who
Bob

What
Rockwell PLC

When
11:00 AM EST on April 10th

Where
Extrusion, Zone-2, Cell-1

How
Wired Access

Compliance
Yes

Threat
None

Vulnerability
CVSS score of 6

IND shares industrial asset identity with ISE over pxGrid

... this Visibility combined with Context, becomes a force-multiplier for Security
Industrial Asset Visibility with IND

ISE profiling rules based on attributes like *Make, Model, Serial Number, Device Type* etc. instead of just IP address

*Custom Attributes* allows IND to signal higher order information that is common to a group of assets
OT user intent driven policy updates
Putting OT in the driver’s seat

OT personnel use with IND UI to express intent

pxGrid update results in automatic policy update

 PxGrid attribute "Cell-1" matches profiling policy-X and triggers Authorization policy-Y

IT manages ISE. OT uses IND to express intent to influence the IT owned Security Policy
Use Case#1 - Cell Segmentation

Segmentation Requirement

• Segment the industrial network
• OT user have the ability classify the assets into segments
Use Case#1 - Cell Segmentation

Segmentation Requirement

• Segment the industrial network
• OT user have the ability classify the assets into segments

Security Policy Pre-Staging

• IT and OT decide on the segmentation policy
• IT configures ISE with Secure Group Tags (SGT), TrustSec policy to match rules
Use Case#1 - Cell Segmentation

Segmentation Requirement

• Segment the industrial network

• OT user have the ability classify the assets into segments

Security Policy Pre-Staging

• IT and OT decide on the segmentation policy

• IT configures ISE with Secure Group Tags (SGT), TrustSec policy to match rules

Workflow during Asset Classification

1. OT user selects assets and groups them in IND as Cell-1 and Cell-2

2. OT user assigns a tag to C2-PLC

3. IND sends OT user intent and asset details to ISE in pxGrid
Use Case#1 - Cell Segmentation

Segmentation Requirement

• Segment the industrial network

• OT user have the ability classify the assets into segments

Security Policy Pre-Staging

• IT and OT decide on the segmentation policy

• IT configures ISE with Secure Group Tags (SGT), TrustSec policy to match rules

Workflow during Asset Classification

1. OT user selects assets and *groups* them in IND as Cell-1 and Cell-2

2. OT user assigns a *tag* to C2-PLC

3. IND sends OT user intent and asset details to ISE in pxGrid
Use Case#1 - Cell Segmentation

Segmentation Requirement

• Segment the industrial network
• OT user have the ability classify the assets into segments

Security Policy Pre-Staging

• IT and OT decide on the segmentation policy
• IT configures ISE with Secure Group Tags (SGT), TrustSec policy to match rules

Workflow during Asset Classification

1. OT user selects assets and groups them in IND as Cell-1 and Cell-2
2. OT user assigns a tag to C2-PLC
3. IND sends OT user intent and asset details to ISE in pxGrid
Use Case#1 - Cell Segmentation

Segmentation Requirement

• Segment the industrial network
• OT user have the ability classify the assets into segments

Security Policy Pre-Staging

• IT and OT decide on the segmentation policy
• IT configures ISE with Secure Group Tags (SGT), TrustSec policy to match rules

Workflow during Asset Classification

1. OT user selects assets and groups them in IND as Cell-1 and Cell-2
2. OT user assigns a tag to C2-PLC
3. IND sends OT user intent and asset details to ISE in pxGrid
4. Profiling policy match in ISE results TrustSec policy distribution

<table>
<thead>
<tr>
<th>SGT 33</th>
<th>SGT 100</th>
<th>SGT 200</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✘</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Remote Access Requirement
• Only specific asset in the machine must be accessible
• No dependency on IT

AnyConnect to check security posture, establish VPN, and collect application telemetry info – Track user session in ISE along with SGT role.
Use Case#1 On-Demand Remote Access

Remote Access Requirement
• Only specific asset in the machine must be accessible
• No dependency on IT

Security Policy Pre-Staging
1. IT user pre-defines profiling rules in ISE to match custom attributes
2. IT user pre-defines SGT firewall rules in ASA to allow remote Access

AnyConnect to check security posture, establish VPN, and collect application telemetry info – Track user session in ISE along with SGT role.
Use Case #1 On-Demand Remote Access

Remote Access Requirement
- Only specific asset in the machine must be accessible
- No dependency on IT

Security Policy Pre-Staging
1. IT user pre-defines profiling rules in ISE to match custom attributes
2. IT user pre-defines SGT firewall rules in ASA to allow remote access

Workflow during Maintenance Window
1. During machine maintenance, OT user changes asset attribute tag in IND which denotes intent to allow remote access

AnyConnect to check security posture, establish VPN, and collect application telemetry info – Track user session in ISE along with SGT role.
Use Case#1 On-Demand Remote Access

Remote Access Requirement
• Only specific asset in the machine must be accessible
• No dependency on IT

Security Policy Pre-Staging
1. IT user pre-defines profiling rules in ISE to match custom attributes
2. IT user pre-defines SGT firewall rules in ASA to allow remote Access

Workflow during Maintenance Window
1. During machine maintenance, OT user changes asset attribute tag in IND which denotes intent to allow remote access
2. IND sends OT user intent and asset details to ISE in pxGrid, which results in asset reauthorization

AnyConnect to check security posture, establish VPN, and collect application telemetry info – Track user session in ISE along with SGT role.
Remote Access Requirement
- Only specific asset in the machine must be accessible
- No dependency on IT

Security Policy Pre-Staging
1. IT user pre-defines profiling rules in ISE to match custom attributes
2. IT user pre-defines SGT firewall rules in ASA to allow remote Access

Workflow during Maintenance Window
1. During machine maintenance, OT user changes asset attribute tag in IND which denotes intent to allow remote access
2. IND sends OT user intent and asset details to ISE in pxGrid, which results in asset reauthorization
3. ISE distributes new TrustSec policy to Firewall and access switches to enable remote access

AnyConnect to check security posture, establish VPN, and collect application telemetry info – Track user session in ISE along with SGT role.
Use Case#1 On-Demand Remote Access

Remote Access Requirement
- Only specific asset in the machine must be accessible
- No dependency on IT

Security Policy Pre-Staging
1. IT user pre-defines profiling rules in ISE to match custom attributes
2. IT user pre-defines SGT firewall rules in ASA to allow remote access

Workflow during Maintenance Window
1. During machine maintenance, OT user changes asset attribute tag in IND which denotes intent to allow remote access
2. IND sends OT user intent and asset details to ISE in pxGrid, which results in asset reauthorization
3. ISE distributes new TrustSec policy to Firewall and access switches to enable remote access

AnyConnect to check security posture, establish VPN, and collect application telemetry info – Track user session in ISE along with SGT role.
Use Case#3 Flow Based Anomaly Detection

Requirement
• Group assets in communication trust zones and detect anomalous traffic behavior
• Easily detect the source of anomaly
Use Case#3 Flow Based Anomaly Detection

Requirement
- Group assets in communication trust zones and detect anomalous traffic behavior
- Easily detect the source of anomaly

Security Policy Pre-Staging
- Assets grouped in IND by OT user, automatically creates Host Groups in StealthWatch
- IT defines Alarms in StealthWatch for Host Group zone map violations
- IT configures policies in ISE to quarantine devices on violations
Use Case#3 Flow Based Anomaly Detection

**Requirement**
- Group assets in communication trust zones and detect anomalous traffic behavior
- Easily detect the source of anomaly

**Security Policy Pre-Staging**
- Assets grouped in IND by OT user, automatically creates Host Groups in StealthWatch
- IT defines Alarms in StealthWatch for Host Group zone map violations
- IT configures policies in ISE to quarantine devices on violations

**Workflow**
1. Compromised Camera in Cell-2 initiates Port Scan
Use Case#3 Flow Based Anomaly Detection

**Requirement**
- Group assets in communication trust zones and detect anomalous traffic behavior
- Easily detect the source of anomaly

**Security Policy Pre-Staging**
- Assets grouped in IND by OT user, automatically creates Host Groups in StealthWatch
- IT defines Alarms in StealthWatch for Host Group zone map violations
- IT configures policies in ISE to quarantine devices on violations

**Workflow**
1. Compromised Camera in Cell-2 initiates Port Scan
2. StealthWatch raises Recon Alarm, and zone map violation alarm
Use Case#3 Flow Based Anomaly Detection

Requirement
• Group assets in communication trust zones and detect anomalous traffic behavior
• Easily detect the source of anomaly

Security Policy Pre-Staging
• Assets grouped in IND by OT user, automatically creates Host Groups in StealthWatch
• IT defines Alarms in StealthWatch for Host Group zone map violations
• IT configures policies in ISE to quarantine devices on violations

Workflow
1. Compromised Camera in Cell–2 initiates Port Scan
2. StealthWatch raises Recon Alarm, and zone map violation alarm
3. StealthWatch sends quarantine request to ISE
Use Case#3 Flow Based Anomaly Detection

**Requirement**
- Group assets in communication trust zones and detect anomalous traffic behavior
- Easily detect the source of anomaly

**Security Policy Pre-Staging**
- Assets grouped in IND by OT user, automatically creates Host Groups in StealthWatch
- IT defines Alarms in StealthWatch for Host Group zone map violations
- IT configures policies in ISE to quarantine devices on violations

**Workflow**
1. Compromised Camera in Cell-2 initiates Port Scan
2. StealthWatch raises Recon Alarm, and zone map violation alarm
3. StealthWatch sends quarantine request to ISE
4. ISE moves camera access port to isolated VLAN to quarantine
Industrial Network Security Framework
CPwE - Holistic Defense-in-Depth

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

Level 3 – Site Operations
Level 2 – Area Supervisory Control
Level 1 - Controller
Level 0 - Process

Cisco © 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Industrial Network Security Framework
CPwE - Holistic Defense-in-Depth

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

Control System Engineers

Level 3 – Site Operations
Level 2 – Area Supervisory Control
Level 1 - Controller
Industrial Network Security Framework
CPwE - Holistic Defense-in-Depth

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

Level 0 - Process
- Control System Engineers
- FactoryTalk Security
- Level 3 – Site Operations
- Level 2 – Area Supervisory Control
- FactoryTalk Client
- Controller

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

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

Level 3 - Site Operations
- Distribution Switch Stack
- LWAP
- 2.4 GHz
- 5 GHz
- SSID
- Active
- Standby

Level 0 - Process
- Distribution Switch Stack
- LWAP
- 2.4 GHz
- 5 GHz
- SSID
- Active
- Standby

Enterprise
- Identity Services
- External DMZ/Firewall

Internet

Control System Engineers

FactoryTalk Security

Level 3 – Site Operations

Level 2 – Area Supervisory Control

Level 1 - Controller

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

Ciscolive!
Industrial Network Security Framework
CPwE - Holistic Defense-in-Depth

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

- FactoryTalk Security
- Application Hardening
- FactoryTalk Client

Level 3 – Site Operations

Level 2 – Area Supervisory Control

Level 1 - Controller

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

Control System Engineers

Enterprise Identity Services

External DMZ/Firewall

Internet

Core Switches

Distribution Switch Stack

FactoryTalk Security

FactoryTalk Client

Controller

Controller

Soft Starter

MCC

Drive

WGB

SSID 2.4 GHz

SSID 5 GHz

LWAP

Active

Standby

Wireless LAN Controller (WLC)

Active

Standby

Core Switches

Distribution Switch Stack

FactoryTalk Security

FactoryTalk Client

Controller

Controller

Soft Starter

MCC

Drive

WGB

SSID 2.4 GHz

SSID 5 GHz

LWAP

Active

Standby

Wireless LAN Controller (WLC)

Active

Standby

Control System Engineers
Industrial Network Security Framework
CPwE - Holistic Defense-in-Depth

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

Level 0 - Process

Level 1 - Controller

Level 2 - Area Supervisory Control

Level 3 – Site Operations

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

Application Hardening

FactoryTalk Security

Core Switches

FactoryTalk Client

Distribution Switch Stack

Controller

Controller

Port Security
- Physical
- Electronic

Soft Starter

MCC

Drive

SSID 2.4 GHz

SSID 5 GHz

Wireless LAN Controller (WLC)

Active

Standby

Control System Engineers

Industrial Demilitarized Zone (IDMZ)

Enterprise Identity Services

External DMZ/ Firewall

Enterprise

Internet
Industrial Network Security Framework
CPwE - Holistic Defense-in-Depth

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

Level 3 – Site Operations
- FactoryTalk Security

Level 2 – Area Supervisory Control
- Application Hardening
- FactoryTalk Client
- Wireless LAN, Segmenting Domains of Trust

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

Control System Engineers

Cisco Live!
Industrial Network Security Framework
CPwE - Holistic Defense-in-Depth

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

Level 3 – Site Operations
- Application Hardening
  - FactoryTalk Security

Level 2 – Area Supervisory Control
- FactoryTalk Client
- IACS Device Hardening
  - Policies and Procedures
  - Physical Measures
  - Electronic Measures
  - Encrypted Communications

Level 1 - Controller
- Soft Starter
- MCC
- Drive

Industrial Firewall
- Port Security
  - Physical
  - Electronic

Wireless LAN Controller (WLC)
- Active
- Standby

Core Switches
- SSID 2.4 GHz
- SSID 5 GHz

Distribution Switch Stack
- LWAP
- Standby

Enterprise Identity Services

Control System Engineers

BRKIOT-2108 © 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Industrial Network Security Framework
CPwE - Holistic Defense-in-Depth

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

Level 0 - Process
Controller

Level 1 - Controller

Level 2 - Area Supervisory Control
FactoryTalk Security
Application Hardening
IACS Device Hardening
- Policies and Procedures
- Physical Measures
- Electronic Measures
- Encrypted Communications

Level 3 – Site Operations
FactoryTalk Security
Distribution Switch Stack

Control System Engineers in Collaboration with IT Network Engineers (Industrial IT)
Industrial Network Security Framework
CPwE - Holistic Defense-in-Depth

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
- FactoryTalk Security
- OS Hardening
- Application Hardening

Level 3 – Site Operations
- IACS Device Hardening
  - Policies and Procedures
  - Physical Measures
  - Electronic Measures
  - Encrypted Communications
  - VLANs, Segments, Domains of Trust

Level 2 – Area Supervisory Control
- Controller
- Controller

Level 1 - Controller
- Soft Starter
- MCC

Control System Engineers in Collaboration with IT
Network Engineers (Industrial IT)
Industrial Network Security Framework
CPwE - Holistic Defense-in-Depth

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

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

Control System Engineers

OS Hardening
Application Hardening
FactoryTalk Security

Level 2 – Area Supervisory Control

Level 3 – Site Operations

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

Network Infrastructure
- Hardening
- Access Control
- Resiliency

Controller
Industrial Firewall

Soft Starter
MCC
WGB

Level 1 - Controller

Level 0 - Process

LWAP
SSID 2.4 GHz
SSID 5 GHz
WGB

LWAP
SSID 2.4 GHz
SSID 5 GHz
WGB

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

Active
Standby
Core Switches
Distribution Switch Stack

Drive

Enterprise Identity Services
External DMZ/Firewall
Internet

BRKIOT-2108 © 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Industrial Network Security Framework
CPwE - Holistic Defense-in-Depth

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

Level 0 - Process
- Physical Measures
- Electronic Measures
- Encrypted Communications

Level 1 - Controller

Level 2 - Area Supervisory Control
- OS Hardening
- Application Hardening

Level 3 - Site Operations
- 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)
Industrial Network Security Framework
CPwE - Holistic Defense-in-Depth

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

Enterprise Zone: Levels 0-3

Industrial Zone: Levels 0-3
- FactoryTalk Security
- Remote Access Server (RAS)
- OS Hardening
- Application Hardening

Control System Engineers in Collaboration with IT
Network Engineers (Industrial IT)
Industrial Network Security Framework
CPwE - Holistic Defense-in-Depth

Enterprise Zone: Levels 4-5

Industrial Demilitarized Zone (IDMZ)
- Physical or Virtualized Servers
  - Patch Management
  - AV Server
  - Application Mirror
  - Remote Desktop Gateway Server

Enterprise Zone: Levels 0-3

Industrial Zone: Levels 0-3

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

IT Security Architects in Collaboration with Control Systems Engineers

Control System Engineers

Industrial Demilitarized Zone (IDMZ)
- FactoryTalk Security
- Remote Access Server (RAS)

Level 3 – Site Operations
- OS Hardening
- Application Hardening
- FactoryTalk Client

Level 2 – Area Supervisory Control
- VLANs, Segregating Domains of Trust
- IACS Device Hardening
  - Policies and Procedures
  - Physical Measures
  - Electronic Measures
  - Encrypted Communications

Level 1 - Controller
- Controller
- Controller
- Industrial Firewall
- LWAP
- SSID 2.4 GHz
- SSID 5 GHz
- Wireless LAN (WLAN)
  - Active
  - Standby
  - Core Switches
  - Distribution Switch Stack

Level 0 - Process
- Soft Starter
- MCC
- Drive

Network Infrastructure
- Hardening
- Access Control
- Resiliency

Port Security
- Physical
- Electronic

Network Status and Monitoring
- Wireless LAN Controller (WLC)
- Active
- Standby

Wireless LAN (WLAN)
- Access Policy
  - Pre-Shared Key
  - 802.1X - (EAP-FAST)
- Trusted Partners SSID
- WPA2 with AES Encryption
- Autonomous WLAN
- Unified WLAN
- 802.1X - (EAP-TLS)
- CAPWAP DTLS

Industrial Zone: Levels 0-3

Control System Engineers

Industrial Zone: Levels 0-3

External DMZ/ Firewall
- Enterprise
- Internet

Identity Services

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Industrial Network Security Framework
CPwE - Holistic Defense-in-Depth

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)

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

IT Security Architects in
Collaboration with Control Systems
Engineers

Cisco live!

BRKIOT-2108 © 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Industrial Network Security Framework
CPwE - Holistic Defense-in-Depth

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

Control System Engineers

Enterprise Identity Services
Identity Services Engine (ISE)
FactoryTalk Security
Remote Access Server (RAS)

Active Directory (AD)
OS Hardening
Application Hardening

Level 3 – Site Operations
Level 2 – Area Supervisory Control
Level 1 - Controller

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

FactoryTalk Client
WLANs, Segregating Domains of Trust

Industrial Firewall
Soft Starter
MCC

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

SSID 2.4 GHz
SSID 5 GHz
Active
Standby
Core Switches
Distribution Switch Stack

LWAP
I/O Active
WGB
IFW
BRKIOT-2108
© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public 114
Industrial Network Security Framework
CPwE - Holistic Defense-in-Depth

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

Level 0 - Process
- IACS Device Hardening
  - Policies and Procedures
  - Physical Measures
  - Electronic Measures
  - Encrypted Communications

Level 1 - Controller
- Network Infrastructure
  - Hardening
  - Access Control
  - Resiliency

Level 2 - Area Supervisory Control
- FactoryTalk Security
- Remote Access Server (RAS)
- OS Hardening
- Application Hardening
- WLANs, Segmentation and Domains of Trust

Level 3 - Site Operations
- FactoryTalk Security
- Core Switches
- Distribution Switch Stack

Network Status and Monitoring
- 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 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)

IT Security Architects in
Collaboration with Control Systems
Engineers
Industrial Network Security Framework
CPwE - Holistic Defense-in-Depth

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)
- FireSIGHT Management Center
- Cisco Security Manager
- Identity Services Engine (ISE)
- FactoryTalk Security
- Remote Access Server (RAS)

Level 3 - Site Operations
OS Hardening
Application Hardening

Level 2 - Area Supervisory Control
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

Level 1 - Controller
- Controller
- Controller
- Industrial Firewall
- Distribution Switch Stack
- Core Switches

Level 0 - Process
- Plant Firewalls
  - Active/Standby
- Inter-zone traffic segmentation
- ACLs, IPS and IDS
- VPN Services
- Portal and Remote Desktop Services proxy

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

IT Security Architects in
Collaboration with Control Systems
Engineers

Cisco live!
BRKIOT-2108 © 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public 116
Cisco Kinetic IoT Platform & Vertical use cases
Cisco Kinetic Platform

Cisco Kinetic
IoT Data Fabric

Extract Data
Compute Data
Move Data

Gateway Management Module
Edge & Fog Processing Module
Data Control Module
Cisco Kinetic Platform

- IoT Devices
- IoT Gateway

Protocol Translation SW

Extract Data

Business Intelligence Applications
Cisco Kinetic Platform

IoT Devices

Extract Data

Compute Data

Business Intelligence Applications

IoT Gateway

Protocol Translation SW

Edge Compute SW

Protocol Translation SW

Cisco Kinetic Platform

Sensors

Sensors

Sensors

IoT Devices

IoT Gateway

Protocol Translation SW

Edge Compute SW

Protocol Translation SW

Cisco Kinetic Platform

Sensors

Sensors

Sensors

IoT Devices

IoT Gateway

Protocol Translation SW

Edge Compute SW

Protocol Translation SW
Cisco Kinetic Platform

IoT Devices

Extract Data

Compute Data

Move Data

Business Intelligence Applications

Visualization SW
Cisco Solutions+ (DGLux5)

Protocol Translation SW
Edge Compute SW
IoT Gateway
Energy Monitoring Solution

Capabilities

- Real-time monitoring of energy consumption
- Consumption data by machine, line, area and building
- Automated policy to notify factory staff potential about peak power or issues before they occur

Solution Benefits

- Real-time visibility
- Policy automation to improve energy optimization: identify leaks, inefficient machines, peak loads
- Easy-to-use, accurate cost reporting for compliance
- Simplified deployment
Equipment Health Monitoring Solution

Capabilities

• Real-time monitoring of equipment state and condition
• Easy to read trending data
• Automated policy to notify factory staff potential issues before they occur

Solution Benefits

• Real-time visibility
• Enables steps toward predictive maintenance
• Improved issue response time
• Simplified deployment and meter deployment
Key Takeaways

• Connected Factories reference architectures - Simplified design, quicker deployment, reduced risk in deploying new technology to achieve business outcomes

• Factory Network: Secure, scalable and resilient network infrastructure

• Factory Wireless: Enables mobility, secure personnel access, equipment to equipment communication and asset tracking

• Factory Security: Defense-in-depth security for multiple layers of threat detection and prevention

• Cisco Kinetic: IoT Platform to Extract, Compute and Mode data
Connected Factory in Practice
Achieving Business Outcomes
Cyber-physical systems monitor physical processes, create a virtual copy (“Digital Twin”) of the physical world, and make decision decentralized decisions.

Cyber-physical systems communicate and cooperate with each other and with humans in real time.

Internal and cross-organizational services are offered and used by participants of the value chain.

Includes “soft” topics like work/life balance.
IoT, IIoT, Industrie 4.0 and the Connected Factory
Drivers for the Connected Factory

• Becoming an Insight-Driven Manufacturer
• Have the Ability to Accurately Track Machine Utilization (e.g. OEE)
• Facilitate the Use of Advanced Sensor Technologies and Enabling Predictive Maintenance
• Continuously Innovating Products, Services, and Relationships
• Create Connected Environments Inclusive of Partners (Internal and External ones)
• Becoming Agile While Maintaining Control of the Business
• We Want New Operational and Business Models
Connected Factory - Achieving Business Outcomes

Reduce Costs (Optimize Operations)
Increase Revenues (More Capabilities)
Meet Responsibilities (Environmental, Safety, Regulatory)

Production Automation
Inventory Management
Quality Control
Cost Management
Workforce Enablement
Product Enhancement

Applications
- Building Management
- SCADA
- Facilities Management
- Ind. Access & Control
- Safety
- Security
- Real Time Location Services
- Manu. Execution Systems
- Ent. Resource Planning
- Reports
- Internet
- Analytics
- Collab.

Unified Application Layer (Any Device - Any Application)

Networks
- Automation Network
- Management Network
- Collaboration Network (IT)

Devices
- Sensors
- Robots
- Supply Chain
- Tracking
- Energy
- Personal Devices
- Voice
- Video

Building Management
SCADA
Ind. Access & Control
Safety
Security
Real Time Location Services
Manu. Execution Systems
Ent. Resource Planning
Reports
Internet
Analytics
Collab.

Unified Network Management Layer (Deployment + Service Management)

BRKIOT-2108 © 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Connected Factory in Practice

Factory Security Case Study
Hope is NOT a Strategy

Manufacturing is the most targeted category…and small to medium manufacturers are the most targeted.

- 40 percent of manufacturing companies ended up affected by cyber incidents in the past 12 months,
- 38 percent of those that felt the effects indicated cyber breaches resulted in damages in excess of $1 million,
Industrie 4.0 Driving the Connected Factory

Enterprise-wide Systems

Supply chain

- OEM
- Corporate Headquarters
- Other Plant
- Customer

OEM

Corporate Headquarters

Other Plant

Customer

Plant-wide Systems

Production floor

- Receiving
- Processing
- Material Handling
- Control Room
- Utilities
- Batching/Blending
- Packaging
- Shipping

Lower Total Cost of Ownership | Faster Time to Market | Better Asset Optimization | Broader Risk Management
Industrie 4.0 Driving the Connected Factory

Connect

Enterprise-wide Systems

Supplier → OEM → Corporate Headquarters → Other Plant → Customer

Plant-wide Systems

Receiving → Processing → Material Handling → Control Room → Utilities

Batching/Blending → Packaging → Shipping

Lower Total Cost of Ownership | Faster Time to Market | Better Asset Optimization | Broader Risk Management
Industrie 4.0 Driving the Connected Factory

Connect

Lower Total Cost of Ownership | Faster Time to Market | Better Asset Optimization | Broader Risk Management
Industrie 4.0 Driving the Connected Factory

Connect

Enterprise-wide Systems

North

Supplier

Corporate Headquarters

Other Plant

Customer

West

Plant-wide Systems

Protect & Detect

South

Receiving

Processing

Batching/Blending

Material Handling

Packaging

Shipping

East

Lower Total Cost of Ownership | Faster Time to Market | Better Asset Optimization | Broader Risk Management
Industrie 4.0 Driving the Connected Factory

Lower Total Cost of Ownership | Faster Time to Market | Better Asset Optimization | Broader Risk Management
Industrie 4.0 Driving the Connected Factory

Connect

Protect & Detect

Collect

Enterprise-wide Systems

West

North

South

East

Plant-wide Systems

Supplier

OEM

Corporate Headquarters

Other Plant

Customer

Receiving

Processing

Batching/Blending

Packaging

Shipping

Control Room

Material Handling

Lower Total Cost of Ownership  |  Faster Time to Market  |  Better Asset Optimization  |  Broader Risk Management

Connect

Collect

Protect & Detect

Enterprise-wide Systems

West

North

South

East

Plant-wide Systems

Supplier

OEM

Corporate Headquarters

Other Plant

Customer

Receiving

Processing

Batching/Blending

Packaging

Shipping

Control Room

Material Handling

Lower Total Cost of Ownership  |  Faster Time to Market  |  Better Asset Optimization  |  Broader Risk Management
Security is NOT a Product but a Process

Where do I Begin?

NIST Cybersecurity Framework – MFG Profile

<table>
<thead>
<tr>
<th>Function</th>
<th>Unique Identifier</th>
<th>Function</th>
<th>Unique Identifier</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td></td>
<td>Identify</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ID.AM</td>
<td>Asset Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ID.BE</td>
<td>Business Environment</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ID.GV</td>
<td>Governance</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ID.RA</td>
<td>Risk Assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ID.RM</td>
<td>Risk Management Strategy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PR</td>
<td></td>
<td>Protect</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PR.AC</td>
<td>Access Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PR.AT</td>
<td>Awareness and Training</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PR.DS</td>
<td>Data Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PR.IP</td>
<td>Information Protection Processes and Procedures</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PR.MA</td>
<td>Maintenance</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PR.PT</td>
<td>Protective Technology</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DE</td>
<td></td>
<td>Detect</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DE.AE</td>
<td>Anomalies and Events</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DE.CM</td>
<td>Security Continuous Monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DE.DP</td>
<td>Detection Processes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RS</td>
<td></td>
<td>Respond</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RS.RP</td>
<td>Response Planning</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RS.CO</td>
<td>Communications</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RS.AN</td>
<td>Analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RS.MI</td>
<td>Mitigation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RS.IM</td>
<td>Improvements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RC</td>
<td></td>
<td>Recover</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RC.RP</td>
<td>Recovery Planning</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RC.IM</td>
<td>Improvements</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RC.CO</td>
<td>Communications</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Audit

Learn

Monitor

Assess

Implement

Design
Assess the Threats

Targeted of Not

- Employee carelessness
- Employee(&former employee) sabotage
- Internet
- Phishing email
- Infected CD
- Infected PDF file
- Infected memory stick
- A printer
Develop the Transformation

Current State
Security through Obscurity

Flat and Open
IACS Network Infrastructure
Develop the Transformation

Current State
Security through Obscurity
Develop the Transformation

Current State
Security through Obscurity

Future State

Flat and Open
IACS Network Infrastructure

Structured and Hardened
IACS Network Infrastructure
Develop the Transformation

Current State
Security through Obscurity

Future State

Structured and Hardened IACS Network Infrastructure

Flat and Open IACS Network Infrastructure

Cisco live!
Strategic Factory Security Approach

Phase 1
- Factory (OT) Architecture
- IDMZ (IT – OT Separation)
- Secure Remote Access to OT
- OT Network Segmentation

Phase 2
- OT Identity Base Network (ISE)
- OT Dedicated Security Appliances at Major Demarcation
- OT Network Security Monitoring

Phase 3
- Convergence of IT and OT Network Security

Phased Factory Security Maturity
# Factory Security

## Challenge

Need to connect machines from the factory floor for visibility, but have “Security by Obscurity” posture. Need protect IT from OT and OT from IT.

## Solution

Factory Cyber Security Assessment  
Industrial DMZ  
Defense in Depth Framework

## Business Outcomes

- Reduced downtime  
- Protect brand reputation  
- Minimize cyber theft  
- Increase Visibility to Factory Floor
Why Segmentation?

- manages attacks

Securing Environment

- **Segment infrastructure** – Protect inbound and outbound communications and each other

- **Scalable software defined segmentation** – Separate systems and users based on role and policy. Reducing security complexity

- **Identity based access** – Restrict connection to known systems and devices

- **Profiling IoT** – Evaluate and determine characteristics and posture to see if a device is Misbehaving
Map out IDMZ Traffic Flow

- Requirements for the network services and application data flow
- Applications and protocols may have to be allowed
- A certain network services may be allowed to communicate directly while ICS applications use IDMZ assets to exchange data.
IDMZ Implementation - Current State
Connected Factory - Holistic Defense-in-Depth

- Implement Purdue model with level segmentation via firewall with routing controls
  - Proper configuration and maintenance on Firewalls and ACL’s
- Build and commission a DMZ at level 3.5 for IT services, agents, patch management etc.
IDMZ Implementation- Access Migration
Connected Factory - Holistic Defense-in-Depth

Enterprise Zone: Levels 4-5
Industrial Demilitarized Zone (IDMZ)

Industrial Zone: Levels 0-3

Layer 3
Layer 2
IDMZ Implementation - Server Migration
Connected Factory - Holistic Defense-in-Depth

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)
- FireSIGHT Management Center
- Cisco Security Manager
- Identity Services Engine (ISE)

Level 3 – Site Operations
- Core Switches
- Distribution Switch Stack
- Controller
- Controller
- MCC
- Soft Starter

Level 0 - Process
- Plant Firewalls
  - Active/Standby
  - Inter-zone traffic segmentation
  - ACLs, IPS and IDS
  - VPN Services
  - Portal and Remote Desktop Services proxy

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Protect Critical Infrastructure: Through Network Segmentation – Zone Definition
How TrustSec Simplifies Network Segmentation

Traditional Segmentation

- Static ACL
- Routing
- Redundancy
- DHCP Scope
- Address
- VLAN

Security Policy based on Topology
High cost and complex maintenance

TrustSec

- Micro/Macro Segmentation
- Central Policy Provisioning
- No Topology Change
- No VLAN Change

Use existing topology and automate security policy to reduce OpEx

Employee Tag
Supplier Tag
Non-Compliant Tag
Switch automatically downloads all policies from ISE for only devices connected.

- **SGACL Policy**
  - Source: SF Operator, SF Development, SF Device, Suspicious, Vendor/Contractor
  - Destination: SF Operator, SF Development, SF Device, Suspicious, Vendor/Contractor

**Data Center**
- MES Server
- Historian
- DC FW

**Factory FW**
- Factory Backbone

**Shop Floor Device**
- SW 2 (SGACL)

**Vendor / Contractor**
- SF Operator, SF Development, SF Device, Suspicious, Vendor/Contractor

**Engineering Workstation**
- SF Operator, SF Development, SF Device, Suspicious, Vendor/Contractor

**Vendor / Contractor**
- SF Operator, SF Development, SF Device, Suspicious, Vendor/Contractor

TrustSec Policy (SGACL) configured and provisioned by ISE.
Switch automatically downloads all policies from ISE for only devices connected.

Switch 1

Switch 2

Traffic filtered even in same VLAN

Traffic filtered even in same VLAN

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Factory Data Access Control using TrustSec
Software-Defined Segmentation - TrustSec

ASA Firewall Policy

<table>
<thead>
<tr>
<th>IP</th>
<th>SGT</th>
<th>Source Criteria:</th>
<th>Destination Criteria:</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>HTTPS</td>
<td>✓</td>
</tr>
<tr>
<td>any</td>
<td>SF Operator</td>
<td>any</td>
<td>EHR Server</td>
<td>HTTPS</td>
<td>✓</td>
</tr>
<tr>
<td>any</td>
<td>SF Device</td>
<td>any</td>
<td>SF Device</td>
<td>HTTPS</td>
<td>✓</td>
</tr>
<tr>
<td>any</td>
<td></td>
<td>any</td>
<td>Historian</td>
<td>HTTPS</td>
<td>✓</td>
</tr>
<tr>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Data Center

MES Server

DC FW

Factory FW (SGFW)

MES Server

Historian

SW 2

Factory Backbone

Vendor / Contractor

Engineering Workstation

OS Type: Windows XP Embedded
User: Frank
AD Group: Shop Floor
Device Group: Eng Workstation
Security Group = Shop Flr Device

OS Type: Windows 8.1
User: contractor123@acme.com
AD Group: None
Device Group: BYOD Laptop
Security Group = Contractor

Access Privilege Authorization with Security Group
Factory Data Access Control using TrustSec
Software-Defined Segmentation - TrustSec

ASA Firewall Policy

<table>
<thead>
<tr>
<th>Source Criteria</th>
<th>Destination Criteria</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>Doctors</td>
<td>HTTPS</td>
<td></td>
</tr>
<tr>
<td>any</td>
<td>SF Operator</td>
<td>HTTPS</td>
<td></td>
</tr>
<tr>
<td>any</td>
<td>SF Development</td>
<td>HTTPS</td>
<td></td>
</tr>
<tr>
<td>any</td>
<td>Device</td>
<td>HTTPS</td>
<td></td>
</tr>
</tbody>
</table>

OS Type: Windows XP Embedded
User: Frank
AD Group: Shop Floor
Device Group: Eng Workstation
Security Group = Shop Flr Device

OS Type: Windows 8.1
User: contractor123@acme.com
AD Group: None
Device Group: BYOD Laptop
Security Group = Contractor

Access Privilege Authorization with Security Group
Factory Data Access Control using TrustSec
Software-Defined Segmentation - TrustSec

ASA Firewall Policy

<table>
<thead>
<tr>
<th>Source Criteria</th>
<th>Destination Criteria</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>any SF Operator</td>
<td>any SF Device</td>
<td>HTTPS</td>
<td>✓</td>
</tr>
<tr>
<td>any SF Operator</td>
<td>any SF Device</td>
<td>HTTPS</td>
<td>✓</td>
</tr>
<tr>
<td>any SF Operator</td>
<td>any SF Device</td>
<td>HTTPS</td>
<td>✓</td>
</tr>
<tr>
<td>any SF Operator</td>
<td>any SF Device</td>
<td>HTTPS</td>
<td>✓</td>
</tr>
</tbody>
</table>

OS Type: Windows XP Embedded
User: Frank
AD Group: Shop Floor
Device Group: Eng Workstation
Security Group = Shop Flr Device

OS Type: Windows 8.1
User: contractor123@acme.com
AD Group: None
Device Group: BYOD Laptop
Security Group = Contractor

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Factory Data Access Control using TrustSec
Software-Defined Segmentation- TrustSec

ASA Firewall Policy

<table>
<thead>
<tr>
<th>Source Criteria:</th>
<th>Destination Criteria:</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>SGT</td>
<td>IP</td>
<td>SGT</td>
</tr>
<tr>
<td>any</td>
<td>Doctors</td>
<td>any</td>
<td>any</td>
</tr>
<tr>
<td>any</td>
<td>SF Operator</td>
<td>any</td>
<td>any</td>
</tr>
<tr>
<td>any</td>
<td>SF Development</td>
<td>any</td>
<td>any</td>
</tr>
<tr>
<td>any</td>
<td>SF Device</td>
<td>any</td>
<td>any</td>
</tr>
<tr>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
</tr>
</tbody>
</table>

Data Center

MES Server

DC FW

Factory FW (SGFW)

Historian

SW 1

SW 2

Vendor / Contractor

Engineering Workstation

MES Server

SF Operator

SF Development

SF Device

BRKIOT - 2108

OS Type: Windows XP Embedded
User: Frank
AD Group: Shop Floor
Device Group: Eng Workstation
Security Group = Shop Flr Device

OS Type: Windows 8.1
User: contractor123@acme.com
AD Group: None
Device Group: BYOD Laptop
Security Group = Contractor

Access Privilege Authorization with Security Group

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Introduction into Data and Analytics: Insight Driven Operations
Manufacturing has always had Big Data. We have been collecting data with historians, and MES systems for decades.

Manufacturing is an untapped market for Big Data. There is lots of data, lots of different types of data, and hardly any of it is being used for analysis today.
# Data Opportunities and Challenges in Manufacturing

<table>
<thead>
<tr>
<th>Opportunities</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Improve quality and increase throughput</td>
<td>▪ Extreme composition of data require new approaches, infrastructure, and tools</td>
</tr>
<tr>
<td>▪ Better insights into root cause of manufacturing issues</td>
<td>▪ Data scientist nor business analysts required</td>
</tr>
<tr>
<td>▪ Reduce machine failure and downtime</td>
<td>▪ Little time to for refining data models, massaging analytical tools, and teasing out insight</td>
</tr>
<tr>
<td></td>
<td>▪ Need simple intuitive analytical tools and dashboards</td>
</tr>
<tr>
<td></td>
<td>▪ Lack of expertise derive algorithm to predictively models.</td>
</tr>
</tbody>
</table>
“Can analytics system answer questions we didn’t know to ask?”

- Data and Analytics can bring together:
  - Structured
  - Time series
  - Unstructured data
  - Artificial intelligence (AI)
- based analytics on top these are the solutions answering unasked questions to drive real and unexpected value
Data analytics applied to factory equipment and sensors can bring operational efficiencies and cost savings to manufacturing processes.
# Data and Decision Time within the Purdue Model

<table>
<thead>
<tr>
<th>Level</th>
<th>Function</th>
<th>Decision</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Planning</td>
<td>Month/Year</td>
<td>Enterprise</td>
</tr>
<tr>
<td>4</td>
<td>Business Systems</td>
<td>Days/Weeks</td>
<td>Enterprise</td>
</tr>
<tr>
<td>3</td>
<td>Manufacturing Operation Management</td>
<td>Seconds/Minutes/Hours</td>
<td>Plant/Enterprise</td>
</tr>
<tr>
<td>2</td>
<td>Equipment and Process Control</td>
<td>Sub-second</td>
<td>Plant</td>
</tr>
<tr>
<td>1</td>
<td>Sensors, Instrumentation, and Data Collection</td>
<td>Sub-second</td>
<td>Plant</td>
</tr>
<tr>
<td>0</td>
<td>Production Assets</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Manufacturing Data Examples

- Data is characterized by huge data sets with varied data types, which can be classified as structured, real-time structured, or unstructured.

<table>
<thead>
<tr>
<th>Real-Time Structured Data</th>
<th>Unstructured Data</th>
<th>Structured Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Sensors (vibration, pressure, value, and acoustics), Relays</td>
<td>- Operator shift reports</td>
<td>- RDBMS database</td>
</tr>
<tr>
<td>- RFID</td>
<td>- Machine logs</td>
<td>- NoSQL</td>
</tr>
<tr>
<td>- Direct from PLCs, Motor and Drives</td>
<td>- Error logs</td>
<td>- Enterprise data warehouse</td>
</tr>
<tr>
<td>- Direct from motion controllers, robot arm</td>
<td>- Texts</td>
<td>- Files stored in manufacturing PC</td>
</tr>
<tr>
<td>- Manufacturing historians (time series data structure)</td>
<td>- Vision Images</td>
<td>- Spreadsheets</td>
</tr>
<tr>
<td>- Audio/Video</td>
<td>- Manufacturing collaboration social platforms</td>
<td></td>
</tr>
</tbody>
</table>
Data Types and Sizes

- Manufacturing generate massive data files
- Limits the ability to store, analyze, and extract useful information from them using conventional methods.
- Extremely hard to even visualize the information in large data sets from various sources

<table>
<thead>
<tr>
<th>DATA TYPES</th>
<th>DATA SIZE (per week)</th>
<th>EXAMPLES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine Parameters and error logs</td>
<td>~5 GB per machine</td>
<td>Used to monitor machine performance: dispense height, placement(x,y,z), belt speed, flow rate, over temperature, laser power, etc</td>
</tr>
<tr>
<td>Machine events</td>
<td>~10 GB per machine</td>
<td>Used to measure process time: start dispense, end dispense, start setup, and end setup</td>
</tr>
<tr>
<td>Defect images from vision equipment</td>
<td>~50 GB per unit or 750 GB per lot</td>
<td>Used to identify root cause of failure modes, defect commonality, defect mapping</td>
</tr>
</tbody>
</table>
What problems are we solving for customers?

Environmental Sensing
- Plant Hazard Awareness
- Pollution
- Security

Business Outcomes
- Safety
- Compliance

Remote Visibility
- Condition Monitoring
- Preventive & Predictive Maintenance
- Asset Health

Business Outcomes
- Cost Avoidance
- Reliability

Efficiency through Process Automation
- Cost Reduction
- Efficiency
- Consistency

Business Outcomes
- Increased up time
- Faster and accurate decision
Factory Wireless
Autonomous Guided Vehicle (AGV) Roaming
Factory Wireless

Use Cases
- Wireless tooling
- Monitoring hard-to-reach and restricted areas
- PLCs and automated guided vehicles (AGVs)

Key Enabling IW3702 Features
- Seamless roaming at low to moderate speeds
- Supports prioritized PROFINET traffic for industrial applications
- PRP (Parallel Redundancy Protocol) over wireless for high resilience
## Factory Wireless WGB Roaming Evolution

<table>
<thead>
<tr>
<th>Basic WGB roaming</th>
<th>Fast WGB roaming</th>
<th>PRP enhanced roaming</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Low to moderate speed</strong></td>
<td><strong>High speed</strong></td>
<td><strong>Highest speed</strong></td>
</tr>
<tr>
<td>• Limited Scanning of channels</td>
<td>• 802.11v BSS Fast Transition on WGB</td>
<td>• PRP over wireless</td>
</tr>
<tr>
<td></td>
<td>• RSSI smoothing filter</td>
<td>• Dual radios enables always-best-connected</td>
</tr>
<tr>
<td></td>
<td>• Optimized rate-shifting algorithm</td>
<td>• Roaming coordination prevents two radios from roaming at the same time</td>
</tr>
</tbody>
</table>
Parallel Redundancy Protocol (PRP) over Wireless

Wireless Network Without PRP

Each data transmission goes through single radio path

RF interference, hand off results in packet loss

PRP Enabled Wireless Network

PRP over wireless creates redundant radio path for data transmission

Zero recovery time in event of temporary failure

PRP is defined in the International Standard IEC 62439-3 and designed to provide hitless redundancy (zero recovery time after failures) in networks
PRP over Wireless Redundancy Options

**Dual WGBs, Dual Radios - WLC 8.4**

- External PRP switch as RedBox (redundancy box) performs packet duplication/duplication discard function
- **Application examples:** Industrial automation and AGV applications

**Single WGB, Dual Radios - WLC 8.5**

- WGB as RedBox (redundancy box) performs packet duplication/duplication discard function
- **Application examples:** Autonomous vehicles and straddle carriers and mission critical applications etc.
Roaming Coordination

- WGB sends an indication to the other WGB indicating it wants to start roam
- Other WGB shall wait for 100ms (configurable) by default if it also needs to roam
- Once the roam event on the WGB is complete or if the timeout expires, the other WGB is free to roam
Sample Topology for Dual WGBs PRP Function

- **Infrastructure Side**
  - An aggregate switch in the infrastructure side carries the duplicated packets
  - APs in flex connect mode
  - The APs transmits/receives the redundant data traffic over different SSIDs, tag with different VLANs

- **Mobile Client Side**
  - Each WGB associates to different SSIDs and locates in different VLANs

- **Roaming Coordination**
  - WGBs are connected to provide roaming coordination function, preventing both WGBs from roaming at the same time
Conclusion: Measure Twice, Cut Once

• Availability / Resiliency / Performance
• Protocol Awareness (Prioritize and Protect)
• **Wireless**: Capacity and Access
• **Holistic Security**: Threat Centric Approach (Discover, Detect and Remediate)
• Asset Tracking and Network Management
• Energy Source (Battery? PoE?)
• **Virtual vs. Physical** (e.g. ownership and policies)
• Traffic Patterns Beyond Local System (WAN, Cloud, Uni/Bi-Directional)
• Data Aggregation and Storage (Local, Remote, Transit)
• Day-2 Support Model (Enable your Successor)
Recommended Resources

Reference Architectures

- Websites
  - Design Zone Industry Solutions

- Whitepapers
  - Top 10 Recommendations for Plant-wide EtherNet/IP Deployments
  - Securing Manufacturing Computer and Controller Assets
  - Achieving Secure Remote Access to plant-floor Applications and Data
  - Design Considerations for Securing Industrial Automation and Control System Networks
Q & A
Cisco Spark

Questions?
Use Cisco Spark to communicate with the speaker after the session

How
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space

cs.co/ciscoclivebot#BRKIOT-2108
• Please complete your Online Session Evaluations after each session

• Complete 4 Session Evaluations & the Overall Conference Evaluation (available from Thursday) to receive your Cisco Live T-shirt

• All surveys can be completed via the Cisco Live Mobile App or the Communication Stations

Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at www.ciscolive.com/global/on-demand-library/.
Continue Your Education

• Demos in the Cisco campus
• Walk-in Self-Paced Labs
• Tech Circle
• Meet the Engineer 1:1 meetings
• Related sessions
Thank you
# Internet of Things (IoT) Cisco Education Offerings

<table>
<thead>
<tr>
<th>Course</th>
<th>Description</th>
<th>Cisco Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NEW! Managing Industrial Networks for Manufacturing (IMINS2 v1.3)</strong></td>
<td>An associate level instructor led lab based training focuses on common industrial application protocols, security, wireless and troubleshooting designed to prepare you for the CCNA Industrial certification.</td>
<td>CCNA® Industrial</td>
</tr>
<tr>
<td>Managing Industrial Networks with Cisco Networking Technologies (IMINS)</td>
<td>This instructor led lab based training addresses foundational skills needed to manage and administer networked industrial control systems for today’s connected plants and enterprises. It helps prepare plant administrators, control system engineers and traditional network engineers for the Cisco Industrial Networking Specialist certification.</td>
<td>Cisco Industrial Networking Specialist</td>
</tr>
<tr>
<td>Control Systems Fundamentals for Industrial Networking (ICINS)</td>
<td>For IT and Network Engineers, provides an introduction to industry IoT verticals, automation environment and an overview of industrial control networks (E-Learning)</td>
<td>Pre-learning for IMINS, IMINS2 training &amp; certifications</td>
</tr>
<tr>
<td>Networking Fundamentals for Industrial Control Systems (INICS)</td>
<td>For Industrial Engineers and Control System Technicians, covers basic IP and networking concepts, and introductory overview of Automation industry Protocols.</td>
<td>Pre-learning for IMINS, IMINS2 training &amp; certifications</td>
</tr>
</tbody>
</table>

For more details, please visit: [http://learningnetwork.cisco.com](http://learningnetwork.cisco.com)

Questions? Visit the Learning@Cisco Booth
# Wireless Cisco Education Offerings

<table>
<thead>
<tr>
<th>Course</th>
<th>Description</th>
<th>Cisco Certification</th>
</tr>
</thead>
</table>
| • Designing Cisco Wireless Enterprise Networks  
• Deploying Cisco Wireless Enterprise Networks  
• Troubleshooting Cisco Wireless Enterprise Networks  
• Securing Cisco Wireless Enterprise Networks | Professional level instructor led trainings to prepare candidates to conduct site surveys, implement, configure and support APs and controllers in converged Enterprise networks. Focused on 802.11 and related technologies to design, deploy, troubleshoot as well as secure Wireless infrastructure. Course also provide details around Cisco mobility services Engine, Prime Infrastructure and wireless security. | CCNP® Wireless Version 3.0               |
| Implementing Cisco Unified Wireless Network Essential | Prepares candidates to design, install, configure, monitor and conduct basic troubleshooting tasks of a Cisco WLAN in Enterprise installations.                                                                                           | CCNA® Wireless                            |
| Deploying Basic Cisco Wireless LANs (WDBWL)  | Understanding of the Cisco Unified Wireless Networking for enterprise deployment scenarios. In this course, you will learn the basics of how to install, configure, operate, and maintain a wireless network, both as an add-on to an existing wireless LAN (WLAN) and as a new Cisco Unified Wireless Networking solution. | 1.2                                      |
| Deploying Advanced Cisco Wireless LANs (WDAWL) | The WDAWL advanced course is designed with the goal of providing learners with the knowledge and skills to successfully plan, install, configure, troubleshoot, monitor, and maintain advanced Cisco wireless LAN solutions such as QoS, “salt and pepper” mobility, high density deployments, and outdoor mesh deployments in an enterprise customer environment. | 1.2                                      |
| Deploying Cisco Connected Mobile Experiences (WCMX) | WCMX will prepare professionals to use the Cisco Unified Wireless Network to configure, administer, manage, troubleshoot, and optimize utilization of mobile content while gaining meaningful client analytics. | 2.0                                      |

For more details, please visit: [http://learningnetwork.cisco.com](http://learningnetwork.cisco.com)

Questions? Visit the Learning@Cisco Booth
# Cybersecurity Cisco Education Offerings

<table>
<thead>
<tr>
<th>Course</th>
<th>Description</th>
<th>Cisco Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding Cisco Cybersecurity Fundamentals (SFUND)</td>
<td>The SECFND course provides understanding of cybersecurity’s basic principles, foundational knowledge, and core skills needed to build a foundation for understanding more advanced cybersecurity material &amp; skills.</td>
<td>CCNA® Cyber Ops</td>
</tr>
<tr>
<td>Implementing Cisco Cybersecurity Operations (SECOPS)</td>
<td>This course prepares candidates to begin a career within a Security Operations Center (SOC), working with Cybersecurity Analysts at the associate level.</td>
<td>CCNA® Cyber Ops</td>
</tr>
<tr>
<td>Securing Cisco Networks with Threat Detection and Analysis (SCYBER)</td>
<td>Designed for security analysts who work in a Security Operations Center, the course covers essential areas of security operations competency, including SIEM, Event monitoring, security event/alarm/traffic analysis (detection), and incident response</td>
<td>Cisco Cybersecurity Specialist</td>
</tr>
<tr>
<td>Cisco Security Product Training Courses</td>
<td>Official deep-dive, hands-on product training on Cisco’s latest security products, including NGFW, ASA, NGIPS, AMP, Identity Services Engine, Email and Web Security Appliances, and more.</td>
<td></td>
</tr>
</tbody>
</table>

For more details, please visit: [www.cisco.com/go/securitytraining](http://www.cisco.com/go/securitytraining) or [http://learningnetwork.cisco.com](http://learningnetwork.cisco.com)

Questions? Visit the Learning@Cisco Booth
# Cybersecurity Cisco Education Offerings

<table>
<thead>
<tr>
<th>Course</th>
<th>Description</th>
<th>Cisco Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New! CCIE Security 5.0</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implementing Cisco Threat Control Solutions (SITCS) v1.5</td>
<td>Implement Cisco’s Next Generation Firewall (NGFW), FirePOWER NGIPS (Next Generation IPS), Cisco AMP (Advanced Malware Protection), as well as Web Security, Email Security and Cloud Web Security</td>
<td>CCNP® Security</td>
</tr>
<tr>
<td>Implementing Cisco Secure Access Solutions (SISAS)</td>
<td>Deploy Cisco’s Identity Services Engine and 802.1X secure network access</td>
<td></td>
</tr>
<tr>
<td>Implementing Cisco Secure Mobility Solutions (SIMOS)</td>
<td>Protect data traversing a public or shared infrastructure such as the Internet by implementing and maintaining Cisco VPN solutions</td>
<td></td>
</tr>
<tr>
<td>Implementing Cisco Network Security (IINS 3.0)</td>
<td>Focuses on the design, implementation, and monitoring of a comprehensive security policy, using Cisco IOS security features</td>
<td>CCNA® Security</td>
</tr>
</tbody>
</table>

For more details, please visit: [www.cisco.com/go/securitytraining](http://www.cisco.com/go/securitytraining) or [http://learningnetwork.cisco.com](http://learningnetwork.cisco.com)

Questions? Visit the Learning@Cisco Booth
# Data and Analytics Cisco Education Offerings

<table>
<thead>
<tr>
<th>Course</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANDMB – Data Management, Architecture and Applications</td>
<td>Provides hands on training with a technical mix of application, compute, storage and networking topics concerning the deployment of Big Data clusters.</td>
</tr>
<tr>
<td>ANDMA – Advanced Data Management, Architecture and Applications</td>
<td>Covers major architecture design to cater to different needs of the application, data center or deployment requirements. It provides architectural designs and advanced hands-on training on topics covering Scaling of cluster to thousands of nodes and management, Data Life Cycle management with HDFS tiered storage, and different approaches for Multi-tenant Hadoop cluster deployments with Openstack</td>
</tr>
<tr>
<td>ANCISB – Basic Course in Data Virtualization based on Cisco Information Server</td>
<td>Hands-on accelerated training on installing and developing with Cisco Information Server Application Data Services. It provides technical guidance to engineers who will be performing complex integration activities.</td>
</tr>
<tr>
<td>ANCISV – Advanced Course in Data Virtualization based on Cisco Information Server</td>
<td>Recommended course for administrators who need to understand how Cisco Information Server fits into their environment and the types of administration tasks typically required by the product.</td>
</tr>
<tr>
<td>ANCISM – Administration Course in Data Virtualization based on Cisco Information Server</td>
<td>Course is for candidates who are familiar with Cisco Data Virtualization “basics” and want to focus on advanced Cisco Information Server features.</td>
</tr>
</tbody>
</table>

For more details, please visit: [http://learningnetwork.cisco.com](http://learningnetwork.cisco.com)
Questions? Visit the Learning@Cisco Booth