LET'S
BUILD
TOMORROW
TODAY
CCNA Industrial Overview

Sudarshan Krishnamurthi – Sr.Product Manager
Rami Kandah – Technical Architect
Learning@Cisco
BRKCRT-1901
Agenda

- Market Transitions and Skills Gap
- CCNA Industrial Introduction
- Difference between Enterprise vs Industrial Networks
- Overview of Converged Plant-wide Ethernet Architectures
- Overview of Industrial Protocols, CIP and Profinet
- Overview of Wireless Technologies for Connected Factory
- Overview of Security Technologies for Connected Factory
- Conclusion
Market Transitions and Skills Gap
All Jobs Will Require Technology Competence

**MANUFACTURING**
- Robotics

**TRANSPORTATION**
- Automation

**DEFENSE AND SECURITY**
- Big Data/Analytics
- Security

**ENERGY**
- Government

**HEALTHCARE**
- Healthcare

**RETAIL**
- Retail

**BANKING AND FINANCE**
- Banking and Finance
A Growing Workforce for the Next Industrial Revolution - IoT

Industries Reinventing their Business with IP

Existing Talent needs to be reskilled in many industries

New Talent Needed to connect 50B Devices

2 Million Jobs by 2022

IP traffic will increase 20x by 2017

IT + OT Convergence on the Industrial Plant floor

220,000 New Engineers needed every year until 2022

Thousands of New Jobs Being Created in Every Industry
Questions For Consideration

• Given the Pace of Change and Disruptions how does the talent keep up?
• How do you motivate and challenge talent in a rapidly changing world?
• How do you realize the full value of IoT and Digitization?

Connectivity ➔ Data ➔ Outcomes
IoT Education - Goals

• Help Address Skill Gaps in the Industry for IoT by providing best in class Education curriculum
• Provide Career and Learning Paths for Individuals to reskill/up skill
• Help hiring managers address Skills gap challenge
• Bring new individuals, Customers and partners into the IoT ecosystem through Education and Certifications
• Enable Cisco’s Partners, Customers and Employees drive adoption of IoT Products, Solutions and Services
Curriculum Building Process

Market Analysis

• How big is the Challenge?
• What is the Business Impact?

Job Role Analysis

• Job Roles for today and the future?
• Specific Domains and Tasks for the Job Roles?
• Curriculum and Learning Map

Industry Partnerships

• IoT is an Ecosystem Play
• Cisco Certifications are designed outside → In
• Partnerships in building the curriculum
Training and Certifications Portfolio: Adapting to Meet Real-World Needs

Career Certifications

**Architect:**
Cisco Certified Architect

**Expert:**
- CCIE® Routing and Switching, SP, SP Ops, Security, Collaboration, Wireless, and CCDE®

**Professional:**
- CCNP® Routing and Switching, CCNP Security, CCSP®, CCNP Voice, CCNP Wireless, CCNP SP Ops, and CCDP™

**Entry/Associate:**
- CCENT®, CCT™, CCNA® Routing and Switching, CCNA Security, CCNA Voice, CCNA Wireless, and CCDA®

Specialist Certifications

- Business
- Data Center
- Internet of Things
- Network Programmability
- Operating System Software
- Security
- Service Provider
- Video

Soft Skills/Business

LVCI, Business Transformation
(Selling, Positioning, Services)

Product Training

NPI, Solutions, Multi-vendor
(Design, Implement, Support)
Why Certify?

**KNOWLEDGE**

8 out of 10 managers agree certified employees are more knowledgeable

**ADVANCEMENT**

Over two-thirds of managers agree employees are ready for more responsibilities

**VALUE**

Almost three-quarters agree these employees are more valuable.

86% of IT hiring managers consider certifications a strong priority for evaluating candidates*

*Source: 2014 IT Skills and Salary Report, Global Knowledge and Windows IT Pro
IoT Education Offerings

Certifications
- Job Role Based Certification covering Domains, Tasks, Skills needed to perform Job Duties

Solutions Training
- Knowledge and understanding of complete solutions – Vertical Specific

Product Training
- Deep knowledge of IoT Products – Ruggedized switches, routers, wireless and security products

Basic/Skills Training
- Recommended or Mandatory Pre-Reqs

Cisco Industrial Networking Specialist
- CCNA Industrial

Connected Health, Connected Safety, Connected Utilities
- Connected Mining, (future)

IE2K/3K Switch (Available)
- ISR 819 (Future)
- CSS, CGR, Wireless

IT for OT (eLearning)
- OT for IT (eLearning)
CCNA Industrial – Introduction
CCNA Industrial – Addressing IT and OT Job Roles

Career Certification
Hands on Instructor Led Training + Exam

Specialist/Career Certification
Hands on Instructor Led Training + Exam

Basic Skills Training

CCNA Industrial – Manufacturing (IMINS2)

Cisco Industrial Networking Specialist Certification (IMINS)

Networking Fundamentals

Control Systems Fundamentals

OT/Plant Engineer

Network Engineer
Paths to get CCNA Industrial

IT Audience
- CCNA Exam (200-120)
- ICND1 (100-101)
- CCENT
- CCNA R&S

OT Audience
- IMINS (200-401)
- Cisco Industrial Networking Specialist

IMINS2 (200-601)
IMINS Exam Blueprint - Domains

- 1.0 Install, Replace, and/or Remove an End-Device
- 2.0 Install, Replace, and/or Remove an Infrastructure Device
- 3.0 Install, Replace, and/or Remove Cables (Network and/or Power)
- 4.0 Troubleshooting - Layer 1, Layer 2, End-to-End
- 5.0 Maintain Appropriate End-Devices and Industrial Network Infrastructure Devices
IMINS2 Exam Blueprint - Domains

- 1.0 IP Networking
- 2.0 Common Industrial Protocol (CIP)
- 3.0 ProfiNET
- 4.0 Security
- 5.0 Wireless
- 6.0 Troubleshooting - General, CIP, ProfiNET
Enterprise vs Industrial Networks
Industrial vs. Enterprise Architecture
IACS Network Design Requirements

7 Key features that manufacturers expect as best practices:

- Industrial characteristics
- Interconnectivity and interoperability
- Real-time communication, determinism, and performance
- Availability
- Security
- Manageability
- Scalability

IACS – Industrial Automation Control Systems
Overview of Converged Plant-wide Ethernet Architecture CPwE
Converged Plantwide Ethernet (CPwE)

- Dedicated Cisco Validated Design for automated manufacturing environment
- Co-developed with Rockwell Automation
- Architecture provides design and implementation guidance
- Achieve real-time communication and deterministic requirements for Industrial Automation Control Systems
IACS Framework – Purdue Model

Uses a logical framework to describe the basic functions and composition of a manufacturing system.

- International Society of Automation ISA-99
- Identifies and defines levels of operations
- Levels refer to this concept of levels of operations.
Provide predictable fail-safe shutdown of the IACS application upon the occurrence of a safety event.
Cell/Area Zone

The Cell/Area zone is a functional area within a plant facility.
Level 0 - Process

• Level 0 - sensors and actuators involved in the basic manufacturing process.
• Performs the basic functions of the IACS - driving a motor, measuring variables, painting, welding, bending, and so on.
• These functions can be very simple (temperature gauge) to highly complex (a moving robot).
Level 1 - Basic Control

- Consists of controllers that direct and manipulate the manufacturing process.
- Interface with the Level 0 devices (e.g., I/O, sensors, and actuators).
- Historically in discrete manufacturing, the controller is typically a programmable logic controller (PLC).
- In process manufacturing, the controller is referred to as a distributed control system (DCS).
Level 2 - Area Supervisory Control

 Represents the applications and functions associated with the Cell/Area zone runtime supervision and operation:

 - Operator interfaces or HMIs
 - Alarms or alerting systems
 - Control room workstations
Manufacturing Zone

- The Manufacturing zone:
  - Cell/Area zones and site-level activities.
- The Manufacturing zone:
  - IACS applications, devices, and controllers critical to the plant floor
Level 3 - Site Level

Systems and applications that exist at this level manage plant-wide IACS functions.

The applications and functions that exist at this level include the following:

- Level 3 IACS network
- Reporting (e.g.: cycle times, predictive maintenance)
- Plant historian
- Detailed production scheduling
- Site-level operations management
Enterprise Zone Level 4

- Includes access to enterprise network services such as the following:
  - Access to the Internet
  - Access to E-mail (hosted in data centers)
  - Non-critical plant systems such as manufacturing execution systems and overall plant reporting
  - Access to enterprise applications such as SAP and Oracle (hosted in data centers)
  - Typically under the management and control of the IT organization.
Level 5-Enterprise

• Level 5 is where the centralized IT systems and functions exist
• Enterprise resource management - B2B, and B2C services.
• External partner or guest access systems exist here
• Managed and operated by the IT organization.
Converging Reference Models
Overview of Industrial Protocols: CIP and ProfiNet
Typical Application Areas

- **Discrete Automation**
  - Car manufacturing
  - Bottling systems
  - Storage systems
  - Robotics

- **Process Automation**
  - Water and waste water treatment
  - Chemical and petro-chemicals

- **Power Industry**
  - Power plants
  - Substations
Exploring Ethernet/IP Communications
EtherNet/IP

- EtherNet/Industrial Protocol introduced in 2001
- Managed jointly by Open Device Vendor Association (ODVA) and ControlNet International
- Defines the encapsulation protocol to structure CIP (Common Industrial Protocol) over standard Ethernet.
- It has two primary purposes:
  - Transport of control-oriented data associated with I/O devices (Implicit Messaging)
  - Transport of other information that is related to the system being controlled, such as configuration parameters and diagnostics (Explicit Messaging)
What is CIP?

CIP Motion™ Profiles | Motor Control Profiles | Transducer Profiles | I/O Profiles | Other Profiles | Semiconductor Profiles | CIP Safety™ Profiles
---|---|---|---|---|---|---
Object Library
(Communications, Applications, Time Synchronization)

Data Management Services
Explicit and I/O Messages

Connection Management, Routing

TCP/UDP
Internet Protocol
Ethernet CSMA/CD
Ethernet Physical Layer

CompoNet Network and Transport
ControlNet Network and Transport
DeviceNet Network and Transport

CompoNet Time Slot
ControlNet CTDMA
CAN CSMA/NBA

CompoNet Physical Layer
ControlNet Physical Layer
DeviceNet Physical Layer

EtherNet/IP™
CompoNet™
ControlNet™
DeviceNet™
Encapsulation of Messages

RSLinx Classic passes the message on to the TCP program which adds on pieces to guarantee the integrity of the message.

TCP program the new message to the IP program which adds information to get the message routed.

IP program passes the new message to Ethernet program which adds on the Ethernet part needed to send it over the network.

Ethernet Frame is sent out the PHY.
CIP Connections

Peer to peer object oriented protocol
CIP is a connection-based protocol
The Producer/Consumer model can be unicast or multicast.

- Producers are field devices that generate data on a CIP network at a pre-established rate.
- Consumers are the devices on a CIP network that use the data that is generated by a producer device.
What is CIP Sync? (Cont.)

- CIP Sync is based on the IEEE 1588 standard – Precision Time Protocol (PTP).
- CIP Sync defines time synchronization services for CIP.
- Time synchronization on the EtherNet/IP network is a method to synchronize clocks across devices on the network.
Precision Time Protocol (PTP)

- The Precision Time Protocol (PTP) is a time-transfer protocol standard that allows precise synchronization of networks.
- The goal of this protocol is to have a set of slave devices determine the offset between time measurements on their clocks and time measurements on a master device.
Precision Time Protocol (PTP) Messages

Precision Time Protocol contains the following messages:

- Announce Messages
- Sync Messages
- Follow-up Messages
- Delay Request Message
- Delay Response Message
Precision Time Protocol (PTP) Review

Master Clock

D1

TS

Follow-up

Sync

D2

TS

Delay Request

Delay Response

Slave Clock

TS

Sync

Follow-up

TS

Sync

Follow-up

Delay = (D1+D2)/2

Time

TS

Time Stamp
CIP Motion

• CIP Motion is an extension to the CIP standard for multi-axis, synchronized motion control on an EtherNet/IP network.

• Uses CIP Motion Profiles (position, speed and torque)

• Uses IEEE-1588-based CIP Sync

• CIP motion delivers the data and the timestamp for execution (time-based)
CIP Safety

A safety network is a communication network designed to have high integrity.

• Operates correctly or it goes to a predefined safe state
• Has a more stringent timing requirement (deterministic)
• Has dual channel design
• Media and data link independent
Configuring CIP

- Upload Electronic Data Sheet File (EDS) to Rockwell Automation Studio 5000
- Configure CIP on the Cisco IE or Stratix Series Switch
- Use Rockwell Automation Studio 5000 software to download a project file to a PLC
- Use Rockwell Automation Studio 5000 to validate I/O operation
Upload EDS file

- IE2K-x#\textbf{dir flash:ie2000-universalk9-mz.152-1.EY}
- Directory of flash:/ie2000-universalk9-mz.152-1.EY/
- 3 -rwx 41307 Mar 14 1993 21:41:08 +00:00 Cisco_IE2000_GSD.zip
- 6 -rwx 17092095 Mar 14 1993 21:41:56 +00:00 ie2000-universalk9-mz.152-1.EY.bin
- 7 drwx 4608 Mar 14 1993 21:54:44 +00:00 html
- 750 -rwx 149564 Mar 14 1993 22:14:42 +00:00 controlfpga.bin
- 751 -rwx 143335 Mar 14 1993 22:15:17 +00:00 dc_default_profiles.txt
- 751 -rwx 72603 Mar 30 2011 01:28:06 +00:00 EDSCollection.gz
- 752 -rwx 72603 Mar 30 2011 01:27:55 +00:00 EDSCisco.gz
- 57931776 bytes total (5821952 bytes free)
Upload EDS File
Check Device Availability
Configuring CIP

• Enable the CIP protocol on SVI interface
• IE2K-3(config)#int vlan 101
• IE2K-3(config-if)#cip enable
• IE2K-3(config-if)#end
Configure Device
Download Project File to PLC
Check CIP Status

IE2K1-3#show cip status
State: Enabled
Vlan: 25

IE2K1-3#

IE2K1-3#show cip session
Id: 4
Socket: 2
Tag: 0x59382110
State: OpenSessionEstablished
Idle: yes
Timeout: 354950 msec
Incoming: 1
Host IP: 192.168.3.35
Client IP: 192.168.13.101
Service Count: 336
PROFINET Functionality and Connection Method

PROFINET
Protocol Characteristics

• PROFIBUS International (PI) open Industrial Ethernet Standard

• Uses TCP/IP and IT standards for automation control

• Defines communication paths to meet speed requirements:
  
  • Normal non-real-time communication uses TCP/IP and cycle times of approximately 100 ms. (Conformance Class A, CC-A)
  
  • Real-time communication enables cycle times of approximately 10 ms. (Conformance Class B, CC-B)
  
  • Isochronous real-time communication enables cycle times of approximately 1 ms. (Conformance Class C, CC-C)
Protocol Characteristics (Cont.)
Protocol Characteristics (Cont.)
Discovery and Configuration Protocol (DCP)

• All PROFINET devices use a device name and an IP address.
• Configure names and IP addresses in the engineering software (I/O supervisor). Or via DHCP
• I/O Supervisor sees new device via Link Layer Discovery Protocol (LLDP). Pushes config (device name)
• The I/O Controller pushes IP address and config parameters to I/O device via DCP
PROFINET Communications

AR - Application Relation
CR - Communication Relation
PROFINET Communications (Cont.)
PROFINET Communications (Cont.)

- IRT communication achieves the highest performance through synchronizing all devices and scheduling data transmissions, i.e., a time-slot technology.

- A communication cycle includes both IRT, RT, and NRT communication
Clock Synchronization

- All devices in the synchronous communication must have a common clock.
- A clock master uses synchronization frames to synchronize the clocks of the devices.
- All devices must be connected directly to one another without crossing any non-synchronized devices.
PROFIsafe

- Replaces separately wired safety circuits
- Is an additional software layer that is used on top of the existing PROFINET protocol
- Adds functional safety to your existing PROFINET network
- Does not have any impact on standard bus protocols
Cisco Switch Configuration

1. Copy the GSD file from the switch
2. Install the GSD file into TIA Portal software
3. Add and configure the switch in the TIA Portal project
4. Set the PROFINET ID and the IP address for the PROFINET VLAN at the switch
Install GSD File in TIA
Cisco Switch Configuration (Cont.)
Cisco Switch Validation
Manufacturing Automation – Wireless
Advantages of a wireless network include:

- Lower installation and operational costs
  - Cabling and hardware reduction
  - Eliminating cable failures
- Connection to hard-to-reach and restricted areas
- Equipment mobility
  - New and more efficient applications
  - Personnel mobility
  - Higher productivity and less downtime
Technology Overview

Challenges

Wireless is different from wired media

- Half-duplex shared medium
  - Only one device can transmit at a time

- Wireless coverage area cannot be precisely defined
  - Site survey is required
  - Signal may reach beyond the intended area

- Signal quality may change over time
  - Interference sources and obstructions

- Higher latency and packet loss compared to wired Ethernet

Advantages > Challenges

If designed correctly and used for the right application
## Technology Overview

### Knowing the Industrial Wireless Terminology

<table>
<thead>
<tr>
<th>Type of Industrial Application</th>
<th>Wireless Technology</th>
<th>Characteristics</th>
<th>Throughput</th>
</tr>
</thead>
</table>
| Supervisory Control Peer to Peer Control Distributed I/O Control Safety Control Mobile Operator (HMI) | IEEE 802.11a/g/n                            | • Point to multipoint topology  
• Static or mobile equipment  
• May require plant-wide coverage and roaming                                   | Moderate to high |
| Long Haul SCADA Remote site connectivity                         | IEEE 802.11a/g  
Cellular 3G / LTE WiMAX  
FHSS 900 MHz  
FHHS 2.4 GHz Licensed bands                                           | • Outdoor point to point, point to multipoint, or mesh topology  
• Small or moderate number of nodes  
• Typically static equipment                                                   | Low to moderate  |
| Process Instrumentation Wireless Sensors Condition Based Monitoring | ISA-100.11a  
WirelessHART®  
ZigBee®  
Bluetooth®                                                               | • Mesh topology with large number of nodes  
• Self-healing auto-provisioning network  
• Low cost and power consumption                                               | Low              |
Technology Overview

Industrial Wireless Mobility Types

• **Static equipment**
  - Permanent operational location
  - Wire replacement for hard-to-reach locations
  - Examples: process control, condition monitoring, stand-alone OEM machines

• **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.

• **Mobile equipment (no roaming)**
  - Changes position during an operation
  - Remains connected to the same AP
  - Examples: rotary platforms, assembly systems with tracks, overhead cranes

• **Mobile equipment (fast roaming)**
  - Moves between different APs during an operation
  - Examples: AGVs, overhead cranes, train cars.
Technology Overview

Wireless Client Types

Embedded adapter issues:
• Lack of antenna options
• Placement restrictions
• Node density
• Migration costs

External adapter (wireless bridge):
• Single wired client

Workgroup Bridge (WGB):
• Multiple wired clients
• Single wireless client for the AP

Workgroup Bridge is the main method of connecting to WLAN
Technology Overview

Autonomous WLAN Architecture

- Each autonomous AP is managed individually
- Limited coordination between APs
- Standalone IACS applications
- Small number of APs and clients
Technology Overview

Unified WLAN Architecture

- Lightweight APs (LWAPs) are configured and managed by a Wireless LAN Controller (WLC)
- Large scale plant-wide coverage
- Plant-wide mobility, RF and security policies

Note: WGB can join a Unified WLAN as a client to an LWAP
## Technology Overview

### Choosing the Right Wireless Architecture

<table>
<thead>
<tr>
<th>Unified WLAN Architecture</th>
<th>Autonomous WLAN Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Large number of APs (&gt;10)</td>
<td>• Small number of APs (&lt;10)</td>
</tr>
<tr>
<td>• Plant-wide coverage</td>
<td>• Larger number of WGBs per AP</td>
</tr>
<tr>
<td>• Existing infrastructure, IT practices and security policies that call for Unified architecture</td>
<td>• Stand-alone applications</td>
</tr>
<tr>
<td>• Applications that require fast wireless roaming</td>
<td>• Applications with no roaming</td>
</tr>
<tr>
<td>• WLAN is managed jointly by IT and control engineers – greater level of expertise</td>
<td>• WLAN is integrated into a stand-alone OEM machine and delivered to a plant</td>
</tr>
<tr>
<td></td>
<td>• WLAN is managed mostly by control engineers – lower level of expertise</td>
</tr>
<tr>
<td></td>
<td>• Lower initial cost</td>
</tr>
</tbody>
</table>
## Application Recommendations
### Choosing an Appropriate Application

<table>
<thead>
<tr>
<th>IACS Traffic Type</th>
<th>CIP Standard</th>
<th>Use with Wireless</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information and diagnostics, process control, peer to peer messaging</td>
<td>CIP Class 3 (HMI) CIP Class 3 (MSG)</td>
<td>Yes</td>
<td>&lt;20% of total packet rate if combined with CIP Class 1 Standard and Safety traffic</td>
</tr>
<tr>
<td>Peer to Peer Control I/O Control</td>
<td>CIP Class 1 Produced / Consumed or I/O</td>
<td>Yes</td>
<td>Application should tolerate higher latency and jitter</td>
</tr>
<tr>
<td>Safety Control</td>
<td>CIP Safety</td>
<td>Yes</td>
<td>Very fast safety reaction times may not be supported</td>
</tr>
<tr>
<td>Time Synchronization</td>
<td>CIP Sync</td>
<td>Limited</td>
<td>Limited accuracy, may be suitable for SOE and event logging applications</td>
</tr>
<tr>
<td>Motion Control</td>
<td>CIP Motion</td>
<td>No</td>
<td>Not feasible due to higher latency and jitter and poor CIP Sync accuracy</td>
</tr>
</tbody>
</table>
Deploying 802.11 Wireless LAN Technology within a Converged Plantwide Ethernet Architecture

Design and Implementation Guide

November 2014
Manufacturing Automation – Security
## Security Requirements Differ Between IT & OT

<table>
<thead>
<tr>
<th>Focus</th>
<th>OT</th>
<th>IT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• 24/7 Operations, High OEE</td>
<td>• Protecting Intellectual Property &amp; Company Assets</td>
</tr>
<tr>
<td>Precedence of Priorities</td>
<td>• Availability</td>
<td>• Confidentiality</td>
</tr>
<tr>
<td></td>
<td>• Integrity</td>
<td>• Integrity</td>
</tr>
<tr>
<td></td>
<td>• Confidentiality</td>
<td>• Availability</td>
</tr>
<tr>
<td>Types of Data Traffic</td>
<td>• Converged Network of Data, Control, Information, Safety &amp; Motion</td>
<td>• Converged Network of Data, Voice &amp; Video</td>
</tr>
<tr>
<td>Access Control</td>
<td>• Strict Physical Access</td>
<td>• Strict Network Authentication &amp; Access Policies</td>
</tr>
<tr>
<td></td>
<td>• Simple Network Device Access</td>
<td></td>
</tr>
<tr>
<td>Implications of a Device Failure</td>
<td>• Production is Down</td>
<td>• Work-around or Wait</td>
</tr>
<tr>
<td></td>
<td>• ($$'s/hour … or Worse)</td>
<td></td>
</tr>
<tr>
<td>Threat Protection</td>
<td>• Isolate Threat but Keep Operating</td>
<td>• Shut Down Access to Detected Threat</td>
</tr>
<tr>
<td>Upgrades</td>
<td>• Scheduled During Downtime</td>
<td>• Automatically Pushed During Uptime</td>
</tr>
</tbody>
</table>
The Attack Continuum

- **Before**: Discover, Enforce, Harden
- **During**: Detect, Block, Defend
- **After**: Scope, Contain, Remediate

Visibility and Context

- Firewall
- VPN
- NGIPS
- Advanced Malware Protection
- NGFW
- UTM
- Web Security
- Network Behavior Analysis
- NAC + Identity Services
- Email Security
Security Principles Enable Secure Architectures

Access Control
- User and Device Identity
- Authentication, Authorization & Accounting

Data Confidentiality & Data Privacy
- Network Segmentation
- Secure Connectivity

Threat Detection & Mitigation
- Security Zones
- Intrusion Prevention; Application Visibility

Device & Platform Integrity
- Device Hardening, Secure Platform Virtualization
- Configuration Assurance
# IT/OT Converged Security Model

<table>
<thead>
<tr>
<th>IT</th>
<th>Access Control</th>
<th>Threat Detection</th>
<th>Device Integrity</th>
</tr>
</thead>
<tbody>
<tr>
<td>DMZ</td>
<td>OT Partners &amp; Services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OT</td>
<td>Enterprise Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Demilitarized Zone</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Process, Supervisory</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Control, Automation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Cloud

- Internet
- IT
- DMZ
- OT

**Cisco Live!**
IT/OT Converged Security Model – Manufacturing

**Enterprise Network**
- Levels 4–5
  - Web Apps
  - DNS
  - FTP
  - Internet
  - Gbps Link for Failover Detection
  - Firewall (Active)
  - Firewall (Standby)
  - Patch Mgmt.
  - Terminal Services
  - Application Mirror
  - AV Server

**Demilitarized Zone**
- Level 3.5
  - Factory Application Servers
  - Girps Link for Failover Detection
  - Core Switches
  - Aggregation Switch

**Manufacturing Zone**
- Level 3
  - Factory Application Servers
  - Core Switches
  - Access Switch

**Cell/Area Zone**
- Levels 0–2
  - Drive Controller
  - HMI
  - Distributed I/O
  - Cell/Area #1 (Redundant Star Topology)
  - Cell/Area #2 (Ring Topology)
  - Cell/Area #3 (Linear Topology)

**Identity Services**
- Cloud-based Threat Protection
- Network-wide Policy Enforcement
- Access Control (application-level)
- VPN & Remote Access Services
- Next-Generation Firewall
- Intrusion Prevention (IPS)
- Stateful Firewall
- Intrusion Detection (IDS)
- Physical Access Control Systems
- Ruggedized Firewall
- Ruggedized IDS / IPS
- Remote Monitoring / Surveillance
Figure 1 - CPwE Industrial Network Security Framework
Secure Access - Cisco Identity Services Engine (ISE)
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
Adding ISE to CPwE

Enterprise Zone
Levels 4 and 5

Industrial Demilitarized Zone (IDMZ)

1) All endpoints must authenticate before being allowed on the network.
2) Centralizing authentication for all three mediums (wired, wireless, remote access)
3) Centralizing your network policy/privileges
4) Full reporting capability on every endpoint accessing the network.

--- Device type
--- Username/MAC/IP
--- Where they Auth’d from
Employee Access Example - Wired

NOTES
1. Employee endpoint is examined by ISE
2. ISE sends back a dACL allowing access to that zone, but denies communication to other zones.
3. Employee has Mgmt. software on laptop, and receives direct access to controller
Contractor/Vendor example - Wireless

- **Redundant Star Topology**
- **Ring Topology**
- **Linear/Bus/Star Topology**

**NOTES**

Contractor /Vendor access restricted to devices via RDP machine
Appendix A
IMINS2 Lab Topology
IMINS2 Pod Topology
Participate in the “My Favorite Speaker” Contest

Promote Your Favorite Speaker and You Could Be a Winner

• Promote your favorite speaker through Twitter and you could win $200 of Cisco Press products (@CiscoPress)

• Send a tweet and include
  • Your favorite speaker’s Twitter handle SudarshanKCisco
  • Two hashtags: #CLUS #MyFavoriteSpeaker

• You can submit an entry for more than one of your “favorite” speakers

• Don’t forget to follow @CiscoLive and @CiscoPress

• View the official rules at http://bit.ly/CLUSwin
Complete Your Online Session Evaluation

• Give us your feedback to be entered into a Daily Survey Drawing. A daily winner will receive a $750 Amazon gift card.

• Complete your session surveys though the Cisco Live mobile app or your computer on Cisco Live Connect.

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

- Demos in the Cisco campus
- Walk-in Self-Paced Labs
- Table Topics
- Meet the Engineer 1:1 meetings
- Related sessions
Thank you
TOMORROW starts here.
## 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! CCNA Industrial</strong></td>
<td>An associate level instructor led training course 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 curriculum addresses foundational skills needed to manage and administer networked industrial control systems. It provides plant administrators, control system engineers and traditional network engineers with an understanding of the networking technologies needed in today's connected plants and enterprises</td>
<td>Cisco Industrial Networking Specialist</td>
</tr>
<tr>
<td>Control Systems Fundamentals for Industrial Networking (ICINS)</td>
<td>For IT and Network Engineers, covers basic concepts in Industrial Control systems including an introduction to automation industry verticals, automation environment and an overview of industrial control networks</td>
<td></td>
</tr>
</tbody>
</table>

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

Questions? Visit the Learning@Cisco Booth or contact ask-edu-pm-dcv@cisco.com