

IT and OT Convergence - Recommendations for Building an IoT-Ready Manufacturing Network

Arun Siddeswaran
Manager, Solution Engineering
Cisco Systems, Inc.

Gregory Wilcox
Global Business Development Manager
Rockwell Automation

Paul Didier
Global Solutions Architect
Cisco Systems, Inc.

Presented at the ODVA
2017 Industry Conference & 18th Annual Meeting
February 21-23, 2017
Palm Harbor, Florida, USA

Table of Contents

Abstract	3
Keywords.....	3
Business outcomes of Industrial IoT	3
Industrial OT vs Enterprise IT Networks	3
Reference Architecture	6
Segmentation (Zoning)	6
Zoning through Segmentation	7
Cell/Area Zone.....	8
Industrial Zone.....	9
Enterprise Zone	10
Converged Plantwide Ethernet Architecture	11
Wired Access	11
Cell zone Components	13
Cell/Area Zone Traffic Flow	13
Real-Time Communication, Determinism, and Performance	14
Network Address Translation (NAT)	16
NAT IACS Use Cases	16
Single Skid/Machine Aggregated by One NAT Switch, Single VLAN	16
Single Skid/Machine Aggregated by One NAT Switch, Multiple VLANs	17
Multiple Skids/Machines Aggregated by One NAT Switch, Multiple VLANs	18
Wireless Access.....	19
WLAN IACS Equipment Use Cases.....	19
Autonomous and Unified WLAN Architectures	20
Holistic Defense-in-depth Security.....	22
Secure Remote Connectivity.....	24
Acronyms and Initialisms	24
References.....	25

Abstract

Manufacturing networks are evolving towards a converged architecture with integrated IT and OT systems. Connecting devices and assets in a converged architecture enables data acquisition, remote monitoring and cloud based predictive analytics. This leads to lower costs, higher productivity, and greater visibility into plant operations. However the converged network design must ensure that security and performance requirements are not compromised as a result. This paper will provide an overview of various use cases, best practices and architecture recommendations in the areas of resiliency, wireless, defense-in-depth security as well as cloud connectivity and integration

Keywords

IT OT Convergence, best practices, architecture, manufacturing, design, industrial

Business outcomes of Industrial IoT

By utilizing a resilient, scalable and secure network, business leaders can achieve various business outcomes which includes improving efficiency, minimizing downtime, increase OEE and enable real time operational visibility.



Source: SCM World/Cisco "Smart Manufacturing and the Internet of Things 2015" survey of 418 Manufacturing Business Line Executives and Plant Managers across 17 vertical industries.

Industrial OT vs Enterprise IT Networks

Industrial OT network's and typical enterprise IT networks have similarities and differences that must be accounted for. Below tables summarizes those based on various criteria's.

Criteria	Industrial OT Networks	Enterprise IT Networks
Environment	Plant-floor Control Room, Industrial Data Center Control Panel, Industrial Distribution Frame (IDF)	Carpeted Space, Data Center Data Communication or Wiring Closet, Intermediate Distribution Frame (IDF)

Switches	Managed and unmanaged Layer 2 is predominant DIN rail or panel mount is predominant	Managed Layer 2 and Layer 3 Rack mount
Wireless	Autonomous (locally managed) – point solutions Mobile equipment (emerging) and personnel (prevalent)	Unified (centrally managed) solutions Mobile personnel – Corporate provided or Bring Your Own Device (BYoD) Guest access
Computing	Industrial Hardened Panel Mount Computers and Monitors Desktop, Notebook Tablets, Smart Phones (emerging) 19” Rack Server Virtualization - becoming prevalent Hardening – sporadic patching and white listing	Desktop, Notebook Tablets, Smart Phones 19” Rack Server and Blade Server Unified Computing Systems (UCS) Virtualization - widespread Hardening - patching and white listing
Environment	Plant-floor Control Room, Industrial Data Center Control Panel, Industrial Distribution Frame (IDF)	Carpeted Space, Data Center Data Communication or Wiring Closet, Intermediate Distribution Frame (IDF)
Switches	Managed and unmanaged Layer 2 is predominant DIN rail or panel mount is predominant	Managed Layer 2 and Layer 3 Rack mount
Network Technology	Standard IEEE 802.3 Ethernet and proprietary (non-standard) versions Standard IETF Internet Protocol (IPv4) and proprietary (non- standard) alternatives	Standard IEEE 802.3 Ethernet Standard IETF Internet Protocol (IPv4 and IPv6)
Network Availability	Switch-Level and Device-Level Topologies	Switch-Level topologies Redundant Star Topology is predominant

	Ring Topology is predominant for both, Redundant Star for switch topologies is emerging Standard IEEE, IEC and vendor specific Layer 2 resiliency protocols	Standard IEEE, IETF, and vendor specific Layer 2 and Layer 3 resiliency protocols
Service Level Agreement (SLA)	Mean time to recovery (MTTR) - Minutes, Hours	Mean time to recovery (MTTR) - Hours, Days
IP Addressing	Mostly Static	Mostly Dynamic
Traffic Type	Primarily local – traffic between local assets Information, control, safety, motion, time synchronization, energy management Smaller frames for control traffic Industrial application layer protocols: CIP, PROFINET, IEC 61850, Modbus TCP, etc.	Primarily non-local – traffic to remote assets Voice, Video, Data Larger packets and frames Standard application layer protocols: HTTP, SNMP, DNS, RTP, SSH, etc.
Performance	Low Latency, Low Jitter Data Prioritization – QoS – Layer 2 & 3	Low Latency, Low Jitter Data Prioritization – QoS – Layer 3
Security	Open by default, must close by configuration and architecture Industrial security standards – e.g. IEC, NIST Inconsistent deployment of security policies No line-of-sight to the Enterprise or to the Internet	Pervasive Enterprise security standards Strong security policies Line-of-sight across the Enterprise and to the Internet
Focus	24/7 operations, high OEE	Protecting intellectual property and company assets
Precedence of Priorities	Availability Integrity	Confidentiality Integrity

	Confidentiality	Availability
Access Control	Strict physical access Simple network device access	Strict network authentication and access policies
Implications of a Device Failure	Production is down (\$\$'s/hour ... or worse)	Work-around or wait
Threat Protection	Isolate threat but keep operating	Shut down access to detected threat
Upgrades	Scheduled during downtime	Automatically pushed during uptime

Reference Architecture

Modern industrial automation and control system (IACS) applications require a network infrastructure to be scalable, reliable, safe, secure and future-ready to support the industrial internet of things (IIoT). A structured and hardened architecture, with key tenets, helps to create smaller connected LANs which restores the segmentation and natural boundaries found in legacy 3-tier networks. Key tenets such as: Smart Endpoints, Segmentation (Zoning), Managed Infrastructure, Resiliency, Time-critical Data, Wireless – Mobility, Holistic Defense-in-Depth Security, Convergence-ready solutions.

Segmentation (Zoning)

Plant-wide Zoning

- Functional / Security Areas
- Smaller Connected LANs
 - Smaller Broadcast Domains
 - Smaller Fault Domains
 - Smaller Domains of Trust
- Building Block Approach for Scalability

To understand the security and network systems requirements of an industrial automation and control system (IACS), this document uses a logical model to describe the basic functions and composition of an IACS application. The Purdue Reference Architecture and ISA 95 are common and well-understood models that use Levels to segment devices and equipment into hierarchical functions. The concept of operational Levels has been incorporated into many other models and standards in the industry. Based on this segmentation of the plant operations, standards such as IEC 62443, NIST 800-82 and ICS-CERT recommended practices organize the operational Levels into Security Zones as shown in Figure 1

Zoning through Segmentation

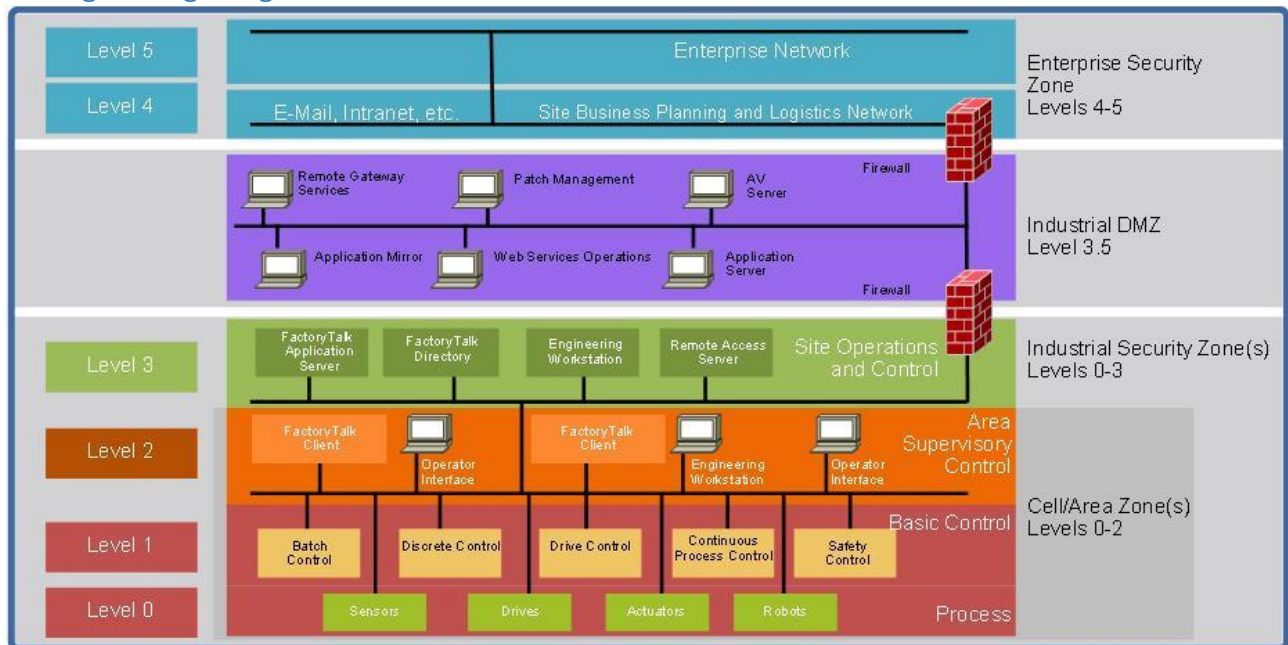


Figure 1 Zoning through Segmentation

This logical model identifies Levels of operations which are organized into Zones based on functionality and domains of trust. The Open Systems Interconnection (OSI) and Reference Model is also commonly referred to when discussing network architectures. The OSI model refers to Layers of network communication functions. In this paper, unless specified, Layers refer to layers of the OSI model and Levels refer to operational levels of this logical model.

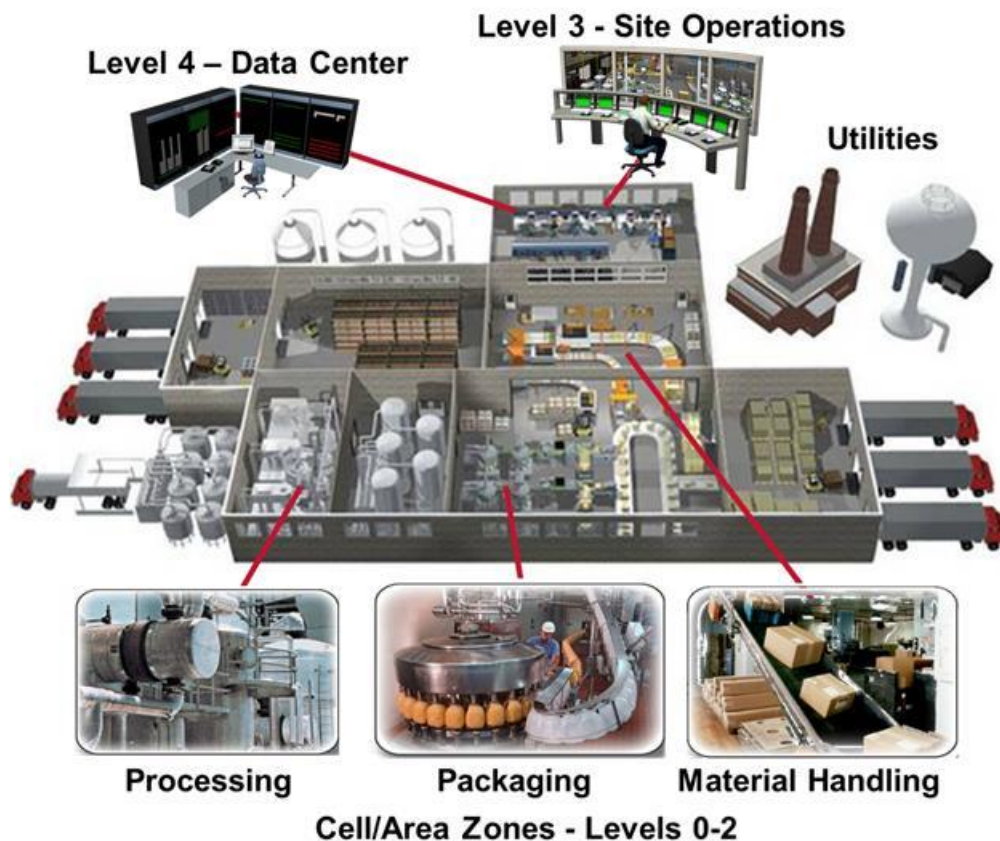


Figure 2 Segmentation layout

Cell/Area Zone

The Cell/Area zone is a functional area within a plant facility; many plants have multiple Cell/Area zones. In an automotive plant, it may be a bodyshop or a sub-assembly process. In a food and beverage facility, it may be the batch mixing area. It may be as small as a single controller and its associated devices on a process skid, or multiple controllers on an assembly line. Each plant facility defines the Cell/Area zone demarcation differently and to varying degrees of granularity. For the purposes of this paper, a Cell/Area zone is a set of IACS devices, controllers, etc. that are involved in the real-time control of a functional aspect of the manufacturing process. To control the functional process, they are all in real-time communication with each other. This zone has essentially three levels of activity occurring, as described in the following subsections.

Level 0—Process Level 0 consists of a wide variety of sensors and actuators involved in the basic manufacturing process. These devices perform the basic functions of the IACS, such as driving a motor, measuring variables, setting an output, and performing key functions such as painting, welding, bending, and so on.

These functions can be very simple (temperature gauge) to highly complex (a moving robot). These devices take direction from and communicate status to the control devices in Level 1 of the logical model. In addition, other IACS devices or applications may need to directly access Level 0 devices to perform maintenance or resolve problems on the devices.

- Drive the real-time, deterministic communication requirements
- Measure the process variables and control process outputs
- Exist in challenging physical environments that drive topology constraints
- Vary according to the size of the IACS network from a small (10s) to a large (1000s) number of devices

- Once designed and installed, are not replaced all together until the plant line is overhauled or replaced, which is typically ten or more years

Control System Engineers (operational technology - OT) such as electrical, process, and so on, and not the IT departments, typically design and implement these devices and the IACS networks that support them.

Level 1—Basic Control Level 1 consists of controllers that direct and manipulate the manufacturing process, which its key function is to interface with the Level 0 devices (e.g., I/O, sensors, and actuators). These applications are typically implemented and maintained by the operational technology (OT) organization

Controllers act alone or in conjunction with other controllers to manage the devices and thereby the manufacturing process. Controllers also communicate with other functions in the IACS (for example, historian, asset manager, and manufacturing execution system) in Levels 2 and 3. The controller performs as a director function in the Industrial zone translating high-level parameters (for example, recipes) into executable orders, consolidating the I/O traffic from devices and passing the I/O data on to the upper-level plant floor functions.

Thus, controllers produce IACS network traffic in three directions from a Level perspective:

- Downward to the devices in Level 0 that they control and manage
- Peer-to-peer to other controllers to manage the IACS for a Cell/Area zone
- Upward to HMIs and information management systems in Levels 2 and 3

Level 2 —Area Supervisory Control Level 2 represents the applications and functions associated with the Cell/Area zone runtime supervision and operation.

These include the following:

- Operator interfaces or HMIs
- Alarms or alerting systems
- Control room workstations Depending on the size or structure of a plant, these functions may exist at the site level (Level 3). These applications communicate with the controllers in Level 1 and interface or share data with the site level (Level 3) or enterprise (Level 4/5) systems and applications through the Industrial DMZ.

These applications can be implemented on dedicated IACS vendor operator interface terminals, or on standard computing equipment and operating systems such as Microsoft Windows. These applications are typically implemented and maintained by the operational technology (OT) organization.

Industrial Zone

The Industrial zone is comprised of the Cell/Area zones (Levels 0 to 2) and site-level (Level 3) activities. The Industrial zone is important because all the IACS applications, devices, and controllers critical to monitoring and controlling the plant floor IACS operations are in this zone. To preserve smooth plant operations and functioning of the IACS applications and IACS network, this zone requires clear logical segmentation and protection from Levels 4 and 5 of the plant/enterprise operations.

Level 3—Site Level 3, represents the highest level of the IACS. The systems and applications that exist at this level manage plantwide IACS functions. Levels 0 through 3 are considered critical to site operations. The applications and functions that exist at this level include the following:

- Level 3 IACS network
- Reporting (for example: cycle times, quality index, predictive maintenance)
- Plant historian
- Detailed production scheduling
- Site-level operations management
- Asset and material management

- Control room workstations
- Patch launch server
- File server
- Other domain services, e.g. Active Directory (AD), Dynamic Host Configuration Protocol (DHCP), Dynamic Naming Services (DNS), Windows Internet Naming Service (WINS), Network Time Protocol (NTP), etc.
- Terminal server for remote access support
- Staging area
- Administration and control applications

The Level 3 IACS network may communicate with Level 1 controllers and Level 0 devices, function as a staging area for changes into the Industrial zone, and share data with the enterprise (Levels 4 and 5) systems and applications through the Industrial DMZ. These applications are primarily based on standard computing equipment and operating systems (Unix-based or Microsoft Windows). Additionally, because these systems tend to be aligned with standard IT technologies, they may also be implemented and supported by personnel with Industrial IT (OT-IT) skill sets. These Industrial people may belong organizationally to either OT or IT.

Enterprise Zone

Level 4—Site Business Planning and Logistics Level 4 is where the functions and systems that need standard access to services provided by the enterprise network reside. This level is viewed as an extension of the enterprise network. The basic business administration tasks are performed here and rely on standard IT services. These functions and systems include wired and wireless 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, such as inventory, performance, etc.
- Access to enterprise applications such as SAP and Oracle (hosted in data centers)

Although important, these services are not viewed as critical to the IACS and thus the plant floor operations. Because of the more open nature of the systems and applications within the enterprise network, this level is often viewed as a source of threats and disruptions to the IACS network. The users and systems in Level 4 often require summarized data and information from the lower levels of the IACS network. The network traffic and patterns here are typical of a branch or campus network found in general enterprises where approximately 90 percent of the network traffic goes to the Internet or to data center-based applications. This level is 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, business-to-business, and business-to-customer services typically reside at this level. Often the external partner or guest access systems exist here, although it is not uncommon to find them in lower levels (e.g., Level 3) of the model to gain flexibility that may be difficult to achieve at the enterprise level. However, this approach may lead to significant security risks if not implemented within IT security policy and approach.

The IACS must communicate with the enterprise applications to exchange manufacturing and resource data. Direct access to the IACS is typically not required. One exception to this would be remote access for management of the IACS by employees or partners such as system integrators and machine builders. Access to data and the IACS network must be managed and controlled through the Industrial DMZ to maintain the security, availability, and stability of the IACS.

The services, systems, and applications at this level are directly managed and operated by the IT organization.

Converged Plantwide Ethernet Architecture

The Purdue, ISA, IEC and NIST have identified Levels of operations and key Security Zones for the IACS logical model. In addition to the Levels and Zones, this document include an Industrial Demilitarized zone (IDMZ) between the Enterprise and Industrial zones as part of architecture. The purpose of the IDMZ is to provide a buffer zone where data and services can be shared between the Enterprise and Industrial zones. The IDMZ is critical in maintaining availability, addressing security vulnerabilities, and abiding by regulatory compliance mandates. In addition, the IDMZ allows for segmentation of organizational control; for example, between the IT organization and manufacturing. This segmentation allows different policies to be applied and contained. For example, the manufacturing organization may apply security and quality-of-service (QoS) policies that are different from the IT organization. The IDMZ is where the policies and organizational control can be divided.

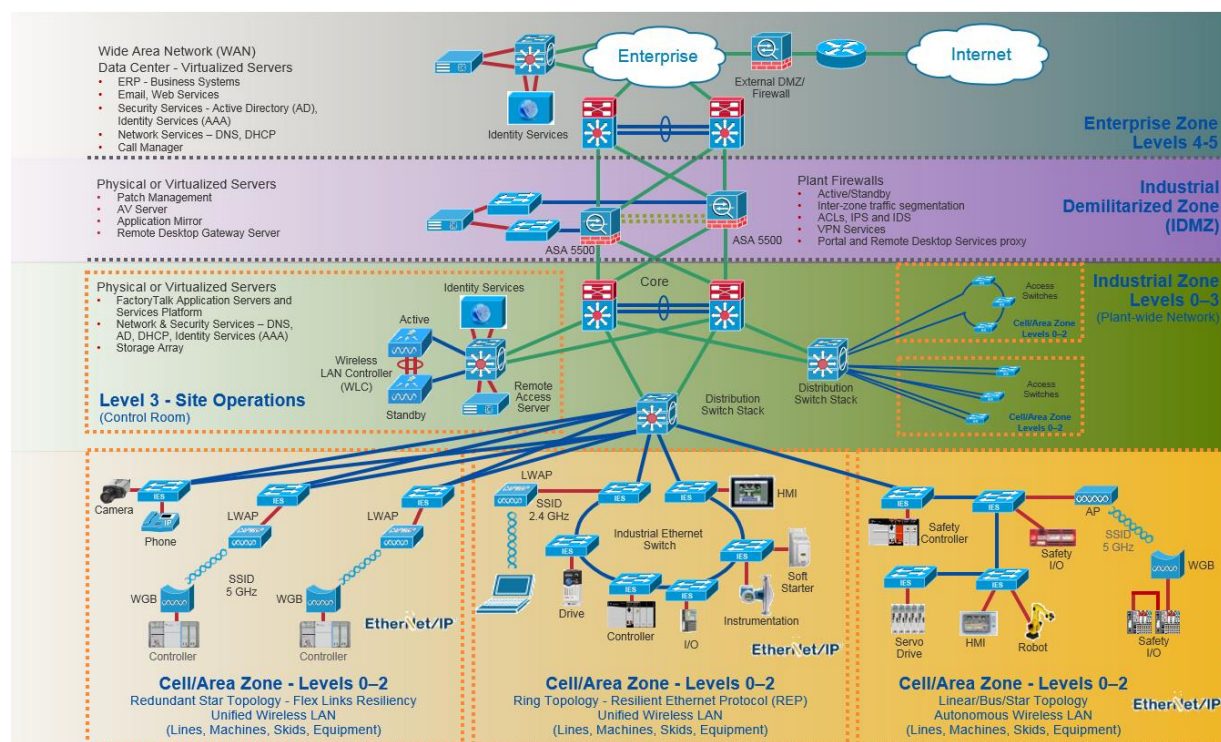


Figure 3 Reference Architecture

Wired Access

The Industrial Automation and Control Systems (IACS) network within the Cell/Area zone is the major building block of plant-wide architecture. This is the network that connects sensors, actuators, drives, controllers and any other IACS devices that need to communicate in real-time (I/O communication). This section outlines the key requirements and technical considerations for the Cell/Area zone and related IACS applications.

It is important to consider the Cell/Area zone as a separate entity of the Industrial zone. For most industrial applications, the Cell/Area zone is where the primary IACS activities are performed. The availability and performance requirements are most distinct in the Cell/Area zone. These requirements are different than those typically found in an IT network. In summary, the key design considerations are as follows:

- **Industrial Characteristics**—The environmental conditions of the plant floor such as ability to withstand shock, vibration, humidity, dust, varying operating temperatures, must be taken into consideration because the equipment must be able to perform in these conditions. This drives the industrial characteristics of all the equipment, including the network infrastructure. The network topology must be shaped to fit appropriately into the plant floor environment.
- **Interconnectivity and interoperability**—Standardization on a single vendor's IACS or industrial Ethernet network equipment within the Cell/Area zone may not be practical.
- **Real-time communications and network performance**—Cell/Area IACS network must be designed to meet the latency and jitter requirements of the IACS it supports. This can impact the size of the LAN, the number of routing hops, the VLAN configuration, and a number of other network parameters. Typical communication ranges depends upon specific application requirements as summarized in Figure 6 below.
- **Availability**—The availability of the Cell/Area zone is critical to the manufacturing process. Without a properly functioning Cell/Area IACS network, some or all of the plant operations may come to a halt. This can severely impact plant efficiency and the manufacturer's bottom line. Availability itself is a function of equipment, infrastructure, configuration, software, etc.. For example, the network must also be able to recover from network impacting events, such as a connection break, faster than the cycle time of the IACS to avoid the system automatically shutting down. Availability impacts the network design, topology, and even the type of network infrastructure used.
- **Manageability**—plant floor is usually not supported in the same manner as an IT network. The plant floor maintenance personnel tend not to have the same networking experience as IT. The setup and maintenance of network equipment and configuration must be simplified to meet the experience level of the plant floor maintenance personnel.
- **Security**—OT/IT network convergence calls for evolved security policies for industrial networks which no longer remain isolated. IACS assets have become susceptible to the same security vulnerabilities (for example, denial of service) as their enterprise counterparts. Protecting IACS assets requires a defense-in-depth security approach to assure the availability, confidentiality and integrity of IACS data.
- **Unmanaged versus managed**—Although the cost of the network infrastructure may not represent a large proportion of the plant floor, the same cost reduction mentality is often applied as to other aspects of the manufacturing facility. Without clear understanding of the qualities of a managed, intelligent network, the additional hardware costs they represent may lead network developers to choose less intelligent solutions based purely on initial cost considerations; only later do they determine that the cheaper, unmanaged infrastructure cannot scale, perform, integrate, or be as easily maintained as an intelligent, managed network.

All these factors directly impact the IACS components, network topology, drive particular requirements of the Cell/Area zone IACS network design.

The Cell/Area zone is also distinct in that most of the network communication is of a local nature—one device communicating with another in the same vicinity. From a network perspective, the Cell/Area zone correlates primarily with a Layer 2, or local area network (LAN), network. In the campus design, the Cell/Area zone aligns with the access-layer and many of the recommendations and considerations are applied, albeit with a consideration for the plant floor and the IACS applications.

Below summarizes some key recommendations:

- Design small Cell/Area zones in a VLAN to better manage and shape the traffic.
- Use managed switches (diagnostics, segmentation, prioritization, resiliency, network address translation (NAT) and security).
- All connections should be auto-negotiate for speed and duplex and thereby apply full-duplex communication to avoid collisions.

- Use fiber Gigabit Ethernet ports for trunks/uplinks for distance, quick recovery, lower latency, and jitter.
- Use Internet Group Management Protocol (IGMP) snooping/querier functions to control multicast traffic volume, preferably with the querier on the Layer-3 distribution switch.
- Use resilient network topologies, ring, or redundant star
- Understand the availability requirements of the manufacturing process and IACS to properly select, design and implement the network resiliency capabilities. The selected network resiliency may or may not meet these requirements depending on the type of IACS application. Implementer should design the IACS systems appropriately and understand the implications of a network event on the IACS applications.
- Apply port security to Layer-2 industrial Ethernet switch to limit use of open ports.

Cell zone Components

- Levels 0, 1, and 2 components; for example, devices, controllers, and HMIs
- Layer-2 access switches
- Layer-3 distribution switches or routers
- Media to connect all of the above

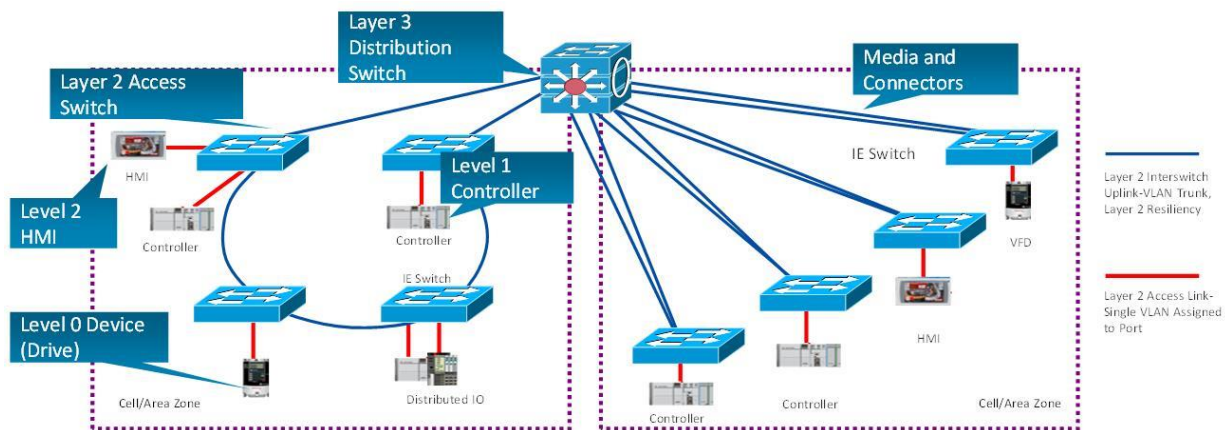


Figure 4 Cell Zone components

Cell/Area Zone Traffic Flow

Traffic flow in a Cell/Area IACS network is largely determined by the design and implementation of the IACS. These systems produce very different traffic patterns than the client-server and Internet-based applications in the IT domain or enterprise network. For example, 80 to 90 percent of the Cell/Area traffic is local as compared to a typical IT LAN in which perhaps less than 10 percent of the traffic is local. This is primarily driven by the cyclical I/O data being communicated on very short intervals (milliseconds) from devices to controllers and workstations/HMIs all on the same LAN or VLAN.

A network infrastructure should be designed to support the proper traffic flows. Features such as network segmentation can impact the network traffic flows and network performance.

Key considerations when designing traffic flows include the following:

EtherNet/IP implementations have traditionally been unable to route multicast traffic since the time-to-live field in the IP packet is set to 1. The use of multicast for Implicit CIP I/O traffic is an application choice. Explicit messaging data has always been unicast delivery via TCP. Devices and controllers configured for multicast delivery need to be located within the same Cell/Area IACS network as these packets cannot be routed, meaning that any router will drop the packet before forwarding it outside of

the subnet/VLAN. Devices and controllers configured for unicast delivery, Implicit I/O or Explicit messaging, do not need to be within the same Cell/Area zone as that communication is routable.

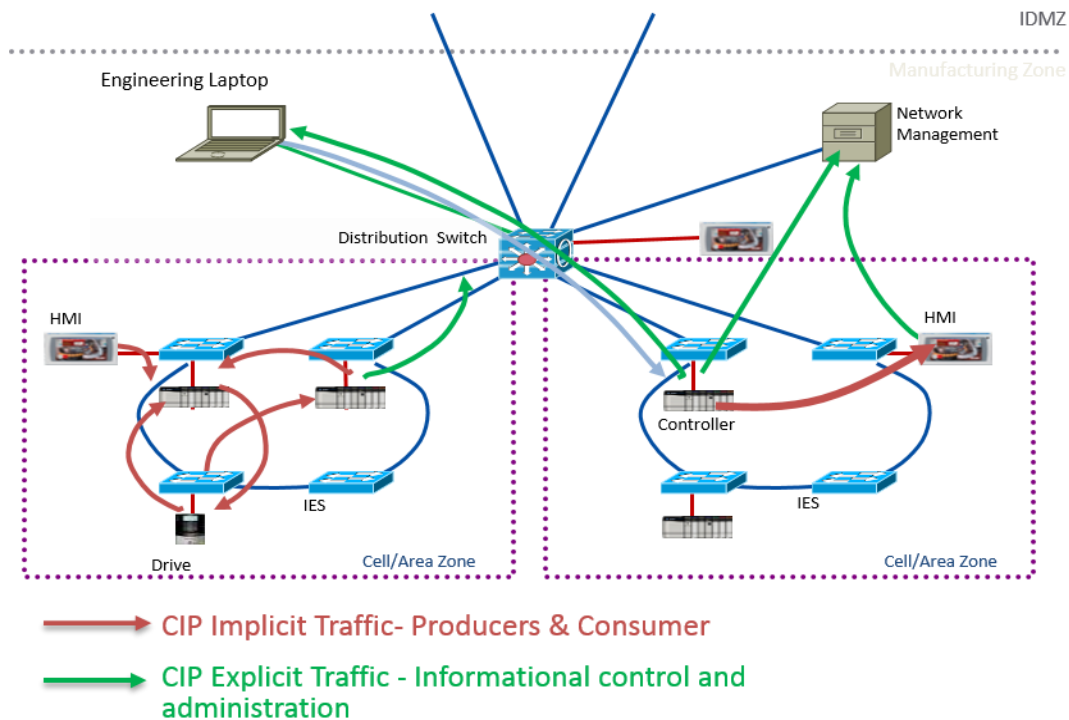


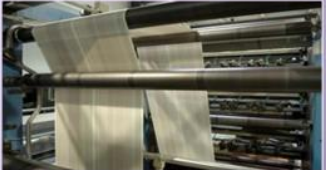


Figure 5 Cell/Area Zone Traffic Flow

Real-Time Communication, Determinism, and Performance

IACS networks differ significantly from their IT counterparts in their need to support real-time communications, which means communicating messages with minimal latency (time delay between message sent and message received) and jitter (the variance of the latency), significantly lower than typical Enterprise applications. Real-time communications help the IACS become more deterministic. Although the network plays a role in the deterministic nature of a system, a number of other factors, such as end-device latency and response time, are also involved. But the network has an important role, not just by sending packets quickly and consistently, but in the services it offers and supports, such as quality-of-service (QoS) and precision time. IACS networks have different real-time communications requirements based on the type of application. Figure 6 represents examples of application requirements as developed by ARC research in 2006.

	Process Automation 	Discrete Automation 	Loss Critical 
Function	Information Integration, Slower Process Automation	Time-critical Factory Automation	Multi-axis Motion Control
Comm. Technology	.Net, DCOM, TCP/IP	Industrial Protocols, CIP, Profinet	Hardware and Software solutions, e.g. CIP Motion, PTP
Period	1 second or longer	1 ms to 100 ms	100 µs to 10 ms
Industries	Oil & Gas, chemicals, energy, water	Auto, food and bev, electrical assembly, semiconductor, metals, pharmaceutical	Utilities Subset of Discrete automation
Applications	Pumps, compressors, mixers; monitoring of temperature, pressure, flow	Material handling, filling, labelling, palletizing, packaging; welding, stamping, cutting, metal forming, soldering, sorting	Life/equipment safety, Synchronization of multiple axes: printing presses, wire drawing, web making, picking and placing

Source: ARC Advisory Group

Figure 6 Performance Requirements

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

Figure 7 Network Resiliency Protocols

Figure 7 provides guidance in choosing the right protocol and access network topology based on application requirements. Please refer to “Acronyms and Initialisms” section for term definitions

Network Address Translation (NAT)

NAT is a networking technology that enables Control System Engineers (OT) to build IACS applications reusing IP (IPv4) addresses, while allowing those IACS applications to integrate into the larger plant-wide architecture. Plant-wide architectures require unique IP addressing. NAT can be configured to translate only specific IP addresses from inside the IACS application to the outside plant-wide architecture. Doing so provides the added benefit of effectively hiding the inside IP addressing schema of the IACS application.

Whether you are an end user, OEM or system integrator, Internet Protocol (IP) addresses within your Industrial Automation and Control System (IACS) application may need to be reused. Network Address Translation (NAT) enables the reuse of IP addressing without introducing a duplicate IP address error into your IACS application architecture.

Technology and business aspects drive the decision to use NAT:

- From a business perspective, OEMs use NAT to enable the replication of skids and machines, including IP addressing. This helps to reduce development and commissioning costs.
- From a technology perspective, end users use NAT when the IP address space within the plant-wide network infrastructure is limited and not every device needs to communicate outside the skid or machine-level network.

NAT IACS Use Cases

Single Skid/Machine Aggregated by One NAT Switch, Single VLAN

A common use case, as depicted in Figure 8, is the coordination of control functions of an OEM skid or machine by a line controller. In this use case, a single Layer 2 virtual LAN (VLAN 2) exists; however, the skid or machine IACS devices have a different IP address range (inside) than the line controller (outside). The machine industrial Ethernet switch (IES) translates the inside IP address (192.168.1.x) of the machine controller to an outside IP address (10.10.10.x) on VLAN 2.

This scalable use case enables the integration of multiple skids or machines with duplicated IP addressing into the same line controller VLAN. Each skid or machine IES would have to translate the duplicated inside IP addresses to unique outside IP addresses to avoid a duplicate IP error within the VLAN.

For this use case, a NAT-capable Layer 2 IES is required for each skid or machine. A Layer 3 switch is not required since a single VLAN is used.

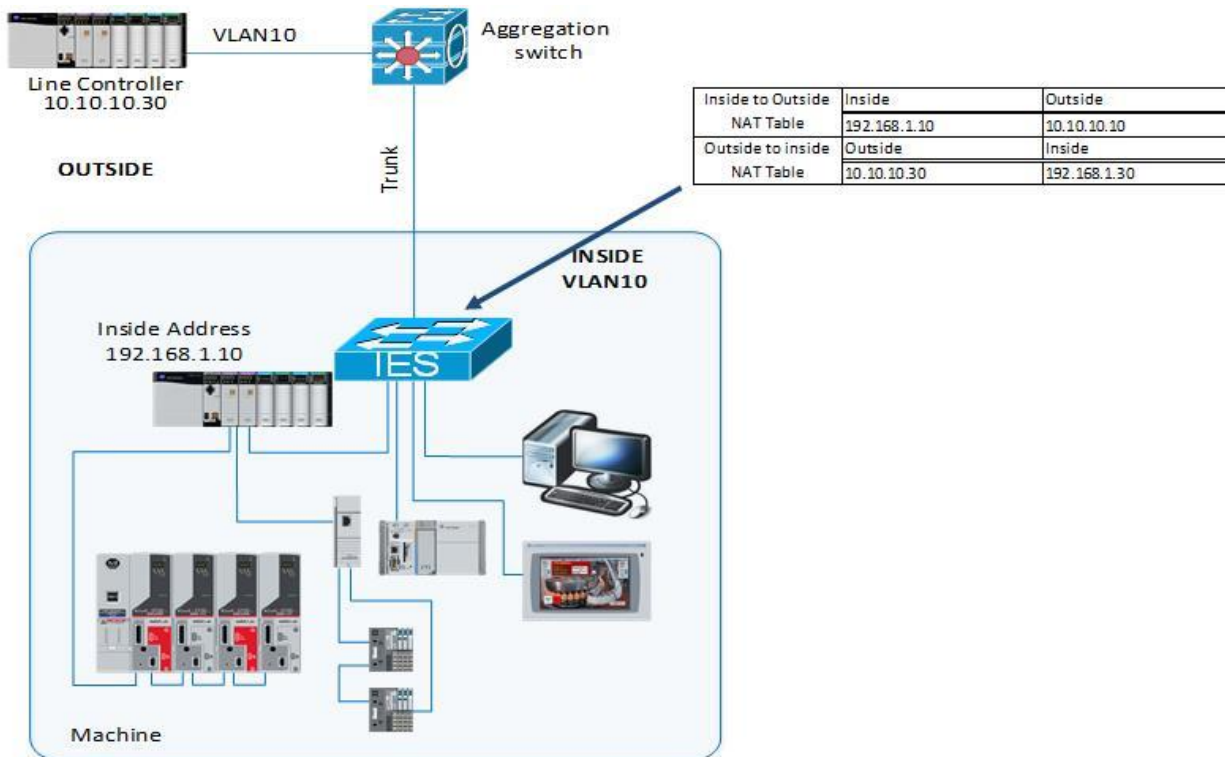


Figure 8 Single Skid/Machine Aggregated by One NAT Switch, Single VLAN

Single Skid/Machine Aggregated by One NAT Switch, Multiple VLANs

A variation of the previous use case, as depicted in Figure 9, uses multiple VLANs—VLAN 10 for skid or machine 1, VLAN 20 for skid or machine 2 and VLAN 30 for the line controller. As in the previous use case, the IP addresses are duplicated for the IACS devices within each skid or machine.

The machine 1 IES translates the inside IP address (192.168.1.x) of the machine controller to an outside IP address (10.10.10.x) on VLAN 10. The IES switch also translates the outside IP address of the default gateway (Layer 3 switch) to an inside IP address.

The machine 2 IES translates the inside IP address (192.168.1.x) of the machine controller to an outside IP address (10.10.20.x) on VLAN 20. Likewise, the machine 2 IES switch also translates the outside IP address of the default gateway to an inside IP address.

Each machine controller has a unique outside IP address and default gateway IP address on its own respective VLAN. The Layer 3 switch routes the outside IP address of each machine controller either to the line controller (vertical interlocking) on VLAN 30, or to the other machine VLAN (horizontal interlocking).

This scalable use case enables the integration of multiple skids or machines with duplicated IP addressing into the same line controller VLAN. Each skid or machine IES would have to translate the duplicated inside IP addresses to unique outside IP addresses to avoid a duplicate IP error within the VLAN.

For this use case, a NAT-capable Layer 2 IES is required for each skid or machine. A Layer 3 switch is required to enable routing between the VLANs.

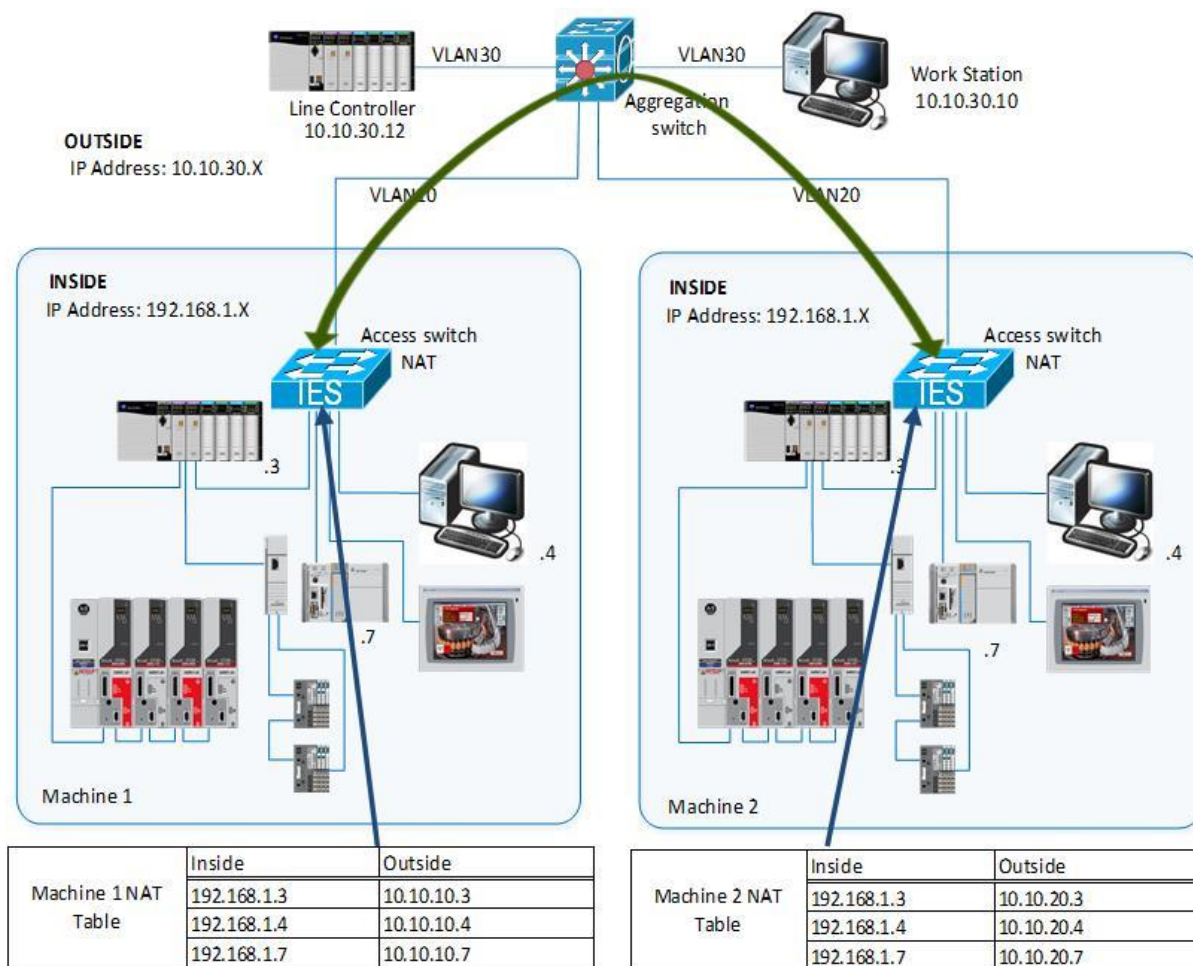


Figure 9 Single Skid/Machine Aggregated by One NAT Switch, Multiple VLANs

Multiple Skids/Machines Aggregated by One NAT Switch, Multiple VLANs

A variation of the previous two use cases, as depicted in Figure 10, uses a single NAT-capable IES to translate IP addresses from multiple skids or machines. In this use case, the NAT IES supports multiple instances of NAT, on a per-VLAN basis. As in the previous use cases, the IP addresses are duplicated for the IACS devices within each skid or machine.

Each machine IES aggregates the IACS devices onto its VLAN. The single NAT IES translates the inside IP addresses (192.168.1.x) within each VLAN to its outside IP addresses—VLAN 10 (10.10.10.x) and VLAN 20 (10.10.20.x)—using a separate instance of the NAT table for each VLAN. Each machine controller has a unique outside IP address on its own respective VLAN. The single NAT IES also translates the IP addresses of the default gateway, which is a Layer 3 switch.

The Layer 3 switch routes the outside IP addresses of each machine controller either to the line controller (vertical interlocking) on VLAN 40, or to the other machine VLANs (horizontal interlocking). This scalable use case enables the integration of multiple skids or machines with duplicated IP addressing into the same line controller VLAN. Each skid or machine has unique outside IP addresses within their respective VLANs to avoid a duplicate IP error.

For this use case, a single NAT-capable Layer 2 IES can be used to aggregate multiple machines, while a non-NAT IES is used within each machine. A Layer 3 switch is required to enable routing between the VLANs.

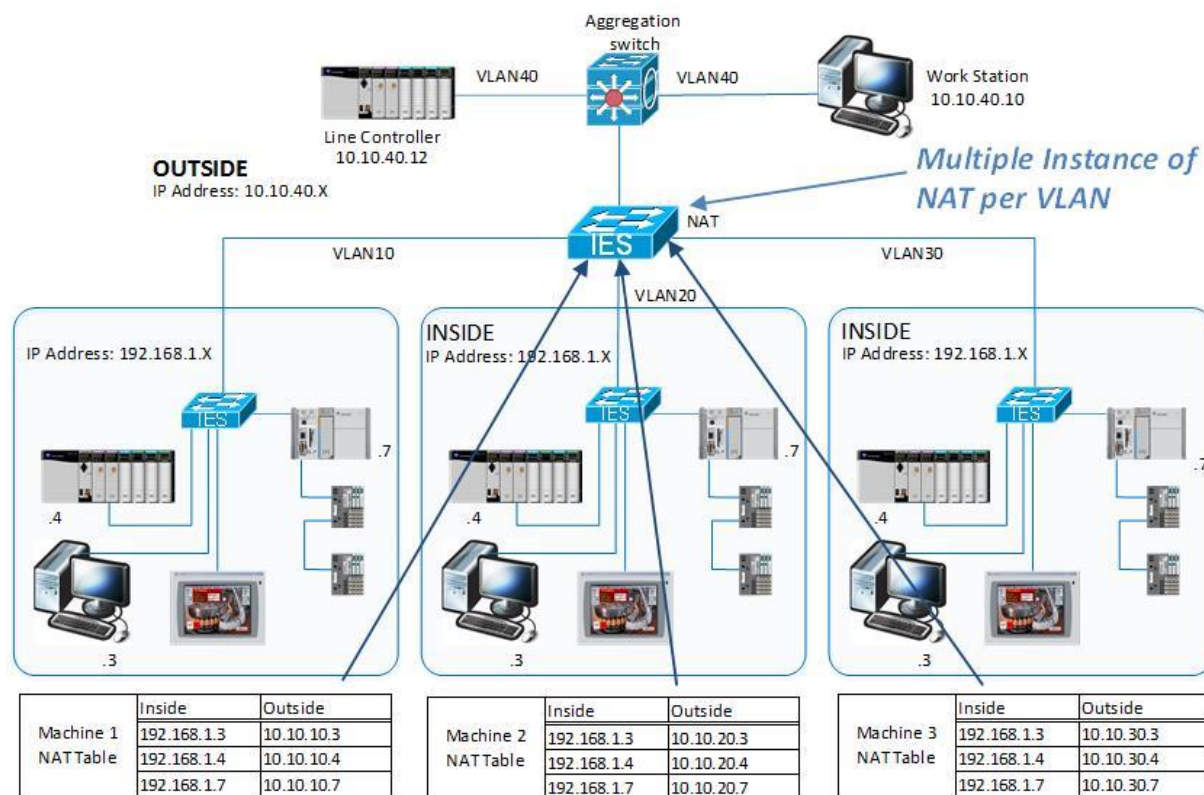


Figure 10 Multiple Skids/Machines Aggregated by One NAT Switch, Multiple VLANs

Wireless Access

Plant-wide architectures increasingly use IEEE 802.11™ wireless networks for critical Industrial Automation and Control System (IACS) applications that require reliable data transmission with low levels of latency and jitter. Wireless Local Area Networks (WLANs) differ significantly from traditional wired LANs in their use of shared radio frequencies, susceptibility to interference and coverage impairments. Deploying a plant-wide WLAN requires thoughtful planning and design as well as periodic monitoring to meet expectations for bandwidth, throughput, reliability and security.

WLAN IACS Equipment Use Cases

Wireless IACS equipment can be characterized by the type of mobility and operational requirements when relocating within the plant-wide architecture. Wireless IACS equipment may stay within a single Cell/Area Zone and remain associated to a single access point (AP) until powered down or disconnected. Wireless equipment may roam across the Industrial Zone and associate to multiple APs while remaining operational.

- Fixed position devices in the WLAN architecture have a permanent operational location, also known as "static." Fixed position wireless is an alternative to a wired connection for hard-to-reach

and remote locations where cabling is too expensive or impossible to install. Usage areas include process control, machine condition monitoring, fixed environmental monitoring and energy industries. In the manufacturing environment, a common use case is a stand-alone OEM machine or skid that needs to be integrated into a plant-wide architecture over a wireless link.

- Nomadic equipment stays in place while operating, then moves to a new location in the shutdown state. After relocation, a new wireless connection needs to be established. Common examples are process skids, storage tanks, reactors and portable manufacturing equipment.
- Mobile (non-roaming) equipment changes position during an operation, remaining in the same coverage area within a Cell/Area Zone. Common examples are rotary platforms and turntables, Automated Storage and Retrieval Systems (ASRS), assembly systems with tracks and overhead cranes. These applications may require rapid changes in position and orientation of the wireless client relative to the AP.
- Mobile (roaming) equipment changes position during an operation by roaming across multiple coverage areas within the Industrial Zone. Common examples are automatic guided vehicles (AGVs), large ASRS, overhead cranes and train cars.

Autonomous and Unified WLAN Architectures

Two different wireless network architectures can be utilized to deploy equipment to equipment communication over wireless: Autonomous WLAN and Unified WLAN. With two differing architectures, WLAN allows users to make an informed architecture selection that meets both business and technical needs for scalability within the plant-wide architecture.

The benefits of the Autonomous WLAN architecture include:

- A lower initial hardware cost
- Simplified design and deployment
- More granular control of Quality of Service (QoS) for prioritization of critical IACS application network traffic

The benefits of the Unified WLAN architecture include:

- Plant-wide scalability
- Support for plant-wide mobility
- Advanced optimization and recovery mechanisms
- Enhanced security

Autonomous WLAN architectures, as illustrated in Figure 11, do not utilize the centralized management structure found in the Unified WLAN. Each Access Point (AP) functions as its own stand-alone device, as an AP or Workgroup Bridge (WGB), without the need for a WLC. The Autonomous WLAN architecture is therefore less costly to implement, thus may be more suitable for smaller IACS applications, such as an OEM machine or skid. Autonomous WLAN APs utilized in the WLAN architecture may be later repurposed to the Unified Access architecture with additional hardware under the following conditions: If deployment needs change or large scale plant-wide growth requires an architectural transitioning If the OEM machine/skid is integrated into a plant-wide architecture

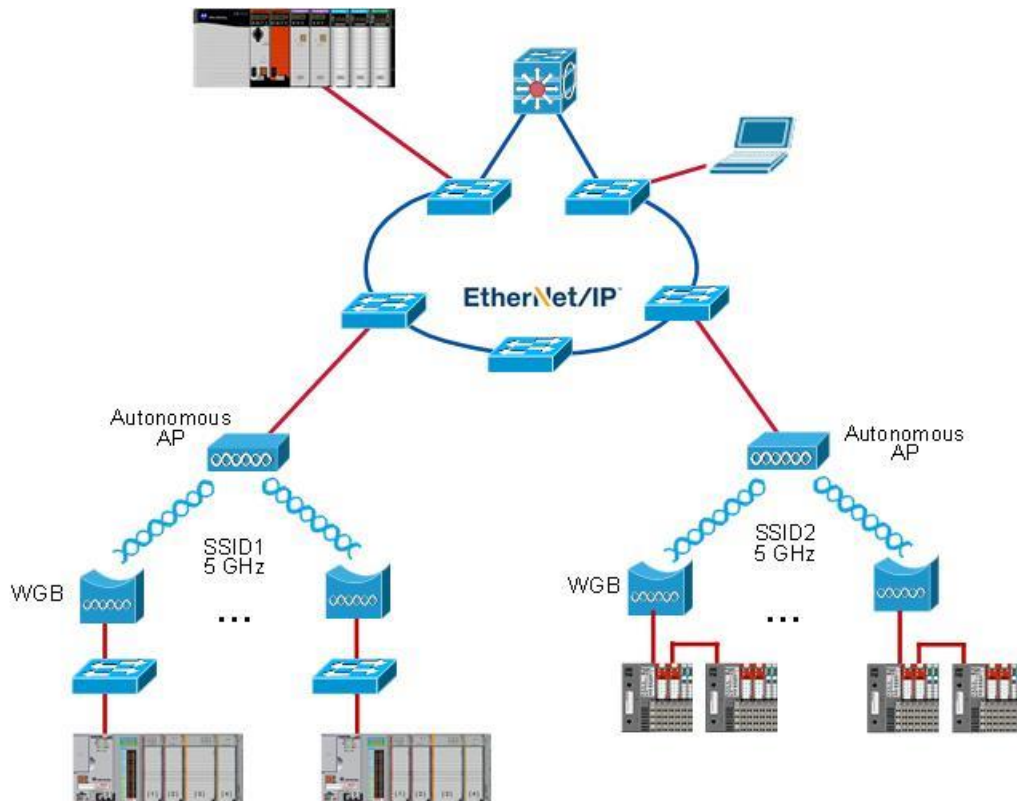


Figure 11 Autonomous WLAN Architecture

The Unified WLAN architecture, as illustrated in Figure 12, has the ability to address large-scale plant-wide 802.11 wireless needs. The Unified Access architecture allows for centralized management and control of the wireless access points distributed throughout the plant. By utilizing a Wireless LAN Controller (WLC) and Lightweight Access Points (LWAP), a centralized management model is created, thus introducing security and self-healing mechanisms to the wireless architecture. The Unified WLAN architecture also introduces foundational services, including intrusion prevention and wireless guest access, for better control over devices seeking to connect to the WLAN.

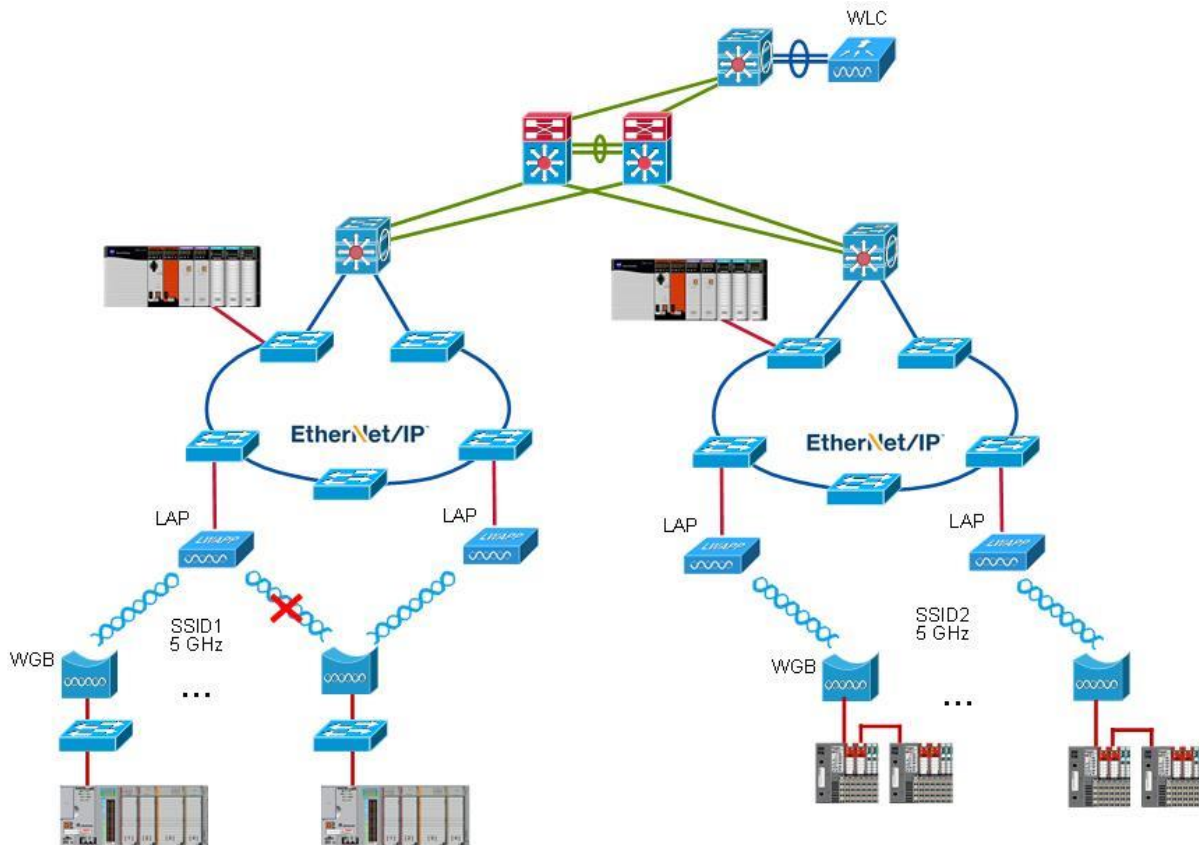


Figure 12 Unified WLAN Architecture

Holistic Defense-in-depth Security

By default, a converged IACS network is generally open. Openness facilitates both technology coexistence and IACS device interoperability, which helps to enable the choice of best-in-class IACS products. This openness also requires that configuration and architecture secure and harden IACS networks. The degree of hardening depends upon the required security stance. Business practices, corporate standards, security policies, application requirements, industry security standards, regulatory compliance, risk management policies and overall tolerance to risk are key factors in determining the appropriate security stance.

No single product, technology or methodology can fully secure IACS applications. Protecting IACS assets requires a defense-in-depth security approach, which addresses internal and external security threats. This approach uses multiple layers of defense (administrative, technical, and physical) at separate IACS levels that address different types of threats. The Industrial Network Security Framework (Figure 13), which uses a defense-in-depth approach, is aligned to industrial security standards such as IEC-62443 (formerly ISA-99) Industrial Automation and Control Systems (IACS) Security and NIST 800-82 Industrial Control System (ICS) Security.

Designing and implementing a comprehensive IACS network security framework should serve as a natural extension to the IACS. Network security should not be implemented as an afterthought. The industrial network security framework should be pervasive and core to the IACS. However, for existing IACS deployments, the same defense-in-depth layers can be applied incrementally to help improve the security stance of the IACS.

Converged Plantwide defense-in-depth layers (Figure 13) include:

- Control System Engineers (highlighted in tan)— IACS device hardening (for example, physical and electronic), infrastructure device hardening (for example, port security), network segmentation (trust zoning), industrial firewalls (with inspection) at the IACS application edge, IACS application authentication, authorization and accounting (AAA)
- Control System Engineers in collaboration with IT Network Engineers (highlighted in blue)— computer hardening (OS patching, application white listing), network device hardening (for example, access control, resiliency), wireless LAN access policies
- IT Security Architects in collaboration with Control Systems Engineers (highlighted in purple)— Identity Services (wired and wireless), Active Directory (AD), Remote Access Servers, plant firewalls, Industrial Demilitarized Zone (IDMZ) design best practices

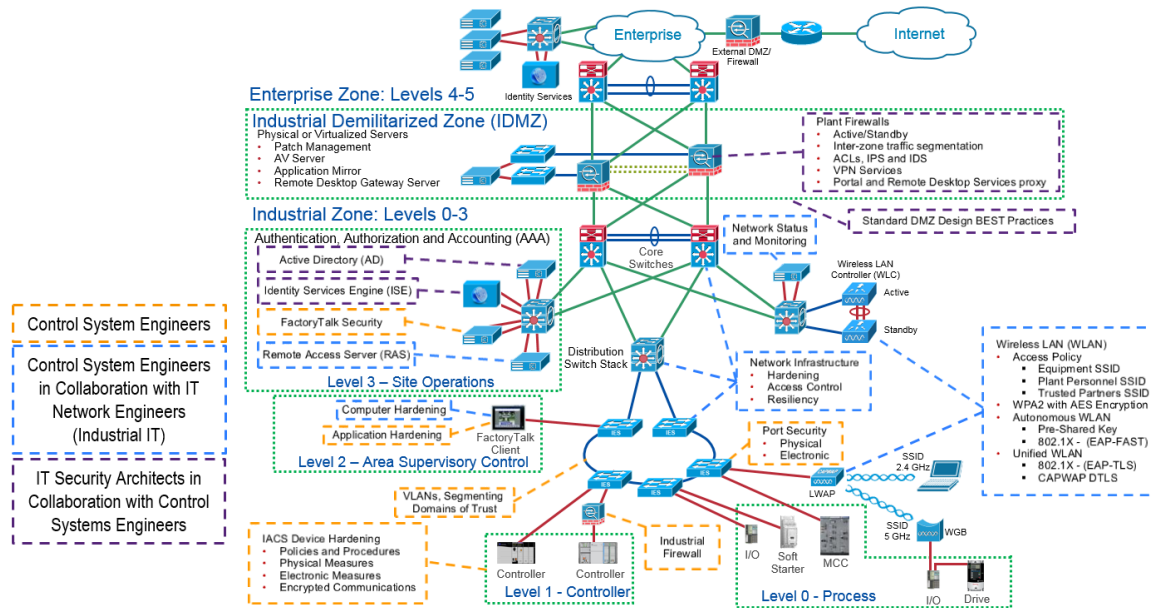


Figure 13 Holistic Defense-in-depth Security

Many organizations and standards bodies recommend segmenting business system networks from plant-wide networks by using an Industrial Demilitarized Zone (IDMZ). The IDMZ exists as a separate network located at a level between the Industrial and Enterprise Zones, commonly referred to as Level 3.5. Sometimes referred to as a perimeter network, the IDMZ is a buffer that enforces data security policies between a trusted network (Industrial Zone) to an untrusted network (Enterprise Zone). The IDMZ is an additional layer of defense-in-depth to securely share IACS data and network services between the Industrial and Enterprise Zones. The demilitarized zone concept is commonplace in traditional IT networks, but is still in early adoption for IACS applications. An IDMZ environment consists of numerous infrastructure devices, including firewalls, VPN servers, IACS application mirrors and reverse proxy servers, in addition to network infrastructure devices such as switches, routers and virtualized services.

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

The management and security of the evolving coexistence of technologies within the plant require an authentication, authorization and accounting (AAA) approach. Identity services is required to support centrally managed secure wired or wireless computer access to the IACS networks by plant personnel and contractors.

Secure Remote Connectivity

Secure Remote Access is a comprehensive and versatile remote-access solution that supports the widest range of connectivity options, endpoints, and platforms to meet your organization's changing and diverse remote access needs. The Secure Remote Access solution gives IT administrators a single point of control to assign granular access based on both user and device. It provides both full and controlled client-based network access to web-based applications and network resources for a highly secure, flexible remote access deployment.

Enterprise Zone: Levels 4-5

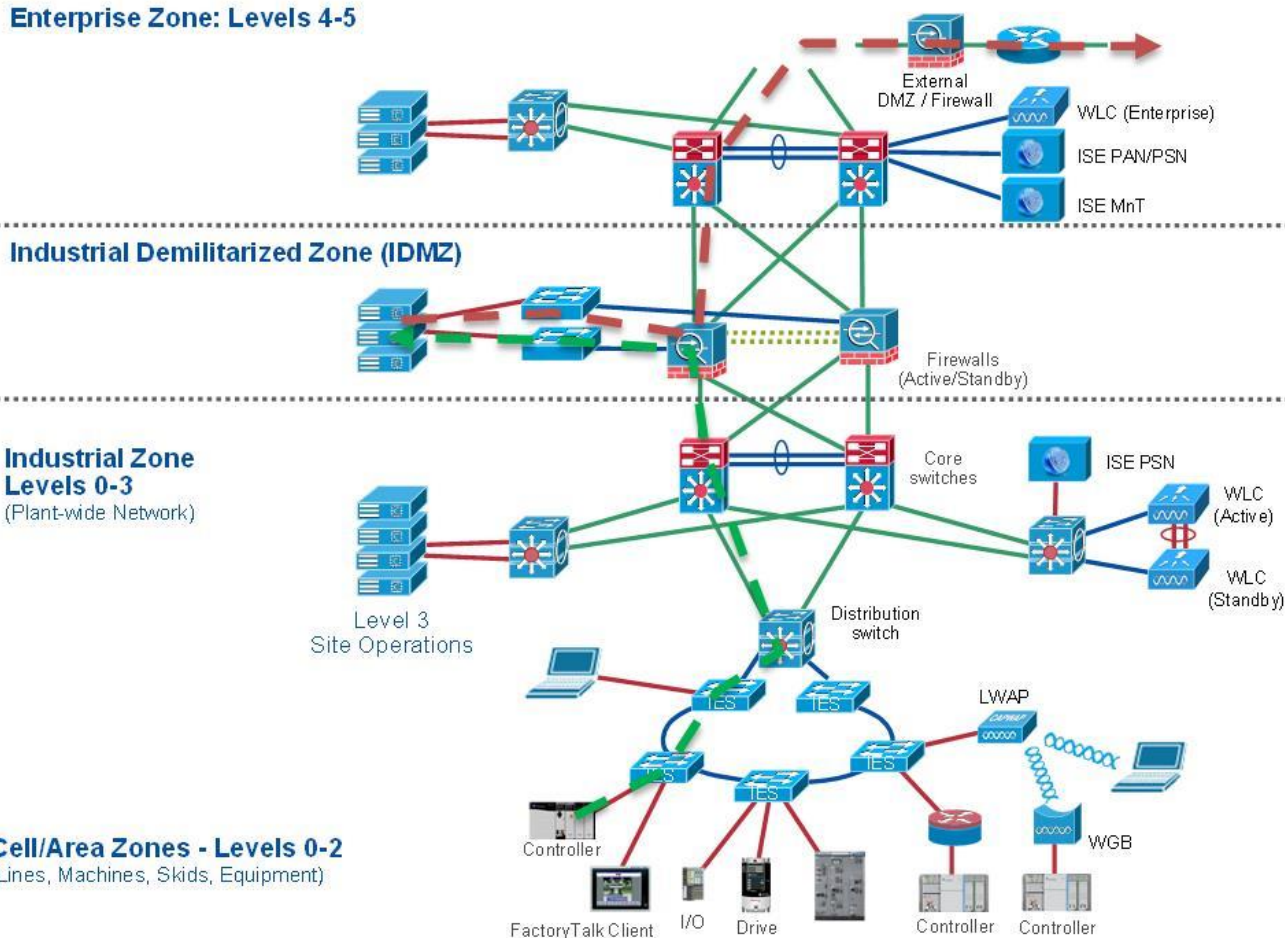


Figure 14 Secure Remote Connectivity

Acronyms and Initialisms

The following is a list of all acronyms and initialisms used in this document.

Term	Definition
IoT	Internet of Things
OT	Operation Technology
IT	Information Technology
NAT	Network Address Translation
IES	Industrial Ethernet Switch
WLAN	Wireless Local Area Network
AP	Access Point
WGB	Work Group Bridge
OEM	Original Equipment Manufacturer
LWAP/LAP	Light Weight Access Point
IACS	Industrial Automation and Control System
VLAN	Virtual Local Area Network
QoS	Quality of Service
IDMZ	Industrial Demilitarized Zone
STP	Spanning Tree Protocol
RSTP	Rapid Spanning Tree Protocol
MSTP	Multiple Spanning Tree Protocol
PVST	Per VLAN Spanning Tree Protocol
REP	Resilient Ethernet Protocol
LACP	Link Aggregation Control Protocol
MRP	Media Redundancy Protocol
PRP	Parallel Redundancy Protocol
HSR	High Availability Seamless Redundancy
DLR	Device Level Ring
HSRP	Hot Standby Routing Protocol
VRRP	Virtual Routing Redundancy Protocol
AD	Active Directory
VPN	Virtual Private Network
IFW	Industrial Firewall
AAA	Authentication Authorization Accounting
ISE	Identity Services Engine
PSN	Policy Service Node
MnT	Monitoring and Troubleshooting
CIP	Common Industrial Protocol
HMI	Human Machine Interface
DNS	Domain Naming Service
DHCP	Dynamic Host Configuration Protocol
NTP	Network Time Protocol
OSI	Open System Interconnection
TCP	Transmission Control Protocol
MTTR	Mean Time To Repair
HTTP	Hyper Text Transfer Protocol
SNMP	Simple Network Management Protocol
RTP	Real Time Protocol
SSH	Secure Shell
OEE	Overall Equipment Effectiveness

References

Cisco Design Zone for Manufacturing - Converged Plantwide Ethernet

http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html

Rockwell Automation – Industrial Network Architectures

<http://www.rockwellautomation.com/global/capabilities/industrial-networks/technical-data/overview.page?>

The ideas, opinions, and recommendations expressed herein are intended to describe concepts of the author(s) for the possible use of ODVA technologies and do not reflect the ideas, opinions, and recommendation of ODVA per se. Because ODVA technologies may be applied in many diverse situations and in conjunction with products and systems from multiple vendors, the reader and those responsible for specifying ODVA networks must determine for themselves the suitability and the suitability of ideas, opinions, and recommendations expressed herein for intended use. Copyright ©2017 ODVA, Inc. All rights reserved. For permission to reproduce excerpts of this material, with appropriate attribution to the author(s), please contact ODVA on: TEL +1 734-975-8840 FAX +1 734-922-0027 EMAIL odva@odva.org WEB www.odva.org. CIP, Common Industrial Protocol, CIP Energy, CIP Motion, CIP Safety, CIP Sync, CIP Security, CompoNet, ControlNet, DeviceNet, and EtherNet/IP are trademarks of ODVA, Inc. All other trademarks are property of their respective owners.