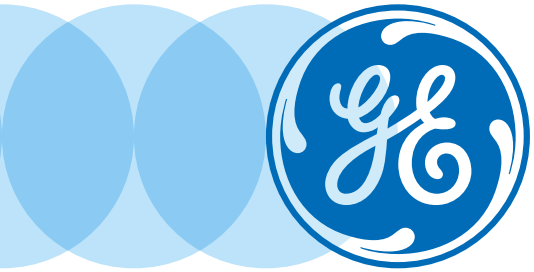
GE's Intelligent Platforms business & CISCO Systems Inc.

Architecting a Robust Manufacturing Network for the Internet of Things

Network Reference Architecture



The Internet of Things (IoT) is creating disruptive opportunities that will define a new set of winners and losers in the industrial space. This white paper provides guidance to chief information officers and associated technologists for implementing network security and designing a robust manufacturing network for the Industrial Internet using the GE-Cisco Joint Network Reference Architecture.

August 2015

Contents

Table of Figures

Abstract

The Internet of Things (IoT) is creating disruptive opportunities that will define a new set of winners and losers in the industrial space. This white paper provides guidance to chief information officers and associated technologists for implementing network security and designing a robust manufacturing network for the Industrial Internet using the GE-Cisco Joint Network Reference Architecture.

This white paper proposes an approach to networks in manufacturing environments, introduces recommended architectures, describes the components of a sound industrial network and highlights areas for special attention, as well as illustrates ancillary benefits when deploying such architectures.

The forces of change

The maturing of the Industrial Internet and the rapid connectivity of devices to internal networks and the Internet are creating fundamental change and significant opportunities for manufacturers. These changes are resulting in the increased need for improved connectivity, network security and management capabilities.

Pace of change

Change is happening at orders of magnitude faster than it did 10 years ago. Startups can develop a product on the back of a credit card and go viral overnight. Traditional industries have been turned upside down, creating a new set of winners and losers. Consider the following examples:

- **Retail**—Amazon threatens brick-and-mortar establishments.
- **Advertising**—Google alters Madison Avenue with targeted web advertising.
- **Hospitality**—Airbnb exercises underutilized assets to turn homes into hotels.
- **Transportation**—Uber circumvents a regulated cab industry.

Similar forces are impacting manufacturing. Take, for example, the flattening of networks. Social networks provide instantaneous insight into customer sentiment, allowing manufacturers to get a jump on product changes. Natural disasters and geopolitical unrest can shift logistics networks overnight, forcing rapid reactions in manufacturing planning.

Similarly, the networks that move data within your manufacturing environment are flattening as Internet Protocol is brought to the control interface and embedded in "smart instruments." The flattening of the manufacturing network creates opportunities for a more inclusive and responsive plant.

Opportunity for competitive agility

Consider the opportunity for competitive agility as:

- Previously unconnected devices become connected to each other in machine-to-machine (M2M) networks and to enterprise reporting and predictive analytics, providing unprecedented real-time feedback on product performance, service and maintenance;
- IT hardware needs are reduced as virtualization removes the need to deploy physically separate networks while still achieving a high-performance and secure environment for manufacturing mission-critical plant floor applications;
- IT maintenance overheads are reduced as manufacturing applications move to private and public cloud;
- These new insights are now shared across the enterprise to enable more than just control, but also can help boost yield, performance, quality and reduce waste;
- And business decisions can be made quickly by analyzing vast data farms, making actionable data available to the user's device of choice.

For manufacturers, these insights enable a cycle of continuous plant improvements for:

- Shortening warranty investigation time
- Cutting work-in-process inventory
- Reducing manufacturing costs
- Improving product cycle times
- Decreasing rework and scrap
- Reducing uncertainty in the supply chain

Leading manufacturers have already realized the benefits of real-time, shop-floor-to-business systems connectivity through

- Common skill sets across information technology (IT) and operations technology (OT) technicians

- Secure data flow between the plant floor and the cloud
- Real-time plant floor visibility to enterprise planning tools
- Reduced downtime with proactive and preemptive maintenance planning
- Manufacturing agility that makes a "lot size of 1" achievable
- Insight and control over energy and utilities in real time
- Visibility and control of remote facilities and resources

The IoT and II

The Internet of Things (IoT) is a concept in which everyday objects have network connectivity, allowing them to send and receive data.

The Industrial Internet (II) refers to the integration of complex physical machinery with networked sensors and software. The Industrial Internet draws together fields such as machine learning, big data, the Internet of Things, machine-to-machine communication and cyber-physical systems to consume data from machines, analyze it in real time and use it to adjust operations.

In simple terms, the IoT is the "idea" and the II is the "plumbing" that makes the IoT work.

Growth in connected devices is widely predicted to be enormous with estimates ranging from 30 billion to 50 billion devices connected by 2020. There are a number of reasons for this growth, including the following factors:

- The price of sensors, processors and networking has dropped to a point that makes it economically viable.
- Wi-Fi is now widely deployed and it is now relatively easy to add new networked devices in the home and in the office, as well as on the shop floor.
- The new version of the Internet Protocol IPv6 enables an almost-limitless number of devices to be connected to networks.
- Major providers Cisco, IBM, GE and Amazon have put their weight behind the IoT with network changes, enabling dramatic simplification and cost reduction for network connectivity.

Not least are new forecasts regarding the IoT opportunity. GE estimates that the Industrial Internet has the potential to add between $10 trillion and $15 trillion to global GDP over the next 20 years, and Cisco increased its forecast to $19 trillion for the economic value created by 2020.

All of this creates tremendous opportunities for business while introducing new challenges for CIOs:

- **Device proliferation**—Ten years ago, CIOs could oversee policies, which provided a reasonable level of control over who and what approved devices were connected to their networks. With the proliferation of smartphones and tablets, CIOs have needed to administer "bring your own device" (BYOD) policies to enable greater productivity. Additionally, IoT technology will connect more devices and sensors than ever to both the manufacturing and enterprise networks. Cisco offers wireless network and security technologies to address the above needs.
- **Security**—Building separate networks and "air gapping" are not solutions to security challenges, with Stuxnet being a primary example of how these methods fail. Obscurity makes an attack only more difficult for the novice hacker. Furthermore, the sophistication of attacks has increased and merely installing firewalls is not sufficient. Real security comes from consistent policy and controls, collection of security data at every level of a system, constant examination of the data, and diligent reaction to signs of trouble, Utilizing the common/converged network and security architecture discussed later in this paper enables common policy, ubiquitous data collection, and multiple levels and methods of security enforcement.
- **System recovery**—Even if a manufacturing network is designed for zero downtime, the systems connected to it may go offline. This can be both planned (system upgrades, additions, etc.) and unplanned downtime. Additionally, system startup can create huge demands on networks as devices come back online and resynchronize data, resulting in sluggish performance. The GE and Cisco approach includes high-performance networking technology coupled with "store and forward" resynchronization of data, enabling just the "missing time" data to be synchronized, rather than everything from time zero. GE's software supports high-availability hardware, hot standby and mirroring techniques to prevent data loss for mission-critical applications. This provides high levels of data reliability and increased read performance.
- **Isolation**—Most manufacturing floors are broken up by process and further into cells and zones. Isolation is sometimes considered to be a substitute for security, but isolated (unconnected) machines can neither be remotely administered nor monitored. Nor can they provide valuable data to higher-lever manufacturing systems. The GE and Cisco approach is to connect all these pieces together on a single network that allows for flexibility of retooling a plant floor, collecting data and administering an optimized process, while at the same time providing logical segmentation of systems.
- **Mobility**—The mobile revolution in the consumer and enterprise space is quickly finding its way onto the shop floor. Flexible communication is an important aspect of mobility. There has been a longstanding need for voice communication using push-to-talk (PTT) radio systems combined with cell phones. Another need is remote access or virtual access to your plant operational systems and analytics from anywhere. Additionally, the industry is introducing a variety of devices to act as remote or virtual HMIs. Finally, video from portable devices is increasing. The network must accommodate and provide services for all these applications. Cisco and GE provide solutions to support mobile devices and mobility for manufacturing.

The GE-Cisco Joint Network Reference Architecture

Why GE and Cisco are providing this capability

GE possesses deep knowledge of controls and manufacturing applications. Cisco has unparalleled experience in networks, network and system security, and collaboration. With more factory assets connected to the network, an increase in data being collected from manufacturing processes, and the emergence of collaboration technology onto the plant floor, GE and Cisco are combining resources to provide an end-to-end solution from the machine interface to the cloud.

Enterprise-class networks with industrial-class form factors

Figure 1 shows a high-level network architecture for manufacturing. Note the myriad of systems that require connectivity in a modern manufacturing enterprise from a simple sensor to cloud-hosted business, analytics and logistics systems. This architecture is not dissimilar to an enterprise campus model (see Cisco Enterprise Campus 3.0 Architecture design guide), with the primary distinction being that a plant-wide network must be ruggedized and support differentiated access for processes and tools not seen in the enterprise. Ethernet and Wi-Fi offer standardized connectivity to allow all components of the manufacturing enterprise to communicate.

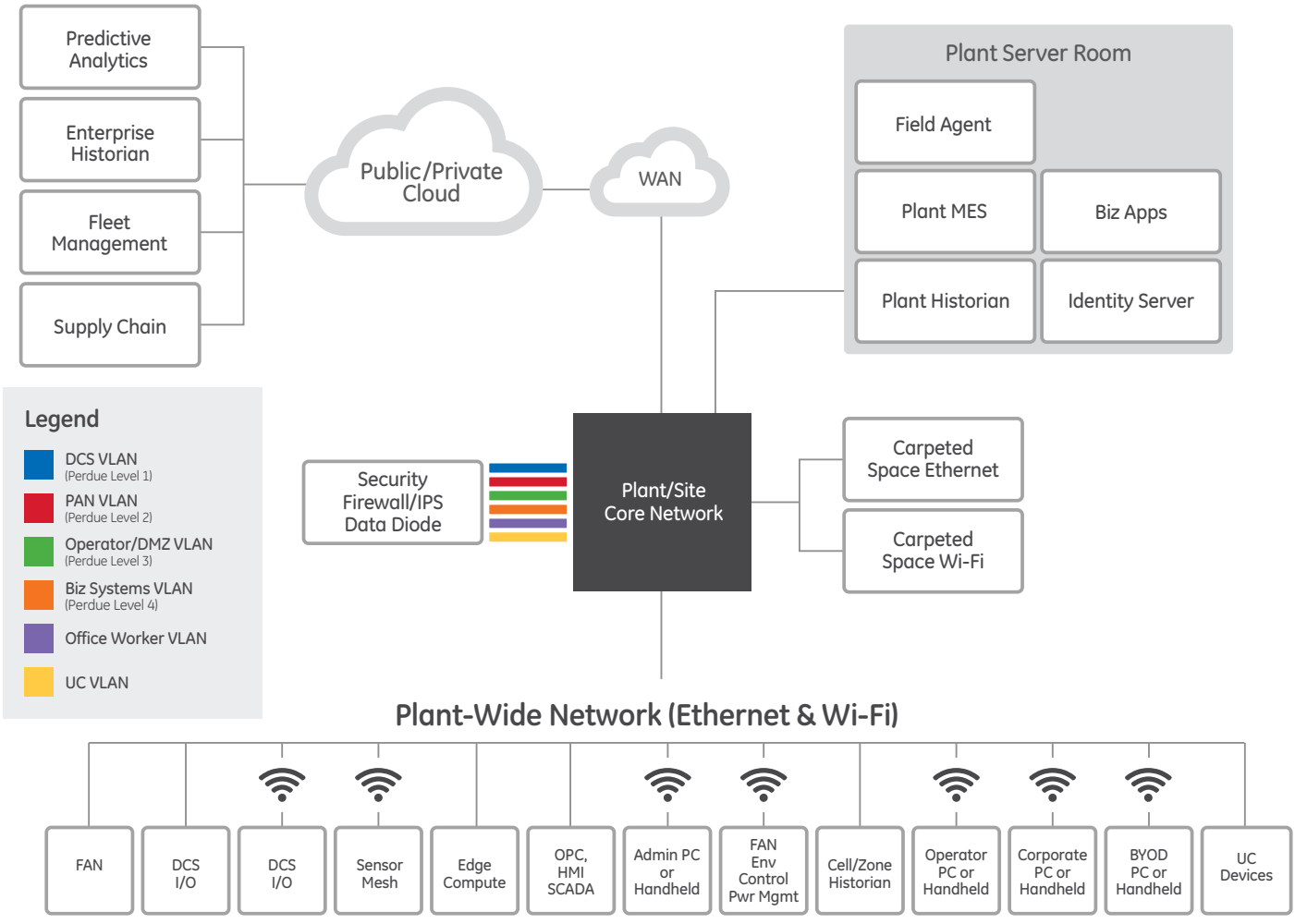


Figure 1: Overall Plant Network Architecture

The ubiquity and capabilities of Ethernet make it possible to collect information in unprecedented volumes and to connect processes that were previously isolated/ un-instrumented. The network is a key enabler of big data. Cisco has long been the world's leading Ethernet switching company and now offers enterprise-class network capabilities in industrial form factors.

The Cisco Industrial Ethernet family of switches (IE2000, IE3000, IE4000, and IE5000) extend the proven Cisco Catalyst technologies prevalent in enterprise networks to industrial networks. These switches provide superior security, video and voice services to industrial applications. They are easy to manage, resilient, and enhanced through support of industry protocols. The series offers IP20-, IP30- or IP67-certified form factors for deployment in the simplest to harshest environments.

Similarly, Cisco brings Wi-Fi leadership to support mobility in industrial applications. Cisco offers both traditional and ruggedized IEEE 802.11 access points (APs), all running on the same OS within the same administrative domain. APs can be deployed in lightweight (controller-based, CAPWAP) or autonomous (stand-alone) mode. Standard wireless LAN, mesh, sensor network (IEEE 802.15.4) and bridged architectures are all supported.

Performance, scale and manageability

Traditional bus-based industrial networks such as PROFIBUS and DeviceNet have limited throughput and supported topologies. Also, troubleshooting such networks can be complex. A standards-based Cisco switching network supports topological flexibility, multi-gigabit or multi-terabit throughput, and common tools (commercial off-the-shelf-software) for administration, ensuring customers are ready for increased data collection on the plant floor. To a GE Software customer, this means reliable and predictable performance across the shop floor and business systems.

Furthermore, Cisco has an enormous worldwide partner (systems integrator, VAR) community, and has certified tens of thousands of engineers and technicians in the configuration and operation of Cisco products. Therefore, OT managers no longer need to struggle to find experts in specialized network technologies as they do today.

Some of the capabilities Cisco offers to provide scalable, high-performance plant networks include the following:

- **Time sensitive networking (TSN)** (future capability)—Scheduled Ethernet for time-sensitive control loops
- **Routing / layer-3 switching**—Allows hierarchical scaling and segmentation for truly huge industrial networks
- **Access control**—Provides treatment of traffic based on attributes like source, destination address or protocol types among other attributes
- **Precision Time Protocol (PTP)**—Machine clock synchronization across a network to the µsec or sub-µsec range, supporting measurement and control systems

Additionally, to ease network bandwidth utilization, GE's industrial software uses exception-based reporting and client-side data compression.

Network segmentation

The throughput increase provided by Ethernet allows multiple traffic types to share the same "pipe" while being segmented for the GE portfolio, operating at each level for:

- **Control**—Using GE programmable logic controllers (PLC) and human-machine interfaces (HMI) that have µsec needs and have uptime requirements critical to shop-floor operations
- **Supervision**—Class-leading GE supervisory control and data acquisition (SCADA) systems that are designed to meet the demanding needs of operators in a production environment
- **Industrial big data collection and management**—GE's historian is designed to manage huge volumes of very fast data needed for data aggregation from SCADA and the provisioning of data for advanced equipment analytics
- **MES / MIS**—Where the shop floor meets the business systems and where time-series data is combined with transactional data to provide operational context
- **Remote monitoring and diagnostics (RM&D)**—For which GE provides class-leading managed and on-site solutions

In general, there are three inflection points where huge value is created when deploying these GE technologies:

- Automating machine operation through the deployment of GE control and HMI/SCADA
- Connecting these subsystems with the historian to provide an unified view of the shop floor
- Connection with business systems such as ERP, PLM and EAM to deliver operational context

Most manufacturing floors are broken up by process. There are clear differences between discrete, batch and continuous processes and how the segmentation of the network may take place. Network segmentation and zone segmentation do not necessarily need to align yet, for administrative or technological reasons, a cell or zone cannot be limitless in size. The network must be built using sophisticated feature-rich equipment to provide flexible segmentation options, limit overhead to protect control traffic and provide secure connectivity between segments.

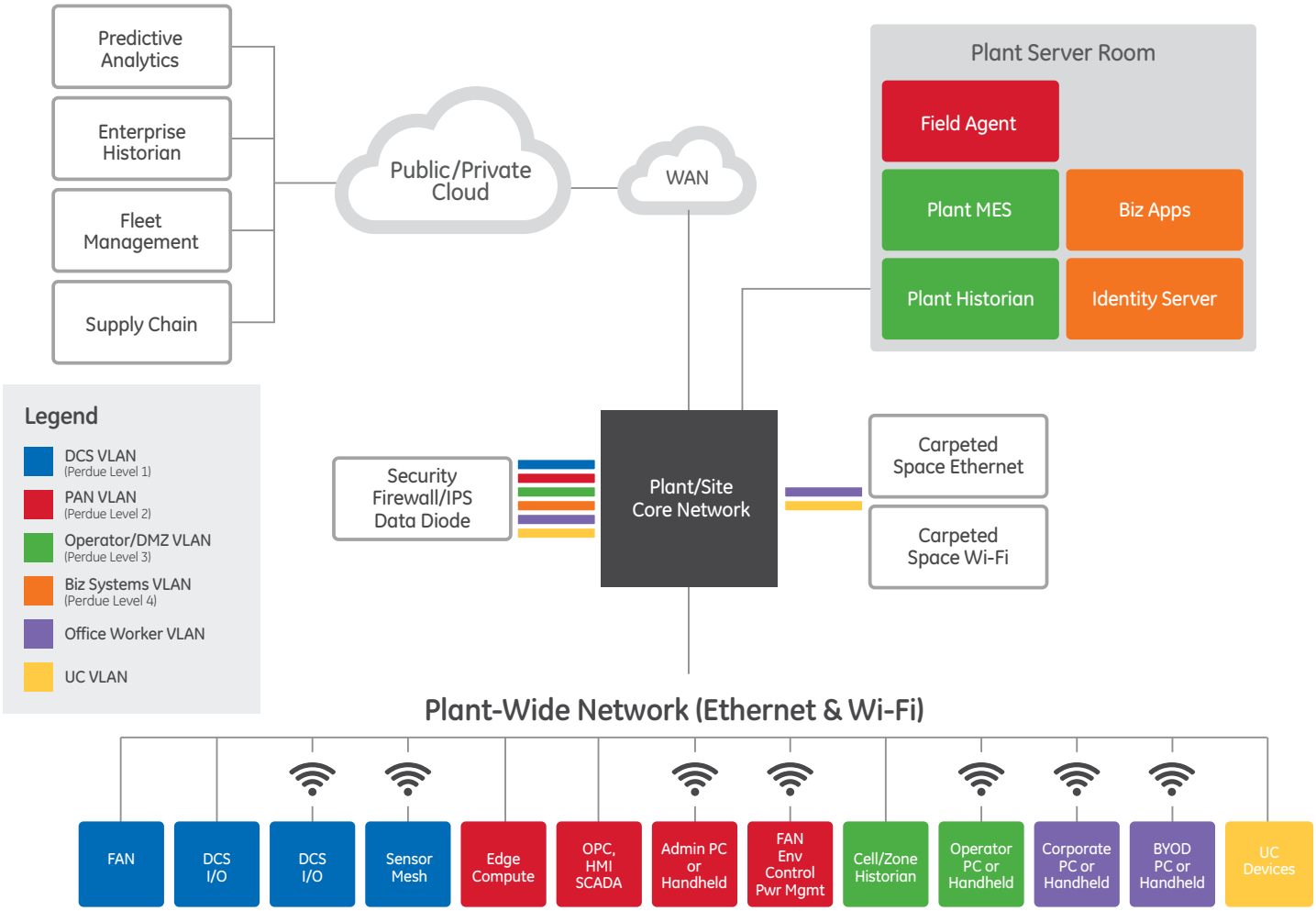


Figure 2: Plant Network Segmentation

Figure 2 highlights how the plant architecture can be logically segmented to address operational, regulatory and security concerns. By utilizing VLANs, differentiated services can be applied to equipment of common capability. For example, equipment belonging to the same Perdue Level 1 group would be connected to the same VLAN plant-wide. "East-West" communication among the members of this group is guaranteed, while "North-South" communication can be restricted through various methods (detailed later).

Firewall, IPS and data diodes

Boundary protection is a requirement for a converged manufacturing network. OT teams typically desire isolation between cells/zones/stages of the manufacturing floor, whether as a security or operational boundary. However, isolation cannot accommodate the need to collect, aggregate, analyze and utilize manufacturing data for business and logistics needs. Using firewalls and other security appliances provides connectivity while at the same time protecting manufacturing assets.

The Cisco ASA firewall protects against advanced threats while reducing complexity and cost. The ASA also integrates Sourcefire IPS to deliver integrated threat defense across the entire attack continuum, including "out-of-the-box" support for common protocols used by GE devices, and is extensible to support custom industrial protocol definitions. The ASA can be deployed in a stand-alone configuration—with separate boxes at every layer—as shown in figure 3. The ASAs protect and limit traffic between manufacturing VLANs.

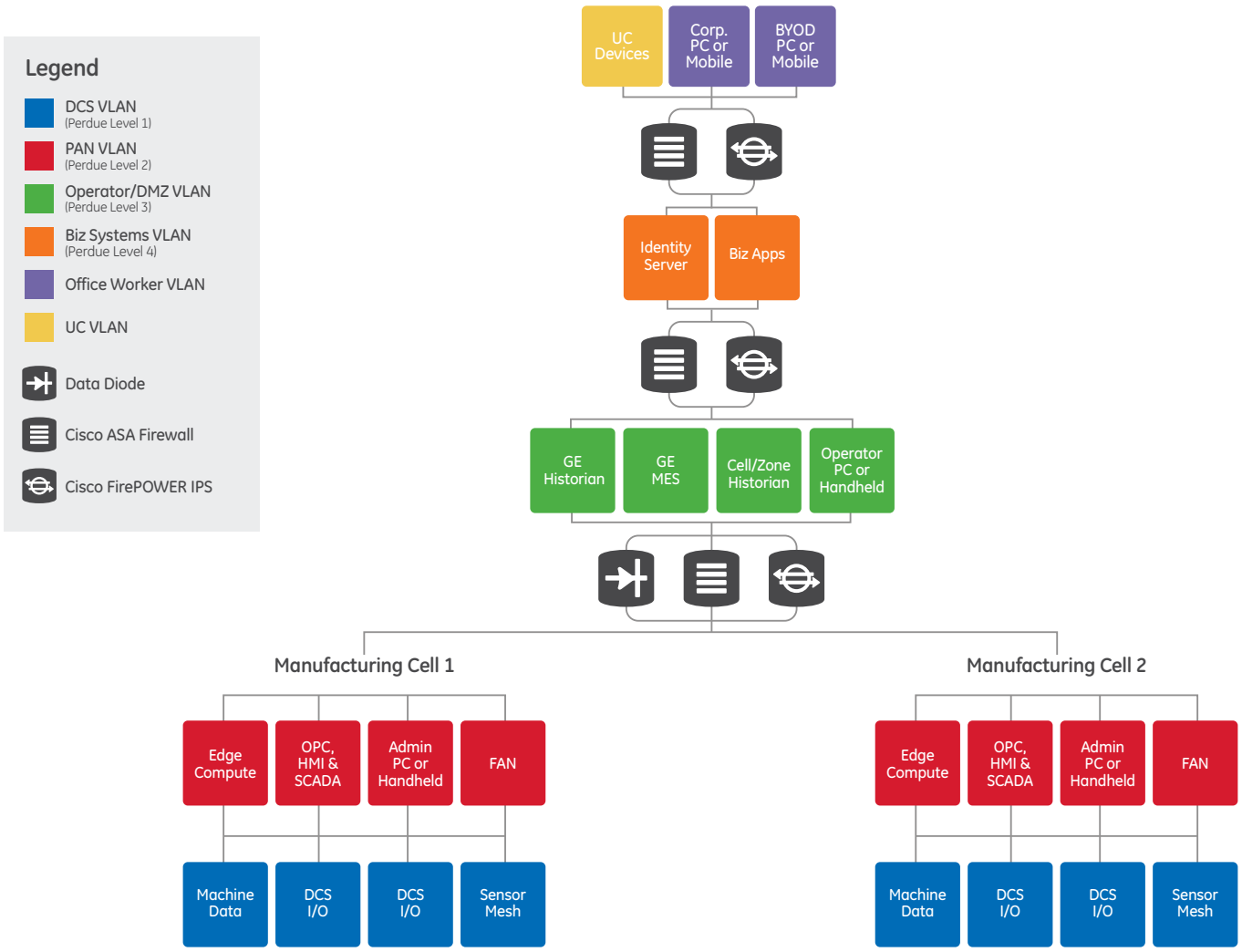


Figure 3: Plant Network Security Logical Architecture

The ASA can also be deployed in multiple context modes, as shown in figure 4. In this model, an ASA appliance is logically separated into multiple virtual firewall/IPS instances. Each virtual instance has its own independent configuration and has no awareness of or dependence on any other firewall or IPS instance running on the same hardware. Using multiple contexts, it is possible to use a single high-scale ASA firewall appliance trunked into the core switches as shown in figures 1 and 2.

There are some manufacturing use cases that require data diodes to guarantee one-way data transfer (*from* the machine *to* higher-level software). Whereas neither Cisco nor GE make data diodes, our reference network model for manufacturing certainly supports them, as seen in figures 3 and 4.

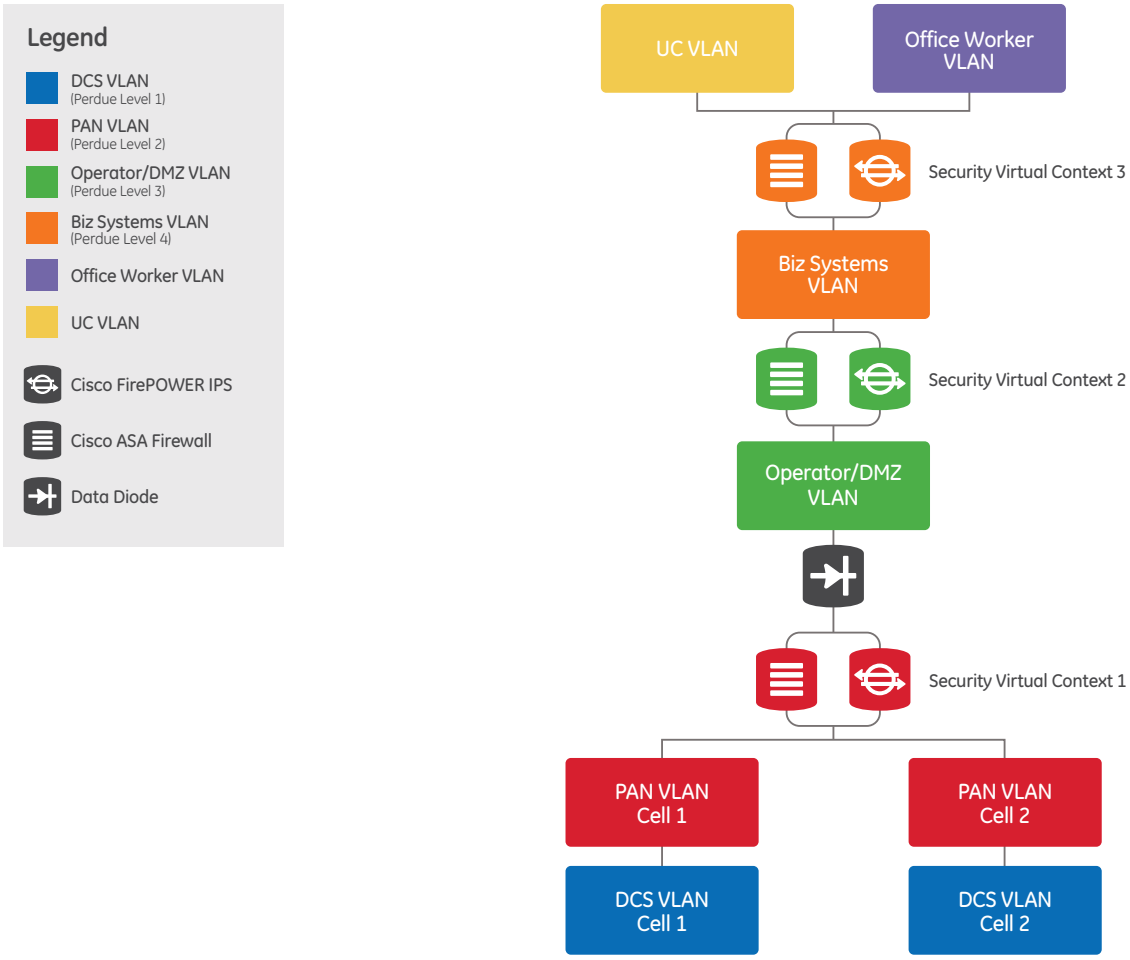


Figure 4: Plant Network Security Virtualization

Identity networking

Modern plant operations require identifying the right person on the right device on the right network at the right time. Service access ports for machines are an example of this. When a technician enters the plant to fix a problem, the technician's PC should not be given unfettered access to the network—just to the machine in question.

The technician's system should be recognized as unauthorized to connect to any port on the network other than the service port for the machine.

Conversely, an administrator using a corporate-owned computer, up to date on all security software and using the correct credentials, should be allowed to connect to any network (wired or via Wi-Fi) and access any system. Using Cisco Identity Services Engine (ISE) and 802.1X on network infrastructure, differentiated, identity-based connectivity can be achieved.

ISE provides a rules-based, attribute-driven policy model for creating flexible and business-relevant access control policies. It provides the ability to create fine-grained policies by pulling attributes from predefined dictionaries.

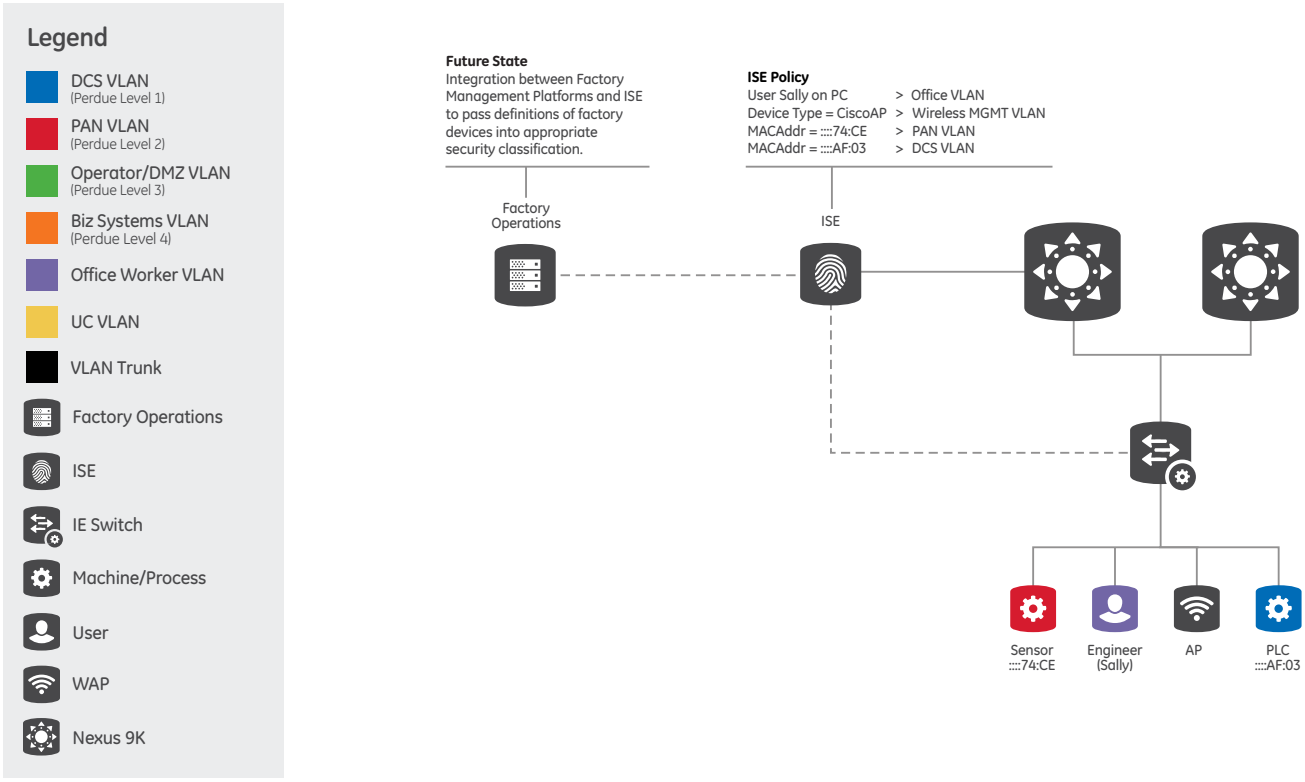


Figure 5: Plant Network Dynamic Port Provisioning

These sources include information about user and endpoint identity (e.g., GE PLCs), role-based security, posture validation, authentication protocols, location or other external attributes from Active Directory, LDAP, RADIUS, RSA OTP and certificate authorities. GE Software products feature S95-standard data models with the ability to identify accessibility to equipment, certification requirements, and system/capability access. A manufacturing enterprise could use these data models as a baseline reference for its ISE policy.

The example in figure 5 shows how ISE can be used to provide differentiated access on a plant floor. The ISE configuration has user Sally the Engineer assigned to the Office VLAN based on her credentials and devices used, while the GE PLC with MAC address :::AF:03 is assigned to the DCS VLAN. As users/devices attempt to connect, ISE is consulted and the network infrastructure assigns VLANs accordingly. Furthermore, ISE can be configured for conditional connectivity.

For example, Sally the Engineer may be assigned to the Office VLAN using her PC, but may be assigned to the PAN VLAN when connecting via Wi-Fi using a corporate-controlled handheld device on the shop floor.

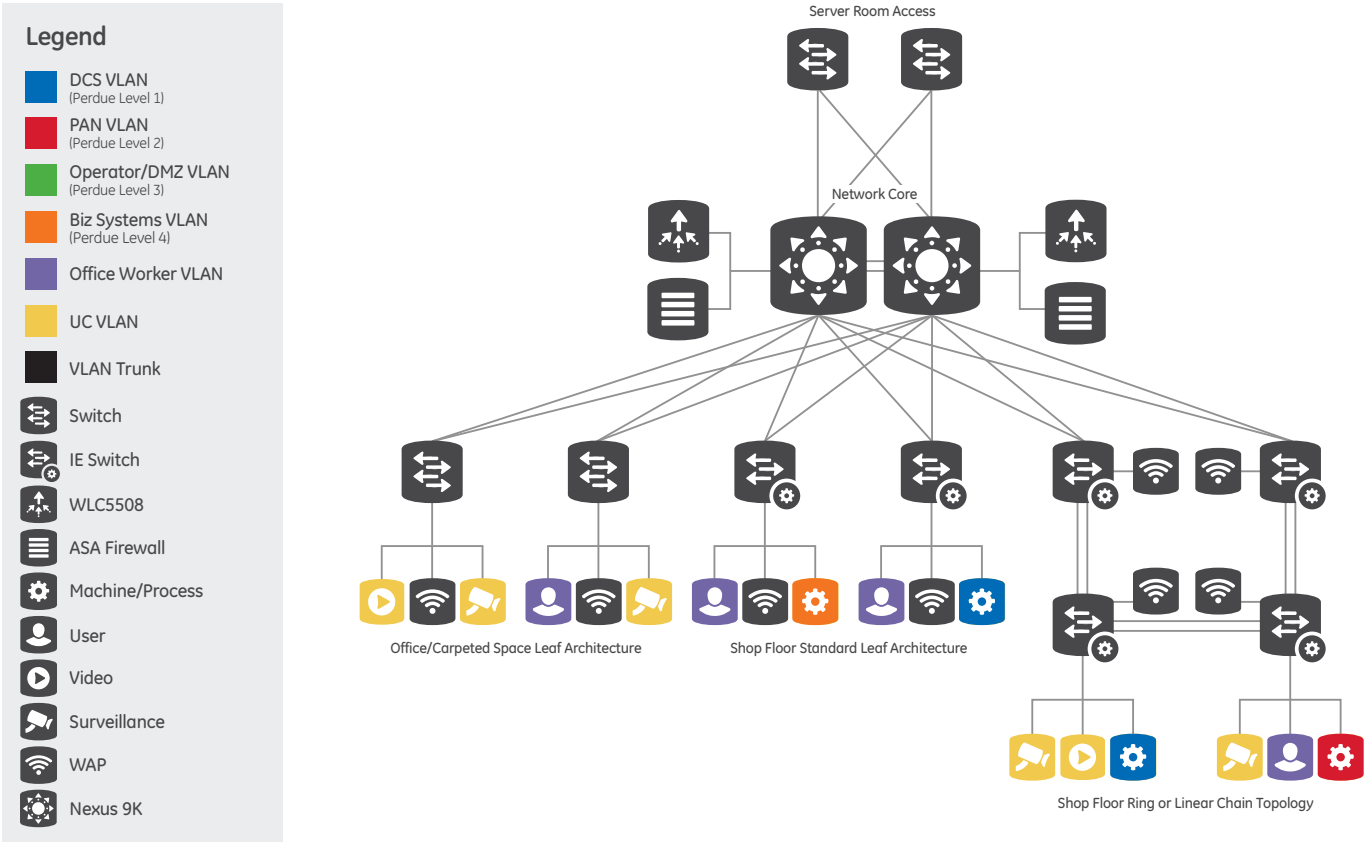


Figure 6: Plant Network Physical Architecture

Encryption

Data encryption is a good practice in most industries, but is mandated in regulatory-controlled environments such as U.S. Export Control. There are multiple methods for encrypting data at rest (OS-level encrypted volumes for example). Similarly, data in flight can be encrypted through multiple methods. Cisco offers link-layer, hop-by-hop encryption (e.g., MACsec for Ethernet or WPA for wireless), as well as end-to-end encryption (e.g., IPSEC VPN). IPSEC is particularly useful for long-haul (WAN) data integrity to address regulatory and corporate policy needs.

IP address reuse

In industrial networks, the task of assigning and reassigning IP addresses can be very cumbersome, as few industrial applications use DNS or DHCP. In some cases, equipment is literally too old to support DNS/DHCP (e.g., devices where the IP address is set through dip switches). In other cases, the traditional convention dictates that hard-coded IP addresses are more reliable because they do not require upper-level services.

Until DNS/DHCP is considered robust enough for industrial applications, administrators must design around their absence. Figure 6 shows a more detailed physical-level representation of the plant network described in figures 1 through 4. The overall architecture is spine-leaf or collapsed-core, with traditional Cisco switches servicing office space and Cisco Industrial Ethernet (IE) switches on the plant floor.

As described earlier, VLANs for common processes/capabilities span the infrastructure. The machine on the DCS VLAN in the "Shop Floor Standard Star Topology" and the machine on the DCS VLAN in the "Shop Floor Ring or Linear Chain Topology" may have the identical hard-coded IP address. They may have both been put on this VLAN during a retooling of the shop floor. Normally, the IP address conflict would cause communication challenges or failures to both machines, but administrators can enable the L2 NAT feature on the IE switches to have one or both of the machines translated to a new address to resolve conflicts and ease deployment of the GE control system more quickly.

Similarly, both the DCS VLAN and the PAN VLAN may be using the same subnet for historical reasons at a particular factory. For example, both may be 192.168.1.0/24 network. Again, using NAT on the network infrastructure can translate the entire subnet to a new address range if necessary. Another method, connected routing, can also be employed to work around the overlapping range problem.

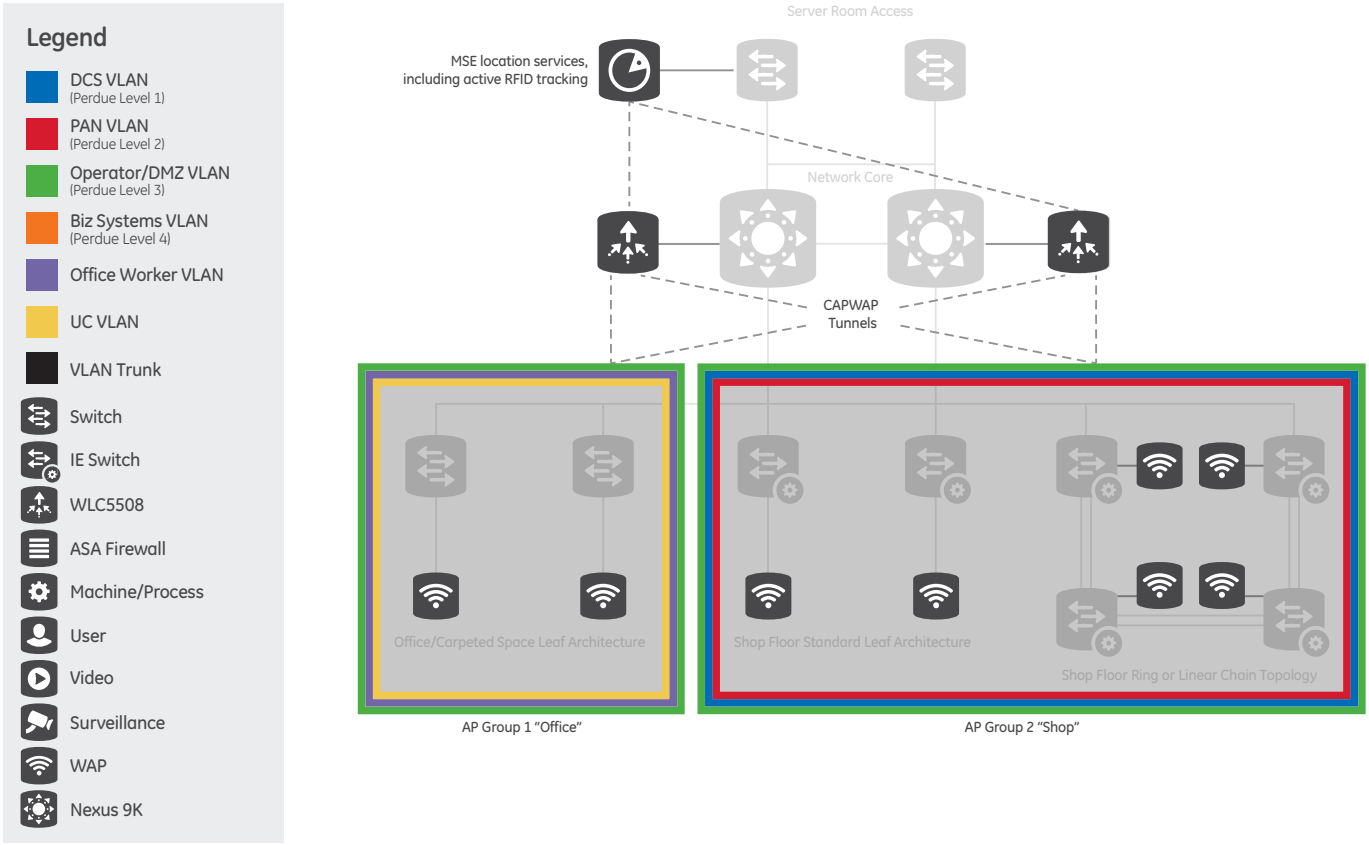


Figure 7: Plant Network Wireless Architecture

Wireless services

Wi-Fi to the plant floor is enabling mobile access to GE HMI interfaces and MES applications. This new flexibility introduces access and security issues similar to wired networks. Figure 7 shows how wireless services are overlaid on the plant network model. For ease of deployment, Wireless LAN Controllers (WLCs) are commonly used. Cisco WLCs support system-wide functions and deliver centralized wireless policy, management and security. Wireless Intrusion Prevention System (wIPS) capabilities and quality of service (QoS) for voice and video are also enabled by the WLC. Additionally, the WLC feeds telemetry data to the Cisco Mobility Services Engine (MSE). The MSE primarily provides location services and helps organizations increase visibility into the network, customize location-based mobile capabilities and strengthen security.

Location services

There are multiple ways in which WLC and MSE provide location-specific services for manufacturing. WLC AP Groups allow for a single wireless administrative domain with common Service Set Identifiers (SSIDs) and features, but restrict which VLANs may exist upon which access points in the network. In figure 7, two AP Groups—one for office space APs and another for shop floor APs—are utilized to assign only those VLANs that belong within each area. In the figure, the Operator, UC, and Office VLANs are allowed in the "Office" AP Group while the Operator, DCS, and PAN VLANs are allowed on the "Shop" AP Group. Working in concert with ISE, the WLC gives the flexibility to authorize only specific users on specific devices in specific locations to access specific VLANs.

WLC plus MSE can provide location-based mobile services, such as pushing mobile alerts to an iOS device based on a warning or emergency in the plant. WLC/MSE APIs can also be used to integrate with GE and third-party apps to notify an operator to service a machine, and provide a map of the route to the machine. Using active Radio Frequency Identification (RFID) technology, WLC/MSE services can pinpoint the location of tools (e.g., a forklift) or inventory items (e.g., a pallet or barrel of raw materials) that have an RFID tag affixed. Similarly, users/operators/technicians can be tracked on the plant floor based on the beacons from their Wi-Fi-enabled devices for safety or compliance reasons. Within the GE portfolio, real-time operational intelligence (RtOI) is able to identify the location of equipment and people and provide a personalized experience based on who you are, where you are and what equipment is within your proximity.

RF integrity

As handheld and mobile devices become more pervasive in manufacturing, availability of a stable, reliable, high-performing Wi-Fi network is paramount. Cisco provides RF integrity in several important ways:

- **Interference detection**—A Cisco Wi-Fi network "listens" for potential interference sources (e.g., a microwave oven) and can alert the administrator and pinpoint the location of the interference.
- **Intelligent channel selection**—The system automatically selects the best channel per access point to maximize coverage based on interference and overlapping Wi-Fi networks.
- **Heat maps**—A visual representation of the RF environment using Cisco's wireless management tool. Heat maps allow administrators to reposition APs for better coverage.
- **Automatic signal strength adjustment**—In the event of an AP failure, remaining APs automatically adjust their channels and signal strength in an attempt to cover the RF "hole" until the failed AP is replaced.
- **Antenna design**—An antenna gives a wireless system three fundamental properties: gain, direction and polarization. Cisco offers several different antennas that vary these properties in order to provide the right coverage pattern for a specific application.

Wireless security

In addition to providing authentication and link encryption as stated above, Cisco Wireless LAN systems offer a number of other security capabilities at each component level. Cisco APs with Cisco CleanAir® technology are equipped with silicon-based intelligence to allow for Layer 1 threat detection of attacks that may come from non-802.11 sources, such as video cameras or RF jammers.

APs intelligently process over-the-air traffic to a large library of wireless intrusion attacks and anomalies to determine whether the network is being attacked or impersonation is in progress. APs relay information such as the MAC address of the victim and attacker, received signal strength indication (RSSI) and time of attack to the WLC. The WLC generates traps to the network management system when security events such as rogue access points are detected or an attack is in progress, as well as mitigates rogue threats as defined by the rogue policy.

The MSE then correlates security events by eliminating duplicate security events and computing an x,y location for all valid clients, clients connected to rogue access points, attackers and non-802.11 interferers. The administrator then uses the location data generated to do forensics and/or physically remove the threat from the area.

Rich media services, compute and cloud

By building an intelligent, converged plant network as described in this paper, IT/OT professionals enable more than just the manufacturing processes and machines. They are building a platform on which additional technologies for manufacturing can be deployed, including video analytics, factory collaboration, edge compute for real-time analytics (Cisco IoX), unified computing systems (UCS) and the service exchange platform (SXP). While a detailed discussion on these technologies is beyond the scope of this paper, numerous resources about them are available at cisco.com

Conclusion

The Industrial Internet of Things is creating disruptive opportunities that will define a new set of winners and losers. Together, GE and Cisco offer customers a world-class manufacturing portfolio that is unrivaled in its ability to feature both a proven global track record as well as Internet of Things technical leadership.

With the GE-Cisco joint architecture, manufacturers can confidently deploy a next-generation system that is scalable and secure—enabling higher productivity for each employee and greater efficiency for each process. It helps manufacturers achieve the critical goals of reducing WIP, cycle times and waste.

In today's connected world, manufacturers can gain a competitive advantage by driving insight and intelligence closer to the machines with the GE and Cisco approach, making the manufacturing plant more integral to the operations of the enterprise.

Glossary

802.11
An IEEE specification for WLANs

802.15.4
An IEEE specification for LR-WPANs

802.1X
An IEEE specification for network authentication

ANSI
American National Standards Institute—an organization promoting and facilitating voluntary consensus standards

AP
Access point—the network device users connect to in Wi-Fi

ASA
Adaptive Security Appliance—a family of network security devices from Cisco that provide firewall, IPS and VPN capabilities

BYOD
bring your own device

CAPWAP
Control and Provisioning of Wireless Access Points—IETF standard for the wireless control protocol utilized by WLCs

DCS
distributed control system

DMZ
demilitarized zone—a network segment that is logically or physically separated from the internal network

Ethernet
A wired link-layer networking protocol defined by IEEE 802.3 standards

firewall
A device that controls/limits/blocks traffic flow between different networks/segments

HMI
human-machine interface

IEC
International Electrotechnical Commission—an organization for the preparation and publication of international standards for all electrical, electronic and related technologies

IEEE
Institute of Electrical and Electronics Engineers—organization that develops standards for the computer and electronics industry

IETF
Internet Engineering Task Force—defines Internet protocol standards

II
Industrial Internet

IoT
Internet of Things

IoX
An edge computing platform built into some Cisco network devices

IP
Internet Protocol—the primary protocol/framework used in Internet communication

IP20
Ingress Protection Rating 20—rating for physical intrusion and moisture protection defined in international standard ANSI/IEC 60529

IP30
Ingress Protection Rating 30—rating for physical intrusion and moisture protection defined in international standard ANSI/IEC 60529

IP67
Ingress Protection Rating 67—rating for physical intrusion and moisture protection defined in international standard ANSI/IEC 60529

IPS
Intrusion Prevention System—devices that monitor networks for malicious activity

IPSEC
Internet Protocol Security—a set of IETF protocols for authenticating and encryption network traffic

ISE
Identity Services Engine—a Cisco product that enables the creation and enforcement of security and access policies for endpoint devices

IT
information technology

LAN
local area network—a system that connects devices within a facility

LR-WPAN
low-rate wireless personal area network—an IEEE low-power, low-rate wireless transmission standard

M2M
machine to machine

MACsec
Media Access Control Security—industry-standard link security method defined in IEEE 802.1AE

MES
manufacturing execution system

MSE
Mobility Services Engine—a Cisco platform that uses Wi-Fi to increase visibility into the network, deploy location-based mobile services, and strengthen security

NAT
network address translation—the process of translating one IP address or block to another for security or address reuse purposes

OT
operations technology

Glossary (continued)

PAN
personal area network—wireless technology intended to connect devices within a very limited range

PTP
Precision Time Protocol—a time synchronization protocol defined by IEEE 1588 standard

QoS
quality of service—the capability of a network to provide better service to selected network traffic types over others

RF
radio frequency

RFID
Radio Frequency Identification—a technology that utilizes electronic tags with unique wireless identities

RSSI
Received Signal Strength Indicator—a measurement of the power in a received radio signal

SSIDs
Service Set Identifier—the name assigned to a Wi-Fi network

switch
An Ethernet device that connect computers, printers servers and other devices within a building or campus

SXP
Service Exchange Platform—a comprehensive cloud solution for delivering business process and automation as a service in both Enterprise B2B and Marketplace Exchange settings

TSN
Time-sensitive Networking—a set of standards developed by the IEEE 802.1 working group for time synchronization and scheduled delivery of network traffic

UCS
Universal Compute System—an (x86) architecture server platform that unites compute, network, storage access, and virtualization into a cohesive system

VAR
value-added reseller

VLAN
virtual local area network—a logical grouping of devices into the same Layer2 domain within a single network device or across a network system

VPN
virtual private network—a trusted/secure connection between entities across a less-trusted network

Wi-Fi
wireless local area network (WLAN) technology based on IEEE 802.11 standards

WIP
work in progress—all materials and in-process goods in a production process

wIPS
Wireless Intrusion Prevention System

WLAN
wireless local area network

WLC
Wireless LAN Controller—a device that provides centralized administration, control, visibility and security for enterprise-scale Wi-Fi networks

WPA
Wi-Fi Protected Access—a security method for authenticating users and encryption wireless networks

Further Reading

GE-Cisco partnership:
ge.com/digital/partners/cisco

GE Industrial Internet:
ge.com/digital/industrial-internet

Cisco Internet of Things:
cisco.com/go/iot

Contacts

GE: ge.com/digital/contact
Cisco: cisco.com/go/offices

Imagination at work

IND029-R102313