Connected Refineries and Processing Plant Cisco Reference Document (CRD)

January 2016

Connected Refineries and Processing Plant Cisco Reference Document (CRD)

About the Authors

Rik Irons-Mclean, Oil & Gas and Energy Architecture Lead, IoE Solutions Group, Cisco Systems

Rik has worked at Cisco for eight years primarily in the Energy industry, including lead roles in Energy Management and Energy Optimization, and Communications and Security for Power Utilities and Process Control Industries. He leads the Energy Architecture team and drives the global development of Cisco's reference architectures, use cases, and security for the Oil & Gas industry.

Rik has represented Cisco in a number of Industry and standards bodies including IEC 61850 for industrial communications, and IEC 62351 and ISA99 for industrial security, as well as UK Lead for Cigre SC D2. He has written industry white papers on Industrial Cyber Security Architectures, Distributed Industrial Control Systems, Next Generation Operational Field Telecoms, Fog computing, Converged Pipeline communications, Secure Access Control for Distribution Systems, and co-authored industry technical brochures.

John Helm, Oil & Gas and Energy Solution Manager, IoE Solutions Group, Cisco Systems

John has worked at Cisco for ten years with most of that tenure at Advanced Services Worldwide Wireless Practice as a senior Network Consulting Engineer where he was technical lead for industrial verticals. He has helped define standards and methodologies with WLAN and wireless and wired Planning/Design/Installation across all business verticals that use Cisco wireless products. John has presented and/or provided tutorials at numerous VT sessions, Cisco Live, technical events, and in classroom environments and has contributed to developing two Cisco certifications.

John has recently joined the Solutions Group after twenty-two years of field and executive level experience with industrial network design and deployment plus an additional four years prior communications experience.

Dimitris Tasidis, Cisco Systems

Dimitris Tasidis is a Solutions Architect with the Internet of Everything (IoE) Services team as a Technical Vertical Lead, focused on architecting Industrial solutions for Oil & Gas customers. As a lead within the IoE services organization, Tasidis is aligned and focused on the IT and OT aspects of Cisco's O&G customers. He also works closely with Cisco's IoT BU, Cisco's Vertical Solutions Group, and 3rd party solution providers, where he has led the network design and services development efforts for Cisco's Connected Solutions, and defined the architecture for future IoE projects.

His previous position with Cisco Advanced Services was as a Network Consulting Engineer in the EMEAR Wireless LAN Practice. He was responsible for delivering scalable designs that enable mobility solutions across many verticals for Cisco's largest customers. Also active in certifications, he has been a subject matter expert in the content development process for the CCIE WLAN lab exam.

Prior to joining Advanced Services in 2007, Tasidis was working since 2000 in the LAN Switching and WLAN teams in Cisco's Technical Assistance Centre in Brussels. Previously, Tasidis was working as an Escalation Engineer at the 3Com European Technical Escalation Centre in the Netherlands since 1997. Tasidis holds a BA in Business Computing from the University of Sunderland and an MSc in Telematics from the University of Sheffield.

Konrad Reszka, Technical Leader, IoE Solutions Group, Cisco Systems

Konrad has designed and validated end-to-end solutions at Cisco for eight years. He has contributed to many architectures and design guides spanning multiple technologies including Data Center, Security, Wireless, and Carrier Ethernet. Most recently he has engaged with the Oil & Gas industry as part of the Internet of Things to modernize and secure industrial networks.

He is a distinguished speaker at Cisco Live where you can catch him giving talks on the Internet of Everything, BYOD, and MPLS VPNs. Konrad holds a degree in Computer Science from the University of North Carolina at Chapel Hill.

CONTENTS

About the Authors i

Preface vii

CHAPTER 1 **Refinery and Processing Facility Overview** 1-1

- Executive Summary 1-1
- The Oil and Gas Value Chain 1-2
- Plant Communication 1-4
  - Operational 1-4
  - Multi-Service 1-5
  - Security 1-6
  - Challenges 1-7
  - Benefits 1-8
- Solution Scope and Features 1-9

CHAPTER 2 **Solution Overview and Use Cases** 2-1

- Architecture Overview 2-1
  - Wired Networks 2-2
  - Wireless Networks 2-3
  - Control Room Networks 2-3
- Mobile Workforce 2-4
- Plant Turnaround 2-5
- Remote Expert 2-6
- Personnel Health and Safety 2-6
- Asset Location Tracking 2-7
- Wireless Instrumentation 2-8
- Safety Shower Monitoring 2-8
- Wireless Bridging and Wired Replacement 2-9
- Physical Security 2-10
- Perimeter Monitoring/Tank Levels 2-11
- Inventory Management and Custody Transfer 2-11
- Predictive Asset Monitoring, Management, and Optimization 2-11

Vehicle Mobility 2-12

CHAPTER 3 **Refinery Local Area Network** 3-1

Access 3-2

Distribution 3-3

Core 3-3

Quality of Service 3-3

Security 3-4

CHAPTER 4 **Refinery Control Room** 4-1

Data Center 4-2

Virtualized Services 4-3

Identity Services Engine 4-3

Prime Infrastructure 4-4

Location Engine 4-4

Mobility Services Engine 4-4

Third Party Location Engine 4-4

Industrial Demilitarized Zone 4-4

Security and Segmentation 4-5

Availability 4-6

CHAPTER 5 **Industrial Wireless** 5-1

Multi-Service Access 5-2

Radio Frequency Coverage and Capacity 5-2

Access Point Deployment 5-3

Wireless LAN Controller Deployment 5-4

Quality of Service 5-5

Application Visibility and Control 5-6

Security 5-7

Availability 5-8

Wireless LANs 5-9

Multi-Service WLAN 5-9

Asset Tracking WLAN 5-9

Guest WLAN 5-10

Operational Access 5-10

WirelessHART with the Cisco 1552 WU 5-11

ISA 100 with the Cisco 1552S 5-12

Security 5-12

Availability 5-13
Quality of Service 5-13
Wireless Co-Existence 5-13
Asset Tracking 5-14
Active Tags 5-15
RSSI Probe Mode 5-15
Associated Mode 5-16
Improving Accuracy 5-16
Security 5-16
Access Point Coverage and Placement 5-17
Access Point Placement for Multi-Service Applications 5-17
Access Point Placement for Operational Applications 5-18
Access Point Placement for RTLS/Asset Tracking 5-18
Wireless Mesh 5-19
Ethernet Bridging 5-21
Traffic Flow 5-21
Availability 5-21
Vehicle Mobility 5-22

CHAPTER 6 **Deployment Considerations** 6-1
ISA-99/IEC-62443 6-1
Wireless Site Surveys 6-3
Processes and Methodology 6-3
Pre-Survey Data Collection 6-3
WLAN Equipment Settings 6-4
Survey and Test Tools 6-5
Premium Site Survey Test Suites 6-6
Site Survey Techniques 6-6
Work Safe 6-6
Baseline Propagation Assessment 6-7
Test Criteria 6-8
Impact on Survey 6-9
Implementation Considerations 6-9
Common RF installation considerations include: 6-9
Passive Survey 6-10
Active Survey 6-10
Predictive Survey 6-10
Two-Dimensional Site Survey 6-10
Three-Dimensional Site Survey 6-12

Advanced Site Survey for VoWLAN and Location-Based Services 6-12
Omni versus Directional Energy Surveys 6-13
Impact of Use Cases and Site Surveys in Oil and Gas 6-14
Network Optimization 6-15
Installation 6-15
Oil and Gas Environments 6-16
Installation Best Practices 6-18

CHAPTER 7 Industry Partnerships 7-1
Emerson 7-1
Honeywell 7-6
SAP 7-10
Wireless Endpoints 7-12
Location Services 7-12
Rice Electronics 7-13

CHAPTER 8 System Components 8-1

APPENDIX A Related Documentation A-1

APPENDIX B Additional Information B-1

APPENDIX C Glossary C-1

Preface

This *Connected Refineries and Processing Plant Cisco Reference Document (CRD*) documents best practice design and implementation of wireless, wired, control room, and security communication networks in petrochemical processing facilities or other refining and processing plant environments. The purpose of this CRD is to identify customer use cases, map those use cases to relevant architectures, and leverage Cisco and partner technology to deliver unprecedented value for our customers. This CRD:

- Documents best practices from real world implementations, detailing the designs and architectures that are mapped back to the customer use cases.
- Addresses real-life customer deployment scenarios by providing a solution that supports implementation of a scalable, secure, and redundant multi-service-enabled network supporting both industrial and multi-service applications. Wireless technologies are leveraged to implement new use cases or to enhance the support of existing ones.
- Outlines support for implementing industrial wired networks, secure remote access, the Industrial Demilitarized Zone (IDMZ), cyber security, and Control Centre application virtualization.
- Specifies network topology, wired and wireless LAN configuration, QoS, high availability, security services, network management services, and proposed Control Centre virtualization implementations.
- Provides information about enforcing cyber security best practices that follow the recognized Industrial Control System (ICS) security guidelines such as ISA99/IEC 62443 and the Purdue Model of Control.
- Documents the suggested equipment and technologies, system level configurations, and recommendations. It also includes description of caveats and considerations that process control customers should understand as they implement best practices.

Although this CRD focuses on refining and processing, the technologies and use cases are applicable at many other parts of the Oil and Gas value chain such as the oilfield, production platform, and pipeline compressor or pump station. As with any architecture and design program, functional requirements, use cases, and architectures evolve. Therefore, this CRD will evolve and will be updated in future phases.

Contributors

In addition to the authors listed in About the Authors, the following individuals have contributed to this *Connected Refineries and Processing Plant CRD*:

- David Bell, Solutions Architect, Emerging Ecosystems
- Jason Greengrass, Technical Lead, IoE Solutions Group
- Mahyar Khosravi, Partner Business Development
- Serhii Konovalov. Oil & Gas Business Lead, Cisco Systems

Refinery and Processing Facility Overview

This chapter includes the following major topics:

- Executive Summary, page 1-1
- The Oil and Gas Value Chain, page 1-2
- Plant Communication, page 1-4
- Solution Scope and Features, page 1-9

Executive Summary

This chapter provides a high level overview of the end-to-end Oil and Gas value chain and where the refining and processing facilities fit. It also provides an overview of the emergence and types of wireless technologies into these environments.

This document is written for an industry with a number of key trends:

- **An Aging Workforce**—Worker age and skillsets have changed. As younger workers with more of an IT-based skillset join the workforce, being able to train and provide remote expertise and consultation to new workers is essential.
- **Productivity Improvement**—With more visibility into operational workflows, the effort to improve the average worker productivity (wrench time) in the field, whether for employees or contractors, has increased dramatically. With average *wrench time* estimates of around 18% in Oil and Gas, this means only two out of ten hours are spent on productive work. The industry is looking to technology and digitization to increase and perhaps double productive time.
- **Lone Workers**—The health and safety of employees continues to be a focus for organizations, but a reduction in workforce due to automation and personnel productivity has meant an increase in the number of lone workers. The industry looks to improve overall worker safety while also providing a safe working environment for remote or unaccompanied workers.
- **Predictive Automation and Process**—Through Big Data, fog or edge compute, and analytics and cloud-based services, sensors are able to provide real-time information on such measures as temperature, vibration, pressure, flow, and current. Combining this with statistical models provides predictive methods for maintenance of equipment and streamlining of processes. The Internet of Things (IoT) has focused on connecting the unconnected through wireless and wired networks, and previously inaccessible data is now available for use.
- **Industrial Mobility**—With a proliferation of intrinsically safe mobile devices now available to host multiple communication and workflow applications, true opportunity exists for the fully mobile worker to operate safely and efficiently anywhere in the refining and processing areas.

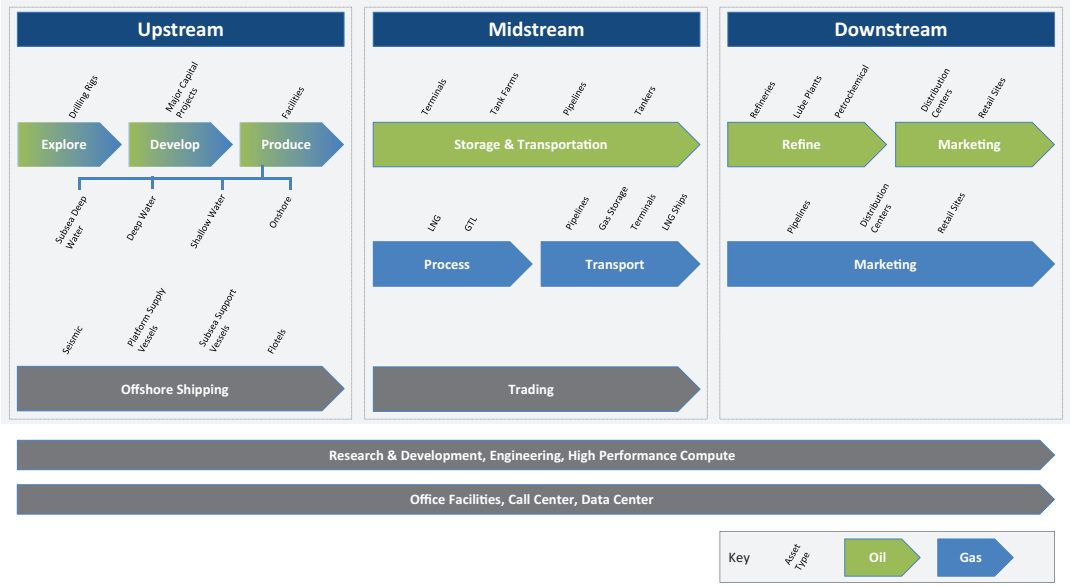
- **Security**—As technology evolves, as more devices are connected to the network, as attackers use increasingly sophisticated methods, and as OT and IT technologies converge, protecting assets, people, and intellectual property from cyber and physical threats becomes ever more important.

It is essential to understand that a single technology cannot enable the industry to meet these requirements. Only a properly architected, secure integration of a number of wired and wireless technologies and applications will help reduce cost, improve efficiencies, keep workers safe, and continue to drive innovation.

The Oil and Gas Value Chain

At a high level, the Oil and Gas value chain starts with exploration to discover resources, then goes through development, production, processing, transportation/storage, refining, and marketing/retail of hydrocarbons. This value chain is normally grouped into the three areas of upstream, midstream, and downstream, as shown in Figure 1-1.

Figure 1-1 Oil and Gas Value Chain



- **Upstream** includes the initial exploration, evaluation and appraisal, development, and production of sites. This is referred to as Exploration and Production (E&P). These activities take place onshore and in the ocean. Upstream focuses on finding wells, determining how best and how deeply to drill, and determining how to construct and operate wells to achieve the best return on investment.
- **Midstream** primarily focuses on the transport and storage of hydrocarbons via pipelines, tankers, tank farms, and terminals, providing links between production and processing facilities, and processing and the end customer. Crude oil is transported downstream to the refinery for processing into the final product.

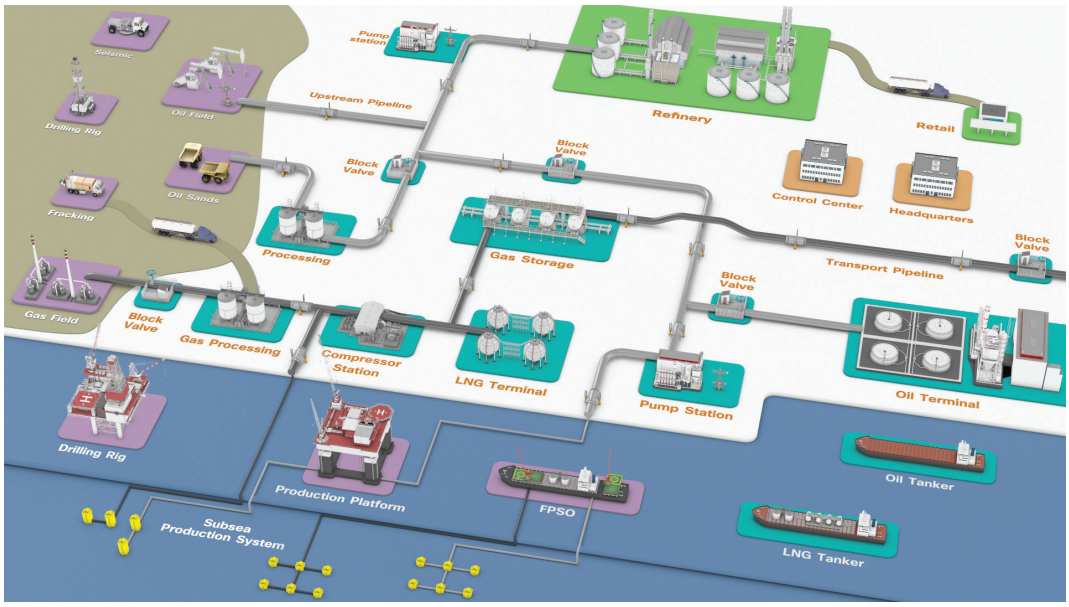
  Midstream also includes the processing of natural gas. Although some of the needed processing occurs as field processing near the source, the complete processing of gas takes place at a processing plant or facility, reaching there typically from the gathering pipeline network. For the wholesale markets, natural gas must first be purified with Natural Gas Liquids (NGLs) like butane, propane,

ethane and pentanes removed, before being transported via pipeline, or turned into Liquid Natural Gas (LNG) and shipped. The gas can be used real-time or stored. The NGLs will be leveraged downstream for petrochemical or liquid fuels, or turned into final products at the refinery.

- **Downstream** is concerned with the final processing and delivery of product to wholesale, retail, or direct industrial customers. The refinery treats crude oil and NGL and then converts them into consumer and industrial products through separation, conversion, and purification. Modern refinery and petrochemical technology can transform crude materials into thousands of useful products including gasoline, kerosene, diesel, lubricants, coke, and asphalt.

A visual overview of the value chain is shown in Figure 1-2.

Figure 1-2 Oil and Gas System



Refineries and processing plants are typically large sprawling complexes with many piping systems running throughout, interconnecting the various processing and chemical units. A large number of large storage tanks also exist around the facility.

The plant can cover multiple acres and many of the buildings and processing units on site are multi-stories high. The processing units and extensive piping networks have a very high metallic element, often with large distances between buildings or treatment areas. The sites are also not static, with various upgrades to plant equipment to ensure they operate as efficiently as possible on a regular basis. In addition, some areas are potentially highly explosive due to gases (see installation section for details) from the chemical processes, and potential challenges with deadly gas leaks or corrosion due to steam and cooling water around site.

The refinery is a complicated working environment with complex equipment and extensive piping networks. Products are being produced on a continuous basis, meaning the system must be continuously monitored via pressure, temperature, vibration, or flow.

At any one time, hundreds of workers including company employees, contractors, and external company support staff may be onsite. Plant operators ensure the entire process is working correctly, engineers monitor efficiency of the process and optimize or redesign where necessary, and maintenance staff ensure equipment is maintained, repaired, and safe. In addition, due to the size of the facility, the types of activities conducted, and the requirement to transport in and out raw materials or finished product, multiple vehicle types from cars to trucks to lorries to oil tankers and trains will be moving through the refinery environment.

To keep all of these systems, processes, and people operating effectively, efficiently, and safely, control systems, management systems, and safety systems are deployed. To ensure these systems are able to operate in a timely manner across the refinery or processing facility, a comprehensive and reliable communications system must be implemented.

Plant Communication

A refinery or processing facility deploys a number of different systems to ensure safety and reliability. Communications must support process control applications from the instrument or sensor to the Control Room application. These include Programmable Logic Controllers (PLCs), Controllers, Intelligent Electronics Devices (IEDs), Human Machine Interfaces (HMIs), operator or engineering workstations, servers, printers, and wireless devices. They can be categorized as operational (those directly involved with supporting refinery operations such as the process control or safety systems), and multi-service applications (either those that support operations such as video surveillance or those more concerned with business applications such as voice and corporate data).

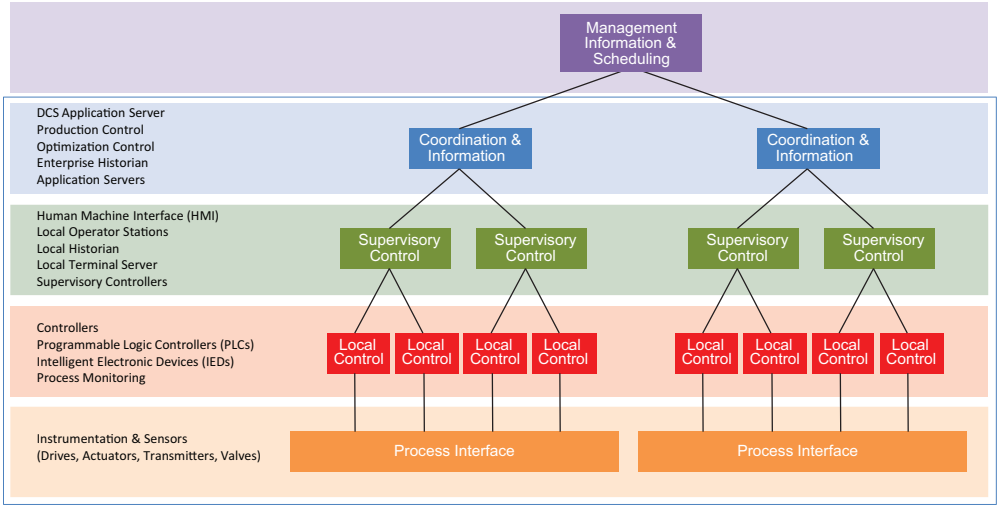
Operational

Historically, a number of these systems would have been deployed independently; however, most process control vendors offer integrated solutions incorporating many or all of the functions into common platforms:

- Process automation and control systems
- Safety critical including Fire and Gas, Emergency Shutdown, and burner management
- Maintenance systems
- Enterprise Resource Planning (ERP)
- Manufacturing Execution Systems (MES)
- Compliance

Unlike a Supervisory Control and Data Acquisition (SCADA) system, which is based on a central command and control model, the typical plant will have a Distributed Control System (DCS) that divides the control tasks into multiple distributed systems. This means that if a part of the system fails, the other parts continue to operate independently, as shown in Figure 1-3.

Figure 1-3 Distributed Control System Architecture



A DCS, which is process-driven rather than event-driven, typically produces a steady stream of process information with less reliance on determining the quality of data, as communication with control hardware is much more reliable. The DCS typically consists of multiple controllers or PLCs implementing multiple closed-loop controls. This makes them suitable for highly-interconnected local plants such as process facilities, refineries, and chemical plants.

Multi-Service

With increased requirements for physical safety and security, employee mobility, access to data, and collaboration with site-based or remote expertise, multi-service use cases are increasing in the facility environment:

- Employee Mobility
- Physical Security and Access Control
- Voice & Video
- Data Access
- Location Tracking (People, Assets, Vehicles)

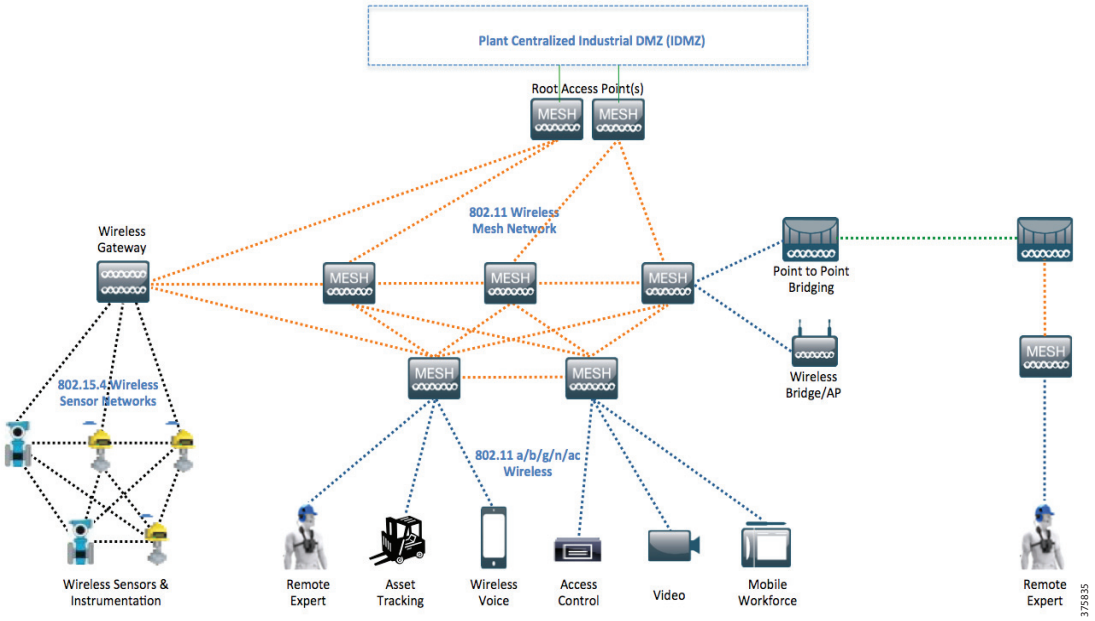
Traditionally, the basis for infrastructure has been wired communications for serial-based technologies, and more recently Ethernet. These have supported both proprietary and standardized protocols. However, many points and parts of the plant have remained unconnected for physical, practical, or economic reasons. Multiple disparate networks exist that sometimes provide overlapping function, but usually have a strict divide between operational and multi-service networks.

More recently, as companies strive to improve operations by trying new technologies, they have increasingly deployed wireless to provide easier and more cost-effective methods of connectivity. Wireless also enables new use cases such as worker mobility and remote expert, and industrial sensor connectivity that wired technologies are not capable of providing. With major process vendors such as Emerson, Honeywell, GE, ABB, Yokogawa, Schneider, and Siemens providing industrial wireless sensing systems over the 802.15.4 spectrum, wireless applications for monitoring and data collection are rapidly increasing and becoming more cost effective. Although deployments are typically for monitoring rather than control in the process domain, wireless is now readily available for process and levels

monitoring, asset health monitoring, and safety applications such as gas sensing and corrosion monitoring in the refining or processing facility, as well as for offshore platforms, onshore well sites, and tank farms.

With a range of intrinsically safe endpoints such as phones, tablets, notebooks, and portable gas detectors, employees' and contractors' ability to operate safely anywhere in the facility leveraging 802.11-based wireless means a seamless non-overlapping wireless infrastructure can be deployed to cover operational and multi-service use cases. 802.11 wireless mesh provides high bandwidth and highly resilient backhaul, and point-to-point bridging enables connectivity across long distances or where it is not practical or cost effective to deploy wires. These are outlined in Figure 1-4.

Figure 1-4 Wireless Technology in the Refinery and Processing Facility



New technology deployments should include the capability to incorporate wired serial and Ethernet and wireless requirements. Cisco's objective is to provide an IP-based open standards communication network that can transport serial protocols and that provides seamless unified integration for both wired and wireless networks to enable operational and multi-service use cases.

Security

Historically, a *security by obscurity* approach was taken to security for the process-control domain. Networks were seen as standalone with no public access, proprietary protocols were seen as being difficult to understand and compromise, and security incidents were more likely to be accidental. Security measures have often been based on the assumption that if the location or access method of a vulnerable point isn't widely known, it will not be exploited.

As Oil and Gas companies continue to adopt new technologies and use cases, new and diverse devices are being connected to the network. This brings with it a potentially wider set of security attack challenges (intentional, unintentional, external, and internal). Companies need to broaden their response away from merely physical segmentation or security by obscurity. In addition, information, resources, and tools have increased, making it easier for hackers to gain an understanding of legacy and traditional

protocols and to gain access to control systems. Many protocols and technologies were designed without security being an integrated element, and although standards are addressing these security holes, the embedded security is not at the same level as for the IP protocol.

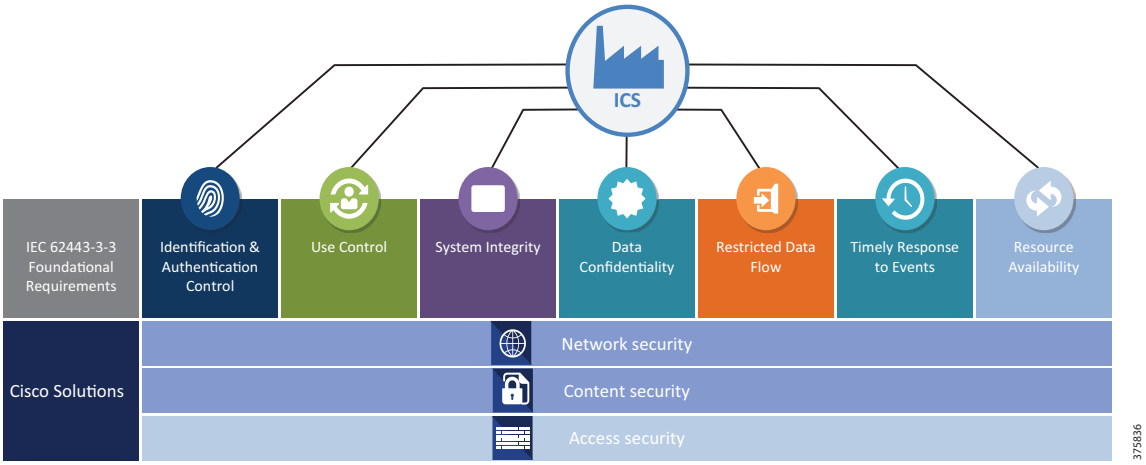
As companies bring together Operational Technology (OT) and Information Technology (IT) and the borders between these traditionally separate domains blur, they must also align security strategies and work more closely together to ensure end-to-end security. This includes architecture following standards such as IEC 62443, management, administration and policy, and communications.

In addition to cyber security, physical safety and security solutions that include CCTV/video surveillance, access control, and analytics also need to exist. A foundation for security must include both cyber and physical elements to best protect the process control environment. Adopting an appropriate risk framework allows plant owners to better:

- Implement and maintain security controls
- Manage cyber security risk
- Manage secure remote access to the process-control network
- Support security compliance
- Integrate third party support, contractors and remote engineers
- Manage physical safety and security

To help adhere to the requirements of IEC 62443 and achieve a robust solution for security and compliance, it is essential to use an end-to-end approach with technologies designed to operate together, minimizing risk and operational complexities, as shown in Figure 1-5.

Figure 1-5 End-to-end Security for IACS



Challenges

Refining and processing are not just technical operations. They are subject to changing market demands and environmental and safety regulations. Final product demand has changed dramatically over the last few decades. For example, a trend towards industrial complexes exists where feedstock, refining, and petrochemical activities occur on the same site or are geographically close. With increased regulations, plants (or parts of a plant) continue to shut down every five years or so for a turnaround period for maintenance and upgrades of equipment and technology.

Facilities are therefore looking to leverage new ways to streamline operations, improve process efficiency and automate, make better use of assets, manage the supply chain better in response to business and market needs, safeguard employee safety, and ensure environmental compliance.

Adding to these challenges, trained and qualified industry experts are in increasingly short supply, with many skilled engineers due to retire in the coming decade. Conversely, new technologies also mean many long-term industry veterans may not have skillsets to cope with some of the advances of newer IP-based communications and applications.

As technology has advanced and customers look to innovate existing and drive new use cases, leveraging technology is required to meet challenges effectively. New and existing data sources need to be accessed, regulations must be complied with, and the safety of employees must be ensured. Technology is now viewed by many as the enabler, particularly through the adoption of wireless-based technology.

Benefits

Unified industrial wireless and standards-based infrastructure help create the following benefits that are outlined in the following sections:

- Real-time access to new data sources in a consistent and easily consumable way:
  - Powerful visibility into every aspect of the refinery operation
  - Faster decision making based on real-time information
  - KPI dashboards for rich data visualization
- Predictive diagnostics and analytics:
  - Proactive and preventative maintenance
  - Higher wrench time of staff
  - Better asset utilization
  - Less Non-Productive Time (NPT)/downtime
- Standardized blueprint, open standard architectures for wired and wireless infrastructure:
  - Flexible implementation of advanced applications, and reduced time to deployment of devices, avoiding expensive cabling
  - Better management of resources and assets with the enablement of mobility applications over the wireless network
  - Streamlined and simpler management and administration
- Pervasive, accurate location-based services and tracking:
  - Improved safety for personnel and property
  - Less NPT locating correct machinery/assets etc
- Cyber and physical security:
  - Greater regulatory and security compliance
  - Enhanced physical safety of personnel
- Worker mobility and anywhere data access:
  - Improved turnaround time and cost savings
  - Lowered costs through greater efficiency and physical security
  - Access to expertise irrespective of location

Solution Scope and Features

This CRD describes how Cisco and partner technologies are deployed and operate in a common, open standard, and secure system architecture based on best practices for industrial environments. While wired infrastructure, secure remote access, and Control Centre/Room virtualization will also be covered, the focus is on leveraging wireless technologies to meet the following use cases:

- Wireless Bridging
- Mobile Workforce
- Wireless Instrumentation
- Personnel Health & Safety
- Turnaround
- Physical Security
- Asset Location Tracking
- Remote Expert
- Vehicle Mobility
- Safety Shower Monitoring
- Perimeter Monitoring
- Inventory Management & Custody Transfer
- Preventative Maintenance / Asset Monitoring

Each of these use cases is detailed in Chapter 2, “Solution Overview and Use Cases” and Chapter 5, “Industrial Wireless.”

Solution Overview and Use Cases

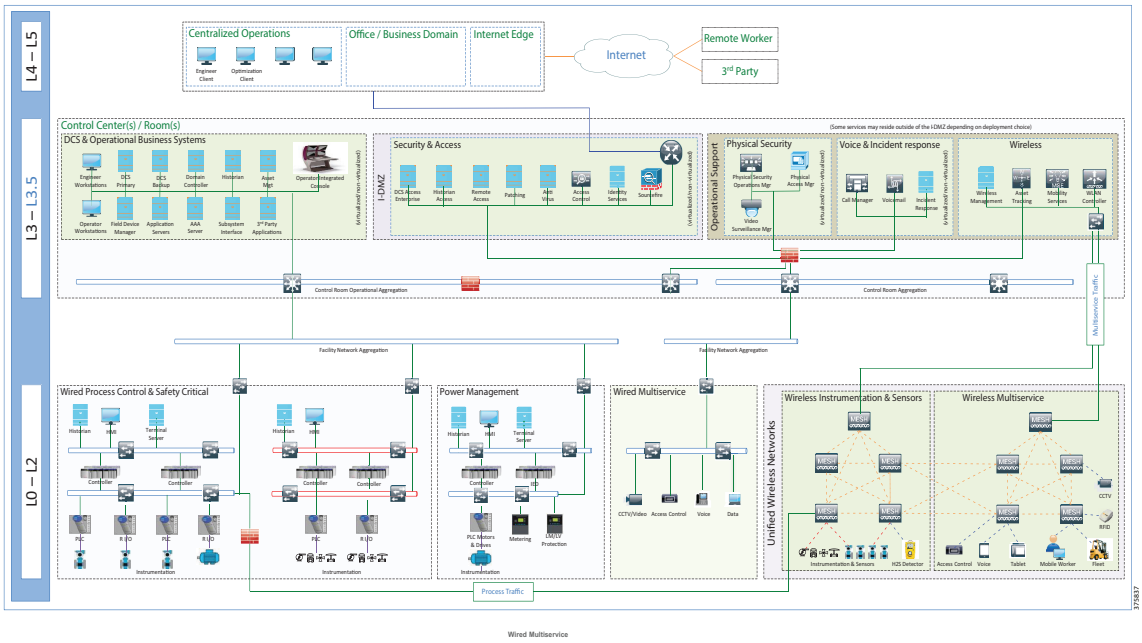
This chapter includes the following major topics:

- Architecture Overview, page 2-1
- Mobile Workforce, page 2-4
- Plant Turnaround, page 2-5
- Remote Expert, page 2-6
- Personnel Health and Safety, page 2-6
- Asset Location Tracking, page 2-7
- Wireless Instrumentation, page 2-8
- Safety Shower Monitoring, page 2-8
- Wireless Bridging and Wired Replacement, page 2-9
- Physical Security, page 2-10
- Perimeter Monitoring/Tank Levels, page 2-11
- Inventory Management and Custody Transfer, page 2-11
- Predictive Asset Monitoring, Management, and Optimization, page 2-11
- Vehicle Mobility, page 2-12

Architecture Overview

The *Cisco Connected Refineries and Processing Plant CRD* defines a reference topology as the recommended architecture. It consists of a number of building blocks (see Figure 2-1). The architecture consists of the plant wired and wireless networks for process control, safety, energy and multi-service, the plant control rooms including data center infrastructure, the IDMZ, and the connectivity to the enterprise and remote engineers or third parties. These building blocks are described below and provide the infrastructure to support the use cases that are outlined later in this chapter.

Figure 2-1 Reference Architecture for Refining and Processing



Wired Networks

Open standard Ethernet (fiber or copper) networks support both operational and multi-service applications. These can be physically or logically separated based on customer requirements.

- **Wired Process Control**—Networks that support the process control equipment used to change or refine raw materials into end products in the facility, reducing variability and increasing efficiency. This includes sensors, instrumentation and actuators, and controllers that manipulate and optimize the process. In addition, applications and functions exist to supervise and operate the local process.
- **Wired Safety Critical**—Critical safety systems that manage multiple complex activities for start-up, normal operation, temporary operations, emergency shutdown, and normal shutdown.
- **Wired Energy Management**—Systems that are used to manage energy integration and energy efficiency of facility assets. This includes IEDs and instrumentation, and applications to manage the local process.
- **Wired Multi-Service**—These enable more traditionally IT-centric use cases such as voice services, video surveillance, access control, and data access, leading to increased worker safety, higher productivity, and an enhanced experience.

Note In some environments. a requirement will exist for serial-based wired networks such as RS-232, RS-422, and RS-485. These will typically support legacy serial-based applications that are based on proprietary or open standard serial protocols, and they will need to be connected and transported across the main Ethernet-based infrastructure.

Wireless Networks

Open standard wireless networks support both operational and multi-service applications. These can be provided on common or separate infrastructure, and can be physically or logically separated based on customer requirements.

- **Wireless Process Control**—Providing IEEE 802.15.4 wireless infrastructure to connect instrumentation and sensors using industry standard ISA100.11a or Wireless Highway Addressable Remote Transducer Protocol (WirelessHART) protocols.
- **Wireless Multi-Service**—Providing IEEE 802.11 wireless infrastructure to enable multi-service use cases such as mobile gas detectors, wearable technology, handheld devices, smart glasses, security, video, and voice. This would also be used for backhaul of wireless traffic and some point-to-point bridging scenarios.

Control Room Networks

Open standard Ethernet (fiber or copper) networks support both operational and multi-service applications. This would typically consist of compute, storage, and data center-based switching infrastructure. These can be physically or logically separated based on customer requirements. These are implemented to support the following centralized functions:

- **DCS and Operational Networks**—Centralized applications and functions associated with the overall facility, running on bare-metal or virtualized server infrastructure.
- **Physical Security**—Centralized applications for CCTV/video surveillance, access control, and visual analytics for devices in control rooms and across the facility.
- **Voice and Incident Response Management**—Centralized applications for voice, video, voicemail, incident response, and other unified communications for control room and across the facility.
- **Security and Access Services**—Security services between central and remote locations including firewalling, Intrusion Prevention (IPS), Intrusion Detection (IDS), remote access, zone traversal, historian, and DCS alias or replicas.
- **Centralized Wireless Management**—Management applications for wireless, mobility, asset and people tracking for control room and facility deployments.
- **IDMZ**—Allowing remote access to operational servers and content in the DMZ from the enterprise, remote engineers and third party support, in addition to the process control domain. It provides secure access to enterprise resources from inside the process domain.

Note Services for physical security, wireless, voice, incident response, and security may reside in the IDMZ or outside the DMZ, depending on customer deployment.

Each domain and its subdomains support use cases that encompass actors. Actors include devices, systems, or programs that make decisions and exchange information necessary for performing applications. HMIs, network switches, and control systems represent examples of devices and systems. The information exchange involves communication of data and security of the data exchanged.

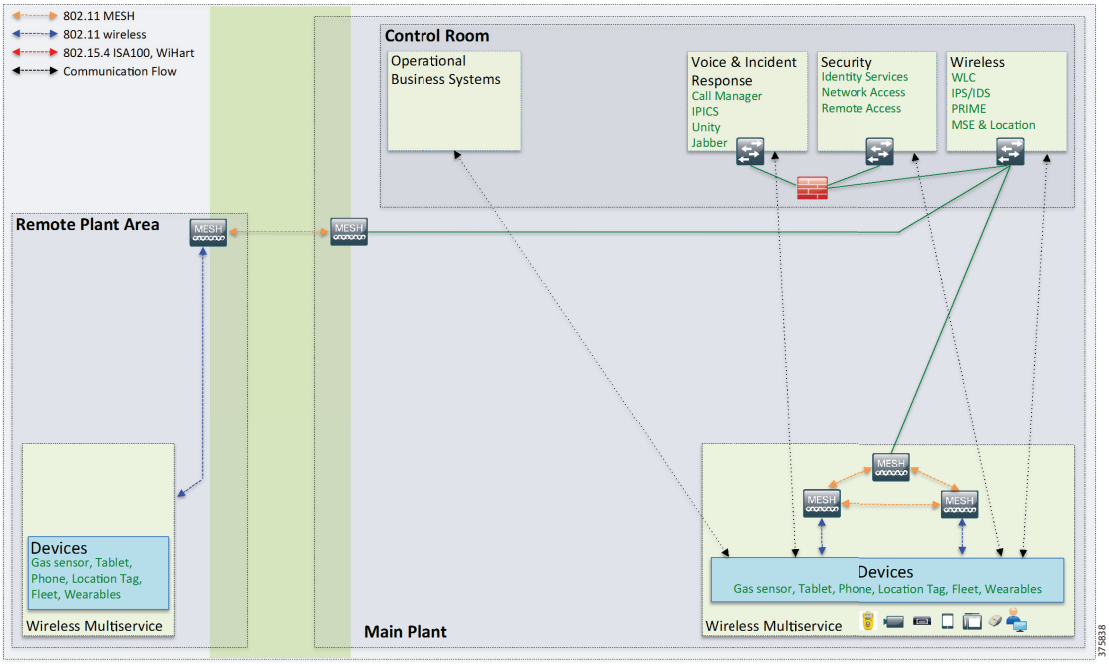
Mobile Workforce

This use case focuses on wireless network connectivity for engineers and workers in the plant, as shown in Figure 2-2. Operations have essential requirements around personnel safety and operational efficiency of the process. Typically, field personnel perform work using information from unconnected ruggedized laptops in the field or from paper-based documents. This information contains useful data including asset information, maps and schematics, work orders, and manuals. This can be challenging as information is not always current or real-time in the field, and centralized information is not current or updated until workers complete a task and provide updates. This lack of automated information exchange between field workers and centralized functions can lead to operating inefficiencies and outdated asset information.

As technology has advanced, and a proliferation of hazardous-certified or intrinsically safe devices have become available, equipping plant based workers with tools to enable them to do their job effectively first time regardless of location has become the norm. This allows workers to perform simple or complex operational tasks in the field, view and complete work orders remotely, make and receive voice and video calls at any location, and have access to data and applications as if they were in the static office environment. These technologies are accessed via mobile devices that are wirelessly connected to the control systems, or to the enterprise, enabling operations to take place directly in the field and providing access to maintenance tools that enhance the worker experience allowing:

- Increased worker productivity and troubleshooting accuracy through real-time access to information from the intranet, and to update information real-time
- Mobile operations visibility and management of the workforce
- Improved asset information that can be leveraged for maintenance and job scheduling
- Comprehensively integrated on-site and remote operations, providing *anywhere* expertise to validate and resolve issues.

Figure 2-2 Mobile Worker Communication Overview



Plant Turnaround

Turnarounds or shutdowns are scheduled periods where a plant will stop production for inspections, maintenance, upgrades, and cleaning that would not be achievable during normal operation. Safety checks from the operator or legal requirements will also occur. While plants are offline, they do not produce finished goods, which has a financial impact.

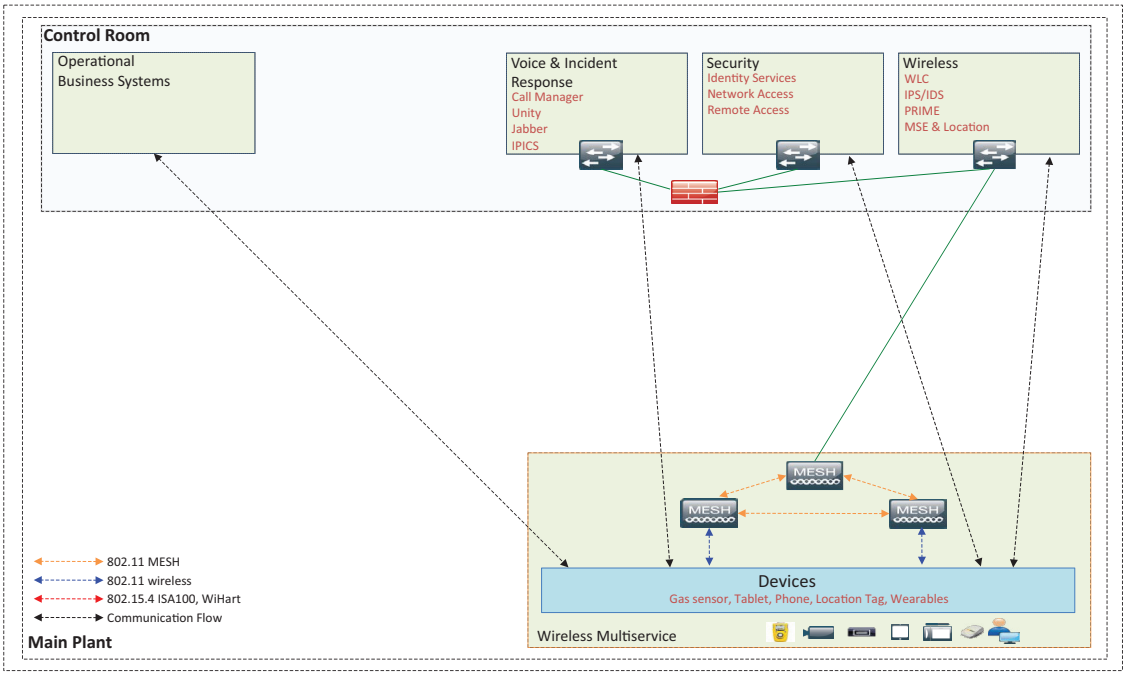
During the turnaround period, plant employees, equipment vendors, and external contractors will work on activities around the clock to try to get the plant operational as quickly and as safely as possible. If a turnaround is well executed, money can be saved, which enables early startup, which means greater output and greater profit. Overruns obviously have a negative financial effect.

The turnaround period is designed to improve plant efficiency; ideally, the plant should return to peak performance levels as soon as it is online. This means task completion and sign-off should be done accurately the first time.

Traditionally, turnaround has been a two-way process with engineers working on tasks around the plant and communicating back to a central engineer via radio who provides support and sign-off for tasks. Deploying a wireless infrastructure and providing workers with tools and processes for independent and remote working will save time and money. In a U.S. refinery example, turnaround was reduced from 4 to 2 weeks, and the workforce to complete the turnaround was halved.

Wireless mobility technologies such as ruggedized phones, tablets, and laptops with engineering tools and applications for job task, job completion, and independent sign-off linked directly back to central workflow and completion tools across the wireless infrastructure. This speeds up completion and improves workflow, activity records, safety, and compliance. See Figure 2-3.

Figure 2-3 Turnaround Communication Overview



Remote Expert

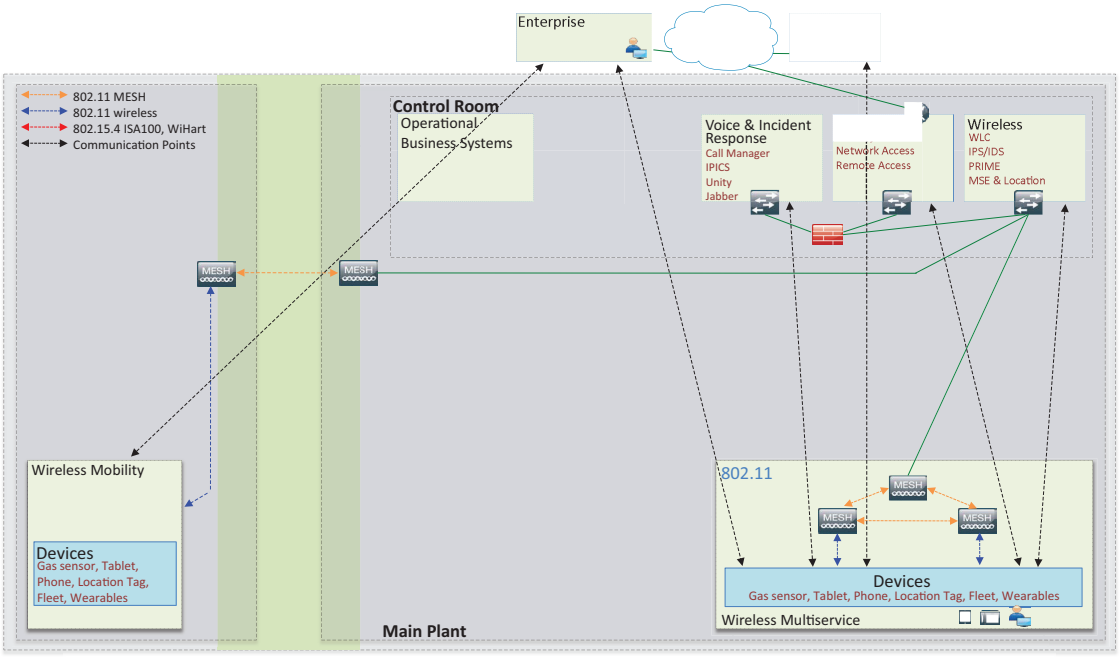
One of the biggest challenges in the plant is loss of productivity and profitability due to unforeseen outages and downtime. With a younger workforce and fewer workers who are experienced in older systems and infrastructure in particular, it is challenging and often not possible to ensure that the right resources are available in the right place and at the right time.

Companies may also need a number of subject matter experts from different disciplines to collaborate on situations real-time, and without the expense and having to wait for them all to travel to the same location.

Leveraging video, voice, and collaboration technologies to connect onsite plant workers with remote experts across an optimized communications infrastructure will mean expertise is available on demand. Experienced operators and staff members with specific skill sets are able to instantly help with support tasks, training, and emergencies regardless of their location, and be instantly connected to the control room or onsite worker.

This creates a centralized pool of specialists available when they are needed to consult, guide, and advise. To comply with risk management and regulations, all aspects of the interaction can be captured on a timeline via digital voice, video, and messaging recording. These recordings can then also be used as training tools. See Figure 2-4,

Figure 2-4 Remote Expert Communication Overview



Personnel Health and Safety

The refining and processing processes, including plant maintenance, wastewater treatment, and product treatments, uses many chemicals. This means potential safety risks for employees, contractors, and first responders, as well as for local communities around the facility due to accidental leaks in the plant.

Hydrogen Sulfide (H2S), Sulfur Dioxide (SO2), and Volatile Organic Compounds (VOCs) leaks may happen due to pipe failures, tank leaks, faulty equipment, and spills during transportation.

In addition, trips, falls, and injuries due to falling or moving objects are common risks to employee safety.

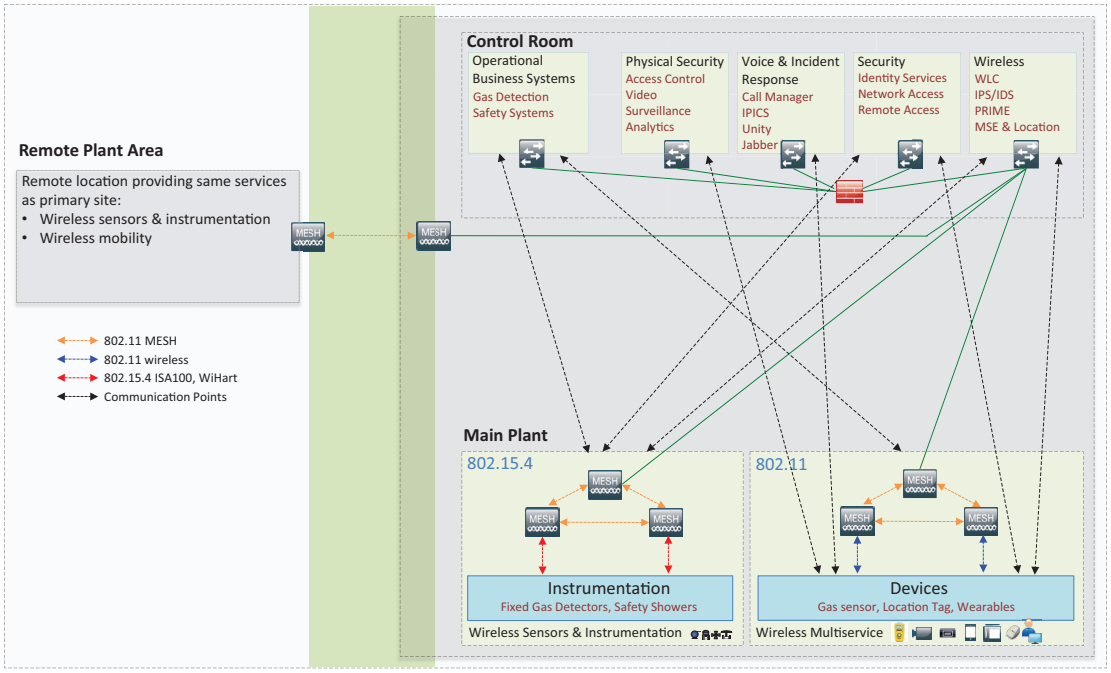
Being able to monitor both fixed locations for gas leaks and liquid spills, and monitor mobile workers for potential exposure to leaks, are essential safety functions. Being able to quickly detect and then isolate hazardous areas will save lives and also help meet regulations.

Having a precise understanding of the location of employees around the plant is also needed to ensure those affected in the leak zone are identified and evacuated, and others outside the zone are prevented from entering.

To achieve this, fixed wireless gas sensors are installed in key locations where leaks are a potential hazard, and workers are provided with a portable gas detector that communicates across the wireless infrastructure. Location tracking of employees can be achieved via an RFID tag that is either integrated into a device like the gas detector or a mobile handset, or is a separate locator tag. Both fixed and wireless sensors are overlaid on a map of the plant for real-time visibility with information backhauled across the wireless infrastructure to a centralized control room.

For *man-down* scenarios, it is also possible to leverage an accelerometer in a mobile device or tag to quickly detect personnel down due to trips or falls. Information can be sent back to a central monitoring location, and can even be tied into live video feeds from the mobile device to show whether it is a real incident or perhaps just a dropped device. Again. information is sent across the wireless infrastructure. See Figure 2-5.

Figure 2-5 Personnel Health & Safety Communication Overview



Asset Location Tracking

Asset location tracking through an RFID tag across an IEEE 802.11 wireless network is a key use case that acts as an enabler for multiple other use cases in this CRD. Plant administrators, security personnel, users, asset owners, and health & safety staff have expressed great interest in location-based services to allow them to better address a number of key issues in the plant:

- Quickly and efficiently locate valuable assets and key personnel
- Improve productivity via effective asset and personnel allocation
- Increase personnel safety via portable gas detectors and sensors, and man-down indicators
- Reduce theft loss due to unauthorized removal of assets from company premises
- Coordinate Wi-Fi device location with security policy enforcement and determine the location of rogue devices
- Monitor the health and status of key assets in their environment and receive prompt notification of changes

Managing the location of key assets and personnel throughout the plant is key to improving operational efficiency. Working with partners such as Stanley Industrial and Ekahau, comprehensive RFID location-based and context-aware services can be deployed over the wireless network. By tagging equipment, vehicles, and containers with active RFID tags, and deploying portable gas detectors and sensors across the same infrastructure, operational efficiency, employee safety, and regulatory compliance can be greatly enhanced.

Wireless Instrumentation

Refineries and processing facilities contain sensors, instrumentation, actuators and other equipment associated with process monitoring and control systems. Historically, it has not been technically or economically feasible to connect all of these systems via a wired communications infrastructure and many of these devices therefore remain standalone. This means manual readings, non-real-time information, and a lack of integrated information for systems to act on.

With the development of more robust and reliable standardized wireless sensor networks, the ability to connect the previously unconnected and to deploy new use cases has become a reality. This includes connectivity to the sensors and instrumentation via 802.15.4 wireless, and the backhaul of the aggregated sensor data via 802.11 wireless mesh.

The typical deployment for wireless instrumentation and sensor networks is for monitoring purposes, and for supervised regulation or control. The main wireless standards for the connectivity are ISA100.11a and WirelessHART.

By deploying wireless technology for instrumentation, the process monitoring and control systems are able to gain real-time visibility and access to sensor level information. This allows consistent condition-based monitoring from equipment at all times, delivering high performance, utilization, and reliability, and reducing unplanned downtime.

Safety Shower Monitoring

Safety showers are essential safety units deployed in the plant designed to provide cascading water over the entire body in the event of an incident. They are designed to dilute any chemicals or substances an employee has been exposed to, be at a consistent temperature to warm or cool the body, flush the skin and eyes clear of chemicals, and to extinguish fires on a person.

An employee should be under a safety shower as soon as possible after any exposure, and should remain under the water in the safety shower for 15 minutes. Therefore, showers should be located close to areas of potential hazard. The shower water should run at a consistent temperature so that the chemical reaction is not enhanced and to ensure that employees are not scalded nor get hypothermia.

By connecting safety showers to the wireless network infrastructure, it is possible to monitor that the shower is operational, the water is the correct temperature, and provide notifications and alarms when they are used. This information, which can be transmitted across the wireless infrastructure to the safety and monitoring applications in the control room, ensures that the safety showers are fit for use. The safety shower notifications can also be correlated with video feeds for incident verification.

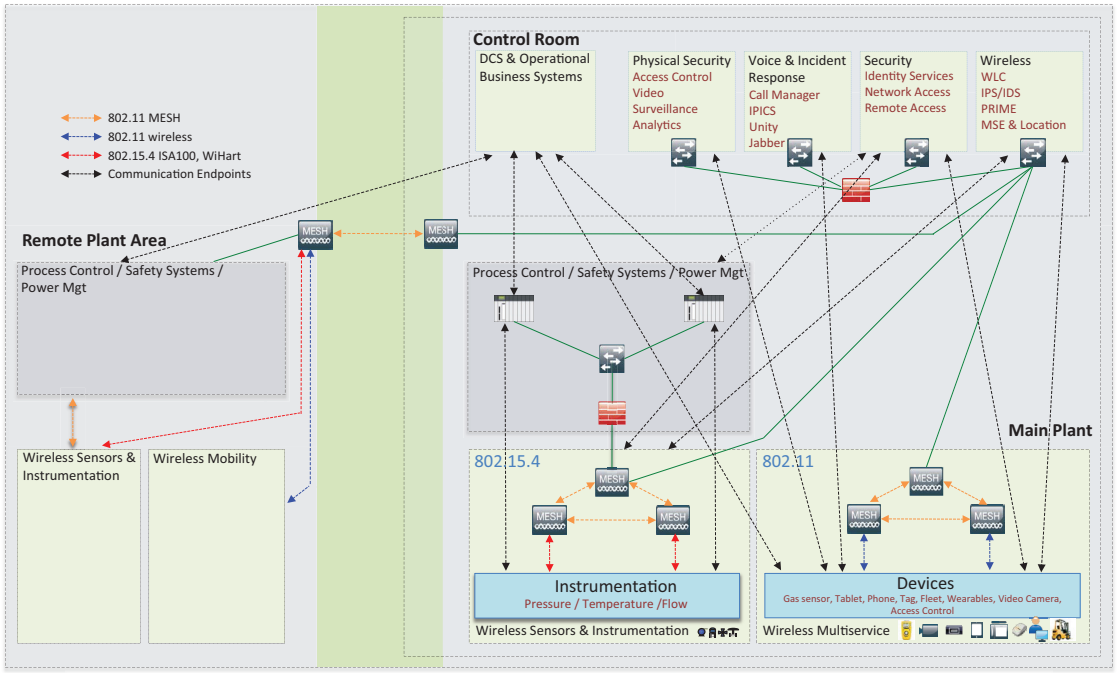
Wireless Bridging and Wired Replacement

With the increased reliability, throughput, and security of wireless technology, wireless can be leveraged to replace cable installation. Parts of the plant where running a cable is impractical or not economically feasible may exist.

For remote device connectivity, wireless instrumentation and sensors over 802.15.4 or wireless multi-service over 802.11 wireless technology can be leveraged for end device communications and/or backhaul.

As a plant expands, new sections that are geographically dispersed such as across a lake, or have a physical barrier such as a road or train line may be created. In these scenarios, running fiber may not be possible so a high-speed wireless bridge to connect sites and provide a seamless network is an option. In addition, a rapid or temporary deployment, such as the running of a wired connection may be required; therefore, wireless bridging can again be a deployment option. These technologies will reduce cost and eliminate islands of control. See Figure 2-6.

Figure 2-6 Wireless Bridging Communications Overview



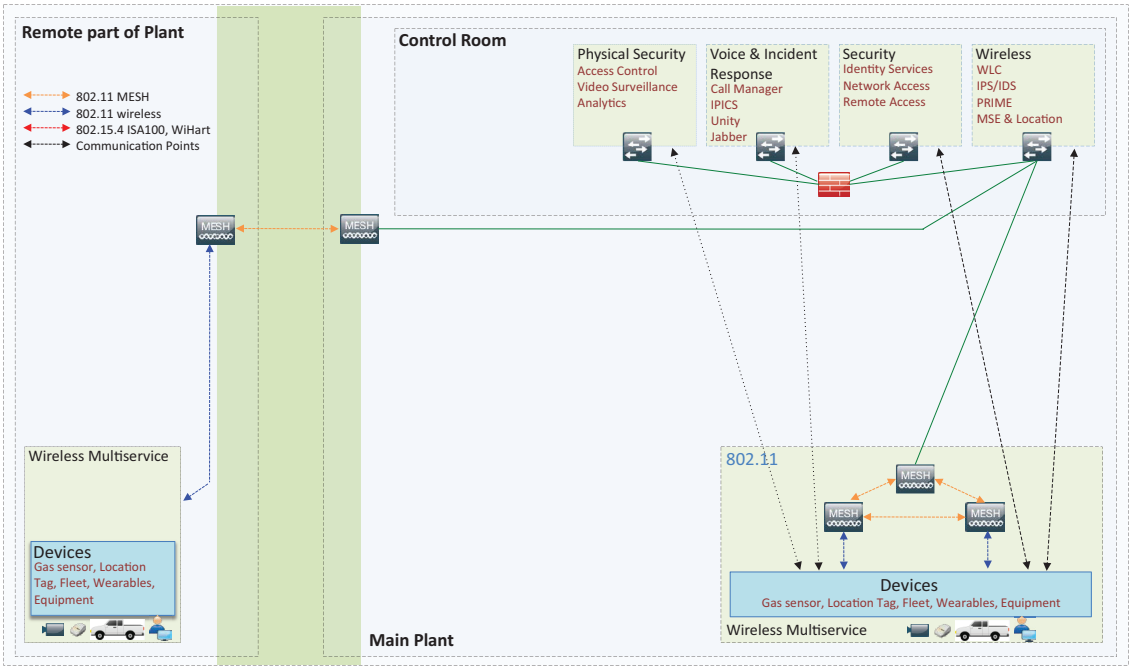
Physical Security

Physical security solutions provide broad capabilities for video surveillance, IP cameras, electronic physical access control, incident response and notifications, and personnel safety. Solutions can provide end-to-end support for safety and security detection, monitoring and management, and threat response in the facility, enabling:

- Video surveillance to monitor the perimeter, fences, gates, restricted areas, and emergency incidents that may occur
- Video surveillance to increase situational awareness by automatically tagging video when an employee or contractor swipes an access card to gain entry.
- Increased identification checks of all persons entering facilities.
- Initiated detailed, visible checks of all vehicles and packages entering facilities
- Verification of safety or emergency incidents such as a leak or man down, and real-time video feeds to safety staff and first responders
- Analytics to notify of unusual activities or behaviors

The 802.11 wireless infrastructure is used to connect cameras and access control gateways at the edge, and backhaul data to the central control room, while at the same time making deployments easier and faster. See Figure 2-7.

Figure 2-7 Physical Security Communication Overview



Perimeter Monitoring/Tank Levels

Process and refining facilities contain a multitude of vessels, tanks, and other storage units, many of which are not part of the communications network and require manual data gathering with levels and inventory not available real-time.

Wireless technologies are easily deployed to the remote parts of a facility, such as tank farms and perimeter areas, eliminating the time and expense required to install cables.

Sensors can be deployed along the perimeter of a facility, or at the edge of zones, to monitor for leaks and air quality. Atmospheric gas levels are monitored to protect employees and contractors from hazardous and potentially flammable gases. The sensors transmit data across the wireless network to a centralized location where real-time gas and radiation data can be seen, or historical information retrieved.

By adding sensors to the storage tanks in the tank farm, measurement data can be sent directly to the control system. This can protect against overfill, identify blockages or leaks early, and also optimize the production process by reducing variability, improving quality, and minimizing waste.

Data from both perimeter and tank sensors can be leveraged to increase plant health and safety and help meet regulatory requirements.

Inventory Management and Custody Transfer

Real-time visibility of product levels, inventory, and movement allows for increased operational efficiency through improved planning and scheduling, and minimizes production errors such as contamination. This requires accurate information of stock in tank farms, pipelines, and the supply chain.

By adding wireless-based sensors into these areas, real-time information can be transmitted to the inventory monitoring and management systems, and can also be leveraged for off-line logistics and planning.

With real-time visibility of data, outcomes include logistical benefits such as reduced emergency deliveries, improved inventory management, and labor optimization. At the same time, tying this back to enterprise management applications results in better asset utilization, accounting, and cash flow management.

Predictive Asset Monitoring, Management, and Optimization

Providing ongoing data updates on plant machinery and asset performance (such as motors, valves, pumps) to optimize performance, and to detect issues proactively before they occur. Information can easily be gathered via wireless sensors.

Predictive or proactive analytics can be leveraged in the facility to better manage asset maintenance on plant equipment such as motors, valves, and pumps. Typically, equipment is assessed on a preventative time-based schedule, or is reactive to issues. Equipment or parts may be replaced even if they do not need to be based on an estimated lifetime use. Physical inspection can be expensive and as data is captured at a point in time, the lack of real-time information can lead to equipment failure, costly unplanned maintenance and non-productive time, and accidents or emergencies resulting from failing equipment.

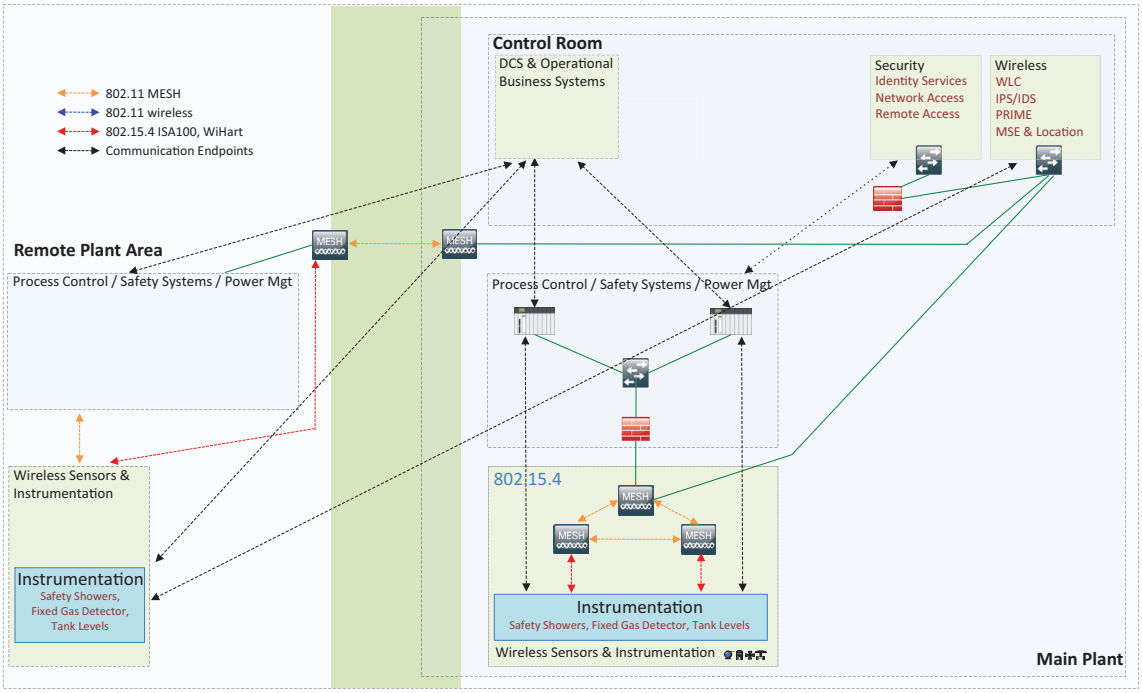
Analytics can be leveraged to make equipment monitoring, management, and maintenance more effective. Models are created for each equipment type to help predict component failure and optimal performance characteristics.

Wireless sensors monitoring plant equipment can measure characteristics such as temperature, vibration, alignment, and lubricant condition. Those characteristics are then compared with the statistical models to assess equipment performance and the likelihood of equipment failure.

From a predictive maintenance perspective, equipment can be fixed or replaced based on actual condition rather than on a preset timescale or use. This can potentially provide replacement cost savings and trigger repair of equipment that may fail before the scheduled maintenance window, preventing accidents or downtime.

Optimized performance of equipment based on real-time feedback of equipment parameters may also be realized, with even small efficiency improvements returning savings. See Figure 2-8.

Figure 2-8 Preventative Maintenance Communication Overview



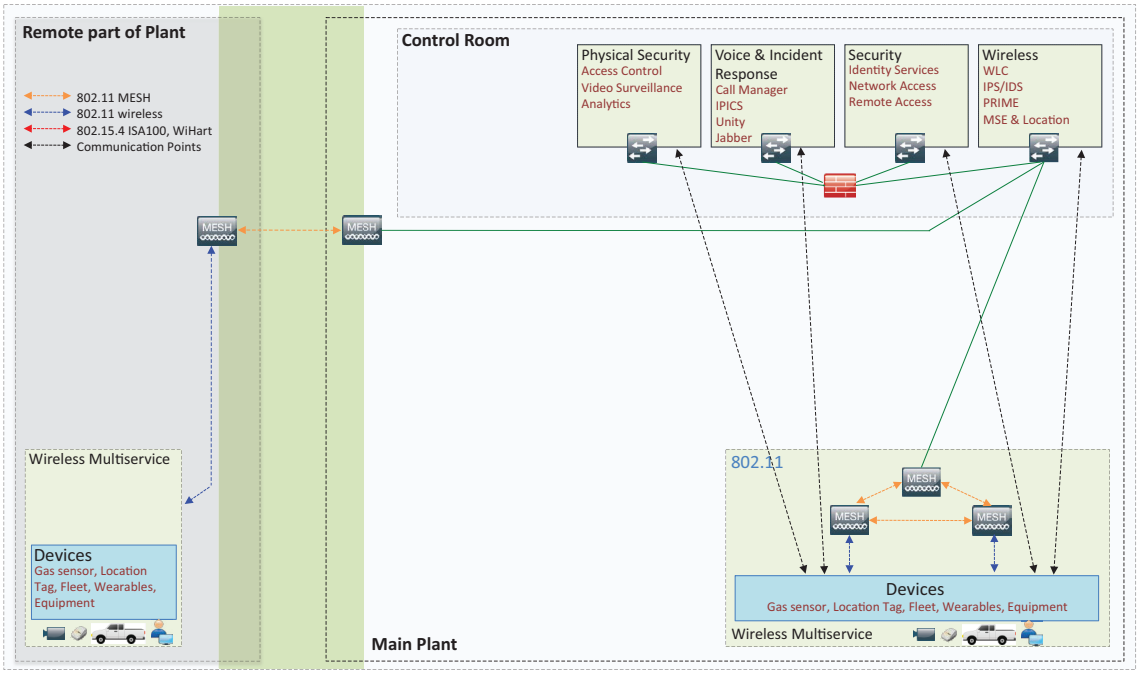
Vehicle Mobility

The wireless infrastructure is able to support a number of mobile worker and vehicle performance use cases. An onboard router can provide an in-vehicle wireless hot spot for mobile working, voice services connectivity to dash or external mounted video cameras, vehicle management services, and data backhaul across the wireless infrastructure.

In-vehicle wireless allows the worker to seamlessly access information such as maps, software, and work orders, while simultaneously transmitting data back to a central location such as completed jobs and instrumentation readings.

Video cameras can be leveraged for incident verification and stream data back real-time to the control room. They can also be used for remote-expert services. Fleet management services can be used for vehicle location tracking, driver behavior, and telematics or proactive maintenance. See Figure 2-9.

Figure 2-9 Vehicle Mobility Communication Overview



Refinery Local Area Network

This chapter includes the following major topics:

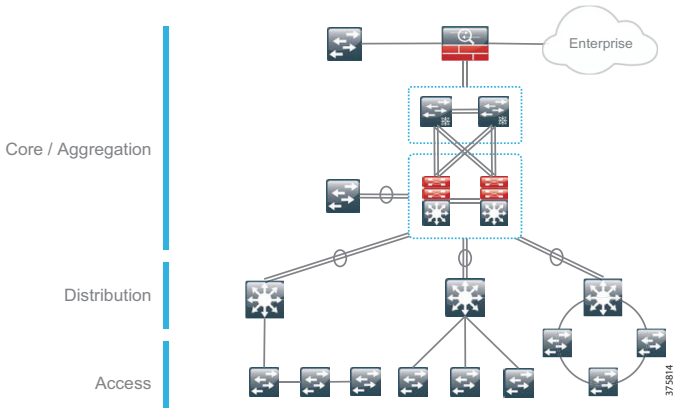
- Access, page 3-2
- Distribution, page 3-3
- Core, page 3-3
- Quality of Service, page 3-3
- Security, page 3-4

The wired network of the Connected Refinery is based on the Cisco Medium Density Campus LAN architecture. The medium-density campus design is a single distribution layer, which can be standalone or used as a collapsed core connected to another distribution or other services. The demands in the access layer for wired ports and WLAN devices typically number in the hundreds versus the thousands for a large design, with requirements for less than 100 APs.

If a larger network is required, it is recommended to follow the Cisco High Density Campus LAN architecture, which can support greater number of end devices and greater resiliency and HA mechanisms. Though detailed design and product guidance is out of scope for this document, a few recommended guidelines are provided to support the wireless services.

The overall LAN follows a tiered, hierarchical design allowing for an easy division of functions per layer, as shown in Figure 3-1.

Figure 3-1 Refinery LAN Overview



Access

The access layer provides connectivity to all endpoints, instruments, sensors, and other user-accessible devices. Wireless connectivity is provided through access points (APs) connected to switches at this layer.

The access layer design must ensure that the network is available for all devices when needed. As the connection point between the network and client devices, this layer is the first line of defense in protecting the network from human error and malicious attacks. When possible, this protection includes verifying that each user and device is allowed onto the network and then ensuring that users and devices have access only to authorized resources. Also, if a device or cable fails, this layer must re-converge in a sufficient time to minimize or eliminate any impact to the end device.

The physical topology of the access layer network will vary depending on physical restrictions of the environment in which it is deployed or device convergence requirements.

A linear topology forms a chain of switches by having each device connected to two adjacent switches. Although this allows for a highly flexible deployment within the plant, it provides for no redundancy to any downstream devices should a switch fail. A modification to the linear topology is a star topology. In a star topology, each switch is directly connected to one central switch. This approach limits the number of hops between the end device and the distribution layer and also isolates any failures to a smaller domain. This central switch, which could be in the distribution layer, acts as a bridge for the industrial Ethernet switches.

Another modification to a linear topology is a ring topology, whereby the last switch is connected back to the first (or each end is connected to a distribution switch). This approach forms a network ring and provides two paths in the case of a failure. If a failure occurs, each switch still maintains connectivity to the remainder of devices in the ring. An alternative to Spanning Tree Protocol (STP) specifically designed for ring topologies is the Resilient Ethernet Protocol (REP). REP can offer a complete view of the state of the network ring, is deterministic and predictable during failures, is easy to configure, and can converge in under 200ms.

It should be noted that with any of these topologies, the connection to the Layer 3 distribution switch can be a network bottleneck when over-subscribed. Although performance and scale are out of scope for this document, it is important to choose sufficient platforms at each network layer to fulfill customer bandwidth utilization requirements, implement proper QoS, and other availability mechanisms such as link aggregation on all uplinks.

Access layer switch ports should be 802.1X capable to ensure proper client and device authentication.

For new deployments, the Cisco Industrial Ethernet (IE) series switches are recommended due to their ruggedized IP30-rated design. For particularly harsh environments, IP67-rated models are available. With DIN rail mounting options, the Cisco IE switch is the ideal access-layer switch for industrial applications.

Many refineries and processing plants have relatively benign environments. Recommended access platforms include:

- Cisco Catalyst 2960
- Cisco Catalyst 3750
- Cisco Catalyst 3850

Most wired instrumentation is connected over 4-10ma loops to marshaling I/O cabinets which are in controlled environments. For any harsher environments, the Cisco Industrial Ethernet (IE) series switches are recommended due to their ruggedized IP30-rated design. And with DIN rail mounting options, the Cisco IE switches are excellent access-layer switches for industrial applications. For particularly harsh environments, IP67-rated models are available.

Management of the wireless operational field device may require a device manager. Certain vendors require Layer 2 adjacency to the field devices and must therefore be deployed before the Layer 3 gateway. See Chapter 5, "Industrial Wireless" for more information.

Distribution

The distribution layer facilitates connectivity between the access layer and other services. At any site with more than two or three access layer devices, it is impractical to interconnect all access switches. The distribution layer serves as an aggregation point for multiple access layer switches. The distribution layer can lower operating costs by making the network more efficient and by requiring less memory, creating fault domains that compartmentalize failures or network changes, and processing resources for devices elsewhere in the network. The distribution layer also increases network availability by containing failures to smaller domains.

Resiliency is provided by physically redundant components like power supplies, supervisors, and modules, as well as stateful switchover to redundant logical control planes.

Core

In larger LAN environments, the need to have multiple distribution layer switches often arises. For example, when access layer switches are located in multiple geographically separate buildings, fiber-optic cable runs between buildings could be costly. Thus, distribution layer switches could be located within each building. As networks grow beyond three distribution layers in a single location, organizations should use a core layer to optimize the design.

While the core layer of the LAN is a critical part of the scalable network, it is one of the simplest by design. The distribution layer provides the fault and control domains, and the core represents the 24x7x365 nonstop connectivity between them, which organizations must have in the modern business environment where connectivity to resources to conduct business is critical.

Suggested platforms here include:

- Cisco Catalyst 4500E Series with Supervisor 8-E pair in a VSS configuration
- Cisco Catalyst 6880-X extensible fixed chassis pair in a VSS configuration
- Cisco Catalyst 3850 Series SSO stack for much smaller sites

Quality of Service

Detailed guidance on policy and class map design throughout the refinery network will depend on the specific hardware and software deployed, and as such will be out of scope for this document.

General guidance regarding the classification and marking of traffic is presented in Table 3-1.

Table 3-1 Sample Refinery Traffic Class QoS Marking

Traffic Type	Class	PHB	DSCP	CoS
Network Infrastructure	Network Management (SSH, SNMP, Syslog)	AF	56	7
	Network Control	AF	48	6
	DC Control (VM, N1k)	AF	48	6

Table 3-1 Sample Refinery Traffic Class QoS Marking

Traffic Type	Class	PHB	DSCP	CoS
Process	Process Control	EF	32	4
Monitoring	SCADA	AF	24	3
PSS	Video Surveillance	AF	2	2
	Access Control	BE	1	1
Collaboration	VoIP	EF	5	5
Synchronization	NTP	AF	7	7
Maintenance	TFTP, Patching	BE	0	0

The network must be capable of transmitting traffic while maintaining the proper Class of Service (CoS) and Differentiated Services Code Point (DSCP) markings in order to ensure the prompt delivery of operational traffic. The entire underlying wired network infrastructure must be configured with QoS policies in line with the strategic application-class model in use for the given enterprise.

For additional information about classification on the wireless network, please see Chapter 4, "Refinery Control Room."

Security

Overall security throughout the wired network will consist of multiple mechanisms, following a defense-in-depth strategy. Throughout both the wired and wireless network, basic device hardening guidelines such as implementing features such as storm control, Terminal Access Controller Access-Control System Plus (TACACS+), 802.1X port authentication, logging, and disabling telnet access, should be followed. For more information, see the *Cisco Guide to Harden IOS Devices* at the following URL:

- http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

Separation of operational traffic from multi-service traffic is a top priority. Protecting the integrity of the operational traffic is paramount. Either intentional or accidental cross pollination of traffic between untrusted entities must be restricted. These requirements are not just restricted to the LAN; they must also be followed throughout the architecture and into the compute and storage areas. These enforcement techniques may be physical or logical. Physical enforcement of traffic segmentation is accomplished through physical segmentation of hardware. Logical segmentation is deployed where there is comfort and familiarity with the techniques such as Virtual Local Area Network (VLAN), Virtual Routing and Forwarding (VRF), Virtual Private Network (VPN), Virtualized Firewalls, and Virtual Storage Area Network (VSANs).

To maintain this separation logically on the refinery LAN, the wired network must support unique VLANs for operational traffic and multi-service traffic, with corresponding VRFs to ensure that no traffic is cross pollinated.

Additional security implementations throughout the refinery network are highlighted in their relevant sections in later chapters.

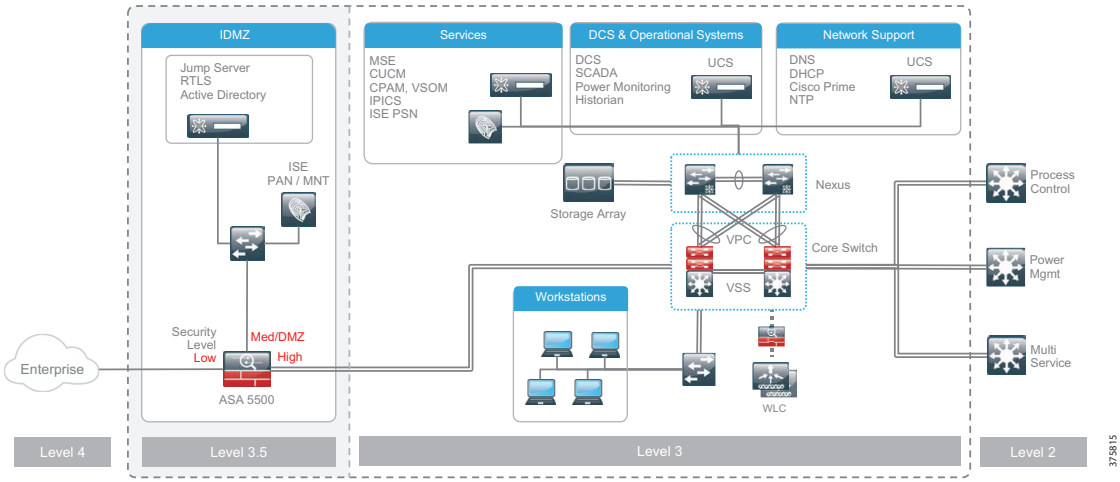
Refinery Control Room

This chapter includes the following major topics:

- Data Center, page 4-2
- Virtualized Services, page 4-3
- Industrial Demilitarized Zone, page 4-4
- Security and Segmentation, page 4-5
- Availability, page 4-6

The Connected Refinery Control Room, as depicted in Figure 4-1, contains the servers and services necessary for the proper functioning and operation of the process control network. It is also the gateway for all communication to and from the enterprise zone and the Internet.

Figure 4-1 Control Room Design



A resilient, high-speed switching core is at the center of the control room. As with many other aspects, the design of the core will vary based on scale and functionality requirements of the deployment. For smaller deployments, a single high-speed VSS pair of switches may have the sufficient port density required to support all devices in the control room. Larger deployments, however, may require a second tier of switches to support additional services.

Wired operator workstations will require a larger number of ports than other services and their state will fluctuate more often than other services. Using a large percentage of the frequently more expensive ports of a core switch for end user applications is not wise. Therefore, to minimize any disruption in the core and provide a more cost-effective design for the quantity of workstations, a second tier switch is

recommended. This switch would either be connected directly to the core switch by port channel for extra bandwidth and resiliency, or use a Fabric Extender (FEX) if the hardware is supported. A FEX can extend the access layer of a switch while simplifying operations by providing a single central point of management and configuration.

For a purely multi-service wireless support, the Wireless LAN Controller (WLC) can be deployed in the control room. Two Cisco 5508 WLCs should be deployed as a single HA pair connected to the core switch or a shared services switch off of the core.

The core switch will extend connectivity to the process control network, wired multi-service network, and the power management network.

Maintaining separation and segmentation of services is paramount to adhere with ISA 85 and ISA 99 standards. Each traffic type will be relegated to its own unique VLAN throughout the refinery network from the Control Room to the field devices, in both wired and wireless domains. At a minimum, multi-service traffic and operational traffic will each exist in their own VLAN with no routing between the two. Further VLAN segmentation can be configured based on the type of multi-service or operational traffic.

Data Center

A Cisco Unified Compute System (UCS) data center will virtualize and host the servers and applications within the control center. Benefits of virtualization in a data center include:

- Simplified physical and virtual networks, reducing cost while increasing manageability
- Better scalability with lower infrastructure cost per server
- Greater flexibility with virtualized environments for development and testing
- Increasing an organization's responsiveness to changing workloads and business conditions through increased flexibility

Virtualized servers have the capability to handle multiple operating systems and applications using a bare metal hypervisor on the compute system (the physical host servers). This allows the organization to lower capital and operating costs by collapsing more applications onto fewer physical servers. The hypervisor technology also provides the ability to cluster many virtual machines into a domain where workloads can be orchestrated to move around the data center to provide resiliency and load balancing, and to allow new applications to be deployed in hours versus days or weeks. Common hypervisors deployed in Oil and Gas environments include VMware ESXi and Microsoft HyperV.

The core of the data center consists of a high bandwidth Ethernet infrastructure to provide resilient Layer 2 and Layer 3 communication. Cisco Nexus series switches are best suited to provide this Ethernet connectivity within data centers. Nexus switches support Virtual Port Channel (vPC) technology, providing a loop-free approach to building out the data center in which any VLAN can appear on any port in the topology without spanning-tree loops or blocking links. See the section on Availability for more information.

Centralized storage can eliminate unused disk space on individual servers and simplifies backup operations. The Universal Port (UP) capabilities on Nexus switches are capable of connecting to multiple storage arrays supporting Ethernet, Fiber Channel, and Fiber Channel over Ethernet (FCoE). This allows the data center core to support multiple storage networking technologies like Fiber Channel Storage Area Network (SAN), Internet Small Computer System Interface (iSCSI), and Network Attached Storage (NAS) on a single platform type. This not only reduces costs to deploy the network but saves rack space in expensive data center hosting environments.

Finally, a high bandwidth Cisco Adaptive Security Appliance (ASA) firewall, such as the ASA 5585-X, has the capability to not only provide traditional firewall services but, with Sourcefire, can also provide Intrusion Protection System (IPS), Intrusion Detection System (IDS), and anomaly detection.

Virtualized Services

Virtualized applications for supporting the network within the control room and throughout the Process Control Network (PCN) such as Dynamic Host Configuration Protocol (DHCP), Domain Name Server (DNS), and NTP will be deployed on a VLAN reachable by all necessary clients.

Other applications that will be deployed in the Data Center include:

- Third Party Asset Tracking Services such as:
  - Ekahau Vision
  - Stanley AeroScout Location Engine
- Emerson AMS Device Manager
- Emerson DeltaV Controller
- Historian

Identity Services Engine

The Cisco Identity Services Engine (ISE) serves as a centralized security policy server. It is the single source of truth regarding all network access. At its core, ISE is a RADIUS server providing Authentication, Authorization, Accounting (AAA) services. When a client requests access to the network, the Network Access Device (NAD) sends a RADIUS request to ISE on behalf of the client. Depending on who, what, where, when, and how that request came in, ISE can push down an appropriate policy. In turn, the network itself (in most cases, the NAD) will be responsible for enforcing that policy through a variety of methods [such as VLAN, Access Control List (ACL), and Security Group Tag (SGT)].

An ISE deployment is comprised of different personas: Administration, Policy Service, and Monitoring. Depending on scalability and administration requirements, all personas can be active together on one server or split up across multiple servers in a distributed deployment. A common deployment model industrial applications places the Administration (PAN) and Monitoring (MNT) nodes in the enterprise level, leaving only a Policy Services Node (PSN) in the control room. If control of the security policy is to be retained within the IACS, the PAN can be placed in the IDMZ. It is the PSN which receives, processes, and responds to network access requests. This PSN would apply security policy and control network access for the control room as well as the process control network (Purdue Levels 3 and below). In order for the PSN to synchronize with the rest of the ISE deployment, the IDMZ would need to allow a connection between the PSN and the administration node. While configuration and policy are now centralized, a separate PSN would be utilized in the enterprise environment to handle access requests there.

ISE can use Lightweight Directory Access Protocol (LDAP) or Microsoft Active Directory to implement Role-Based Access Control (RBAC). These servers should also be virtualized and hosted in the data center.

Prime Infrastructure

Cisco Prime Infrastructure serves as the primary element manager for the network. In conjunction with a WLC and Cisco Mobility Services Engine (MSE), it can be used to position APs on a map of the facility to enable location and presence analytics.

Location Engine

Mobility Services Engine

The Cisco Mobility Services Engine (MSE) calculates the discrete time and location of wireless devices detected within the coverage area of Cisco APs in the network. A device can be identified and have its location estimated without being associated. By logging and measuring the Received Signal Strength Indicator (RSSI) contained within beacon frames periodically broadcast by 802.11 devices, the MSE can track (see) any device within range of its known APs.

The MSE is required if:

- Wireless Intrusion Protect System (wIPS) is to be deployed
- Location services or asset tracking are implemented without third party vendors

Third Party Location Engine

If the MSE will not be the primary application used for asset tracking, a third party application must be deployed. This application will require the configuration of a detailed map of the site, and the location of all APs. It will then need to read probe and/or tag RSSI values collected from the APs.

Industrial Demilitarized Zone

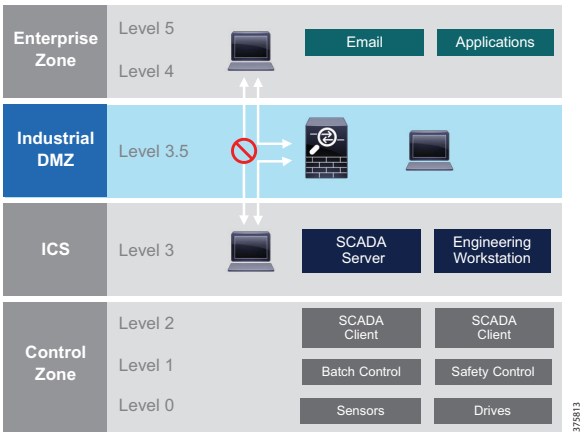
The Purdue Model and ISA-99 have identified levels of operations and key zones for the industrial networks. One key additional zone is the IDMZ.

New industrial security standards such as ISA-99 (now also known as IEC-62443), NIST 800-82, and Department of Homeland Security INL/EXT-06-11478 include an Industrial DMZ as part of a defense-in-depth strategy. The IDMZ provides a buffer zone between the enterprise zone and the industrial/plant zone. Data and services can be shared here between zones in a controlled manner. The IDMZ plays a critical role in maintaining availability of the industrial zone, addressing security issues, and compliance with regulatory standards.

In addition, the IDMZ allows for segmentation of organizational control, for example, between the IT organization and refinery operations. This segmentation allows different policies to be applied and contained. For example, different security and QoS policies may be used in the enterprise environment than in the industrial zones. The IDMZ is where the policies and organizational control can be divided.

All communication between the lower levels of the operational and process control networks and the higher levels of the carpeted enterprise or corporate environment must be tightly controlled and kept separate with no direct access or communication. Instead, this traffic traverses and potentially terminates at the IDMZ. This zone is crucial in securing and isolating the mission-critical operations network from the corporation's own support services as well as from the outside world. See Figure 4-2.

Figure 4-2 IEC-62442/ISA-99/Purdue Model of Control and the IDMZ



In the Purdue model of control hierarchy, this zone exists at Level 3.5.

The ASA should be configured for three zones with varying security levels.

- By default, the ASA will block all communications from a lower security level to a higher security level. Thus, the inside zone will have the highest security level configured. This zone defines the process control network and is connected to the control room network at Level 3.
- The outside or enterprise zone should be configured for 0, the lowest security level. This zone provides a connection to the carpeted corporate network at Level 4 for office functions, as well as to the Internet if required. All traffic from this zone is considered untrusted and must be dealt with accordingly.
- A third interface and zone should be configured at security Level 50 for the IDMZ itself.

Since the enterprise and the process control network should have no direct connection, the IDMZ network will house a remote access jump server. Users wishing to access the PCN remotely would log into the jump server in the IDMZ and, from that server. access the required instruments or applications.

The ASA in the IDMZ can also be used to implement a remote access VPN. Using the Cisco AnyConnect client, users can securely connect to the ASA and subsequently the IDMZ and jump server from outside the network.

Security and Segmentation

An ASA firewall is protecting the perimeter of the control room from the enterprise level and above. No traffic can enter the control room unless the request is initiated from inside. In addition to those basic firewall protections offered by the ASA in the IDMZ, an ASA running the Sourcefire module can offer advanced intrusion detection and prevention systems.

The Sourcefire module in the Industrial DMZ is capable of analyzing all the traffic passing through it and identifying the types of applications present therein. The Sourcefire FirePOWER platform provides context-sensitive threat prevention and contextual awareness. In this specific application, the Sourcefire FirePOWER services provide monitoring and auditing capabilities for industrial and enterprise protocols that may pass between through the IDMZ. Additional functionality that are available include granular Application Visibility and Control (AVC) to support over 3,000 application-layer and risk-based controls and filters on hundreds of millions of URLs in over 80 categories.

Access layer ports that are made available to users or end devices, such as operator workstations, should be secured with 802.1X for authentication. Upon trying to access the network, the client must first be successfully authenticated. The ISE will validate against a local LDAP or Active Directory domain controller and then determine the appropriate level of security policy to be applied to that client. It is up to the network access device to enforce the security policy.

VLANs will provide logical Layer 2 segmentation throughout the control room Ethernet network between operational and multi-service traffic, while VRFs will be used to maintain separation at Layer 3 and prevent any cross-pollination of traffic. VLANs are extended to the virtual environment, providing path isolation to the Virtual Network Interface Card (vNIC) of the UCS host.

Note Depending on the redundancy model, servers in a virtual environment may move between physical hardware under failure conditions. The design should consider VM security and segmentation policies should VMs move between physical hosts.

Availability

The control room network is designed so that there is no single point of failure.

Protection against the failure of a single link is achieved using Ethernet Port Channels (EPCs). One or more Ethernet links are bundled together to form a single EtherChannel. This logical interface is used to connect the core switches to each other, to each of the Nexus DC switches, to the ASA in the IDMZ, and to the distribution Process Change Notification (PCN) switches.

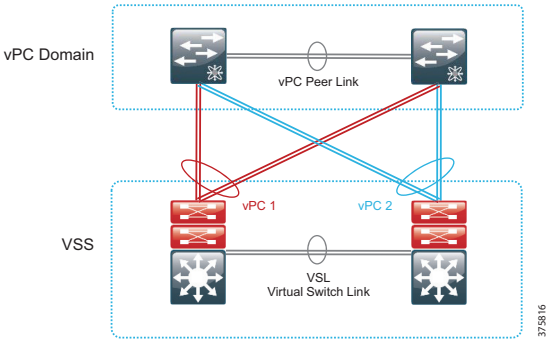
If capable, the core switches should be configured to use VSS. VSS combines a pair of capable switches into one logical network element. A peer device connects to both chassis of the VSS using one logical port channel. The VSS automatically manages redundancy and load balancing on the port channel. This capability enables a loop-free Layer 2 network topology. The VSS also simplifies the Layer 3 network topology because the VSS reduces the number of routing peers in the network.

The Nexus Data Center (DC) switches use a similar concept for enabling multi-chassis ether-channels. Virtual Port Channels (vPC) on Cisco NX-OS devices allows links that are physically connected to two different Nexus switches to appear to a peer device as a single connection. This peer device can be a server, switch, or any device supporting 802.3ad port channels.

The data center needs to provide a topology where any data center VLAN can be extended to any server in the environment to accommodate new installations without disruption. It also needs to provide the ability to move a server load to any other physical server in the data center. The use of vPCs allows the two data center core switches to build resilient, loop-free Layer 2 topologies that forward on all connected links instead of requiring STP blocking for loop prevention.

A vPC consists of two vPC peer switches connected by a peer link. Of the vPC peers, one is primary and one is secondary. The system formed by the switches is referred to as a vPC domain. See Figure 4-3.

Figure 4-3 vPC and VSS in the Control Room Network



The vPC used in the data center and the Catalyst VSS used in the core are similar technologies in that they allow the creation of Layer 2 port channels that span two switches. For Cisco EtherChannel technology, the term Multi-Chassis EtherChannel (MCEC) refers to both technologies interchangeably. MCEC links can provide loop-free topologies, allowing VLANs to be extended across the data center while maintaining a resilient architecture.

If required, the ASA in the IDMZ can be deployed in an Active/Standby configuration. Active/Standby failover enables a standby ASA to take over the functionality of the failed unit. When the active unit fails, it changes to the standby state while the standby unit changes to the active state. The unit that becomes active assumes the IP addresses and MAC addresses of the failed unit and begins passing traffic. Because network devices see no change in the MAC to IP address pairing, no Address Resolution Protocol (ARP) entries change or time out anywhere on the network.

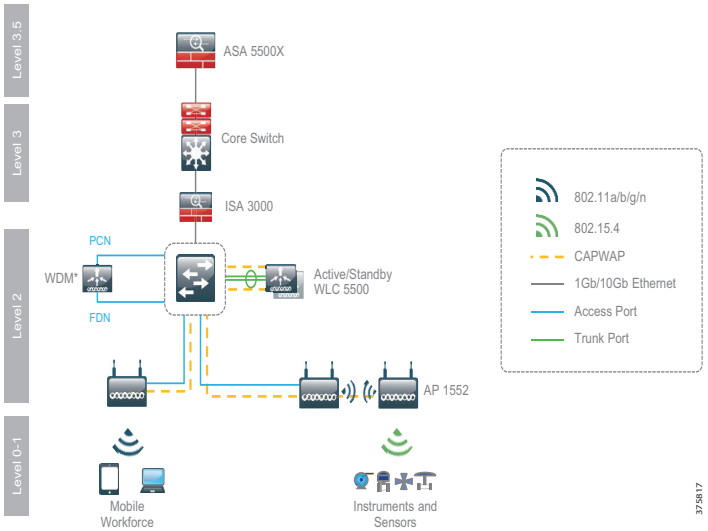
Industrial Wireless

This chapter includes the following major topics:

- Multi-Service Access, page 5-2
- Operational Access, page 5-10
- Wireless Co-Existence, page 5-13
- Asset Tracking, page 5-14
- Access Point Coverage and Placement, page 5-17
- Wireless Mesh, page 5-19
- Vehicle Mobility, page 5-22

The wireless network, as shown in Figure 5-1, within the Connected Refinery will provide support for 802.11 clients for various voice, video, security, and other (multi-service) applications and access for industrial 802.15.4 clients for sensor and instrument data retrieval (operational). The same APs (Cisco 1550 series) will serve both applications.

Figure 5-1 Wireless Access Topology



Multi-Service Access

The multi-service wireless design provides the necessary infrastructure to support the mobile workforce, enhance plant turnaround time, provide access to a remote expert, and monitor the health and safety of the refinery's employees. It lays the critical foundation for subsequent services to be enabled.

To support these use cases, the Wireless LAN (WLAN) design is based on the Cisco Unified Wireless Network architecture. At the heart of this architecture is the Wireless LAN Controller (WLC) which handles all necessary functions related to system-wide operations and policies such as mobility, security, QoS, and radio frequency management. Wireless APs work in conjunction with the controller to connect wireless devices to the LAN and support lower level functions such as beacon handling, client handshakes, and media access layer control encryption. Three primary deployment models can be considered for a WLAN design: Centralized, FlexConnect, and Converged Access.

- In a **Centralized** deployment model, also known as local-mode, the WLAN controller and the APs are located within the same site (that is, there are no remote or branch locations). All client wireless traffic is tunneled between the AP and WLC using the Control and Provisioning of Wireless Access Points (CAPWAP) protocol. This model benefits by using one central location to manage IP addresses, configurations, and troubleshooting.
- With a **FlexConnect** deployment, some traffic can be terminated directly at the AP, rather than being backhauled to the controller. Due to this bandwidth saving feature, this model is best suited for deployments containing multiple remote sites.
- The **Converged Access** deployment model is best suited for smaller remote sites. In this model, the WLAN controller is integrated within the access layer switch and allows for local termination of traffic.

Due to the simplicity in configuration, greater control over traffic, and flexibility in access layer devices, a Centralized deployment model is recommended for refinery deployments.

Wireless APs in a centralized deployment are lightweight; they cannot operate without a WLAN controller. Upon registering with the controller, the AP will download the appropriate firmware or software image and configuration.

All communication between the AP and the controller takes place over a CAPWAP tunnel.

Radio Frequency Coverage and Capacity

The Connected Refinery wireless access design must provide sufficient coverage and capacity to support the previously described use cases. Coverage defines the ability of a client to connect to an AP with sufficient signal strength to overcome any radio frequency interference. The edge of the coverage for an AP is based on the signal strength and signal-to-noise ratio (SNR) measured as the client device moves away from the AP. The signal strength required for good coverage will vary depending on the specific type of client devices and applications on the network.

The Radio Resource Management (RRM) feature in the Cisco WLC acts as a built-in RF engineer to provide real-time RF management of the wireless network consistently to relieve frequent manual intervention. RRM enables Cisco WLCs to continually monitor their associated lightweight APs for the following information:

- **Track load**—The total bandwidth used for transmitting and receiving traffic to track and plan network growth ahead of client demand
- **Interference**—The amount of traffic coming from other 802.11 sources
- **Noise**—The amount of non-802.11 traffic that is interfering with the currently assigned channel

- **Coverage**—The RSSI and signal-to-noise ratio for all connected clients
- **Other**—The number of nearby APs

Using this information, RRM can periodically reconfigure the RF network for best efficiency. RRM automatically detects and configures new lightweight APs as they are added to the net- work. It then automatically adjusts associated and nearby lightweight APs to optimize coverage and capacity. RRM produces a network with optimal capacity, performance, and reliability.

Overlapping cell coverage is just as important as cell boundaries. Excessive overlap of coverage can result in some channel interference, unnecessary AP-to-AP roaming (by client devices that have a limited roaming algorithm), and added expense because of more APs being required.

For data networks, a typical overlap in coverage is set to about 10 percent to 15 percent of the overall cell coverage area. In contrast, for voice networks, a higher overlap in coverage is recommended to ensure seamless call hand-off when roaming between APs. For voice networks, the recommended overlap is 15 to 20 percent of the overall cell coverage area.

Access Point Deployment

Antenna selection and proper placement of each wireless AP should be determined by a wireless site survey (see Deployment Considerations). If location services will be deployed, such as Cisco Connected Mobile Experiences (CMX), it is important to document the MAC address as well as the physical location of each AP. This step is critical for accurate location triangulation.

Lightweight Wireless Access Points (LWAPs) must be associated and registered with a controller before being operational. Upon booting up, the AP will try to discover a controller in a variety of ways. Once a controller is discovered, the AP will request to join it. If an AP is not aware of a controller to join, it will attempt to find one using the following steps:

1. The AP will broadcast a Layer 3 CAPWAP Discovery message on the local subnet. A valid WLC that receives this message will unicast back a Discovery Response message.
2. If the AP has previously learned a WLC, its IP address will be locally stored in Non-Volatile Random-Access Memory (NVRAM). The AP will send a unicast discovery request to each WLC it has stored.
3. If the AP is requesting a dynamic IP address, the DHCP server can be configured to include a WLC IP address using Option 43 in the DHCP Offer message it responds with. The AP will then send a CAPWAP Discovery message to this WLC.
4. If those methods fail, the AP will attempt to resolve the DNS name *CISCO-CAPWAP-CONTROLLER.localdomain*. If the name is resolved to one or more IP addresses, the AP will send a CAPWAP Discovery message to each address.
5. If the AP does not receive a CAPWAP Discovery Response, it will reboot and restart this process until a controller is found.

If the controller is located in the control room, it most likely will not be on the same subnet as the APs so option 1 is not valid. Since recovery and convergence speed is critical in a refinery, the DHCP and DNS methods are also not viable options. The only remaining option for an AP to discover a controller is to already have discovered one. For controllers deployed at level 2 supporting operational device managers, option 1 may be an alternative.

Therefore, before deployment, each AP should be set up with an initial configuration or *primed*. This priming consists of first deploying each AP on the same subnet as the controller within the IDMZ. The AP will be assigned a temporary IP address by way of DHCP and learn the address of the controller using

Option 43. Once it has joined the controller, a static IP address should be assigned to it. DHCP for the AP is acceptable during the initial setup, but once deployed, a static IP address will avoid any needless delays in the event of a reload.

An additional security measure to prevent any rogue APs from joining the network is to enable a MAC filtering list for APs on the WLC. The MAC address of every AP must be added to this list prior to the AP discovering the controller.

APs require power in addition to a wired connection to the LAN. This can be achieved using a dedicated power supply per AP. However, depending on the model of AP being deployed and location/environment, this requirement can be simplified by deploying Power over Ethernet (PoE) capable access layer switches. With PoE-capable switches, supported APs can be powered over the same physical cable that enables data transport.

For more information regarding placement of APs for various traffic types, see Access Point Coverage and Placement, page 5-17.

Wireless LAN Controller Deployment

The Cisco 5500 series WLC is best suited for centralized wireless deployments. The 5508 WLC can support a maximum of up to 500 LWAPs and 7,000 clients while the new 5520 WLC can support up to 1,500 APs and 20,000 clients. Different licenses, however, can vary the number of supported APs.

To support the operational device managers, the WLC should be deployed at Level 2 and within the same Layer 2 domain as the access-points. All multi-service wireless traffic arrives at the WLC via CAPWAP before being de-encapsulated. On egress, traffic should pass through a firewall and be explicitly granted access before being forwarded to the control room (at Level 3) or any other zone.

The 5500 series WLCs have multiple Gigabit or TenGigabit Ethernet ports that can be joined using a Link Aggregation Control Protocol (LACP), bundling the ports into a single high-speed port-channel interface. Since all wireless traffic is backhauled to the controller, this aggregation eliminates the throughput limitation of a single port. When LAG is enabled, the controller dynamically manages redundancy and load-balancing.

Each WLAN should be placed onto a unique VLAN to ensure proper segmentation of traffic. On egress from the controller, the port-channel link facing the control room core switch must be enabled for 802.1Q trunking. Likewise, the uplink ports from that core switch must also be configured as 802.1Q trunk ports. Only the required VLANs should be allowed on this trunk. Restricting the trunk to only the VLANs required allows the WLC to process only relevant frames, resulting in improved performance.

Beginning with AireOS 8.1, a best practices checklist is available on WLC dashboards. This simple tool can be used to tune the WLC configuration to match the best practices recommended by Cisco. This tool not only checks the running configuration, but also provides basic options to enable those best practices if not already met. Some of the configuration options this tool validates include:

- Controller High Availability
- Use of HTTPS for Management
- WLANs with 802.1X
- Rogue AP Policies
- Dynamic Channel Assignment
- Transmit Power Control
- Client Log In Policies

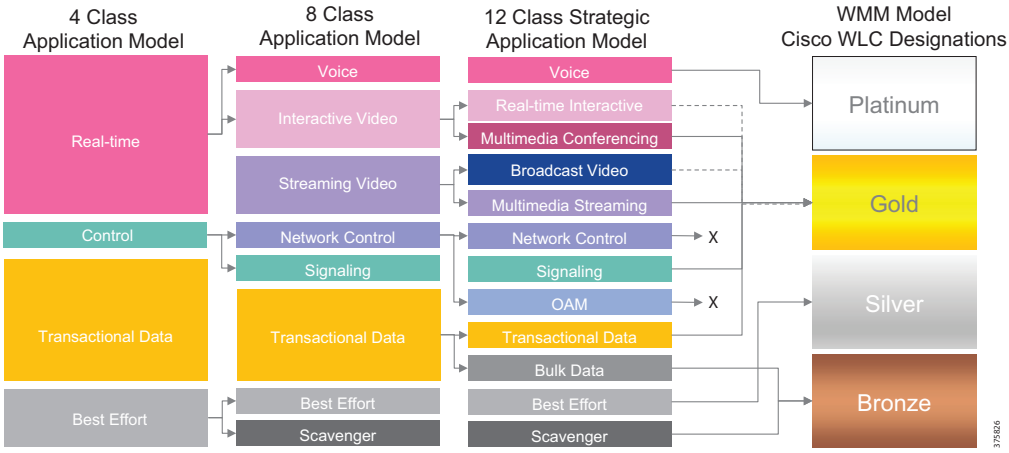
Quality of Service

Due to the half-duplex nature and Layer 2 media access control (MAC) of 802.11 networks, QoS functions differently than do wired networks. Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance specification subset of 802.11e and defines four QoS classes: Voice, Video, Best Effort, and Background. The Cisco WLC uses more generic terms for these classes with a designation based on precious metals: Platinum, Gold, Silver, and Bronze.

Although a WLAN only has four classes, that does not mean that the entire network can not utilize more than those four classes. Rather the overall end-to-end QoS strategy should be based on the organizational requirements and then mapped into these four classes at the WLAN

Figure 5-2 shows various application models, including a complex 12-class application model and its fit in the WLC WMM categories.

Figure 5-2 Application Class Expansion Models Mapped to WMM



In the 12-class application model, Network Control and OAM traffic types are not typically generated by wireless clients and therefore are not mapped to a WMM category.

Once the traffic leaves the WLC and continues upstream to its wired destination, the corresponding VLAN onto which the WLC places the traffic must be configured for the same QoS policies.

By default, 6-bit DSCP values are mapped to 3-bit 802.1p CoS and 802.11e UP values by taking the three Most-Significant Bits (MSB) of the DSCP and copying these as the CoS and/or UP values. For example, DSCP EF/46 (binary 101110) is mapped to CoS or UP 5 (binary 101) by default. For example, by default, the network switch that connects to the Cisco WLC will generate 802.1p CoS values (for the 802.1Q-trunked traffic) by setting these to match the three MSB of the DSCP values.

Table 5-1 Default Downstream DSCP to WMM Mapping

Application	DSCP	802.11e UP	WMM Profile
Network Control	56 (CS7)	7	Platinum
Internetwork Control	48 (CS6)	7	Platinum
Voice	46 (EF)	6	Platinum
Multimedia Conferencing	34 (AF41)	5	Gold
Multimedia Streaming	26 (AF31)	4	Gold
Transactional Data	18 (AF21)	3	Silver

Table 5-1 Default Downstream DSCP to WMM Mapping (continued)

Application	DSCP	802.11e UP	WMM Profile
Bulk Data	10 (AF11)	2	Bronze
Best Effort	0 (BE)	0	Silver

Conversely, in the reverse direction, the CoS or UP values are simply multiplied by 8 (in order to shift these three binary bits to the left) to generate a DSCP value. Continuing the example, CoS or UP 5 (binary 101) would be mapped (that is, multiplied by 8) to DSCP 40 (binary 101000), also known as CS5.

Table 5-2 Default Upstream WMM to DSCP Mapping

WMM Profile	DSCP
Platinum	EF (DSCP 46)
Gold	AF41 (DSCP 34)
Silver	DF (DSCP 0)
Bronze	AF11 (DSCP 10)

As can be seen in the above pair of examples, because information is being truncated from 6-bits to 3-bits, marking details can get lost in translation. In this example, the original voice packet was sent with DSCP EF, but was received as DSCP CS5 (based solely on default Layer 3/Layer 2 mapping). This needs to be taken into account when mapping from wired-to-wireless and vice versa.

Note It is critical to remember that QoS for wireless only offers a greater probability of one traffic type being differentiated or preferred over another; it is not a guarantee.

Application Visibility and Control

More granular QoS can be achieved through Application Visibility and Control (AVC). AVC increases the efficiency, productivity, and manageability of the wireless network. Also, the support of AVC embedded within the WLAN infrastructure extends Cisco's application-based QoS solutions end-to-end. AVC is available from Cisco WLC release 7.4 onwards.

AVC features include:

- Next-generation Deep Packet Inspection (DPI) technology called Next Generation Network-Based Application Recognition (NBAR2), which allows for identification and classification of applications.
- Ability to remark application QoS using DiffServ, which can then be leveraged to prioritize or de-prioritize applications over both the wired and wireless networks.
- A template for Cisco NetFlow v9 to select and export data of interest to Cisco Prime or a third-party NetFlow collector to collect, analyze, and save reports for troubleshooting, capacity planning, and compliance purposes.

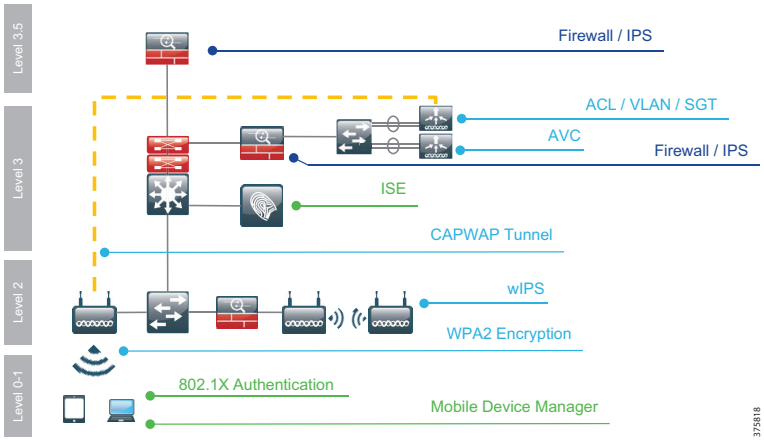
Provisioning end-to-end mobile application QoS requires policy configuration at the following points in the wired and wireless networks for downstream flows:

- WLC AVC Profiles can be configured and assigned to WLANs to identify applications and marked with DSCP or dropped. Additionally, AVC Profiles can be used to assign applications to downstream WMM access categories.
- WLC QoS Profiles can be assigned to each WLAN and define a default and maximum priority per WLAN.

Security

Security for wireless access in the refinery should follow a defense-in-depth strategy; no one box will be the solution to all security requirements. Instead, secure access is implemented at several different levels of the network. This approach is beneficial as it provides a level of redundancy by leveraging different network devices at different *choke points* in the network. The network is the enforcement point. See Figure 5-3.

Figure 5-3 Wireless Defense-in-Depth



Wireless traffic between client endpoints and the APs should be secured using WPA2 with AES-CCMP encryption. Please note that WPA2 with AES-CCMP does not extend to management frames. It is advisable to enable protected management frames on secured WLANs if the client endpoints are capable.

Clients connecting to the employee WLAN should be authenticated using 802.1X, which requires an AAA server such as the Cisco Identity Services Engine (ISE) or Cisco Access Control Server (ACS) that provides centralized policy-based management. Communication between the WLC and the AAA server uses the RADIUS protocol. Authentication of the end-user is accomplished using the Extensible Authentication Protocol (EAP). Multiple variants of EAP are available such as Protected Extensible Authentication Protocol (PEAP) and EAP-TLS. PEAP makes use of standard user credentials (username and password) while EAP-TLS uses a digital certificate for authentication, which makes the process less painless for the end user but may not be supported on all devices.

The AAA server can authenticate the user against a number of different identity stores such as LDAP or Microsoft Active Directory (AD). When a service such as AD is used, further authorization status can be determined based on the groups to which the user belongs. For example, users in a contractor group may have a different set of access policies than a user belonging to the employee group. The use of an external identity store provides a single point for granting or revoking credentials.

The AAA server can make further authorization decisions based on the type of device connecting (for example. Apple iPad or Lenovo Laptop), the OS version running on the device (iOS 9.1 or Windows 8.1), the level of anti-virus installed, the location of the end user, and time of day. All of these different parameters can be used to create differentiated access policies. Using a Mobile Device Manager (MDM)

installed on the device (for example, on Android or iOS mobile devices), Cisco ISE can make even more granular decisions based on installed applications (or lack thereof) and security polices (such as passcode enforcement). With these measures in place, devices can also be blacklisted, if lost or stolen, or even remote-wiped, if deemed necessary for security reasons.

Once the appropriate policy is determined, an ACL, VLAN, or Cisco TrustSec Security Group tag can be pushed down to the WLC and applied to the client.

All multi-service wireless traffic is terminated at the WLC and must pass through an ASA firewall before proceeding to any other zone. Any access lists specific to the client, as pushed down from a policy node such as ISE, are enforced at the WLC or ASA. If the traffic is deemed appropriate, the ASA can be configured for analysis and inspection. Any suspicious traffic can be flagged or blocked, logged, and dealt with appropriately.

The Cisco Wireless Intrusion Prevention System (wIPS) is a complete wireless security solution that uses the Cisco Unified Access infrastructure to detect, locate, mitigate, and contain wired and wireless rogues and threats at Layer 1 through Layer 3. The APs, wireless LAN controller, MSE, and Prime Infrastructure work together to provide the wIPS solution. The wIPS solution can provides a number of benefits including:

- Rogue Access Points Detection and Mitigation
- Over the Air Attack Detection
- Security Vulnerability Monitoring
- Performance Monitoring
- Management, Monitoring, Reporting

Note wIPS is not supported on the Cisco 1552 APs. In order to implement a complete wIPS deployment, Cisco 3700 series AP would be required to be deployed alongside the 1552 APs. These APs would not be handling any client or instrument data, thus their deployment and coverage will be different. The Cisco 3700 series APs, however, are not rated for outdoor use and thus would need to be deployed in a sheltered environment, if available or constrained to use only within the Control Room.

Availability

The preferred option for providing high availability for wireless controllers is a feature known as High Availability SSO. In an High Availability SSO configuration, a second WLC is effectively configured as a hot standby. The configuration and software images on the primary WLC are automatically synchronized to the standby WLC.

High Availability SSO is a stateful switchover event for both APs and clients; CAPWAP tunnels do not need to be re-established. In the event of a controller disruption, recovery times using High Availability SSO are in the sub-second range.

The standby controller can be cost-effectively licensed, using the High Availability SKU, specifically as a standby controller with the AP license count automatically inherited from the paired primary WLAN controller.

As previously discussed, when Link Aggregation (LAG) is enabled on the uplinks, the WLC can dynamically manage the port redundancy and can load-balance traffic on the APs. Furthermore, if any of the LAG ports fail, traffic is automatically transferred to one of the other ports. Thus, as at least one of the WLC uplinks is operational, the WLC and the APs will remain operational.

Further redundancy can be configured through the use of link aggregation between multiple switches in a VSS deployment. A VSS can also be referred to as multi-chassis EtherChannel.

In a mesh deployment, the wireless network is also self-healing. The Adaptive Wireless Path Protocol (AWPP) constantly monitors and adapts to changes in the network; should a node fail a new optimal root path is automatically established.

Furthermore, with Radio Resource Management (RRM) enabled, the WLC can dynamically adjust transmit power levels for a WLAN to make up for the loss of an AP.

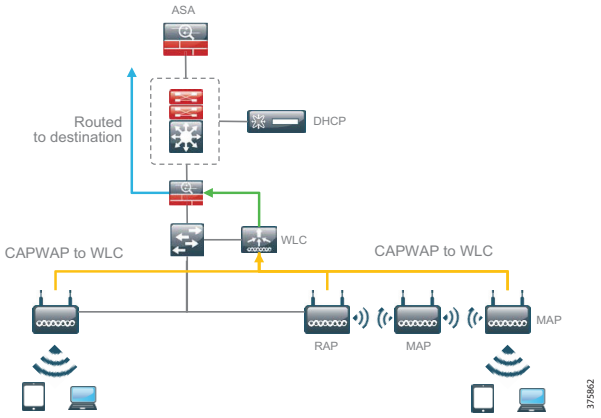
Wireless LANs

Multi-Service WLAN

The multi-services WLAN should be deployed for all APs within the refinery and secured at Layer 2 using WPA2 and 802.1X for authentication. The Cisco ISE is the ideal RADIUS/AAA server for client authentication and central policy determination. The policy will be enforced by the WLC.

Wireless client IP addresses should be handled by a DHCP server, located within the control room. The WLC should be configured with a DHCP relay for the employee WLAN virtual interface pointing to the DHCP server. See Figure 5-4.

Figure 5-4 Multi-Service Traffic Flow



Asset Tracking WLAN

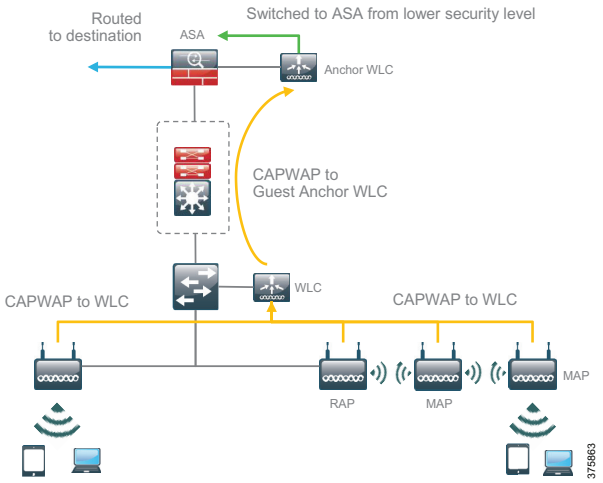
If dedicated Active RFID tags are in use for asset tracking and two-way communication with the tags is required (for example, for emergency notifications), then the tags must be associated to a WLAN. The tags will need a path to reach the location and DHCP servers in the control room. A dedicated WLAN can be deployed to maintain isolation of all traffic types. Depending on the vendor used for the tags, some encryption options may not be available for securing the WLAN. Typically, Wired Equivalent Privacy (WEP) and WPA2 (AES) are supported options.

If the tags are operating only in a beacon mode and no additional communication is required with the tags, association and thus a WLAN is not required.

Guest WLAN

Policies permitting, a guest or Internet-only WLAN can easily be deployed alongside the employee WLAN. By design, all traffic will terminate in the IDMZ, ensuring that no industrial zones can be accidentally accessed by wireless clients. This is accomplished by deploying a Guest Anchor WLC entirely outside of Level 3 the control room. By establishing a mobility tunnel between the primary WLC in the IDMZ and the Guest Anchor WLC in the corporate DMZ, this lower security traffic can be tunneled entirely outside of all critical industrial zones in the refinery and into the corporate enterprise DMZ where it can egress directly to the outside world and the Internet. See Figure 5-5.

Figure 5-5 Guest Traffic Flows

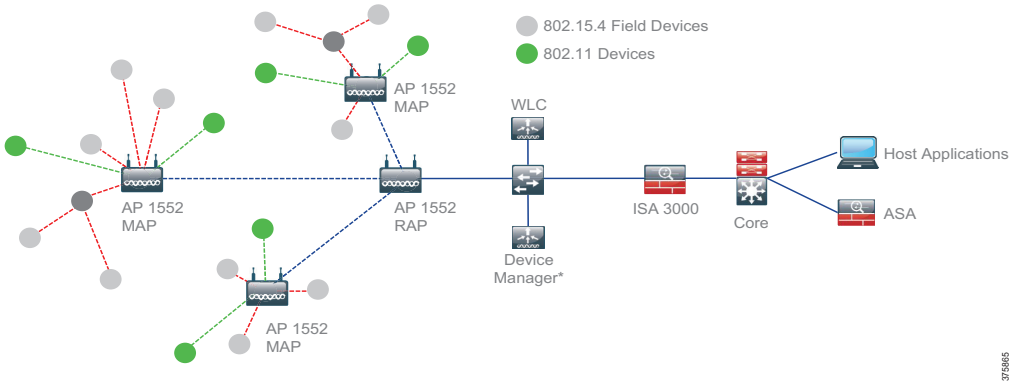


Operational Access

The refinery LAN and centralized WLAN design documented in previous sections provide the necessary infrastructure to support operational wireless traffic for communication with field instruments that use either WirelessHART or ISA100 industrial protocols. The instrumentation vendor deployed within the refinery will determine which industrial protocol should be used. Likewise, the corresponding design of the specific system managing the instrumentation will vary based on the vendor selected, but that is out of scope of this document. Emerson and Honeywell are two such vendors with whom Cisco has an established partnership and has conducted extensive testing. The primary intent of this design is to simply provide for a communications network between the field devices and their destination.

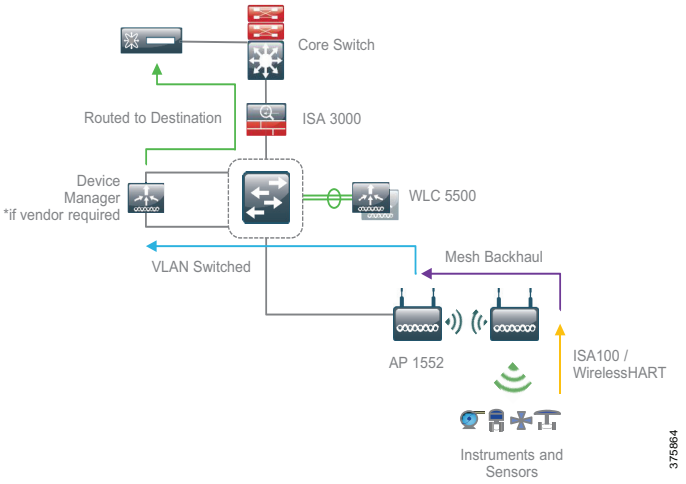
Both WirelessHART and ISA100.11a are based on the IEEE 802.15.4 standard for physical and media access control layers for low-rate wireless networks. Unlike the 802.11 Wi-Fi standard used for Multi-Service traffic, IEEE 802.15.4 was designed to offer low power, low cost, and low speed communication between devices. Both WirelessHART and ISA100 operate in the 2.4 GHz band. See Figure 5-6.

Figure 5-6 802.15.4 Mesh and 802.11 Mesh Networks



In addition to enterprise and carrier-grade 802.11a/b/g/n Wi-Fi for Multi-Service traffic, the Cisco Aironet 1550 Series outdoor wireless APs support these two industrial protocols, providing a cost-effective deployment with easier management, installation, and troubleshooting. Specifically, the Cisco Aironet 1552WU has an integrated WirelessHART radio and Emerson Smart Wireless Gateway. The Cisco Aironet 1552S has an integrated ISA 100.11a radio for use with the Honeywell OneWireless gateway. See Figure 5-7.

Figure 5-7 Operational Traffic Data Flow



WirelessHART with the Cisco 1552 WU

The Emerson Smart Wireless solution is supported with the Cisco 1552WU Wireless Access Point. A WirelessHART network consists of three primary elements:

- Wireless field devices
- Gateways to enable communication between the wireless devices and the host applications
- Network manager to configure the network, schedule and manage communication

Emerson field devices using WirelessHART are not assigned an IP address. Only the gateway on the 1552WU AP has an IP address that should be statically assigned for maximum availability. The wireless field devices send their data directly to the WirelessHART gateway on a 1552WU AP. This gateway serves as the interface between the low bandwidth field network and the higher bandwidth refinery LAN

or WLAN. The network manager can be integrated directly on the gateway. If the AP happens to be a mesh access point (MAP), then the operational traffic will be sent across the mesh network until it reaches the root access point (RAP). At the RAP, operational traffic is split off from any multi-service traffic and placed directly onto the wire on an appropriate VLAN. Meanwhile, multi-service traffic from 802.11 radios continues via CAPWAP tunnel back to the WLC. At this point, the operational traffic is routed directly to the host application in the control room via the refinery LAN. Operational traffic remains on its own VLAN from the RAP to the control room. In the most basic mode, the 1552WU access point is be natively integrated into DeltaV. The WirelessHART gateway inside the 1552WU is configured as a DeltaV node and all WirelessHART data traffic is then directed to the DeltaV switch on the primary DeltaV control network.

However, in this mode the 1552WU cannot drive WirelessHART outputs. A second approach has the WirelessHART Gateway inside the 1552WU communicating to DeltaV via specific device networks cards such as VIM (Virtual I/O Modules) or EIOC (Ethernet I/O Card) which can handle Modbus-TCP, EtherNet/IP, etc. The process traffic from WirelessHART devices is sent on one VLAN to the DeltaV switch, while a second VLAN is used to send data from the 1552WU to a DeltaV Workstation running AMS Device Manager.

The integrated WirelessHART gateway in the 1552WU mesh access points can be made redundant by directly connecting two AP gateways via an Ethernet cable. Connectivity to AMS remains the same via mesh backhaul to the RAP.

ISA 100 with the Cisco 1552S

The Honeywell OneWireless solution is supported with the Cisco 1552S Wireless Access Point. The 1552S APs requires two IP addresses, one for AP management (via the Cisco WLC) and one for the ISA 100 Backbone Router management (via the Honeywell WDM). The AP management IP can be statically assigned for maximum availability, while the ISA 100 IP will be assigned via DHCP from the WDM. The WDM needs to be Layer 2 adjacent to the wireless RAP. The WDM Field Device Network (FDN) interface must be on the same VLAN as the WLC AP management VLAN. The WDM should be the only DHCP server on the Layer 2 domain.

Field devices will communicate directly with the integrated ISA100.11a radios on the Cisco 1552S APs. Once this traffic reaches an AP, it does not go over CAPWAP to the WLC. ISA100 traffic is instead placed directly onto the wired network onto an appropriate VLAN. If the AP happens to be a MAP, then the operational ISA 100 traffic will be bridged across the mesh network until it reaches the RAP. At the RAP, the traffic is placed onto the appropriate VLAN and switched to the Wireless Device Manager (WDM) containing the Honeywell ISA 100.11a gateway. Operational traffic remains on its own VLAN from the RAP to the control room. The WDM has an embedded firewall that ensures only process data is communicated to the control system.

Security

The operational traffic is placed onto the wire at the RAP and thus can be inspected. The Industrial Security Appliance ISA-3000 is a firewall designed for industrial applications. This firewall can be placed inline between the access and distribution layers. It should operate in Layer 2 or transparent mode. The integrated Sourcefire module can be configured to inspect the traffic before it leaves or enters the process control network

Multiple security measures are built into the WirelessHART standard. Some of these features include:

- AES-128 encryption between field device and AP

- Individual device session keys to ensure end-to-end message authenticity, data integrity, receipt validation, and secrecy
- Hop-by-hop Cyclic Redundancy Check (CRC) and Message Integrity Check (MIC) calculations to also ensure message authentication and verification as to source and receiver of communications
- Devices must have a *join key* preconfigured on the device
- White listing (ACL): If individual join keys are used, devices are explicitly given permission to join the network via the gateway/network manager via an ACL entry that also includes their globally unique HART address

Security from the gateway/AP to the host system in the Control Room is secured further through:

- An internal firewall on the gateway that is easily configured to permit only the protocols and ports required for the field solution to be enabled for communication
- Ethernet-based protocols (Modbus, OPC, Ethernet/IP, AMS, HART Port, https) all support SSL-protected communications
- The gateway's internal firewall's default configuration denies all traffic
- Traffic segmentation through VLANs

Availability

Both WirelessHART and ISA100 protocols are self-healing and self-organizing. If an AP is out of range, obstructed, disabled, or otherwise unavailable, a field device will try to communicate through a neighboring device that can act as a repeater. Thus, as long as one field device can communicate with an AP, any neighboring field devices can communicate through it. In this way, multiple paths can be made available and it is important to plan for the increase traffic capacity should such an event occur. It is important to note that this relaying will require additional power and thus shorten the battery life of the device. See Access Point Coverage and Placement, page 5-17 for additional information regarding best practices for coverage to enable multiple paths.

The Cisco 1552 APs are also capable of self-healing when deployed as a wireless mesh. Thanks to the Adaptive Wireless Path Protocol (AWPP), should a MAP fail, AWPP will automatically select the optimal path to the RAP based on the number of hops and SNR. AWPP constantly monitors and adapts to changes in the network; should a node fail, a new optimal root path is automatically established.

Additional AP level redundancy for the WirelessHart gateways can be implemented with the 1552WU APs when deployed as a mesh.

Quality of Service

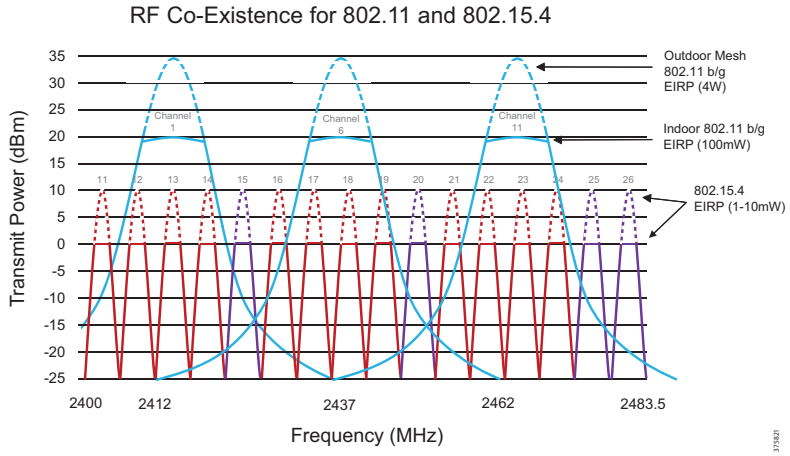
The QoS mechanism does not exist on the RF side for WirelessHART and ISA100 applications. However, once the operational traffic egresses the wireless gateway/AP, it is placed onto its own VLAN, which will have an appropriate class-map and policy-map applied.

Wireless Co-Existence

Multi-service wireless traffic using 802.11 protocols and operational wireless traffic using 802.15.4 protocols both share the same 2.4GHz frequency band. Thus, packets can interfere with each other when transmitted at the same time and frequency with sufficient energy. Both protocols use mechanisms to mitigate these issues including:

- **Frequency Diversity**—Channel hopping
- **Time Diversity**—Time Division Multiplexing
- **Power Diversity**—Low power output (<= 10dBm)
- **Space Diversity**—Mesh technology that allows for space coverage through multiple hops instead of using just output power
- **Coding Diversity**—Direct Sequence Spread Spectrum

Figure 5-8 Channel Interference for 802.11 and 802.15.4



The redundant paths offered by the meshing capabilities significantly increase reliability compared to solutions requiring direct line of site. If the network or environment changes, the self-healing, self-organizing networks find new, optimal paths for increased reliability. Combined, these features help mitigate problems not just from other RF devices, but also EM noise from other nearby sources typical in refinery and plant environments.

Based on joint testing between Cisco and Emerson conduced in a process facility with both 802.11 and 802.15.4 deployments, no significant degradation occurred in either the 802.11 network performance or the 802.15.4 sensor network performance. The sensor network did exhibit some packet loss, but, due to features such as retries and path diversity, not enough to affect the overall data reliability. The baseline data reliability was 100% and the data reliability during the test period remained at 100%. VoIP testing was also conducted in the environment with no detectable impact to voice quality.

Asset Tracking

Wireless assets can be tracked throughout the refinery network, whether or not they are associated to the network. Depending on the tag system deployed, location accuracy can be determined to within a few feet, or provide two-way communication for emergency notifications.

A Cisco-only Real Time Location System (RTLS) will require the deployment of Cisco Prime Infrastructure and the MSE alongside the WLC. These three components will work together to aggregate client data, triangulate a position, and highlight the location on a map.

Identifying an accurate location begins with an accurate map. Building or site floor plans must be uploaded to Prime Infrastructure and appropriate scaling parameters defined. It is critical that this step is properly completed to ensure accurate measurements. Multiple floors or areas can be defined.

The WLC must be added to Cisco Prime Infrastructure as a network device to be managed. Once fully discovered, Prime will be able to import the APs managed by the WLC. With the site maps are defined and APs can be placed on the map corresponding to their physical location. Client locations will be determined relative to the design of this map. To improve absolute location accuracy, GPS markers may be added to the map.

Finally, the MSE must be added to Prime Infrastructure and the maps must be synchronized.

This RTLS method is ideal for tracking any wireless clients on the premises without additional hardware. However, the interval at which beacons are sent vary from device to device, diminishing the currency of location information. If a device is turned off, no beacons are sent and a location cannot be determined. Furthermore, not all devices that need to be tracked will be using 802.11 radios in the first place. For those assets that need to be tracked in a consistent manner a dedicated system is required.

Active Tags

Radio Frequency Identification (RFID) is already a common method for tracking assets within a confined environment, but requires additional hardware to be deployed for comprehensive location information. Active RFID tags contain a battery that directly powers RF communication, allowing the tag to transmit information about itself, either by constantly beaconing this information to a tag reader or by transmitting prompted to do so by an exciter. Active tags are typically used in real-time tracking of high-value assets in closed-loop systems (that is, systems in which the tags are not intended to physically leave the control premises of the tag owner or originator).

Wi-Fi Active RFID tags are another variation, designed to operate in the same bands as 802.11 wireless networks. These tags exhibit the characteristics of active RFID tags, but also comply with applicable IEEE 802.11 standards and protocols. Wi-Fi RFID tags can use the existing Cisco wireless infrastructure without additional hardware.

Multiple vendors manufacture Wi-Fi Active RFID tags for asset tracking. These tags are battery operated and send out beacons at consistent intervals so that location currency is always known and maintained.

Tags can typically operate in two modes. The first is a one-way communication mode, whereby the tag does not need to associate and simply sends beacons that are heard by an AP. The second mode is an associated mode, whereby the tag is associated to a WLAN and both sends and receives data from a RTLS server. This data can be for maintenance purposes such as firmware upgrades or for various emergency notifications.

Some vendors use Cisco Compatible Extensions (CCX) on the WLAN to transmit additional information that can be used to track an asset or perform maintenance without association.

When using a dedicated system for asset tracking with Active RFID tags, a vendor-specific RTLS server may also need to be deployed in the control room. Depending on the vendor, the tags themselves may also need to be programmed before initial use using a tag activator. It is also important to note the frequency at which the tags will operate, with most active tags transmitting beacons at 2.4 GHz.

RSSI Probe Mode

The most basic method to determine the location of a wireless client is to collect and analyze the Received Signal Strength Information (RSSI) from 802.11 probe request frames. This method may also sometimes be referred to as Beacon Mode or Blink Mode. Probe requests are sent when the wireless client actively scans for APs with which to join. Probes are typically sent on multiple channels in order to allow the client to determine the best AP to join with. This makes the probes visible by all APs (operating on different channels) within range of the client.

The RSSI data from the probes is then forwarded from all APs to the wireless LAN controller. The WLC, in turn, forwards the aggregate RSSI data to the MSE. The MSE analyses all of the received RSSI data per client and, in conjunction with the knowledge of physical AP placement data defined in Cisco Prime, the MSE can triangulate the location of the client. The calculation is based on proximity; the closer the transmitter is to the receiver, the higher the RSSI value will be. It is thus important to have sufficient wireless coverage to allow for at least three APs to be capable of hearing probe requests from any client to effectively triangulate a location.

Assuming sufficient signal strength and AP visibility, using only probe RSSI information, client location accuracy can be achieved to within 5 meters.

Associated Mode

In associated mode, tags are configured to associate and authenticate to the WLAN for each location and maintenance update. In this mode, tags send probe requests to APs on their SSID and measure AP responses to obtain RSSI. Tags then associate/authenticate to the network to send this data to the server. In this mode, tags are capable of two-way communication and require an IP address for communication. As mentioned earlier, in this mode the tags will need a path to reach the RTLS server in the control room and a DHCP server.

In an associated mode, the RTLS server can acknowledge the tag messages and if an acknowledgment is not received, the tag can retry transmission to ensure that its location is always updated. The largest downside of an associated mode is decreased battery life.

Improving Accuracy

To improve accuracy where AP coverage may not be ideal due to environmental or cost constraints or where a much higher degree of accuracy is required, beacons or choke points exciters may be deployed. These small devices are designed to *activate* any nearby wireless tag using a short range communication method such as infra-red, Bluetooth Low Energy (BLE), or RFID. Once *activated*, the tag can send to the location appliance information about the beacon it just *saw*.

Chokepoints are tightly defined physical areas (such as entrances, exits or other types of constrictions) that provide passage between connected regions. Like an AP, these activators/beacons are placed on a map and due to their typical small range of operation, a very accurate location can be determined for that tag.

These methods should only be used to augment the broader asset tracking system.

Security

In an associated mode, depending on the vendor used for the tags, some encryption options may not be available for securing the WLAN. However, WEP and WPA2 (AES) are typically supported options.

One of the benefits of associated mode is that tags can tags can be upgraded or send additional information. This traffic will require additional scrutiny as it traverses the network. A dedicated VLAN can be used for tag traffic within the Control Room on egress from the WLC. Traffic between the RTLS server and the Control Room network should pass through an ASA firewall or the IDMZ with the appropriate ports opened.

For example, the following ports are required for proper Ekahau tag communication:

- **Location Update Port**—8552 TCP/UDP

- **Maintenance Update Port**—8553 TCP/UDP
- **Firmware Update**—8554 or 8562 TCP/UDP (device dependent)
- **Temperature Sensors**—8557 TCP/IP

Access Point Coverage and Placement

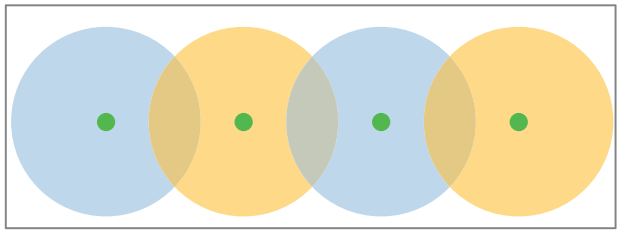
The Connected Refinery wireless network supports multi-service traffic, operational traffic, and location services for asset tracking. The placement of APs and their coverage affects the reliability and effectiveness of all services. Many refineries will include a mix of environments and thus have a variety of requirements in different areas of the refinery. The Control Room, for example, may require only a basic *data grade* network, with sufficient coverage for some workers and their laptops. However, in a different, larger, and more hazardous area of the refinery, the network must be capable of accurately tracking the locations of worker and equipment as they move around. Therefore, the network must be able to support a combination of AP deployments of varying densities.

Ultimately, AP placement will depend on customer requirements, plant design, and the RF environment. In general, the guidelines described in the following sections should be considered.

Access Point Placement for Multi-Service Applications

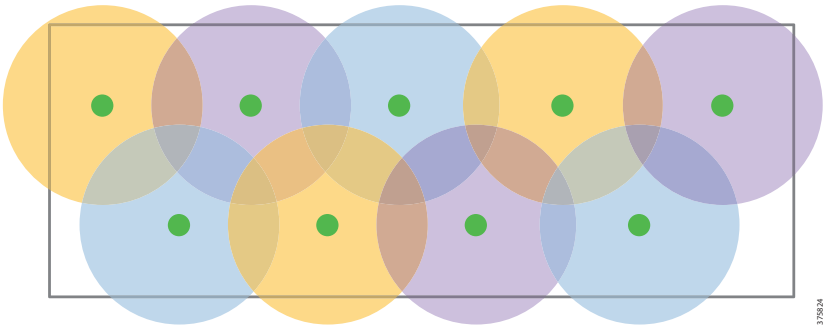
For data networks, a typical overlap in coverage is set to about 10 to 15 percent of the overall cell coverage area. See Figure 5-9.

Figure 5-9 AP Coverage—Data Grade Network



In contrast, for voice networks, a higher overlap in coverage is recommended to ensure seamless call hand-off when roaming between APs. For voice networks, the recommended overlap is 15 to 20 percent of the overall cell coverage area. See Figure 5-10.

Figure 5-10 AP Coverage—VoIP Grade Network



Access Point Placement for Operational Applications

AP placement for operational traffic will heavily depend on the environment (such as what kind of materials are present and how many obstructions), the field devices themselves, and how often a field device needs to communicate.

In general, field devices can be up to 750 feet away from a wireless gateway if there are no obstructions, they have clear line of sight (LOS), and are mounted at least 6' above the ground. Such an environment is not necessarily typical of most refineries, which will have high concentrations of metal and liquids which will alter the RF signal path.

With heavy obstruction, the typical effective range can be closer to just 100 feet. While tank farm contains large obstructions in the form of the tanks themselves, they typically have a lot of space in between, which can increase the effective range between a field device and AP to approximately 500 feet.

Another consideration when determining AP placement for operational networks is the *self-healing* mesh capabilities of the WirelessHART and ISA100 protocols. If a gateway (AP) is out of range, or for some reason disabled and otherwise unavailable, a field device will try to communicate through a neighboring device which can act as a repeater. In this way, multiple paths can be made available and it is important to plan for the increase traffic capacity should such an event occur.

The following rules should be followed:

1. A network should have a minimum of 5 field devices within range of the AP to benefit from the built in redundancy of the self organizing mesh.
2. Every field device should have a minimum of 3 neighbors to ensure a concentration of devices and provide multiple paths to the gateway.
3. Any network with more than 5 field devices should have a minimum of 25% of the devices within range of the AP to ensure proper bandwidth.

With large networks, the first two rules become irrelevant, but the third becomes critical to ensure sufficient bandwidth for all devices under various conditions.

Access Point Placement for RTLS/Asset Tracking

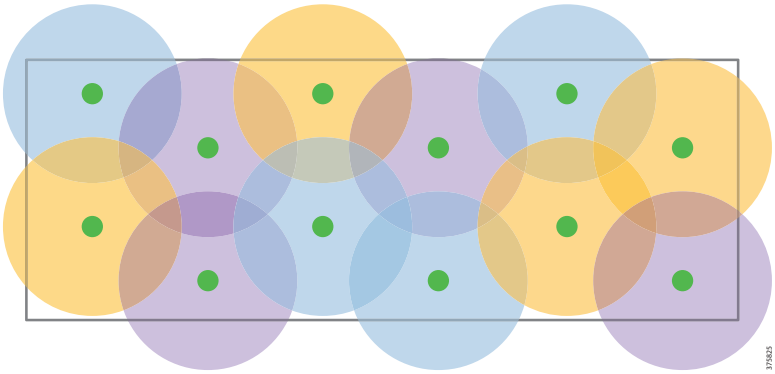
Accurate location tracking of assets will have the most stringent requirements for the placement of APs. If the WLAN is deployed with asset tracking in mind, it should be sufficient for all both multi-service and operational traffic as well. See Figure 5-11.

The design of the WLAN has a direct impact on the accuracy of location calculations. The layout of the APs, their number and density, and power configurations are all important factors for RTLS systems. Assets being tracked should be visible by at least 3 APs, with a minimum signal strength from the strongest AP at -65 dBm or better while being seen by a minimum of three APs at -74dBm or better and a Signal to Noise Ratio (SNR) of 15 dBm or higher. A comprehensive wireless site survey is a necessity in properly designing any wireless network.

These general best practice guidelines, however, should be followed:

- APs should be uniformly distributed.
- Square shapes and equilateral triangles are better than long rectangles and obtuse triangles.
- In narrow areas, avoid placing devices along a line; a zigzag distribution is optimal.

Figure 5-11 AP Coverage—RTLS/Mobility Grade Network



In an ideal environment each asset or tag will be heard by a minimum of three access points at -74dBm while connecting to one of them at -67dBm better to achieve a preferred SNR of 20dBm or better. More RSSI and SNR is required to achieve higher data rates that may be required for various applications.

In general, a greater number of APs transmitting at a lower power provides better location accuracy than a few APs transmitting at a high power. For indoor environments requiring RTLS, APs should typically be deployed within 40 to 60 feet of one another with APs placed along the perimeter of the project area as well as in the center.

Staggering APs between multiple floors, rather than overlapping the same deployment pattern, can improve location accuracy.

Outdoor environments can have less interference so it is possible for the APs to be spaced out at greater distances, from 100-150 feet. However, note that dedicated tags transmit at a much lower power level than APs. The signal from the tag must be able to reach APs, and in outdoor environments this must be considered. Typically, an AP should be no further than 150ft from a tag.

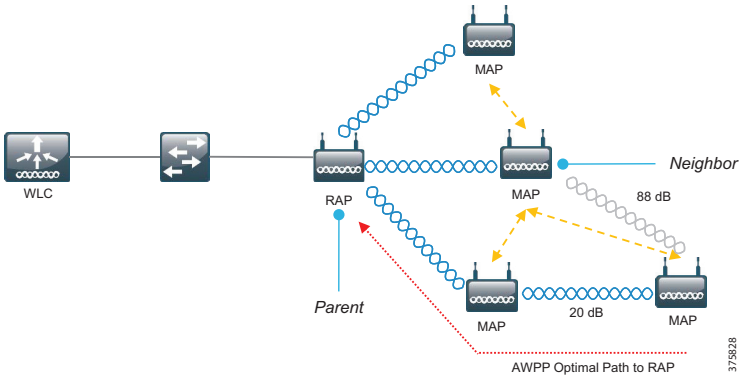
Wireless Mesh

A mesh network allows two or more APs to communicate with each other using their wireless radio. This allows network access and wireless coverage to be extended to areas where a network cable may be cost prohibitive to run. A Cisco wireless mesh network is configured and operated in much the same way as a centralized/local mode wireless deployment. The same Cisco wireless LAN controller monitors and operates mesh and non-mesh networks. Some differences in design and configuration should be considered.

Mesh APs must be configured as either a mesh access point (MAP) or root access point (RAP). A RAP has a wired connection back to the WLC while a MAP has a wireless connection back to a RAP before being able to access the WLC. The default role for all shipping APs is MAP.

Prior to deployment, all APs used in a mesh network must have their MAC address configured in the MAC filter list on the WLC. If the MAC is not present, the AP will not register with the WLC. This will prevent any rogue APs from attempting to join the mesh network. See Figure 5-12.

Figure 5-12 Wireless Mesh Path Selection



MAPs automatically select the best path to the RAP using the Adaptive Wireless Path Protocol (AWPP). AWPP dynamically discovers neighboring APs and establishes the optimal path to the RAP based on the number of hops and signal-to-noise-ratio (SNR). AWPP monitors and adapts to changes in the network; should a node fail, a new optimal root path is automatically established.

This traffic is always AES encrypted when it crosses a wireless mesh link such as a wireless backhaul. AES encryption is established as part of the MAP neighbor relationship with other MAPs. The encryption keys used between MAPs are derived during the EAP authentication process.

It is possible to specify which adjacent APs should be part of the root path calculation by assigning specific APs to a common bridge group. With a Bridge Group Name (BGN) configured, APs will only form a mesh network with other APs with the same BGN.

A MAP will go through the following stages before forwarding traffic:

1. Blocks all traffic
2. Sends adjacency packets to nearby APs to establish hop counts and signal levels
3. Selects parent AP with best route to RAP
4. Authenticates to the mesh network through an X509 certificate exchange with the WLC and enable AES encryption:
   a. Uses the same certificates as CAPWAP
   b. MAC of the AP must be defined in WLC MAC filter list
5. Joins the wireless LAN controller and establish the CAPWAP tunnel
6. Traffic is now allowed to flow through the mesh network

Although the software is capable of supporting eight wireless hops before reaching the RAP, it is recommended to keep the number of hops below 4 with a goal of no more than 2 hops depending on application tolerances for throughput and latencies. Each hop can result in up to 40% loss of throughput.

The connection between MAPs is established using the 5GHZ radio. By enabling *Backhaul Client Access*, the 5GHZ can be enabled for clients, but at the expense of reduced throughput. Depending on the desired throughput, this may or may not be desirable; with the 5GHz radio being shared, it is a tradeoff for performance.

AWPP automatically incorporates 802.11h DFS for radar detection and avoidance when determining the optimal path.

Ethernet Bridging

A wired network can be connected to the remote side of a mesh network using the wired port of the 1552 AP. In this way, a wireless mesh network can be a replacement for long wired cable runs.

Ethernet traffic is encapsulated in a mesh header at the connected MAP and is de-encapsulated at the egress point on the RAP. In a mesh network, Ethernet-bridged traffic does not go over the CAPWAP tunnel.

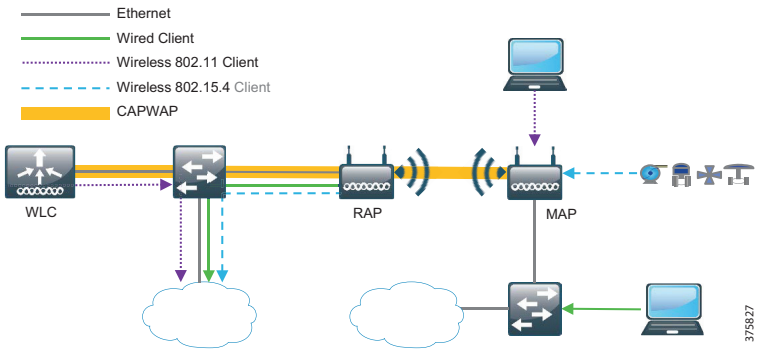
For security reasons, the Ethernet port on the MAPs is disabled by default. It can be enabled only by configuring Ethernet bridging on the Root and the respective MAPs. You must verify that any attached switches to the Ethernet ports of your MAPs are not using VLAN Trunking Protocol (VTP). VTP can reconfigure the trunked VLANs across your mesh and possibly cause a loss in connection for your RAP to its primary WLC. An incorrect configuration can take down your mesh deployment.

Ethernet bridging opens up support for a variety of use cases. IP video surveillance cameras can easily be deployed wherever a MAP is available by connecting to the wired port, requiring only a further power connection.

Traffic Flow

Unlike multi-service 802.11 wireless traffic that must travel via CAPWAP to the WLC, traffic from wired clients will egress directly at the RAP. That is, the wired traffic will continue on to its destination on the wired network as soon as it leaves the RAP. See Figure 5-13.

Figure 5-13 Wireless Mesh Traffic Flow



Availability

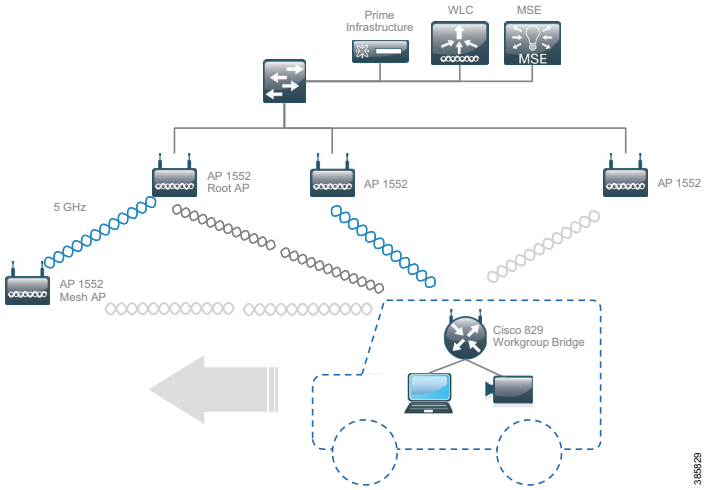
Failure of any MAP is automatically mitigated by the AWPP protocol. A new optimal path to the RAP will be dynamically established when the conditions are changed.

The RAP itself however can represent a single point of failure. Multiple RAPs are recommended to ensure a wired path to the controller will always be available. It is also recommended to maintain fewer than 20 MAPs for every RAP in the mesh network.

Vehicle Mobility

A wireless AP can be used to provide wired client access inside vehicles as they are driven around the refinery. The Cisco 829 Integrated Services Router (ISR) suits this role well with an integrated switch and can associate with APs deployed throughout. For this role, it is recommended to deploy the 829 as a Workgroup Bridge (WGB). In WGB mode, the device associates to another AP as a client and provides a network connection for the equipment connected to its Ethernet port. As a client on the wireless network, the WGB does not need to be registered with the WLC nor can it have MAPs trying to establish paths through it. See Figure 5-14.

Figure 5-14 Vehicle Mobility Connectivity



Note Although it will not be an issue when deployed on a moving vehicle, any AP operating as a WGB can introduce a bridge loop if connected back into the wired LAN.

For vehicle deployments, the WGB should configured as a *mobile station* to enable roaming. With this configured, upon receiving a poor Received Signal Strength Indicator (RSSI), excessive radio interference, or a high frame-loss percentage, the WGB will scan for better radio connections to a new parent AP. It will then roam to the new AP before losing the current association. Without this configuration, the WGB will not change parent AP associations until the current connection is lost.

If the outdoor APs are deployed with a minimal set of channels, roaming efficiency can be improved by limiting the channels scanned when looking for a new parent. By limiting the number of channels, the WGB scans to only those required while the mobile WGB achieves and maintains a continuous wireless LAN connection with fast and smooth roaming.

Note Performance may be severely impacted depending on the speed of the vehicle while it is roaming throughout the network and the hardware deployed inside.

CHAPTER 6

Deployment Considerations

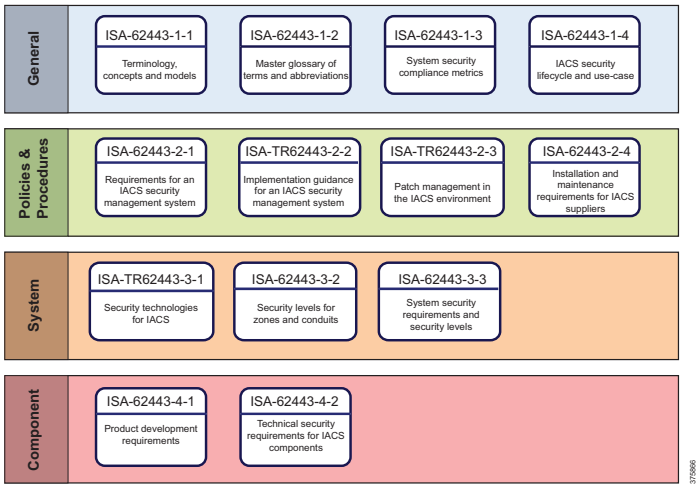
This chapter includes the following major topics:

- ISA-99/IEC-62443, page 6-1
- Wireless Site Surveys, page 6-3
- Installation, page 6-15

ISA-99/IEC-62443

The International Society of Automation (ISA) has developed a set of standards to address cyber security issues in industrial automation and control systems. This collection of documents was referred to as ISA99 to define procedures for implementing Industrial Automation and Control Systems (IACS). In order to align with the International Electrotechnical Commission (IEC), the documents were renumbered to ANSI/ISA-62443. Thus ISA-99 and IEC-62443 are the same standards and refer to the same set of guidelines. See Figure 6-1.

Figure 6-1 Work Products of ISA-99



Specifically, the IEC-62443-3-3 standard focuses on how to secure access, data, and systems that are operationally focused and at the core of any IACS. This standard is based on seven foundational requirements:

1. Identification & Authentication Control

2. Use Control
3. System Integrity
4. Data Confidentiality
5. Restricted Data Flow
6. Timely Response to Events
7. Resource Availability

No single box addresses each of these requirements, but multiple devices and technologies in the Connected Refinery can work together to deliver a comprehensive security solution which helps an organization adhere to these standards.

The Connected Refinery Solution addresses these requirements in the following methods:

- **62443-3-3.5 Identity Authentication and Control** ensures that any user or device accessing the IACS is supposed to be accessing the IACS. The Connected Refinery employs the Identity Services Engine (ISE) for AAA purposes and acts as a single, centralized source of truth for all security policies. ISE allows for the identification and authentication of all users and devices on the network. The NGFW/ASA in the IDMZ provides an additional level of policy management enabling an organization to monitor and control access across zones or from untrusted networks. The Cisco TrustSec solution works in combination with ISE, the ASA, and the access layer devices to simplify policy administration and application. Meanwhile, the access layer switches, routers, and access points act as a sensor on the network, identifying and passing up information about the traffic and devices as they come onto the network.
- **62443-3-3.6** enforces the assigned policies of authenticated users and devices on the network. Here again, ISE can apply security policies for individual endpoints based on a variety of factors for precise control. The access devices of the IACS and the ASA will then enforce that policy.
- **62443-3-3.**7 ensures the integrity of the system to prevent any unauthorized manipulation. ISE again proves its value by combining device posture assessment and threat analysis to ensure conformity to an organizations policies and provide automatic remediation capabilities to identify, track, and quarantine devices to prevent unauthorized access. The trust anchor feature on Cisco platforms ensures that the system is unmodified from start-up through the boot cycle.
- **62443-3-3.8** ensures data confidentiality of communications channels and repositories. Both WirelessHART and ISA100 encrypt their wireless traffic, and the 802.11 multi-service WLAN is configured with AES encryption as well. While in transit, CAPWAP control packets with a WLC 5508 are always encrypted, while data encryption is configurable. Cisco TrustSec also offers MACSEC encryption at the data link layer between each hop.
- **62443-3-3.9** restricted data flows are designed to segment the IACS via zones and conduits to limit unnecessary flow of data. This segmentation is accomplished at a number of levels in the Connected Refinery. The network is logically segmented throughout by use of VLANs and VRFs to ensure that operational and multi-service traffic never meet. Cisco TrustSec on ISE can simplify policy management in one central location by assigning Security Group Tags (SGT) to ensure a consistent access policy and reduce management overhead.
- **62443-3-3.10** deals with the ability to quickly respond to and remediate an event. The network must quickly be able to identify and respond to any event. ISE logs all attempts to access a network and can work with other tools through PxGrid to rapidly identify issues. Depending on policy implementations, ISE can also automatically apply quarantine or blacklist policies to prevent devices from accessing the network when certain conditions are met.
- **62443-3-3.11** ensures that the availability of the IACS. Multiple features deployed within the Connected Refinery help maintain the availability of the IACS. HA deployments of controllers, firewalls, redundant power supplies among others help ensure that no single device can be a point

of failure. Other rapid convergence technologies in the access network such as REP ensure that the critical access layer is always available. In the control room and data center, technologies such as vPC and VSS ensure that no single failure can affect traffic.

Wireless Site Surveys

A radio site survey is highly recommended before the installation of any equipment. The purpose of a site survey is to conduct a detailed engineering study to create a competent network design that, once installed, will meet the needs of each use case that has been identified for the area. At the same time, the site survey gathers site-specific information that will aid in the installation of core infrastructure such as cabling, electrical and AP hardware installation needs.

A proper site survey involves temporarily setting up an appropriate AP and antenna combination in deterministic locations to test and measure several facets of wireless connectivity such as Coverage, Signal Quality, Data Rate, Signal Overlap, RFI/EMI, and Environmental issues. This data is then analyzed to determine the correct hardware and install locations before undertaking the larger project costs of drilling holes, routing cables and conduit, and then mounting equipment.

Without a proper site survey or engineering design study conducted, that equipment might be installed in non-optimal locations that greatly reduce the potential equipment performance resulting in coverage gaps and application problems. This would then require more equipment installed at high costs to overcome the potential coverage gaps and therefore increase overall project costs perhaps far beyond the cost of simply doing the site survey (numerous instances have been experienced supporting the statements in this paragraph).

Processes and Methodology

Pre-Survey Data Collection

An engineer must investigate the customer requirements to ensure that the survey accommodates proposed performance criteria as stated by the customer, equipment, and application vendors. Thorough analysis may reveal non-typical needs that affect the site surveys.

For example, large outdoor areas with low user density would likely require a survey based on fewer AP installation points with more power and higher gain antennas. On the other hand, indoor environments with a high user density would likely require a survey based on a higher density of APs with lower power and less antenna gain to minimize coverage patterns, therefore providing higher aggregate capacity.

Example customer requirements could consist of the following:

1. Areas that require coverage to support WLAN and other applications
2. Density of users to support
3. Client devices to support for WLAN:
    a. Identify equipment parameters of any other WLAN client device
    b. Specific applications that are suspected of requiring high network performance should be documented to understand the following:
        1. WLAN requirements
        2. Throughput requirements
        3. Network access (constant or bursting)

4. Cisco 7925 802.11a/b/g example:
   - All data rates supported, suggest minimal 12Mbps for 802.11a/g
   - 40mW max transmit power for 802.11a/g, 50mW for 802.11b
   - Diversity antenna for 5GHz 802.11a only
   - RSSI greater than 35dBm (minimal -67dBm for 802.11b/g)
   - 25dB Signal to Noise Ratio (SNR) for survey
   - Packet Error Rate (PER) 1% or less
   - 19dBm separation between same channel APs to minimize elevated noise levels and co-channel interference
4. Designated high throughput rates for maximum network performance per AP
5. High density areas such as training rooms, cafeterias, equipment docking stations to be covered
6. 802.11a/b/g/n
7. Support for legacy 802.11b client devices
8. Propagation control to minimize unwanted coverage
9. Support for additional applications in the future not already identified

WLAN Equipment Settings

Access Point Settings

The site survey should be conducted with the same equipment that will be used for deployment such as specific AP and antenna models, Cisco products that are best suited for Oil and Gas locations will have an *H* designation representing Hazardous rating for Class 1 Div 2 / ATEX Zone 2. These hazardous-rated APs may be used in locations rated up to Div 2 / Zone 2, but not in locations beyond such as Class 1 Div 1,0 / ATEX Zone 1, 0 without being housed in additional specific enclosures that are compliant with the more stringent environmental requirements. Cisco has a partner solution that will meet the needs of these more stringent environments.

To maintain some level of flexibility to scale up and down with coverage, it is highly recommended that AP power levels be set at equal to or one power level below maximum client transmit power to ensure testing and design with reciprocal communications between AP and client devices. This way if any minor environmental changes occur that effect coverage, the installed network may stand a better chance to adapt to negative effects caused by those changes. All other AP settings should emulate the installed network such as data rate and channelization.

Equally important is the correct use of antennas with each AP location. It is best to have a small array of antennas available to best fit the environment. Antenna Diversity/ Multiple-Input and Multiple-Output (MIMO) should be employed when possible to enhance performance, this enhancement is most noticeable in areas where WLAN devices are susceptible to negative environmental effects such as multi-path, which is found in areas like that of high density piping in a processing unit.

Client Utility Settings

Client utility settings should represent the worst case scenario WLAN client device to ensure that no coverage gaps or performance issues will occur. Once the client utility is properly set up, then the survey can be conducted to achieve the minimal baseline application requirements as specified during the customer requirements identification. Client utilities will be highlighted in Survey and Test Tools, page 6-5.

Environment RF Assessment

A radio frequency (RF) spectrum analysis is used to thoroughly inspect localized radio spectrum. This analysis is commonly conducted for the purpose of exploring for sources of radio frequency interference (RFI) where suspected communications interference is thought to be of concern. The analysis data can be helpful for equipment channelization and interference avoidance.

Spectrum Analysis

The principle goals of a spectral analysis are to search for and locate sources of mitigating radio frequency interference and then act accordingly to reduce the effects to other equipment and end-user applications. Although comparatively rare in everyday life, RFI opportunities increase proportionally to the density of wireless devices. Therefore, areas such as medical, military, industrial, and commercial environments are more prone to effects of RFI due to wireless equipment being more commonplace as a result of applications needs. Other factors that effect RFI are band utilization from emitter oscillation and dwell times. Identifying these elements may also identify the source.

The following methodology may be used to determine sources of RFI:

1. Choose a location where equipment is sensitive to RFI or suspected and visually inspect for obvious sources such as antennas and transmitters.
2. Inspect the equipment to gather any detailed information such as operating frequencies and statements of Effective Isotropic Radiated Power (EIRP).
3. Energize the spectrum analyzer with a zero gain multi-band antenna that can cross multiple frequencies. The antenna should be free of obstruction to enable proper reception of surrounding signals.
4. Readings should be taken across the spectrum with particular attention and detailed analysis in frequencies of interest. Frequencies of interest include known ranges used by equipment, nearby side bands, and potential harmonics. The information received will illuminate out-of-tolerance operations and potential sources of RFI.
5. If sources of RFI are observed, accurately measure the frequency, amplitude, dwell time and oscillation time to cross-reference with known allowed emitters and determine the level of interference perceived.
6. Locate the sources of mitigating interference by moving the spectrum analyzer around and observing amplitude changes. Or use a directional antenna tuned for that particular frequency for rudimentary direction finding to zero into the area.

Survey and Test Tools

WLAN and Voice over WLAN (VoWLAN) deployments have a growing number of survey and test tools. Many of these tools have common capabilities for generalized site surveys. The following are the variations that may be pertinent to site surveys:

- Free tools are available for generalized WLAN information and have been used incorrectly as a definitive site survey tool.
- Client-specific tools such as the embedded client tools on the Cisco 7925 Wireless IP Phone and client utilities for laptops and tablets can provide very good basic information from the actual client perspective.
- Premium diagnostic hardware and software tools provide more in-depth information about the testing and environment. These tools evaluate passive, active, and even packet level information. AirMagnet and Ekahau are two Wi-Fi survey test tool companies that are commonly used.

Premium Site Survey Test Suites

The AirMagnet Survey product allows field engineers to collect live information on signals, packets, and spectrum data during site surveys. This information may be collected while in active and passive modes; active mode surveys can reveal more detailed information while passive modes may allow for faster survey methodologies.

Survey Pro can coordinate test data with imported drawings and map data that can be correlated to reference points as well as spectrum analyzer data to help visualize wireless network coverage.

Figure 6-2 Indoor Site Survey Channelization

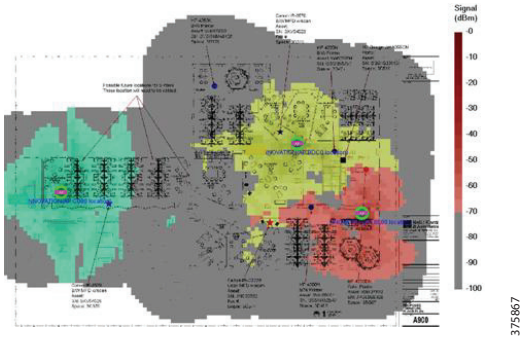


Figure 6-2 shows indoor survey data with colors enhanced to show channelization.

Site Survey Techniques

General site survey techniques vary among engineers based on experience and training, this may result with wide ranging designs for the same environment. Each of these different designs may be sufficient; however, this lack of uniform methodology and design principles can leave a customer or end user questioning these facets of the technology. Topics in this section include Baseline Propagation Assessments, Active Site Survey, Passive Site Survey, 2D Site Surveys, and 3D Site Surveys. These principles can be applied to indoor and outdoor environments, including Oil and Gas facilities onshore and offshore.

Work Safe

Safety is the first priority when working in any environment, especially within Oil and Gas locations. Several levels of safety training and certifications that may include national, regional and site-specific training should be expected. For budgetary purposes, from 8 to 40 hours of instruction that will define the key requirements for safe working conditions at the location can be expected.

Additional site-specific safety training might be required when wireless site survey and installation conditions require:

- Work at heights (platform, lifts and ladders)
- Equipment operator (high lifts)
- Confined Spaces
- Helicopter transport to offshore (dunk tank crash survival training)
- Lockout / Tagout

A best practice for safety and security is to ensure a local site escort be present at all times with the survey/installation team and that this escort be on constant alert for potential hazards during the survey process.

Personal Protective Equipment (PPE) is sometimes available in limited quantity on the job site and is recommended that a field engineer have their own minimum set of items that comply with local standards. Example minimum PPE items include:

- Flame resistant coveralls and clothing
- Steel toed boots with a defined heel and high upper for ankle protection
- Hard hat
- Safety glasses (additional safety goggles sometimes required over the glasses)
- Hearing protection (foam inserts and outer earmuffs)
- Flame resistant leather work gloves
- H2S or 4-in-1 personal gas detector (likely loaned from customer site)

Site Survey equipment must be rated and operated around the environment that it is rated for. Cisco hazardous-rated APs are rated for Class 1 Div 2 / ATEX Zone 2 environments, it is important to note that these devices must be powered externally so be sure to use a compliant safe method of temporarily powering the APs. Site Survey laptops/tablets used for collecting data must also be rated for the environments that they will be taken into.

Figure 6-3 shows Cisco Network Consulting Engineers (NCEs) working at a refinery.

Figure 6-3 Cisco NCEs Working at a Refinery

Baseline Propagation Assessment

The purpose of this assessment is to better understand propagation within an environment to establish general survey guidelines for that facility. Guidelines to consider are acceptable antenna types, maximum or minimal AP power settings, and general separation between APs to maintain as low of a noise floor as possible.

This baseline assessment may be considered more important in multi-floor environments where WLAN infrastructure is deployed in three-dimensional rather than two-dimensional planes. Understanding between floor propagation and attenuation characteristics may affect overall positioning of APs on each floor as the findings may prohibit cookie cutter deployment techniques.

Cookie cutter deployments refer to multiple situations or environments that are the same or very similar. In the case of a multi-floor facility this would refer to the general layout of the floor plan being the same or similar on each floor such as in a hotel, office building, or hospital patient wards. In these environments, a cookie cutter deployment technique would be using the same AP placements on each floor, and creating stacked columns of APs throughout the building.

Two potential issues with the cookie cutter stacked AP deployment occur, depending on the amount of through floor propagation and attenuation values. The first issue is if the attenuation values are minimal between the floors and AP locations on adjacent floors happen to be configured for the same frequency. This deployment would suffer from co-channel interference between the APs and a significant noise floor. The 19dBm of separation between co-channel APs noted in the Cisco 7921 Design Guide (OL-6383-04) should be considered from all directions.

The second potential cookie cutter issue involves roaming algorithms of various client devices. Those devices that may use RSSI levels as the primary or only factor to determine roam have been observed exhibiting *roam-lock* behavior. Roam-lock is a description used when client devices show a tendency to roam between APs continuously, thereby using more cycles to initialize and re-initialize connections rather than pass data. The result of this scenario is very low data throughput with the connectivity issues.

Test Criteria

In a multiple level facility, select any three sequential similar levels to conduct the tests. If the network is to support 802.11a/n/ac and 802.11b/g/n, then these tests should be conducted with both technologies. If both technologies would be used, then it is best practices to first conduct these tests with 802.11a/n/ac, determine the best power settings, and then do 802.11b/g/n and alter power settings for those frequencies to match coverage cells to that of the 802.11a/n/ac coverage cells. This matched coverage cell architecture will ease overall design and deployment issues.

Step 1 Set up one AP in one area of the middle floor. Set Power level on Access Point to at least one power level below the maximum power of supported client devices or to the minimized power level required to provide minimal coverage for the application in that particular environment. This method would allow scaling coverage up or down once installed.

Step 2 If using the actual client device that the facility is being surveyed for such as the Cisco 7925, then use the typical configurations on that device during the survey test activities. It is advisable to use engineering technical tools that specialize in site survey data acquisition. If using a test tool client adapter for testing rather than the actual client, then set client adapter power to emulate the actual client device that this survey is designed for.

Step 3 Begin the site survey for the AP location to determine coverage area of that AP on that level with the specific power setting and antenna configuration while recording the data.

Step 4 If 5GHz 802.11a/n/ac and 2.4GHz 802.11b/g are to be used for this location, then at this point configure AP power for 802.11b/g while standing at the edge of the 802.11a coverage cell to match the cell sizes. Once this is achieved, you have established the baseline power levels for both 802.11a and 802.11b/g. This step is omitted when using outdoor mesh equipment where the 5GHz radio is only used for backhaul communications and not supporting client connectivity.

Step 5 Once this baseline is established, then re-do the site survey process in that same floor for that same AP location for 802.11b/g coverage ensuring that this information is documented.

Step 6 Conduct an active site survey on the two adjacent levels for each wireless band (802.11a and 802.11b/g) and document the results of each test. If the signal strength is not sufficient to obtain detailed diagnostic data, then switch to passive mode and collect any data available.

Impact on Survey

If substantial propagation is found on adjacent levels, then staggering the AP locations on each sequential level rather than stacking them would be prudent to provide additional physical isolation attenuation between AP locations. This testing may yield a survey and installation pattern that could speed up the remainder of the survey process.

Implementation Considerations

Many influencing factors should be considered when designing and deploying a wireless network. Each of the topics listed has a unique ability to affect wireless communications and thus must be considered during the site survey and installation process.

Common RF installation considerations include:

- Fresnel zone
- Knife-edge diffraction
- Obstruction shadowing
- Environmental attenuation
- Reflection and scattering
- Multipath
- Delay spread values
- Antenna polarization, isolation
- Reactive near-field, Radiating near-field
- In-band RFI and out-of-band RFI / Harmonics
- EMI
- RF Noise floor
- Equipment specifications
- Antenna field of view
- Antenna E and H planes
- Survey characteristics:
  - Coverage
  - RSSI
  - SNR
  - Data Rate
  - Retries / Loss
  - Overlap/Redundancy
- Required Infrastructure:
  - High installation costs

Regardless if stacking or staggering AP locations between levels, site survey engineering personnel should also consider how the overall layout applies to applications such as location appliances that rely on RSSI triangulation to determine approximate locations of a client device. In an Oil and Gas processing area, the elevated spaces may only require singular AP locations to provide the needed coverage or connectivity. A suitable location on infrastructure like a vessel or stack may not exist to install APs to support RSSI triangulation; therefore, location information might be limited to the nearest AP and a wider margin of error. Additional accuracy might be yielded with complimentary third-party localized exciters that can monitor when Wi-Fi client devices pass by a near-field micro-area such as a doorway or ladder access.

Passive Survey

Passive site survey results use test tools in a receive-only mode for interpreting WLAN and general RF diagnostic data within an environment. This capability, which is provided by both low- and high-end site survey tools, is integrated into mapping functions of the higher-end tools. Passive survey tools generally provide a bird's eye view of all WLAN devices within an area based primarily on signal strength, however, they may not the provide detailed signal quality information that is obtained with an active site survey.

Conducting a passive site survey with multiple APs will yield overall information of all APs receivable in a test environment. A field engineer must consider the ramifications of this type of survey. For example, this method may place APs in a generally well-guessed correct area, but one that ultimately may not be optimal.

Active Survey

Active site survey results show greater detail of the local WLAN and RF environment. Interpreting this test information can help a field engineer to identify signal strength and quality while also revealing issues of RFI or EMI within the test environment. For example, in an environment where the survey utility experiences high signal strength but very poor quality as represented in high packet retries and/or high packet loss, then this may be an indication of local RFI or EMI. This type of information within a plant can be critical to a field engineer when considering AP placement and antenna choices.

Predictive Survey

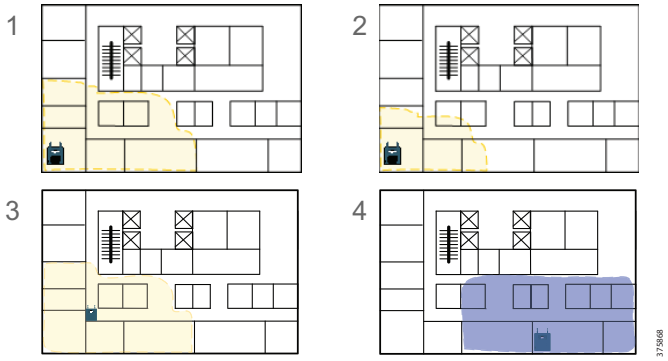
Predictive site surveys are conducted via computer modeling to estimate the approximate location and number of APs required to provide coverage in a given area. Predictive modeling accuracy is highly reliant on the amount and accuracy of data put into the modeling tool to interpret attenuation and reflection boundaries. Predictive is considered a tool best for estimating because it doesn't have the ability to fully simulate local environmental effects of RFI, EMI, environmental, and construction issues that are not represented in drawings or clutter data. Onsite analysis is still required to validate predictive results and then finalize with local testing to determine the actual AP performance and install location data.

Two-Dimensional Site Survey

A two-dimensional site survey only addresses WLAN coverage on a single floor. This has been the common practice for many since the introduction of WLAN devices and is still widely used today.

One methodology for conducting a site survey is referred to as the corner-out method. This process can be considered time consuming; however, the time invested in gathering information will yield the highest level of accuracy for the AP placement within an environment.

Figure 6-4 2D Site Survey



Step 1 The first step in the corner-out method is to locate the AP in the furthest corner of a facility that may need guaranteed coverage with the antennas of choice for that environment. Determine the area of coverage emitted from that location. This defines a boundary in which you could then safely relocate the AP anywhere within while still providing coverage to that remote corner where you began the testing.

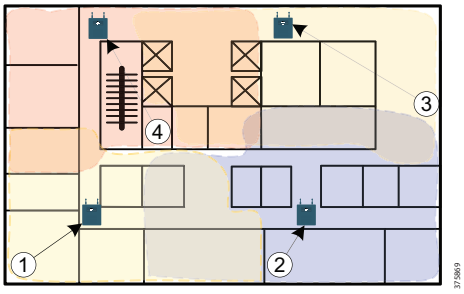
Step 2 The next step is to determine the power levels and coverage cell size based on area WiFi client user density and application density requirements. If this is an 802.11a and 802.11b/g survey, then these power levels should be changed on all interfaces to have a matched coverage cell size. The area of relocation for the first survey point has now become more defined.

Step 3 With the AP moved into its first official test location, the site survey will yield the anticipated controlled results. Depending on the desired results, it may be best to leave an AP in remote rooms for more cellular isolation that directly relates to the density of APs required to support coverage. Utilizing remote rooms with APs on the outer edge of a building and a mix of other AP locations inward of a building may provide more accurate triangulation data for Cisco Wireless Location Services. APs are typically located in hallways where they are more serviceable and where the hallway itself provides an unobstructed conduit allowing further propagation range from a single AP location if so desired.

Step 4 Each additional AP location may be methodically determined in the same manner from the outermost location requiring coverage within a cell.

Step 5 Continuing with this site survey method will yield highly accurate results for the rest of the floor. Each color indicates channels 1, 6, and 11.

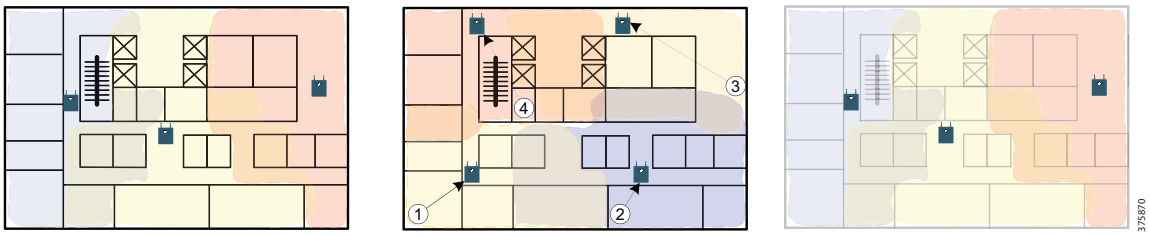
Figure 6-5 2D Site Survey



Three-Dimensional Site Survey

For buildings that have multiple floors requiring coverage throughout, the field engineer must consider the ramifications of AP coverage bleed through from adjacent floors. Remember that the Cisco 7921 Design Guide specifies 19dBm of isolation between APs on the same channel-that isolation is required from all directions not just the same floor.

Figure 6-6 3D Site Survey



This may lend to a survey and deployment method of staggering rather than stacking AP locations between floors to provide greater physical separation and signal isolation. The term *stacking* refers to placing the APs in the same location on every floor, there by reducing the overall physical isolation between them and making them more susceptible to co-channel interference from adjacent floors.

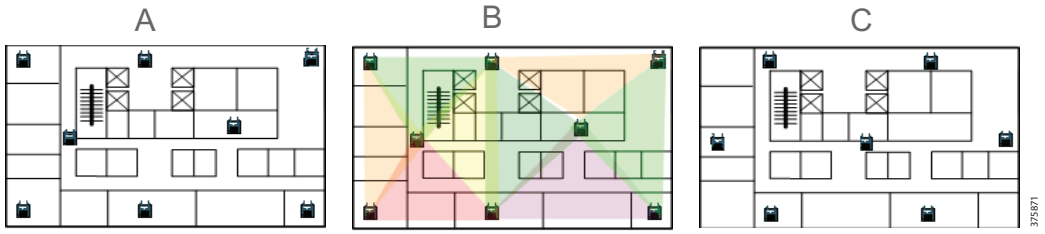
Surveying each AP location for 3D results may require as much as 200% more time. For buildings that have same or similar configured floors, then conducting the baseline survey and establishing an acceptable pattern between floors for every other floor AP placement can significantly reduce the additional time required for this type of survey. Information to determine the amount of space needed for physical isolation can be obtained using the described Baseline Testing Methodology within this document.

Advanced Site Survey for VoWLAN and Location-Based Services

Recent popularity for applications such as Context Aware location services has changed the mechanics of the site survey once again. Cisco's current recommendation for a WLAN that supports Location-Based Services (LBS) is that any area requiring this feature be seen from at least three APs with no less than -74dBm signal strength on the same floor or level. An increase in AP density over traditional methods will be required to do this with 802.11b/g/n and 802.11a/n/ac standards.

One effective method to increase AP density while maintaining a lower noise floor is to provide outside-in coverage. This method uses the physical boundaries of a building to better isolate coverage for more of a *pico-cellular* design to minimize co-channel overlap at the same time.

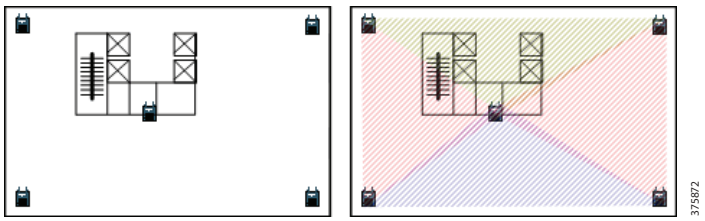
Figure 6-7 Indoor Site Survey Channelization



- In Figure 6-7, Map A illustrates the higher AP density that may be required to support location services for 802.11a/b/g/n/ac devices with greater accuracy. The by product of this method is a higher wireless density for more aggregate wireless capacity.

- Map B illustrates perceived triangulation areas in support of LBS. When planning a survey, the field engineer must consider what their approach will be to provide this triangulation and perhaps visualize the design goals.
- Map C illustrates an adjacent floor installation where the access points have been staggered rather than stacked. This method may not be necessary if minimal through floor penetration is experienced during the baseline survey. Again, generally it is recommended not to stack/replicate locations in order to enhance cellular isolation.

Figure 6-8 Site Surveys for Large Open Spaces



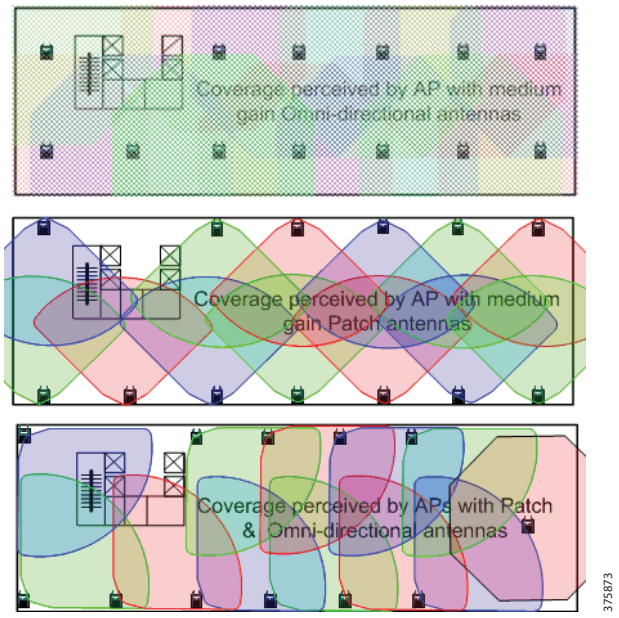
For large open spaces, the AP density will likely be less but accuracy may also be less as a result. One must account for the AP density and determine if this provides the level of accuracy desired given the applications relying on location based services

Omni versus Directional Energy Surveys

Predominant antenna technology used indoors has been and is Omni-directional. These antenna types include the dipole or *rubber duck*, low profile ceiling mount, and medium gain stick type antenna. Generally, these are all very good antennas developed to maximize performance in all directions from a single installation point in the middle of a small or large area while minimizing installation requirements.

Some large-scale, open-air environments where numerous APs required for coverage may also be well within each other's coverage pattern may challenge this type of antenna technology. Remember that higher gain antennas on APs *see* the environment much differently that zero gain antennas on client devices. For these environments, a field engineer must consider the benefits of directional energy to provide controlled propagation while also isolating noise sources that are out of the antenna pattern.

Figure 6-9 Omni versus Directional Energy Survey



The examples above illustrate the concept of controlled propagation to provide a lower noise floor with which the APs and client devices would have to contend. The top graphic shows a noisy environment with all Omni-directional antennas then the same area using directional antennas. These alternative designs have been proven in certain situations to lower the overall noise floor dramatically thereby enabling higher quality WLAN communications. It is important to note that the same baseline concerns then techniques used for two- and three-dimensional surveys still apply when using directional antennas.

Impact of Use Cases and Site Surveys in Oil and Gas

For Oil and Gas process areas, the common AP will be an outdoor hazardous-rated AP and the most common antenna of choice will likely be a medium gain dual band omni-directional antenna. Applying the information from previous sections, we can surmise that many of these outdoor environments will benefit from maximizing coverage with omni-directional antennas from minimal installation points as a means of minimizing installation costs.

The use cases will drive wireless requirements and AP densities within a location. Table 6-1 represents example comparisons of equipment requirements based on different use cases.

Table 6-1 The Size of the Wireless Network

Type of Wireless Network	Approximate # of APs per 10 Acres	Approximate # of APs per 10 Hectares
Process Control Network - wireless monitoring with 802.15 base stations on Cisco Mesh	2-4	5-10
Handheld computer data entry	8	19
Voice over WLAN with Cisco 7925G-EX	12	28
Video over WLAN for Remote Expert	12	28
Video over WLAN for Physical Security	2	5

Table 6-1 The Size of the Wireless Network (continued)

Type of Wireless Network	Approximate # of APs per 10 Acres	Approximate # of APs per 10 Hectares
Location Analytics / Man Down (based on 2D coverage, 3D requires additional APs for elevated structures)	36	84
Wireless data connection of land based oil drilling wells with high power client devices	1	3

Note The numbers in Table 6-1 are case study numbers and serve only as approximations. The actual number of APs required will be determined during a proper site survey and network design.

Network Optimization

The end user should be made aware that the survey is valid for the site as it existed during the onsite survey activities. Any changes made to the environment post survey can potentially invalidate the results. A post installation survey should be completed in order to tune and optimize the WLAN especially for a VoWLAN and/or LBS site survey. Consideration should be given to verifying coverage, roaming, channel, and TX power usage.

Installation

Installation of the Connected Refinery Solution components is an extremely important part of the deployment process.

All relevant stakeholders from the installation site must be consulted in advance and involved throughout the deployment process. Their knowledge about vital issues, when factored into the deployment, will help decrease unnecessary delays.

Examples of such stakeholders are the local site manager, Health Safety and Environment (HSE) staff, and operations manager(s). The actual number will depend on the number of plants in a site that the work will be taking place in addition to the project staff.

The following list contains some important aspects and considerations that need to be taken prior to the commencing of the installation activities, which need to be validated with the local site responsible personnel as mentioned above:

- Adherence to Health and Safety rules
- Electrical installation work that needs to be conducted to enable the equipment to be deployed in the field
- Availability of authorized equipment to use at the site (such as scissor lift and scaffolding that needs to be deployed prior to commencing the installation activities)
- Availability of adequate fiber/copper links to connect the APs to allow for the implementation of the selected use cases
- Ensure that all the appropriate certifications of the products are available and applicable to the specific regulations and bodies that the location of the site is adhering to

- Plan as much in advance as possible for issuing site work permits as required to reflect the installation activities that will be conducted at the plant/customer location
- Ensure that any tools/equipment (such as laptops, battery packs, and cables) that will be used at the customer location have been approved for meeting the standards that are in place for the site location

Oil and Gas Environments

Some of the most notable aspects of any oil and gas environment are the hazards found there in many different degrees. Personal dangers exist in these working locations including fall, crush, electrocution, noise, confined space, exposure and flammable substance. See Table 6-2.

Table 6-2 Interpreting Access Point Hazardous Compliance Labels

Label	Description
Class I, Division 2 Groups A,B,C,D	Defines the environment in which the access point can be used: • Class I - Environment containing flammable gases, vapors, or liquids, • Division 2 - Environmental classification used by the US and Canada, • Groups A,B,C,D - Gas identification for the US and Canada: – A-Acetylene – B-Hydrogen – C-Ethylene – D-Propane
Class I, Zone 2, Group II	Defines the environment in which the access point can be used: • Class I - Environment containing flammable gases, vapors, or liquids • Zone 2 - Environment classification used in North America • Group II - Gas identification for Zone II which includes: – IIa-Propane – IIb-Ethylene – IIc-Acetylene & Hydrogen
EX nA II T5	Defines parameters that the product complies with for U.S. Certification: • Ex - Denotes explosive atmosphere • nA - Non-sparking • II - Group II as defined previously • T5 - Temperature code < 100 degrees C, maximum surface temperature
CSA Certificate 1945576	Identifies the Canadian Standards Association (CSA) certificate number
SIRA 11ATEX4253	Identifies Sira ATEX certificate number

Table 6-2 Interpreting Access Point Hazardous Compliance Labels (continued)

Label	Description
-40 < Ta < +55C	The operating temperature range for the access point in all countries. Note: Current safety certifications only include operation of this outdoor equipment down to -40C
Type 4, IP67	Defines the enclosure degree of protection: • Type 4 = indoor or outdoor use primarily to provide a degree of protection against windblown dust and rain, splashing water, hose-directed water and damage from external ice formation • IP67 = Dust tight (dust, dirt, sand, and so forth) and protected against powerful water jets. Also the unit can be immersed in water up to 1m for short periods of time (30min)

Flammable substances are a significant concern for electrical/electronic equipment operating within said areas. Areas where gases are anticipated to have exposure to the atmosphere will have a rating designation applied to identify the different levels of danger. These levels of danger are generally represented in Table 6-3.

Table 6-3 Interpreting Access Point Hazardous Compliance Labels

Division System	Zone System	Presence of Flammables	Notes
Class 1 Division 1	Zone 0	1000 hours per year or more (10%)	Cisco partners support this level of classification
Class 1 Division 1	Zone 1	10-1000 hours per year or more (0.1% to 10%)	Cisco partners support this level of classification
Class 1 Division 2	Zone 2	Under 10 hours per year (0.01% to 0.1%)	Cisco HZ-rated products
Unclassified	Unclassified	Under 1 hour per year (Less than 0.01%)	Cisco outdoor rated products

Cisco's hazardous environment-rated wireless APs have been engineered for use in locations that are unlikely to experience exposure to flammable substances for more than ten hours per year. The Access Point hazardous location option complies with safety standards for Class I, Division 2, and Zone 2 hazardous locations where ignitable concentrations of flammable gases, vapors, or liquids are not likely to exist under normal operation conditions.

Figure 6-10 Cisco AP Hazardous Classification Labels

When considering the right product for the environment and how the product should be installed within compliance, refer to the product installation guides, including the product regulatory/safety compliance status. For hazardous-rated product, additional document versions exist for hazardous installation guides that can be referenced by global installation contractors and adapted to local electrical safety codes and regulations.

Installation Best Practices

A location's hazardous rating and installation cost can affect AP location, which will also greatly affect overall wireless performance. These factors should be accounted for during the site survey process. When choosing the best location to place an AP, consideration should also be made for both installation and ongoing operation of the equipment.

Installation must accommodate local electrical, safety and regulatory requirements. Installations should also take advantage of existing electrical and data networking infrastructure as a means of minimizing costs when possible. Installations should accommodate and take advantage of available mounting assets that will enable the APs to achieve optimum wireless performance for any given area by maximizing the antenna's RF field of view and minimizing sources of interference.

Ongoing operations of the network and equipment should be addressed prior to installation. In rare instances when mesh radio equipment become stranded from parent nodes, it is important to gain local access to this equipment in an attempt to troubleshoot and fix a potential local issue that might be experienced with configuration, firmware, or hardware. Two additional installation steps of installing a local power disconnect switch and a console cable can be very helpful for local control and access, especially when the AP is installed in a location that is inaccessible without the use of costly aerial lift equipment and operators. An accessible power disconnect will enable a network technician/operator to simply power cycle the AP at times when a stranded AP should be rebooted to force a refreshed network join procedure to receive proper configuration and firmware. This is also good for times when the AP might require maintenance or replacement and the power could be disconnected locally rather than a larger circuit. Some Cisco hazardous-rated APs have a local console connection that would enable a network technician/operator to directly connect and command an AP to run diagnostic and troubleshooting commands. This best practice might not comply with regional hazardous installation requirements so be sure to verify with a certified electrician for proper compliance.

Figure 6-11 illustrates an AP installed in a gas plant. The AP was surveyed and installed at a height of approximately 5 meters, which provided optimal ground level and elevated platform coverage for that area. Fifteen meters above ground elevation would require a lift to access equipment so this installation follows a best practice recommendation of installing a ground level power disconnect and console cable.

Figure 6-11 Hazardous-Rated AP Installed in a Gas Plant

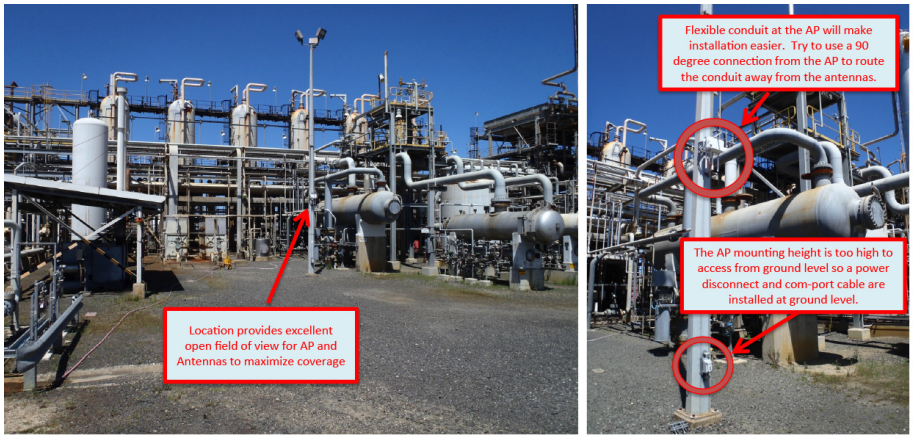


Figure 6-12 shows a hazardous-rated AP properly installed within the refinery piping structure.

Figure 6-12 Hazardous-Rated AP Properly Installed within Refinery Piping Structure

Figure 6-13 illustrates best practice concepts of maximizing coverage by strategic AP placement and also minimizing installation costs by using existing suitable structure that already has power available.

Figure 6-13 Best Practice Concepts

Industry Partnerships

This chapter includes the following major topics:

- Emerson, page 7-1
- Honeywell, page 7-6
- SAP, page 7-10
- Wireless Endpoints, page 7-12
- Rice Electronics, page 7-13

Although the focus of this CRD is industrial wireless technology across a Cisco infrastructure, to create solutions which solve customer challenges and use cases, Cisco works with a number of key partners with complementary technologies. These include wireless sensors and instrumentation, ruggedized mobile devices such as phones, tablets and gas detectors, and a range of communication and workflow applications. The following pages highlight a few of these partners and the technologies that form part of the refinery and processing solutions.

Emerson

Emerson is a global manufacturing company that brings technology and engineering together to provide solutions in industrial, commercial and consumer markets through its Process Management, Industrial Automation, Network Power, Climate Technologies, and Commercial & Residential Solutions businesses. Emerson and Cisco work strategically together at a global level, partnering in a number of these industrial segments.

Emerson Process Management has expertise and capabilities in all aspects of automation and information systems related to the production, transmission, and processing of oil and gas products, including upstream exploration and production, midstream gas processing, terminal and tank management, and downstream petroleum refining.

Emerson and Cisco work closely in a number of industries in oil and gas solutions, with an emphasis on integrated Industrial Wireless technologies and security for the refining and processing environments. The joint work includes reference architectures, focus use cases, product development, solution validation, and a drive to more closely align Operational and IT teams (see Figure 7-1).

Figure 7-1 IT and OT Skill Convergence

Emerson deliver a number of capabilities for the process control environment to:

- **Measure and Analyze**—A broad range of measurement and analytical technologies for process clarity and insight. These include pressure, temperature, level, flow, corrosion, pH, among others.
- **Control and Regulate**—Highly reliable final control technologies to help regulate and isolate the process. These include valves, actuators and regulators.
- **Operate and Manage**—Systems and tools that provide the decision integrity to run the operation at its full potential. These include process control DCS, RTU, SCADA, safety and compliance, operations management, asset reliability, and decision support and data management.

An integral component of the Emerson Wireless plant solution is the wireless plant network. This leverages *pervasive sensing* for the instrumentation and sensor networks, and also for multi-service use cases to support operational activities.

Emerson was part of the development of wireless field instrumentation solutions which resulted in the release of the WirelessHART (HART 7) standard.

The IEC62591 standard (aka WirelessHART, which is based on the HART Communication protocol. The HART application layer has been in existence since the mid-1980s and it was developed by Rosemount, Inc. The HART protocol has evolved from a simple 4-20mA analogue-based signal to the current wired and wireless-based technology with extensive features supporting security, unsolicited data transfers, event notifications, block mode transfers, and advanced diagnostics. Diagnostics now include information about the device, the equipment the device is attached to, and in some cases, the actual process being monitored.

WirelessHART is encapsulated in the HART 7 standard, so all WirelessHART devices share the same characteristics and features of wired HART devices, resulting in common software, tools, and skills for commissioning, maintaining, and integration with today's process host systems. Interoperability and interchangeability are important components for the WirelessHART support that represents ease of use for customers globally.

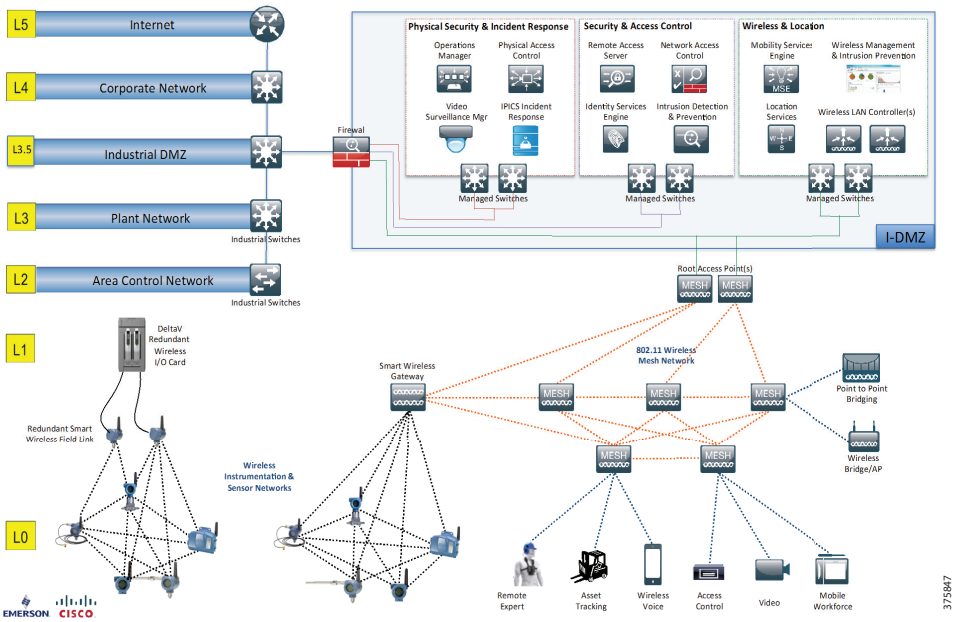
WirelessHART targets sensors and actuators, rotating equipment, environmental health and safety applications, condition monitoring, and flexible manufacturing in which a portion of the plant can be reconfigured for specific products. The standard was designed for devices to take process measurements, communicate those measurements through a mesh network, and integrate the measurement data in a process host system. The standard defined a limit to the power consumed by edge devices meaning they can be battery powered for up to ten years.

For additional architecture and technical information on WirelessHART, please see Chapter 5, “Industrial Wireless.”

The Emerson plant wireless security architecture follows ISA99/IEC 62443, and the ISA95 Purdue Model of Control (see Figure 7-2). While the WirelessHART field instruments and gateways are only found at Level 0 and 1, the wireless plant network must accommodate every other level of the model. It

would be cost prohibitive to install a separate wireless network for each network level, so each wireless network level is virtualized within the shared wireless hardware. Each secure virtual network is fully isolated in software from the other networks on the common wireless hardware.

Figure 7-2 Emerson and Cisco High Level Wireless Plant Reference Architecture



For detailed technical information and integration options of the Emerson solutions into the Cisco Industrial Wireless network offering, please see Chapter 5, "Industrial Wireless."

Emerson and Cisco work together to deliver a number of key use cases for the plant environment:

- Wireless Bridging
- Mobile Workforce
- Wireless Instrumentation
- Personnel Health and Safety
- Turnaround Optimization
- Physical Security (Access Control, CCTV)
- Asset Location Tracking
- Secure Remote Access

In addition to wireless field instrument solutions delivered across IEEE 802.15.4 wireless, Emerson offer plant operation solutions using IEEE 802.11 Wi-Fi technology for applications such as the mobile workforce, mobile voice and video, remote video monitoring, location tracking, and safety mustering.

Emerson has a broad capability to deliver solutions in the field. Pervasive sensing provides infrastructure solutions for IEEE 802.15.4 wireless mesh sensor networks, as well as a wide range of field instruments including temperature, vibration, flow, pressure, differential pressure, level, and corrosion (see Figure 7-3).

Figure 7-3 Emerson Field Instrument Portfolio

To ensure best practice network design, Cisco and Emerson have developed a joint product with the 1552WU wireless AP (see Figure 7-4). This combines a Cisco ruggedized IEEE 802.11 wireless AP with an Emerson WirelessHART sensor gateway. This allows the connectivity of WirelessHART sensor networks and devices, IEEE 802.11 wireless devices, and IEEE 802.11 mesh backhaul, all in a single unit.

Figure 7-4 Cisco and Emerson 1552WU Wireless Gateway

The 1552WU is Class 1, Div 2/Zone 2 hazardous location-certified, designed specifically for hazardous environments like oil and gas refineries, chemical plants, mining pits, manufacturing facilities, and process control applications.

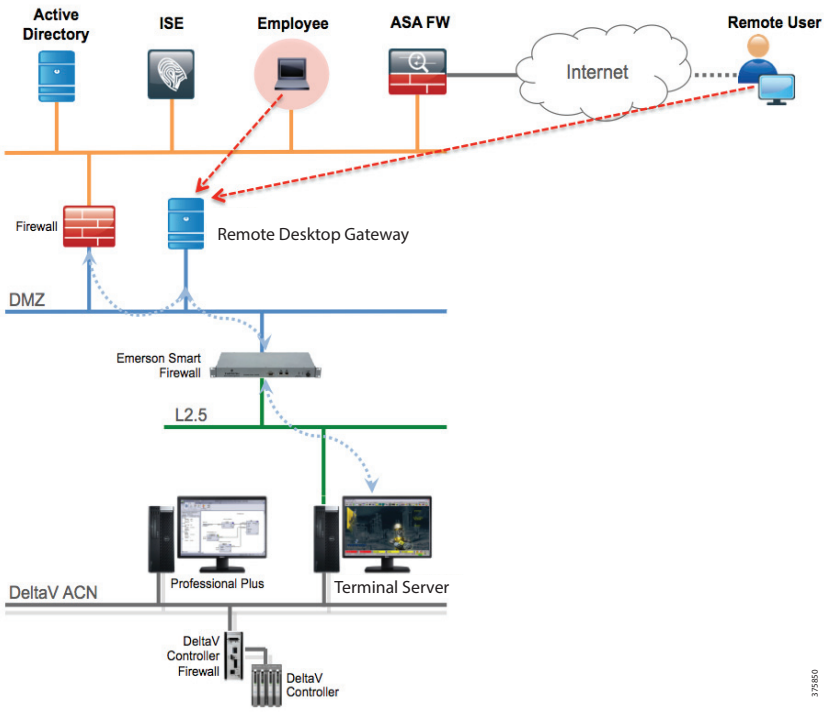
By eliminating the extra power and network connections, which can be expensive to deploy and maintain in hazardous locations, the 1552WU saves costs by reducing deployment times while offering a flexible, highly secure, and scalable mesh network for high-performance wireless coverage for both Wi-Fi clients and WirelessHART field instruments across large facilities.

With security an inherent part of the Emerson and Cisco partnership, secure remote access for the plant environment is essential. Emerson and Cisco have also worked to develop a more secure solution for access to the control room, both from within a customer's network and from an externally located site.

Remote access can be the weak link in an otherwise strong defense-in-depth strategy. By incorporating Cisco's ISE, switches, and firewalls within the business level network, users can more securely enable access to the control system firewall for solutions such as engineering of remote or isolated DeltaV control systems.

The Secure Remote Access solution (see Figure 7-5) includes the Cisco ISE, which provides the technology to examine the remote user's endpoint as it attempts to access the control system, answering the *who, what, when, where, and how*, and uses that information to grant access to the process control system based on identity. The solution provides more granular security control, negating many problems before they start. It also increases scalability, as it centralizes all endpoint authentication and authorization responsibilities.

Figure 7-5 Secure Remote Access Solution



By working closely together to meet joint customer objectives, the following benefits can be realized through a properly architected and validated solution for the plant:

- Control system-enabled ERP
- Business-wide supply chain optimization
- Simplified infrastructure
- Ease of management and reduced support cost
- Borderless collaboration and remote expert support
- Reduce downtime and leverage best expertise
- Multi-site and multi-purpose enabled mobility applications
- Increase employee productivity
- Better security through IT security tools and OT operational rules and practices
- Reliable, safe and secure operations

For additional information on Emerson and their capabilities and solutions, please see Appendix B, "Additional Information."

Honeywell

Cisco and Honeywell have a global strategic alliance covering multiple verticals and technology areas. They have developed joint offerings in Industrial Wireless, life safety and location tracking, industrial cyber security, and smart buildings and cities, and have complementary services capabilities for these areas. At a strategic level, the focus is on the Honeywell Process Solutions (HPS) Vision 2040 for the next generation process control network leveraging Cisco's IP-based architecture, cloud and mobility, and virtualization technologies. In addition, a continued drive exists for a connected sensor platform for HPS' sensing and controls solutions, and cyber security to help with the trend for IT and OT convergence.

In Oil and Gas, HPS works with industrial customers to operate safe, reliable and efficient facilities by delivering technologies from the plant floor to the boardroom. This includes legacy process control systems through to today's leading technologies in the oil and gas, refining, pulp and paper, industrial power generation, chemicals and petrochemicals, biofuels, life sciences, and metals, minerals and mining industries.

In process control, Honeywell and Cisco work closely on converged Industrial Wireless solutions for processing facilities, refining, storage, and the oilfield. The joint work includes validated deployment architectures, proven use case solutions, product development, and an end-to-end communications strategy from instrument to application which securely brings together the Enterprise and the PCN.

Behind the alignment both organizations see disruption to the process control industry through technologies driven by the Industrial Internet of Things (IIOT), the aging workforce, and the mobile workforce, meaning increased requirements for safety, productivity, and compliance.

Honeywell delivers a number of key capabilities:

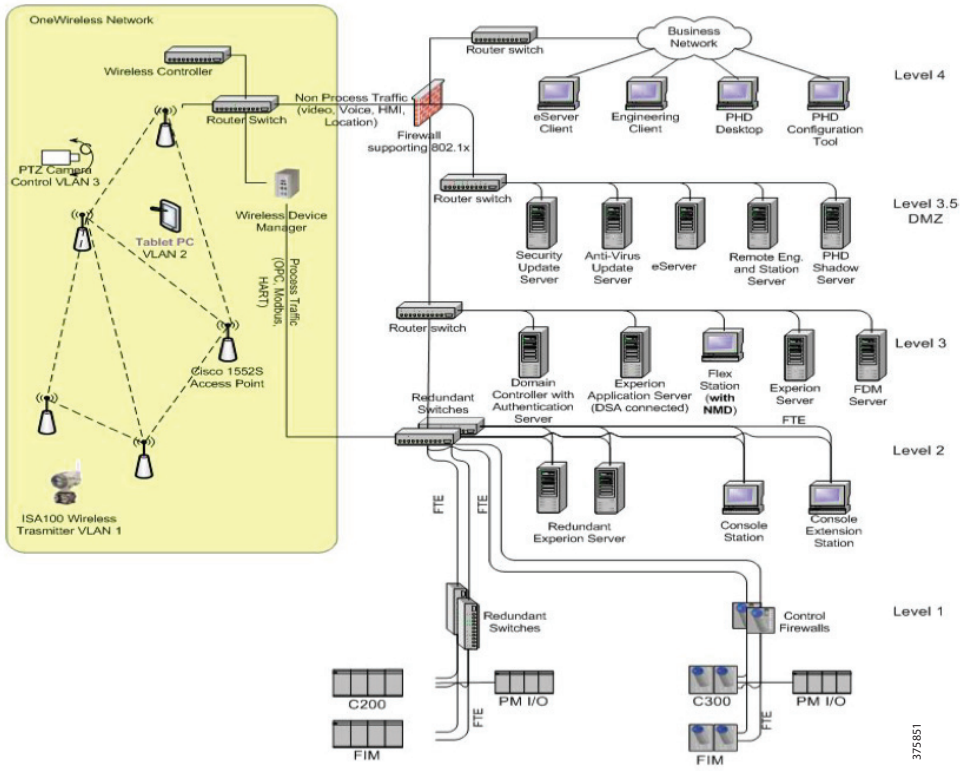
- Integrated DCS, SCADA, and Advanced Process Control Solutions
- Integrated Process Safety and Security Solutions
- Integrated Fire and Gas Solutions
- OneWireless Field Instrumentation and Solutions
- Lean Execution of Automation Projects (LEAP) combines Universal IO, virtualization and cloud engineering to take automation out of the critical path
- Life Cycle Support and Solutions
- Industrial Cyber Security

By combining these capabilities with Cisco's industrial wired and wireless networking infrastructure, industrial security, collaboration and virtualization technologies, a number of key business objectives and use cases for the refining and processing facilities can be addressed:

- Standardized integrated solutions and best practice blueprints
- Cyber and physical security
- Aging workforce and changing skill sets
- Technology advances and introduction of new technologies
- Personnel safety, and safety compliance
- Remote data acquisition
- Increased efficiency and automation, de-manning where appropriate
- Inventory management and asset tracking/visualization

A key element of the partnership is a joint solution for Industrial Wireless. The Honeywell OneWireless offering leverages Cisco Industrial Wireless technologies, as shown in Figure 7-6.

Figure 7-6 Honeywell OneWireless Architecture



The OneWireless industrial wireless network can be tailored to meet the wireless coverage requirements of industrial automation applications, from a simple sensor mesh network providing wireless coverage for ISA100 Wireless (also known as IEC62734)802.15.4-compliant field devices, to a plant-wide network with coverage for ISA100 Wwireless field devices and 802.11 Wi-Fi devices.

The OneWireless network is based on a number of key components:

- **Honeywell OneWireless Wireless Device Manager (WDM)**—The WDM manages all wireless field devices, including ISA100 Wwireless field instruments and network infrastructure devices such as FDAPs and the Cisco APs.
- **Honeywell OneWireless Field Device Access Point (FDAP)**—The FDAP is a rugged industrial AP for ISA100 wireless instruments and is the backhaul bridge between the sensor network and the wireless or wired infrastructure.
- **Cisco 1552S Access Point**—The 1552S is a rugged industrial AP for Wi-Fi (IEEE 802.11 a/b/g/n) clients and ISA100 Wireless field instruments. The 1552S is capable of tunneling data between ISA100 Wireless and Wi-Fi devices and associated host applications such as the control system.
- **Cisco Wireless Local Area Network Controller**—Wireless Controllers manage the Cisco 1552S APs by extending the network policy and security from the wired network core to the wireless edge.

The OneWireless Network scales from a handful of wireless field instruments, to thousands of field instruments, Wi-Fi devices, and other IP-enabled applications, such as hand-held devices and security cameras. It includes a number of security, reliability, and speed features to support ISA100 standard-based wireless transmitters and 802.11-based applications.

The sensor and instrumentation networks are based on the ISA100 Wireless.11a wireless industry standard, also known as IEC62734. The Automation Standards Compliance Institute (ASCI) is a non-profit organization incorporated by ISA in 2006 to provide a home for certification, conformance, and compliance assessment activities in the automation arena. ASCI extends the work that ISA has

conducted for 50 years in standards development by facilitating the effective implementation of automation industry standards.The ISA100 committee is part of ISA and was formed to establish standards and related information for industrial wireless.

ISA100 Wireless is an open, universal IPv6 wireless network protocol that establishes the IIOT. IPv6 addressability makes ISA100 Wireless the only industrial network protocol compatible with the Internet of Things. The standard meets EU ETSI Regulations that went into effect January 1, 2015. ISA100 Wireless is the only industrial wireless network protocol that satisfies the ETSI EN 300.328 v1.8.1 regulation. ISA100 Wireless uses CSMA/CA Listen Before Talk (LBT) Clear Channel Assessment (CCA) technology to ensure co-existence with other unmanaged wireless devices using the same 2.4 GHz frequency spectrum.

The standard extends existing applications; scalability and flexibility are unattainable with traditional wired installations and enables new applications. The standard enables process visibility and control in locations where wiring would be infeasible and/or prohibitively expensive. The ISA100 Wireless standard eliminates protocol barriers. Universal object-oriented application model and tunneling technology supports any protocol, protecting legacy investments. The ISA100 Wireless standard is the only end-user driven standard globally. Oil majors and leading national oil companies have been instrumental in defining the standard. 11a open wireless networking technology standard was developed to deploy managed wireless networks in industrial plants.

- For additional architecture and technical information on ISA100 Wireless.11a, please see Chapter 5, “Industrial Wireless.”

With OneWireless, PCN administrators can secure and manage a single wireless network infrastructure, capable of supporting all types of wireless sensor and wireless IP-based devices.

- For detailed technical information and integration options of the Honeywell solutions into the Cisco Industrial Wireless network offering, please see Chapter 5, “Industrial Wireless.”

As part of this converged offering, Honeywell and Cisco jointly developed the 1552S wireless AP (Figure 7-7).

Figure 7-7 Cisco 1552S Wireless Access Point

The 1552S merges a ruggedized outdoor 802.11 AP with an integrated, ISA100 Wireless-compliant backbone router to provide a seamless solution for wireless sensor networks. The ISA100 Wireless.11a radio has been designated specifically for mission-critical wireless connectivity to industrial sensor equipment. With an ISA100 wireless.11a radio integrated in an 802.11n-based AP, a single solution addresses the growing need for wireless mobility while providing mission-critical connectivity for industrial sensing and monitoring equipment.

The 1552S is Class 1, Div 2/Zone 2 hazardous location certified and designed specifically for hazardous environments like oil and gas refineries, chemical plants, mining pits, and manufacturing facilities. The 1552S offers a single-box solution rather than requiring two separate wireless networks—one for 802.11n and one for ISA100 Wireless sensor networks. The joint solution manages all outdoor 2.4 GHz wireless communication and features prioritization of critical information. This unique unmatched feature avoids congestions now and in the future as the number of Wi-Fi clients and ISA100 Wireless

field instrumentation continues to scale up. The joint Cisco/Honeywell solution assures that end-users can always get their critical information in near real time (wired-like performance), during normal operation, and when it matters most—during abnormal situations.

The Cisco Aironet 1552S Outdoor AP supports multiple-device and multiple network application delivery methods, such as real-time seamless mobility, video surveillance, Third Generation (3G) and Fourth Generation (4G) data offload, and public and private Wi-Fi access.

Honeywell's instrumentation and sensor portfolio includes pressure, temperature, flow, level (up to custody transfer compliant and SIL2 rated) and vibration and valve position sensors, panic buttons, and universal wireless transmitters that fit into any industrial automation application. These sensors have been integrated and validated between Cisco and Honeywell, as well as deployed in multiple operational environments upstream onshore and offshore, midstream, and downstream.

In addition to process monitoring and control edge devices, Honeywell will have a series of safety solutions including the ConnectPro portable multi-H2S-gas sensors (such as H2S, CO, O2, and LEL), man-down alarming, real-time location identification and management applications (see Figure 7-8) that have been integrated and validated across a Cisco infrastructure.

Figure 7-8 ConnectXtPro Portable Gas Sensor and Management Application

ConnectPro is a wireless solution designed for plant-wide applications leveraging location-tracking capabilities across the Cisco wireless infrastructure. It provides continuous monitoring and detection of toxic gases and radiation across a facility, bringing together data from personal, portable, area, and fixed monitors into a single management application providing real-time awareness of conditions in every part of your plant. This information can also be shared online for collaboration with remote experts and stakeholders.

The solution addresses a range of routine and emergency situation including leak detection, man-down, confined space entry, fence line monitoring, plant turnaround, and emergency response. The solution also fully automates management of calibration, bump testing, and compliancy reporting.

For additional information on Honeywell PCN and their capabilities and solutions, please see Appendix B, “Additional Information.”

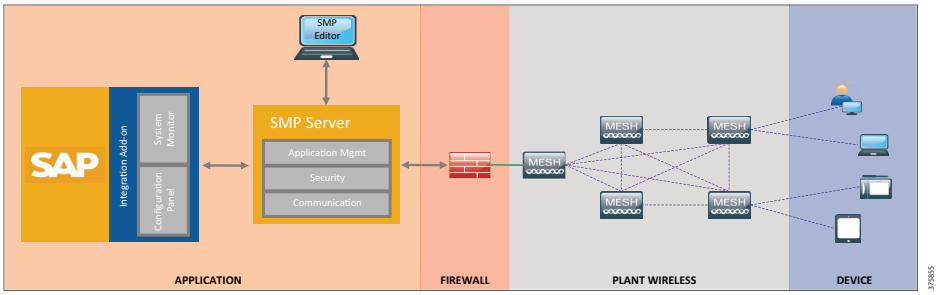
- http://wireless.honeywellanalytics.com/Pages/default.aspx
- http://www.isa100wci.org/en-US/About-ISA100-Wireless/What-is-ISA100-Wireless (download *ISA100 Wireless Technical Overview Brochure*)

SAP

The SAP Mobile Asset Management Solutions is a set of custom-built mobile applications designed for workforce automation in industrial environments. The applications help refinery and processing facility operators gain real-time information of their operations and their workforce. Coupled with a secure Cisco communications infrastructure, plant operators can easily deploy a validated, tested, and integrated solution for mobile worker, plant safety, remote expert, and process streamlining use cases.

In the plant environment, applications are deployed on intrinsically safe and ruggedized phones, tablets, and laptops, and communicate securely through the Cisco wireless infrastructure to the SAP management application servers (see Figure 7-9). The solutions are compatible with Windows, Android, and Apple environments.

Figure 7-9 Example Mobile Application



Applications can be easily and rapidly integrated with SAP CRM and ERP modules to capture more accurate and timely data for reporting and analysis. The SAP mobile applications include:

- **SAP Work Manager**—Provides tools to improve workforce safety and optimize asset life and reliability, as well as streamline processes by eliminating paperwork and shortening work cycles. The mobile application accesses the SAP Enterprise Asset Management (SAP EAM) solution allowing the workforce to efficiently install, inspect, maintain, and repair assets in the field from a mobile device (see Figure 7-10). Work Manager helps with the following use cases:
  - Plant maintenance
  - Geo-tagging of equipment including meters
  - View schematics, history and dependencies of assets
  - Guided work flows
  - Real-time notifications and work orders
  - Worker status, job progress and location

Figure 7-10 Example Mobile Application 2

- **SAP Inventory Manager**—Provides tools to improve and manage inventory levels, efficiently fill customer orders, and track the movement of materials using mobile devices with scanning functionality. The mobile application accesses the SAP EAM solution allowing technicians and warehouse management staff with the ability to execute stockroom operations in an automated and way, ensuring stock parts and spares are effectively managed. Inventory Manager helps deliver the following use cases:
  - Parts management and inventory stores
  - Cycle counts
  - Receive, transfer, issue and adjust stock
  - Parts management during inspections, maintenance, repairs
- **SAP CRM Service Manager**—Extends the SAP Customer Relationship Management (CRM) and Enterprise Resource Planning (ERP) applications to mobile devices in the field. This allows dispatch service requests, data access from the field, and captures complete accurate data for reporting and analysis.
- **SAP Rounds Manager**—Helps with routine conditions monitoring, meter readings and field measurements by recording more accurate data and analyzing it quickly. The application allows users to take immediate action if they find potential problems by generating work orders and notifications on the spot.

The SAP mobile application also integrates the Cisco Remote Expert Manager (REM) application (see Figure 7-11) for voice and video services, which is an integral communication element of the workflow and training process. REM allows direct click-to-call or click-to-video links to remote staff. This allows remote experts to see what the plant worker sees, assist the plant worker with tasks, and provide on the job training and coaching. The REM and SAP integrated architecture is shown in Figure 7-12.

Figure 7-11 Cisco REM Integration

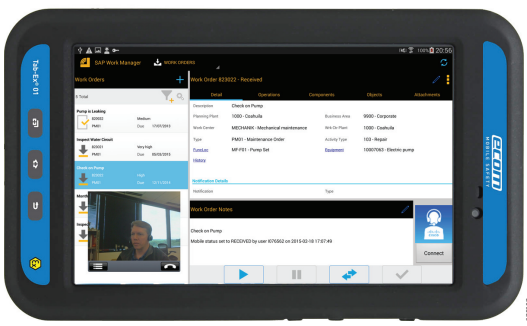
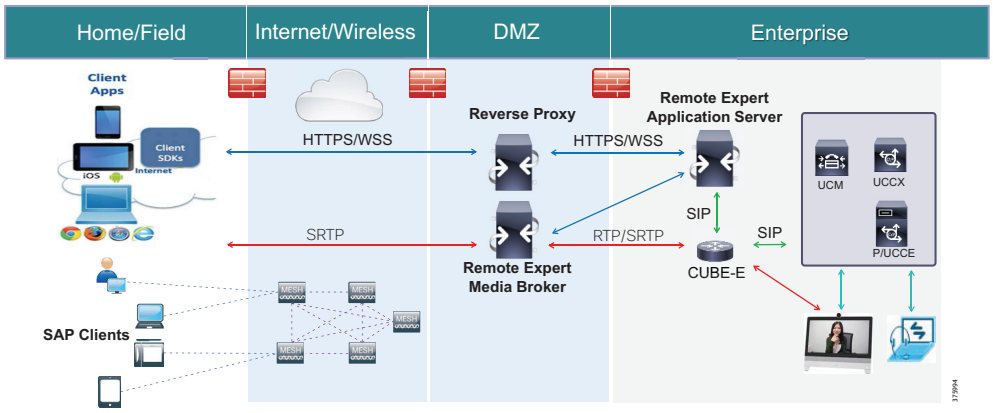


Figure 7-12 REM and SAP Integrated Architecture



By architecting and validating SAP applications across a Cisco communications infrastructure, the mobile application suite allows better operational and strategic decisions. Field-based work is securely linked with decision and process systems, leveraging data that is always complete, accurate, timely and ready for reporting and analysis. Validation helps reduce cost, ensures reliability and scalability, and provides an open standards-based platform to deploy future mobile worker applications.

Wireless Endpoints

Location Services

Following the closing of AeroScout Industrial, Cisco has entered into two separate partnerships for connected asset products and solutions:

- Stanley Healthcare for access to the RFID tags and MobileView software. AeroScout Industrial was part of Stanley and shared tag and software technology with Stanley Healthcare. Stanley Healthcare was not affected by the closing of AeroScout.
- Ekahau, another leading vendor of active RFID tags and software and a long time Cisco partner.

Ekahau and Stanley Healthcare are members of a developing ecosystem of software vendors, wireless technologies, and sensors to create a portfolio of asset tracking capability. Although Ekahau and Stanley Healthcare focus on the healthcare market, both have experience in the industrial space and work closely with Cisco to address this market.

Both Stanley Healthcare and Ekahau products are available for sale through Cisco via a *Solution Plus* agreement. As part of a Solution Plus arrangement, each company provides customer support for their respective products. Under this *cooperative support* model, Cisco and the partner will help each other define a triage model to identify the owner of an issue.

The following is a list of additional information on these partners and products:

- Stanley Healthcare will brand the healthcare version of these products *AeroScout*.
- In some cases, tags might have a lower IP certifications rating (for example, certified as splash proof rather than submersible).
- Stanley customers with existing maintenance agreements can renew maintenance through Cisco.
- Stanley has agreed to continue the T2 Extended Battery tag.
- Stanley will no longer make available the GPS tag nor the bi-directional push button tag.

- MobileView will be based on the healthcare version, but re-skinned as AeroScout with an industrial look and feel.
- The software packages nViz™ gateway and worker safety module will continue to be supported. The nViz Gateway is a Web-based service that provides an interface to exchange XML messages to an HTTP listener on the AeroScout system. These messages can consist of location (relative x/y, global GPS coordinates), GEN 2 passive tag technologies, battery status and telemetry (for example, tamper/button press/temperature).
- With the exception of Extronics, Cisco is currently the only Stanley partner with access to the industrial portfolio.
- Extronics will continue to source the electronics for tags and produce intrinsically safe packaging. Cisco and Extronics work together to provide solutions for customers, particularly in Oil and Gas.
- Ekahau will produce intrinsically safe tags.
- Where Stanley provides exciters as choke points, Ekahau uses a lower cost IR beacon.

For additional information on Stanley, Ekahau, and Extronics, please Appendix B, “Additional Information.”

Rice Electronics

Rice Electronics provides solutions in communications, navigation, explosion-proof intercoms, PBX, Public Address General Alarm (PAGA), and topside and sub-sea CCTV for industrial environments.

Rice is an expert in the development and certification of equipment and solutions for hazardous environments, including explosive and potentially explosive environments found in the Oil and Gas industry.

Rice produces a number of endpoints for hazardous environments such as phones, tablets, and gas detectors, some of which are ATEX and IECEx-intrinsically safe certified (Figure 7-13 and Figure 7-14). These devices can operate in a standalone fashion, or be combined to create mobile worker solutions with a fully integrated voice, video, RFID, and data analytic engine focused on enhancing operational support in harsh and remote environments.

Figure 7-13 Rice Electronics Intrinsically Safe Phone

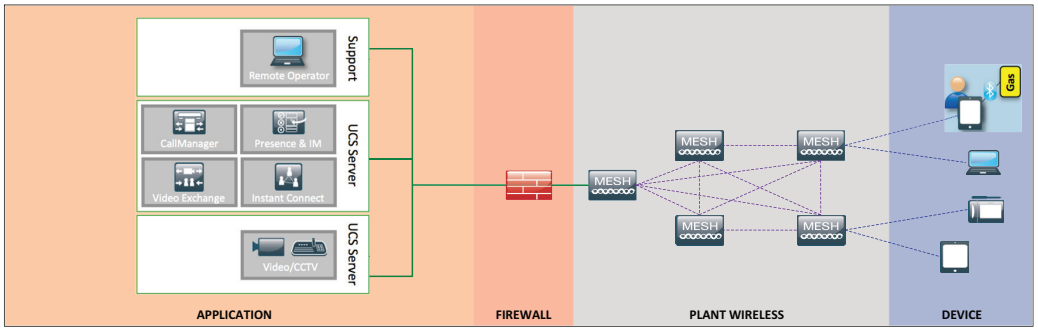
Figure 7-14 Rice Electronics Rugged Tablet

Rice endpoints also support man-down capabilities through a built-in accelerometer, and provide access to workflow applications such as job site authorization and inspection reporting providing remote manager oversight and support. The solutions target the following key business challenges:

- Reduce equipment carried by personnel by using a single device used for cell and mobile radio
- Access operational reports (such as JSA and Inspection)
- Access RTU/PLC - Read/Write authorization and accessibility
- Track and trace of contractors
- Man-down and mustering real time personnel tracking
- Access to remote expertise
- Access to manuals/troubleshooting guides

Rice and Cisco have partnered to validate and ensure operation of these devices and solutions across a Cisco wireless infrastructure (Figure 7-15). The solution also uses the suite of Cisco collaboration tools including IPICS, WebEx, Spark, and Jabber.

Figure 7-15 Mobile Worker Solution Architecture



For detailed technical information and integration options for the mobile worker and safety solutions into the Cisco Industrial Wireless network offering, please see Chapter 5, "Industrial Wireless."

By architecting and validating joint solution offerings for mobility and safety across a secure wireless infrastructure, the following benefits can be delivered:

- Real-time location tracking from a web interface to aid in monitoring workforce and assets in the field.
- Collaboration between central support organizations and remote operating teams for knowledge retention and best practice sharing.
- Intrinsically safe devices (ATEX and IECEx) rated for use in hazardous areas brings enterprise applications to the remote edge.

- Enhanced health and safety by scaling global expert resources, accelerating decision making and decreasing response time.
- Advanced mobile technology for asset management, remote site security, and monitoring production levels.

For additional information on Rice Electronics and their capabilities and solutions, please see Appendix B, “Additional Information.”

Cisco also collaborates with other endpoint vendors such as Pixavi and eCom.

CHAPTER 8

System Components

Table 8-1 lists Connected Refinery system components with relevant Cisco product page links.

Table 8-1 Connected Refinery System Components

Component	Description	More Information
AP 1552S	Hardened Industrial Wireless Access Point with ISA 100 Radios for Honeywell OneWireless	http://www.cisco.com/c/en/us/products/wireless/aironet-1552s-outdoor-access-point/index.html
AP 1552WU	Hardened Industrial Wireless Access Point with WirelessHART Radios for Emerson Smart Wireless	http://www.cisco.com/c/en/us/products/wireless/aironet-1552wu-outdoor-access-point/index.html
AP 3700	Enterprise Wireless Access Point	http://www.cisco.com/c/en/us/products/wireless/aironet-3700-series/index.html
ASA 5500-X	Enterprise Firewall Appliance	http://www.cisco.com/c/en/us/products/security/asa-5500-series-next-generation-firewalls/index.html
Catalyst 2960	Enterprise Access Switch	http://www.cisco.com/c/en/us/products/switches/catalyst-2960-x-series-switches/index.html
Catalyst 3750	Enterprise Access Switch	http://www.cisco.com/c/en/us/products/switches/catalyst-3750-x-series-switches/index.html
Catalyst 3850	Enterprise Access Switch	http://www.cisco.com/c/en/us/products/switches/catalyst-3850-series-switches/index.html
Catalyst 4500E	Core and Distribution Switch	http://www.cisco.com/c/en/us/products/switches/catalyst-4500-series-switches/index.html
Catalyst 6880-X	Core and Distribution Switch	http://www.cisco.com/c/en/us/products/switches/catalyst-6880-x-switch/index.html
Cisco 829	LTE Router and Vehicle Mobility WGB	http://www.cisco.com/c/en/us/products/routers/800-series-industrial-routers/index.html
Identity Services Engine (ISE)	AAA and Policy Server	http://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html
IE-2000	Hardened Industrial Ethernet Access Switch	http://www.cisco.com/c/en/us/products/switches/industrial-ethernet-2000-series-switches/index.html
IE-3000	Hardened Industrial Ethernet Access Switch	http://www.cisco.com/c/en/us/products/switches/industrial-ethernet-3000-series-switches/index.html

Table 8-1 Connected Refinery System Components (continued)

Component	Description	More Information
IE-4000	Hardened Industrial Ethernet Access Switch	http://www.cisco.com/c/en/us/products/switches/industrial-ethernet-4000-series-switches/index.html
ISA 3000	Industrial Firewall Appliance	http://www.cisco.com/c/en/us/support/security/industrial-security-appliance-isa/tsd-products-support-series-home.html
IW 3700	Hardened Wireless Access Point	http://www.cisco.com/c/en/us/products/wireless/industrial-wireless-3700-series/index.html
WLC 5508	Wireless LAN Controller	http://www.cisco.com/c/en/us/products/wireless/5508-wireless-controller/index.html

Related Documentation

The following lists related documentation for Connected Refinery:

- Neil Peterson and Alexandre Peixoto. *Emerson Wireless Security WirelessHART® and Wi-FiTM Security.* November 2014.
- Soroush Amidi, and Amol Gandhi. *An Open, Standard-Based Wireless Network: Connecting WirelessHART® Sensor Networks to ExperionTM PKS Using Honeywell's OneWirelessTM Network*.
- Rajiv Singhal and Eric Rotvold. *Coexistence of wireless technologies in an open, standards-based architecture for in-plant applications*. September 2007
- *Cisco Aironet 1550 Series for Hazardous Locations Installation Guide*. February 2014
- *Cisco Guide to Harden IOS Devices*:
  - http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

Additional Information

Table B-1 lists company websites for Connected Refinery partners.

Table B-1 Connected Refinery Partners

Partner	Website
eCom	https://www.ecom-ex.com/index/
Ekahau	http://www.ekahau.com/
Emerson	http://www2.emersonprocess.com/en-us/plantweb/wireless/pages/wirelesshomepage-flash.aspx
Extronics	http://www.extronics.com/
Honeywell	https://www.honeywellprocess.com/en-US/explore/products/wireless/OneWireless-Network/pages/default.aspx
Pixavi	https://www.pixavi.com/
Rice	http://www.riceelectronics.com/
Stanley	http://www.stanleyhealthcare.com/

Glossary

Table C-1 lists acronyms and initialisms used in this document.

Table C-1 Acronyms and Initialisms

Term	Definition
AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
ACS	Cisco Access Control Server
AD	Microsoft Active Directory
AP	Access Point
ARP	Address Resolution Protocol
ASA	Cisco Adaptive Security Appliance
ASCI	Automation Standards Compliance Institute
ATEX	Appareils destinés à être utilisés en ATmosphères EXplosibles
AVC	Application Visibility and Control
AWPP	Adaptive Wireless Path Protocol
BGN	Bridge Group Name
BLE	Bluetooth Low Energy
CAPWAP	Control and Provisioning of Wireless Access Points
CC	Control Centre
CCA	Clear Channel Assessment
CCTV	Closed Circuit TV
CCX	Cisco Compatible Extensions
CMX	Cisco Connected Mobile Experiences (CMX)
CoS	Class of Service
CRC	Cyclic Redundancy Check
CRD	Cisco Reference Design
CSA	Canadian Standards Association
DCS	Distributed Control System
DHCP	Dynamic Host Configuration Protocol

Table C-1 Acronyms and Initialisms (continued)

Term	Definition
DNS	Domain Name Server
DPI	Deep Packet Inspection
DSCP	Differentiated Services Code Point
E&P	Exploration and Production
EAP	Extensible Authentication Protocol
EIRP	Effective Isotropic Radiated Power
ERP	Enterprise Resource Planning
FCoE	Fibre Channel over Ethernet
FDAP	Honeywell Field Device Access Point
FEX	Fabric Extender
H2S	Hydrogen Sulfide
HART	Highway Addressable Remote Transducer Protocol
HMI	Human Machine Interface
HPS	Honeywell Processing Solutions
HSE	Health, Safety, and Environment
IACS	Industrial Automation and Control Systems
ICS	Industrial Control System
IDMZ	Industrial Demilitarized Zone
IDS	Intrusion Detection System
IE	Cisco Industrial Ethernet
IECEx	IEC System for Certification to Standards Relating to Equipment for Use in Explosive Atmospheres
IED	Intelligent Electronics Device
IIOT	Industrial Internet of Things
IoT	Internet of Things
IPS	Intrusion Prevention Systems
iSCSI	Internet Small Computer System Interface
ISE	Cisco Identity Services Engine
ISR	Cisco Integrated Services Router
IT	Information Technology
LACP	Link Aggregation Control Protocol
LAG	Link aggregation
LBS	Location-based Services
LBT	Listen Before Talk
LDAP	Lightweight Directory Access Protocol
LEAP	Lean Execution of Automation Projects

Table C-1 Acronyms and Initialisms (continued)

Term	Definition
LNG	Liquid Natural Gas
LOS	Line of Sight
LWAP	Lightweight Wireless Access Point
MAP	Mesh Access Point
MCEC	Multi-chassis EtherChannel
MDM	Mobile Device Manager
MES	Manufacturing Execution System
MIC	Message Integrity Check
MIMO	Multiple-Input and Multiple-Output
MSB	Most Significant Bits
MSE	Cisco Mobility Services Engine
NAD	Network Access Device
NAS	Network Attached Storage
NBAR2	Next Generation Network-Based Application Recognition
NGL	Natural Gas Liquids
NPT	Network Prefix Translation
NTP	Network Time Protocol
OT	Operational Technology
PAGA	Public Address General Alarm
PCN	Process Change Notification; Honeywell Process Control Network
PEAP	Protected Extensible Authentication Protocol
PER	Packet Error Rate (PER)
PLC	Programmable Logic Controller
PoE	Power over Ethernet
PPE	Personal Protective Equipment
PSN	Policy Services Node
QoS	Quality of Service
RAP	Root Access Point
RBAC	Rule-Based Access Control
REM	Cisco Remote Expert Manager
REP	Resilient Ethernet Protocol
RFID	Radio-frequency identification (RFID)
RRM	Radio Resource Management
RRM	Radio Resource Management
RSSI	Received Signal Strength Indicator
RTLS	Real Time Location System

Table C-1 Acronyms and Initialisms (continued)

Term	Definition
S02	Sulfur Dioxide
SAN	Storage Area Network
SAP CRM	SAP Customer Relationship Management
SAP EAM	SAP Enterprise Asset Management
SAP ERP	SAP Enterprise Resource Planning
SCADA	Supervisory Control and Data Acquisition
SGT	Security Group Tag
SNR	Signal-to-Noise Ratio
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access-Control System Plus
TLS	Transport Layer Security
UCS	Cisco Unified Compute System
UP	Universal Port
VLAN	Virtual Local Area Network
vNIC	Virtual Network Interface Card
VOC	Volatile Organic Compound
VoWLAN	Voice over WLAN
vPC	Virtual Port Channel
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
VSAN	Virtual Storage Area Network
VSS	Virtual Switching System
VTP	VLAN Trunking Protocol
WDM	Honeywell Wireless Device Manager
WEP	Wired Equivalent Privacy
WGB	Workgroup Bridge
wIPS	Wireless Intrusion Protection System
WLAN	Wireless Local Area Network
WLC	Wireless LAN Controller
WMM	Wi-Fi Multimedia