T04 - Wireless Design Considerations for Industrial Applications
Introduction

Design and Implementation Guide from Cisco Systems and Rockwell Automation®:

*Deploying 802.11 Wireless LAN Technology within a Converged Plantwide Ethernet Architecture*

- Literature Library publication **ENET-TD006**
  - Architecture examples and use cases
  - Best practices and recommendations
  - Configuration examples
Agenda

Technology and Use Case Overview

WLAN Architectures

WLAN Recommendations

Application Recommendations
Technology Overview
Connecting people

- Essential part of the **Connected Enterprise**
- Workforce mobility increases productivity
  - Access to system alarming and production data from anywhere, anytime, on any device
  - Ease of collaboration between plant personnel
  - Faster interaction with control systems for reduced diagnostic and problem resolution time
- Must have **secure and reliable wireless** infrastructure for multi-platform support
Technology Overview
Connecting Equipment

- Wireless process control
- Wire replacement for hard-to-reach areas
- Remote site connectivity
- Integration of standalone assets
  - Remote diagnostics and condition monitoring
  - Smart Equipment within Connected Enterprise
Technology Overview
Connecting Equipment

- Integrating portable equipment
  - Process skids, storage tanks, reactors, other movable equipment
- Minimum time to re-establish connectivity
- Flexibility in factory floor layout

Equipment is static while operating. Moves to a new location in the shutdown state.
Technology Overview

Connecting Equipment

- Machines with moving parts
  - Rotary platforms, assembly lines with mobile carriers on tracks, overhead cranes
- Elimination of cable failures
- Ease of reconfiguration
- New and more efficient machine designs: higher productivity, less downtime

Equipment moves during operation
Remains connected to the same AP (no roaming)
Technology Overview
Connecting Equipment

- Equipment moving over large area
  - AGVs, ASRS, overhead cranes with large spans, train cars, entertainment rides
- Plant-wide connectivity during operation
- Ease of reconfiguration, increased productivity

Site survey and architecture selection are critical
Technology Overview
Challenges of wireless communication

Before you cut the cable…

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

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

- Wireless coverage area cannot be precisely defined
  - Site survey is **required**
  - Spectrum sharing and security concerns
- Signal quality may change over time
  - Interference sources and obstructions
  - Unauthorized transmissions

*Wireless advantages > challenges when*
- WLAN is designed and maintained properly
- Used for appropriate applications
Technology Overview
Why 802.11 Wireless (Wi-Fi)?

Wireless technologies used in industrial automation equipment
(Source: HIS Inc. July 2013)

IEEE 802.11a/g/n/ac

- Supervisory / HMI
- Peer-to-peer Control
- Distributed I/O Control
- Safety Control

- Highest performance
- Plant-wide coverage and roaming
- Enterprise WLAN convergence
- Advanced security
- 5 GHz spectrum with less interference
Technology Overview

Wireless client types

Embedded wireless adapter:
- Typically mobile HMI clients
- Limitations for control platforms: antenna parameters, placement options, density, cost

External adapter (wireless bridge):
- Single wired client
- Vendor compatibility

Workgroup Bridge (WGB):
- Multiple wired clients
- Validated in the CPwE
Agenda

- Technology and Use Case Overview
- WLAN Architectures
- WLAN Recommendations
- Application Recommendations
Autonomous WLAN Architecture

Overview

- Each autonomous AP is configured and managed independently
- Standalone IACS applications
- Small number of APs and clients
- Typically non-roaming clients
- WGB mode is configured on the autonomous AP only

**SSID1**
- Channels: 36, 44

**SSID2**
- Channels: 40, 48

**WGB**
- WGB mode is configured on the autonomous AP only
Autonomous WLAN Architecture
Stratix® 5100 Wireless Access Point and Workgroup Bridge

- Default configuration optimized for EtherNet/IP applications
- Easy Setup in web-based Device Manager
- Diagnostic via Studio 5000® Add-on Profile (AOP) and FactoryTalk® View faceplates
- 802.11 a/b/g/n with 3x4 MIMO (up to 450 Mbps)
- Cisco IOS® software for secure integration with enterprise network
Unified WLAN Architecture

Overview

- Lightweight APs (LWAPs) are configured and managed by a Wireless LAN Controller (WLC)
- Plant-wide coverage, roaming and management of RF spectrum
- Location Based Services (LBS) and HyperLocation
- Advanced security policies and wireless Intrusion Prevention
- Wireless Identity Services

Note: Stratix® 5100 in WGB mode can join a Unified WLAN as a wireless client

- **SSID1** 5 GHz
- **SSID2** 5 GHz
- **SSID3** 2.4 GHz

**LWAP**

**WLC**

**WGB**

**EtherNet/IP**
Selecting the WLAN Architecture

**Unified WLAN**
- Large number of APs (typically >10)
- **Plant-wide** coverage for variety of applications and clients
- Existing Unified WLAN in Enterprise Zone
- Applications require **fast roaming**
- Managed jointly by IT and control engineers – greater level of expertise
- **Additional services**: RF analysis, Location Services, Wireless Intrusion Prevention

**Autonomous WLAN**
- Small number of APs (typically <10)
- **Standalone** applications (machines), mostly WGB clients
- **Ad hoc WLAN** installation
- Applications with **no fast roaming**
- Managed by control engineers – lower level of expertise
- No need for advanced services
Agenda

- Technology and Use Case Overview
- WLAN Architectures
- WLAN Recommendations
- Application Recommendations
WLAN Recommendations

Radio Spectrum

- 5 GHz frequency band for automation control
  - More non-overlapping channels, less interference
  - 2.4 GHz may be used for non-critical applications
- Must perform an RF spectrum survey
  - Existing Wi-Fi networks are the primary concern
  - Extended period and throughout the site
- Reserve a channel exclusively for the application, if possible
  - Devices on the same channel can interfere at 100s of meters
  - Channel re-use is not always possible
  - Wireless spectrum policy is critical
WLAN Recommendations
Site Survey

- Survey conditions should match production environment
  - Wireless hardware, RF channels, transmit power
  - Existing industrial equipment, moving obstacles
  - Installation restrictions, WGB position
  - Complete walk-through of the coverage area

- Perform active survey at the site
  - Do not rely on predictive software results only
  - Verify performance, not just coverage

- Changes in the environment may require a follow-up survey
WLAN Recommendations
SSID and VLAN Segmentation

- Traffic segmentation by SSID/VLAN and channel
  - SSID alone does NOT provide segmentation in a channel
- Avoid connecting a mobile device to the radio channel with critical EtherNet/IP traffic
WLAN Recommendations
Wireless Security - Authentication

- Always use WPA2 security with AES encryption - no performance impact
- WPA2-PSK (pre-shared key) authentication – simple but has limitations
  - One password for all clients, no user-based authentication
  - PSK is part of device configuration
  - May not provide fast roaming times
  - May not satisfy corporate security policy

Is your pre-shared key a secret?
Wireless Security - Authentication

- 802.1X authentication (WPA2 Enterprise)
  - WPA2-Enterprise with EAP-TLS is the most secure method
- Uses individual user credentials and (optional) security certificates
- Requires additional infrastructure and support
  - Active Directory
  - RADIUS server (e.g. ISE)
  - Certificate infrastructure

Security policy and existing infrastructure determine authentication methods
WLAN Recommendations
Wireless Security – Mobile Device Management

- Mobile devices introduce new security risks
  - Connecting to unsecured networks: cellular, home, public Wi-Fi
  - Malware / rootkits / unauthorized applications – including iOS
  - Inappropriate content, bandwidth use
  - Mixing personal and confidential data
- Company policy may not allow BYOD
- Posture and profiling with Cisco ISE and third-party MDM solutions
  - Is this device type allowed? Corporate or BYOD?
  - Is software up-to-date? Whitelist / blacklist of applications
  - Correct credentials and certificates, revoking of access

Source: G Data Software
WLAN Recommendations
Wireless Security – Intrusion Prevention

- On-wire attacks / threats
  - Rogue / unauthorized devices
  - Backdoor access via Wi-Fi

- Over-the-air attacks
  - Frame spoofing / impersonation
  - Denial of service
  - Reconnaissance
  - Cracking tools

- Non-802.11 threats
  - Interferers, RF jammers

Cisco Unified WLAN Solution
- Wireless Intrusion Prevention System (WIPS) – MSE, Prime
- Monitor mode APs, WIPS modules
- Rogue detection and location
- CleanAir
Agenda

Technology and Use Case Overview

WLAN Architectures

WLAN Recommendations

Application Recommendations
### Application Recommendations

Choosing an Appropriate Application

<table>
<thead>
<tr>
<th>IACS Traffic Type</th>
<th>CIP Standard</th>
<th>Use with Wireless</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supervisory information and diagnostics,</td>
<td>CIP Class 3 (HMI)</td>
<td>Yes</td>
<td>Need to control bandwidth if combined with CIP Class 1 Standard and Safety traffic</td>
</tr>
<tr>
<td>peer-to-peer messaging</td>
<td>CIP Class 3 (MSG)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peer-to-peer Control I/O Control</td>
<td>CIP Class 1 Produced/Consumed Distributed I/O</td>
<td>Yes</td>
<td>Application should tolerate occasional high latency, jitter and dropped packets; Packet rate</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>restrictions</td>
</tr>
<tr>
<td>Safety Control</td>
<td>CIP Safety</td>
<td>Yes</td>
<td>Fast safety reaction times may not be supported</td>
</tr>
<tr>
<td>Time synchronization</td>
<td>CIP Sync</td>
<td>Application</td>
<td>Accuracy and reliability can be optimized in specific configurations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dependent</td>
<td></td>
</tr>
<tr>
<td>Motion Control</td>
<td>Integrated Motion on the EtherNet/IP™ network (direct</td>
<td>No</td>
<td>Not feasible due to higher latency and jitter and limited CIP Sync accuracy</td>
</tr>
<tr>
<td></td>
<td>drive control)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Considerations:

- Larger number of EtherNet/IP connections (rack-optimized, safety, analog)
- System size vs. RPIs
Application Recommendations
Fixed PAC to Wireless PAC Topology

Considerations:
- I/O or drives are controlled by the PAC on a mobile equipment
- Larger data sizes, fewer EtherNet/IP connections
- More optimal for wireless
Fixed PAC to Wireless Drives - NOT Recommended

- Do not use Integrated Motion on the EtherNet/IP across wireless media
- Place a PAC on the wireless side to control servo drives

Not recommended: Latency and time sync issues
Application Recommendations
Packet Rate for Wireless EtherNet/IP

EtherNet/IP packet rate must be controlled in wireless media

802.11 wireless
- Half-duplex communication
- Delays due to collision avoidance and retransmissions
- Protocol overhead – not efficient with small data sizes
- Most effective when data is aggregated in a large wireless frame

EtherNet/IP
- Simultaneous communication between many nodes
- Delay and jitter sensitive
- Typically small packets
- Not possible to achieve wireless aggregation

**Maximum rate ~2,200 pps per channel for reliable operation**
Application Recommendations
Packet Rate Optimization

- Do not use RPIs faster than necessary
- Reduce number of EtherNet/IP connections
  - Large arrays and data structures
  - Produced Consumed vs. I/O data
- Aggregate traffic through a single wired controller
- Use more APs / channels per application
- Verify actual packet rate after deployment
  - Wireshark captures (wired and wireless)
- Packet rate calculation tools: Integrated Architecture® Builder
Application Recommendations

Managing Non-critical Wireless Traffic

- Manage HMI and maintenance traffic
  - Reserve and do not exceed 20% of the bandwidth
  - Watch for excessive traffic from Studio 5000® online, downloads, trends
- Reduce or avoid enterprise traffic in the same channel
  - Examples: voice, video, large file transfers, network management
- Monitor for interference from other WLANs and plant floor applications

Use dedicated channel(s) for critical applications

Example: up to 100 pps online with controller
Application Recommendations
Performance and Reliability

- **Average** latency and jitter can satisfy most applications
- Maximum latency and packet loss should NOT cause connection timeouts
  - Conditions: wireless QoS policy, recommended packet rate
- Small percentage of packets can be delayed significantly or lost

Example: Network Latency Wireless PAC to Wired PAC, 12 WGBs

No connection timeouts due to latency or packet loss

<table>
<thead>
<tr>
<th></th>
<th>Produce Consume</th>
<th>CIP Safety</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>20 ms RPI</td>
<td>40 ms RPI</td>
</tr>
<tr>
<td></td>
<td>160 ms CRTL</td>
<td></td>
</tr>
</tbody>
</table>

- Average latency 1.0 ms
- 95% packets < 3.5 ms
- **99.99% packets < 8.0 ms**
- CIP packet loss 0.05% (1 in 2,000)
Conclusion

- Wireless communication brings many advantages to IACS applications
- Wireless advantages > challenges if WLAN is designed and maintained properly
- Select appropriate wireless technology and WLAN architecture based on requirements
- Following the application and WLAN recommendations is essential for successful deployment and operation
- Security, spectrum management and site survey are critical