T26 - Wireless Design Considerations for Industrial Applications
Agenda

- Technology Overview
- WLAN Architectures
- Application Recommendations
- WLAN Recommendations
Benefits of industrial wireless network

- Connection to hard-to-reach and restricted areas
- Lower installation and operational costs
  - Cabling reduction
  - Elimination of cable failures
- Equipment mobility
  - New and more efficient applications
- Personnel mobility
  - Higher productivity and less downtime
Challenges of wireless communication

- Half-duplex shared medium:
  - Only one device can transmit at any given time
- Higher latency, jitter and packet loss compared to wired Ethernet
  - Reasons: media contention, collisions and interference
  - Can be minimized but not completely 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

Wireless advantages > challenges IF
- WLAN is designed and maintained properly
- Used for appropriate applications
Matching wireless technology with application

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

IEEE 802.11a/g/n/ac

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

Long Range SCADA
Remote site connectivity
Outdoor mesh

IEEE 802.11a/g/n
Cellular 3G / 4G LTE / WiMAX
Proprietary 900 MHz / 2.4 GHz Licensed bands

Process Instrumentation
Wireless Sensors

ISA-100.11a
WirelessHART
ZigBee / Bluetooth
Technology Overview

**Wireless client types**

**Embedded wireless adapter:**
- Limited antenna capabilities
- Placement restrictions
- Client density per AP
- Modernization costs

**External adapter (wireless bridge):**
- Single wired client (MAC address)

**Work Group Bridge (WGB):**
- Multiple wired clients
- Single *wireless* client

*Work Group Bridge is the main method of connecting industrial devices*
Wireless mobility types

- Static equipment
  - Permanent location
  - Wire replacement for hard-to-reach places
  - Examples: process control, condition monitoring, standalone OEM machines
Wireless mobility types

- Nomadic equipment
  - Stays in place while operating
  - Moves to a new location in the shutdown state
  - Examples: process skids, storage tanks, reactors, portable manufacturing equipment
Technology Overview

Wireless mobility types

- Mobile equipment (no roaming)
  - Changes position while operating
  - Remains connected to the same AP
  - Examples: rotary platforms, machines with tracks, overhead cranes with small spans
Technology Overview

Wireless mobility types

- Mobile equipment (fast roaming)
  - Connects to multiple APs while operating
  - Does not drop application connections
  - Examples: AGVs, ASRS, overhead cranes, train cars

Site survey and architecture selection are critical
Agenda

- Technology Overview
- WLAN Architectures
- Application Recommendations
- WLAN Recommendations
Autonomous WLAN Architecture

- 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

Stratix 5100™ Wireless Access Point and Workgroup Bridge
Autonomous WLAN Architecture

**Fixed controller to Wireless I/O Topology**

Considerations:
- Large number of connections (rack-optimized, safety, analog)
- System size vs. RPIs
Autonomous WLAN Architecture

**Fixed controller to Wireless controller Topology**

Considerations:

- I/O or drives that are controlled by controller on a mobile equipment
- Second Ethernet module vs. switch
- Larger tag sizes, fewer connections
Autonomous WLAN Architecture

Wireless controller to Wireless controller or I/O

Both source and destination behind WGBs – two wireless frames per single EtherNet/IP packet

Not recommended: x2 wireless bandwidth, higher latency
Unified WLAN Architecture

- Lightweight APs (LWAPs) are configured and managed by a Wireless LAN Controller (WLC).
- Plant-wide coverage and roaming.
- Plant-wide mobility and RF policies.
- Advanced security policies.
- Advanced spectrum analysis, Location Services, and wireless Intrusion Prevention.

Note: Stratix 5100™ in WGB mode can join a Unified WLAN as a client to an LWAP.
Unified WLAN Architecture

Fixed controller to Wireless controller or I/O Topology (No Roaming)

- FactoryTalk® Application Servers
- Wireless LAN Controllers
- Level 3 - Site Operations
- Industrial Zone
- Cell/Area Zones Levels 0-2
- LWAP (FlexConnect)
- Locally Switched
- Wireless Ethernet
- Wired Ethernet
Unified WLAN Architecture
Intra-Cell/Area Zone Fast Roaming

Level 3 - Site Operations
FactoryTalk® Application Servers
Wireless LAN Controllers
LWAP (FlexConnect)
WGB
Wireless I/O
FTView ME
Fixed controller
EtherNet/IP

Cell/Area Zones
Levels 0-2
Wireless controller
LWAP (FlexConnect)
WGB
Wireless controller
LWAP
LWAP
WGB
CAPWAP Tunnel
Wireless Ethernet
Wired Ethernet

Industrial Zone
Unified WLAN Architecture

Plant-wide Fast Roaming

- Wireless LAN Controllers
- Fixed controller
- LWAP
- WGB
- Wireless I/O
- Ethernet/IP
- Inter-Cell/Area Zone
- Roaming WGB
- CAPWAP Tunnel
- Wireless Ethernet
- Wired Ethernet

Level 3 - Site Operations

Industrial Zone

Cell/Area Zone 1
Levels 0–2

Cell/Area Zone 2
Levels 0–2

Centralized Application Servers

FactoryTalk® Application Servers
Unified WLAN Architecture

Wireless User Access

Enterprise Zone: Levels 4–5

Industrial Demilitarized Zone (IDMZ)

Industrial Zone: Levels 0–3

Level 3 Site Operations

Deploying Identity Services within CPwE:
ENET-TD008
ENET-WP037 (whitepaper)
Selecting the WLAN Architecture

**Unified WLAN**
- Large number of APs (>10)
- Plant-wide coverage for variety of applications and clients
- Existing Unified WLAN in Enterprise Zone
- Applications require fast wireless 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 (<10)
- Standalone applications (machines), mostly WGB clients
- Ad hoc WLAN installation
- Applications with no fast roaming
- Managed mostly by control engineers – lower level of expertise
- Can achieve greater performance with real-time EtherNet/IP traffic
Agenda

- Technology Overview
- WLAN Architectures
- **Application Recommendations**
- WLAN 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, peer-to-peer messaging</td>
<td>CIP Class 3 (HMI) CIP Class 3 (MSG)</td>
<td>Yes</td>
<td>Rate may be limited if combined with CIP Class 1 Standard and Safety traffic</td>
</tr>
<tr>
<td>Peer-to-peer Control I/O Control</td>
<td>CIP Class 1 Produced/Consumed Distributed I/O</td>
<td>Yes</td>
<td>Application should tolerate occasional high latency, jitter and dropped packets; Packet rate 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 Specific</td>
<td>Accuracy and reliability can be optimized in specific configurations</td>
</tr>
<tr>
<td>Motion Control</td>
<td>Integrated Motion on the EtherNet/IP network (direct drive control)</td>
<td>No</td>
<td>Not feasible due to higher latency and jitter and limited CIP Sync accuracy</td>
</tr>
</tbody>
</table>
Application Recommendations
Determining Application Parameters

Know your application before WLAN deployment

- Number and type of devices
- Type of wireless traffic
- Connection parameters: RPI, Safety Reaction Time, data size
- Total traffic rate in packet per second (PPS)
- Acceptable latency, jitter and packet loss

- What happens if a packet is delayed or lost?
- Can application survive a connection fault?
- Do mobile devices roam between APs?
- Do they need to remain connected when roaming?
Application Recommendations

Reduced packet rate for wireless EtherNet/IP

802.11
- Half-duplex
- Delays due to collision avoidance
- Retransmissions due to lost frames

EtherNet/IP
- Small packets
- Concurrent transmission to multiple nodes
- Not possible to aggregate in a large wireless frame

Maximum packet rate ~2,200 pps per wireless channel

Wireless frame transmission

<table>
<thead>
<tr>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overhead</td>
</tr>
</tbody>
</table>
Optimize EtherNet/IP traffic to reduce packet rate

- Packet rate optimization:
  - Use rack-optimized I/O vs. direct connections
  - Reduce number of CIP connections
  - Do not use RPIs faster than necessary
  - Use large arrays and data aggregation methods
- Single Produce Consume tag to a wireless controller vs. many wireless I/O connections
- Aggregate traffic through a single wired controller (one to many schemes instead of many to many)
- Packet rate calculation tools: Integrated Architecture® Builder
Application Recommendations

Manage all traffic in the wireless channel

- Control 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

Example: up to 100 pps online with controller

Use dedicated channel(s) for critical applications
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 that is applied, packet rate as recommended
- Small percentage of packets can be delayed significantly or lost

*Example: Wireless PAC to Fixed PAC, 12 WGBs*

- No connection timeouts due to latency or packet loss

2-week tests that are run (Produce Consume 20 ms RPI):
- Average latency 1.0 ms
- 95% packets < 3.5 ms
- 99.99% packets < 7.5 ms

Confirmed by results from customer applications
Based on the performance test results

<table>
<thead>
<tr>
<th></th>
<th>Minimum RPI</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Standard RPI            | ≥ 20 ms     | As low as 10 ms depending on the application sensitivity to delay; RPIs < 10 ms are not suitable for wireless media
| Safety RPI              | ≥ 15 ms     |                                                                                                 |
| Safety Reaction Time (SRT) Worst Case No Fault | ≥ 200 ms     | ≥ 130 ms depending on the system size and RPIs                                                |
| Safety Reaction Time (SRT) Worst Case Single Fault | ≥ 360 ms     | ≥ 200 ms depending on the system size and RPIs                                                |
Use only unicast EtherNet/IP connections with wireless

- Multicast wireless frames are not acknowledged and not repeated if lost.
- Do not use ControlLogix® Redundancy System with wireless I/O or Produced Consumed tags (requires multicast)

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>Unicast Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard I/O</td>
<td>V18</td>
</tr>
<tr>
<td>Standard Produce Consume</td>
<td>V16</td>
</tr>
<tr>
<td>Safety I/O</td>
<td>V20</td>
</tr>
<tr>
<td>Safety Produce Consume</td>
<td>V19</td>
</tr>
</tbody>
</table>
### WLAN Recommendations

**Radio Spectrum**

- **5 GHz frequency band is recommended**
  - Regulations vary by country
  - Need spectrum survey and monitoring
- **Avoid DFS channels (Dynamic Frequency Selection)**
  - Weather / military radars cause disruption of service in DFS channels
  - If DFS channels are used, RF survey and monitoring are required
- **Reserve a channel exclusively for the application, if possible**

*Wireless spectrum management policy is critical!*

<table>
<thead>
<tr>
<th>Country examples*</th>
<th>5 GHz Channels (20 MHz wide)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No DFS</td>
</tr>
<tr>
<td>U.S., Canada, Australia</td>
<td>9</td>
</tr>
<tr>
<td>Europe</td>
<td>4</td>
</tr>
<tr>
<td>China</td>
<td>5</td>
</tr>
</tbody>
</table>

*Regulations change over time*
WLAN Recommendations

Site Survey is critical for any deployment

- RF spectrum survey:
  - Monitoring for interference and existing traffic
  - Extended period throughout the site
- Active survey:
  - Verify performance, not just coverage
  - Verify cell overlap for roaming (if needed)
  - More strict criteria than enterprise WLAN

RSSI -67 dBm
SNR 25 dB
Acceptable for EtherNet/IP

RSSI -70 dBm (1/2 power)
SNR 22 dB
Can associate and pass data but poor EtherNet/IP performance
WLAN Recommendations

Site Survey

- Survey conditions should match production environment
  - Wireless hardware, RF channels, transmit power
  - Installed equipment, moving obstacles
  - Installation restrictions, WGB placement
  - Complete walk-through of the coverage area
- Site survey helps to select antenna type and placement
- Use recommended dual-band MIMO antennas (four antenna ports)
- Follow a manufacturers recommendation for antenna orientation, mounting hardware and installation procedures
- Changes in the environment may require a follow-up survey
WLAN Recommendations
Channel Reuse and Interference

**Devices using the same channel can interfere at a great distance**

- AP must defer transmission if it can decode a valid 802.11 signal
- Co-channel Interference (CCI) can be decreased but hard to eliminate
- With CCI, channel bandwidth is shared between applications
- Do not reuse channels for critical data unless complete signal separation can be reliably achieved.

<table>
<thead>
<tr>
<th>Theoretical example: Open space propagation 5180 MHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radio sensitivity</td>
</tr>
<tr>
<td>Transmit power</td>
</tr>
<tr>
<td>Omni antenna gain</td>
</tr>
<tr>
<td>Potential CCI distance</td>
</tr>
</tbody>
</table>
Radio configuration may vary from typical enterprise WLAN

- Certain 802.11n/ac features may not be relevant
  - Disable higher data rates for real-time control traffic
  - Do not use channel bonding (40 MHz and above channels)
- Use static channel and transmit power allocation (site survey results)
- Some Unified WLAN features may cause EtherNet/IP timeouts due to off-channel scan mechanism:
  - RRM (Radio Resource Management), CleanAir

Reliable transmission is more important than high data rates
WLAN Recommendations
SSID and VLAN Segmentation

Single VLAN / SSID Example

- Only 5 GHz radio used
- Dedicated VLAN for application
- No VLANs configured on the AP or WGBs
- Maintenance traffic via wired ports or different AP/channel
- Avoid connecting a mobile device to the radio channel with critical EtherNet/IP traffic (different QoS scheme)
WLAN Recommendations
SSID and VLAN Segmentation

Two VLANs / SSIDs Example

- 5 GHz radio for control traffic
- 2.4 GHz radio for maintenance traffic on a separate VLAN / SSID
- VLAN trunking on the AP
- No VLANs on WGBs
WLAN Recommendations

Wireless QoS

- Enable QoS support (if not by default) and use latest firmware for Ethernet modules
- Configure Stratix™ switches with Express Setup and Smartports
- Autonomous WLAN:
  - Default Stratix 5100™ configuration helps to optimize QoS and radio parameters for EtherNet/IP data
- Unified WLAN:
  - Less configurable (pre-defined QoS profiles with fixed transmission parameters)
  - Use “Platinum” WMM and Video/Voice Optimized QoS Profile on the WLC for best Performance
WLAN Recommendations

**Wireless Security**

- 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)
  - No fast roaming
- IEEE 802.1X authentication – most secure method
  - User credentials and/or certificates (including WGBs)
  - Require additional infrastructure support (RADIUS, Certificates, ISE, and so on)
- MAC address filtering is not secure by itself
- Other factors (DoS prevention, rogue AP detection): Unified WLAN features

Security policy and existing infrastructure determine authentication methods
Conclusion

- Wireless communication brings many advantages to IACS applications
- Wireless advantages > challenges if WLAN is designed and maintained properly
- Appropriate wireless technology and WLAN architecture selection that is based on requirements
- Following the application and WLAN recommendations is essential for successful deployment and operation
- Security, spectrum management and site survey are critical
Additional Material
CPwE Architectures - Cisco and Rockwell Automation

- Websites
  - Reference Architectures
- Design and Implementation Guides
  - ENET-TD006 - Deploying 802.11 Wireless LAN Technology within a Converged Plantwide Ethernet Architecture
- Whitepapers
  - ENET-WP034 - Deploying 802.11 Wireless LAN Technology within a Converged Plantwide Ethernet Architecture
Additional Material
Training and Certifications

- Cisco Industrial Networking Specialist Training and Certification
  - E-learning modules (pre-learning courses)
    - Control Systems Fundamentals for Industrial Networking (ICINS)
    - Networking Fundamentals for Industrial Control Systems (INICS)
  - Classroom training
    - Managing Industrial Networks with Cisco Networking Technologies (IMINS)
  - Exam
    - 200-401 IMINS

- CCNA Industrial Training and Certification
  - Classroom training
    - Managing Industrial Networks for Manufacturing with Cisco Technologies (IMINS2)
  - Exam
    - 200–601 IMINS2

- Industrial IP Advantage: e-Learning
  - Free training – Network Design eLearning
Additional Material

Education

- A ‘go-to’ resource for educational information about industrial network communication and using standard Internet Protocol (IP) for industrial applications
- Community of like-minded companies – Cisco, Panduit, and Rockwell Automation
- Receive monthly e-newsletters with articles and videos on the latest trends
- Industrial Myths
- e-Learning courses available

www.industrial-ip.org
Thank you for attending!