The Industrial Wi-Fi Shop

Best Practices for CIP Safety over Wireless

Implementing CIP Safety over wireless networks requires careful consideration to ensure functional safety, reliability, and security. Below are the key best practices:

Network Design and Configuration

- Logical Segmentation where applicable: Use VLANs to improve security and reduce broadcast traffic, which minimizes congestion and packet loss.
- Quality of Service (QoS): Prioritize CIP Safety packets to ensure time-critical traffic is handled preferentially over non-safety-related data.
- Fully Switched Network: Eliminate collisions and enhance deterministic behavior by using a fully switched Ethernet network.
- IGMP Snooping: If multicast traffic is present, control multicast messages to reduce unnecessary traffic and improve network performance.

Security Measures

- Encryption: Activate encryption to secure wireless communication against eavesdropping and unauthorized access.
- Disable unused Ethernet ports on CIP safety devices
- Configuration Ownership: Enforce ownership rules to prevent unauthorized changes to safety configurations.

Site Survey and Placement

- Conduct a comprehensive site survey to assess signal strength variations influenced by facility layout, surface finishes, and geometries. Adjust antenna placement accordingly for optimal performance.
- Consider using radiating cables (rcoax) or other methods to:
    - Limit stray signals outside the intended area.
    - Provides deterministic wireless communication and roaming events

Commissioning and Tuning

- Work with your wireless equipment partner to commission and tune the system for optimal performance. Ensure CIP Safety packets are prioritized during tuning.
- Adjust Requested Packet Intervals (RPI) during commissioning to minimize nuisance faults caused by late or lost packets.
- Beyond tuning the control system, optimizing wireless device settings can ensure that frequent, small CIP Safety packets are prioritized over other traffic on the wireless link. These settings may vary slightly between vendors.

Protocol Specific Considerations

- Black Channel Principle (IEC 61508): CIP Safety operates independently of the physical media, ensuring safety integrity even over wireless networks. This principle mitigates errors like packet loss, delays, or out-of-order transmission through techniques such as timestamps and diagnostics.
- Requested Packet Intervals (RPI): Account for fluctuating latency in wireless communication by adjusting update intervals to prevent bus overloads or lost datagrams.

Wireless Technology Selection

- Choose robust wireless technologies such as WiFi (802.11n/ac/ax) or 5G that support CIP Safety requirements for reliability and forward compatibility.

Fail-Safe Behavior and Refresh Rates

- Design the network such that devices default to a safe state (e.g., e-stop) in case of communication failures or packet loss.
- Set CIP Safety refresh rates (RPI) to the slowest acceptable rate for the chosen application yet fast enough to avoid nuisance trips.

By following these practices, you can effectively deploy CIP Safety over wireless networks while maintaining SIL 3 or PLe safety levels as per IEC 61508 and ISO 13849 standards.