Enabling CIP Communication over Bluetooth for Industrial Automation

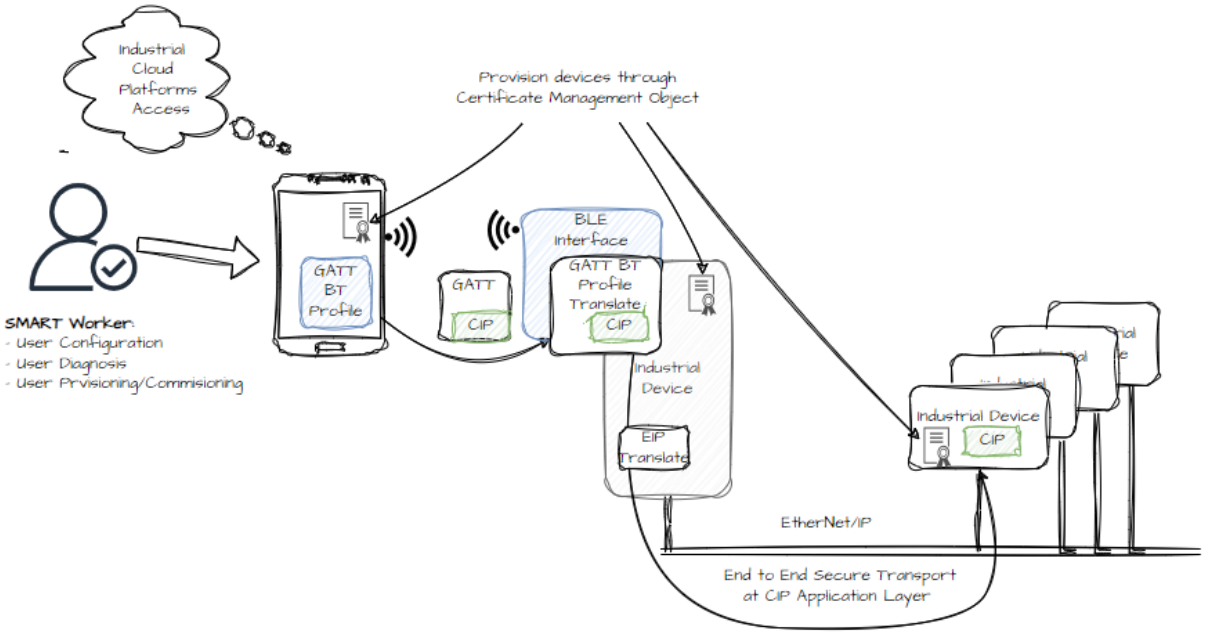
Mark Trautman
Zach Farmer
Todd Wiese

Agenda

- Use Cases & Industrial Considerations
- Bluetooth Primer
  - Bluetooth Classic vs. Bluetooth Low Energy (BLE)
  - Reliability
  - Security
  - Linking
  - Throughput
  - Profiles
- CIP Implementation
  - BLE in OSI/ CIP Model
  - Bluetooth Interface Object
  - Adapting to CIP
  - Mapping CIP to BLE Transport
  - CIP Security & Routability
- Extensions of CIP

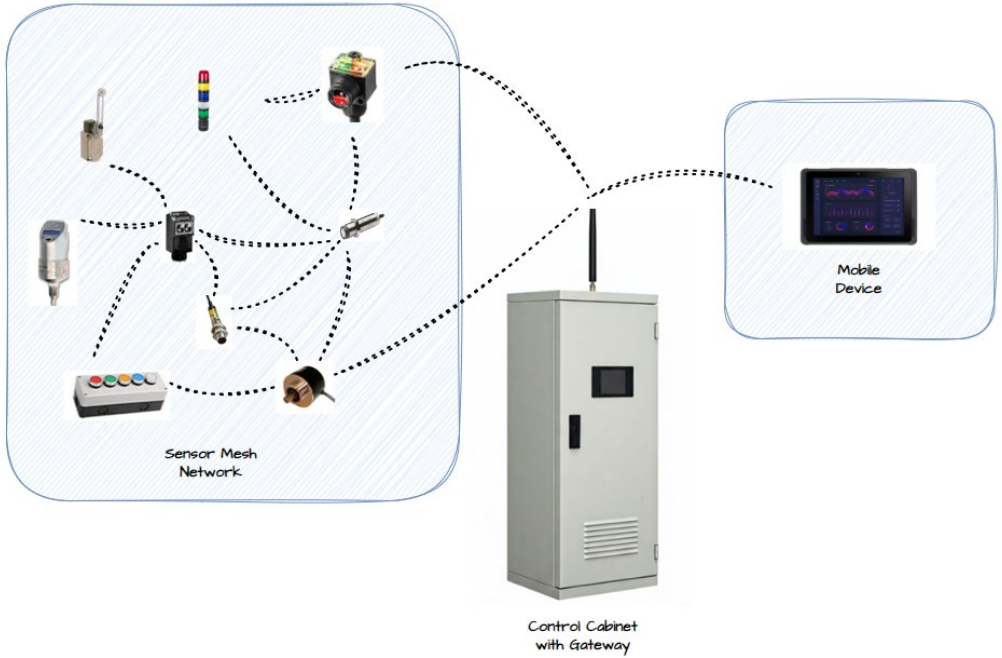
Use Cases

1. Smart Worker



Use Cases

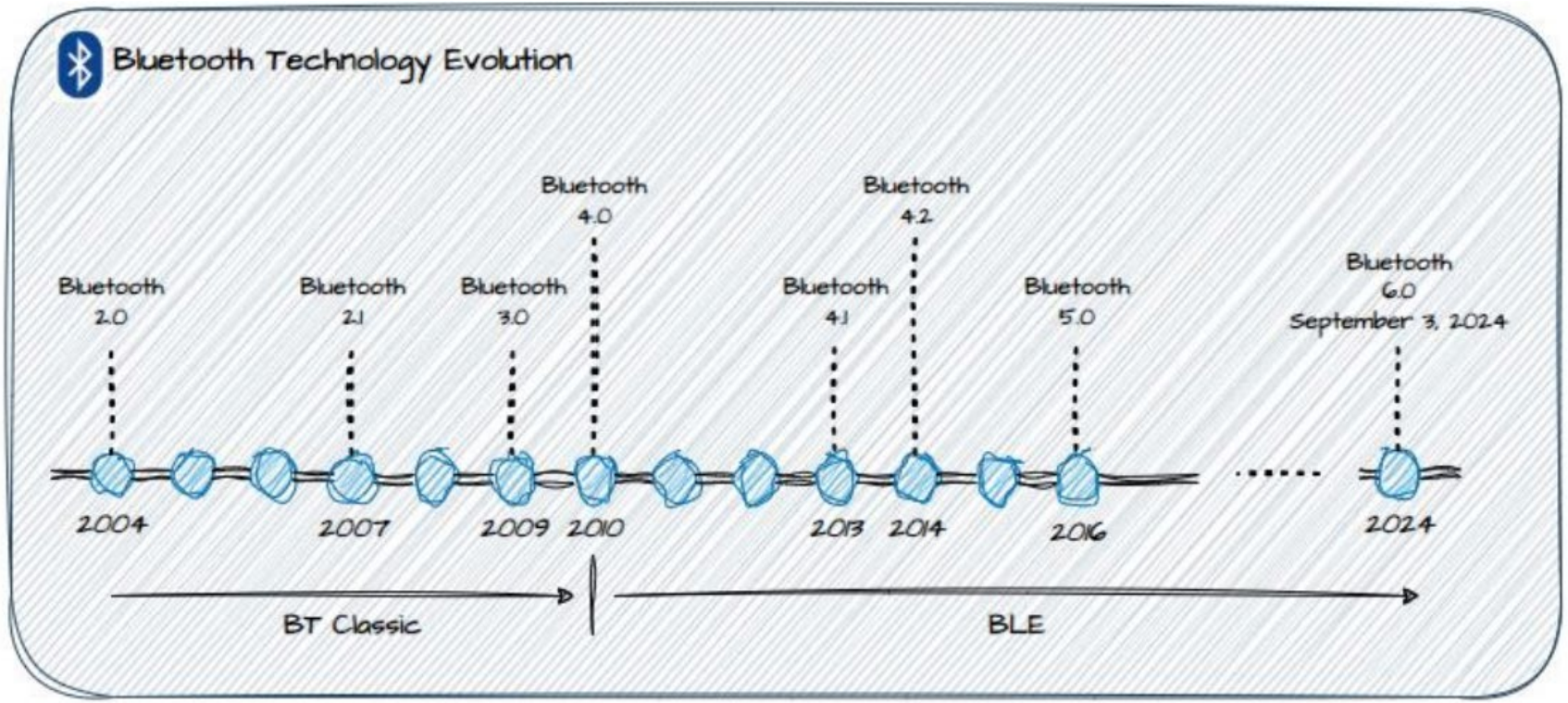
2. Sensor Network



Industrial Considerations

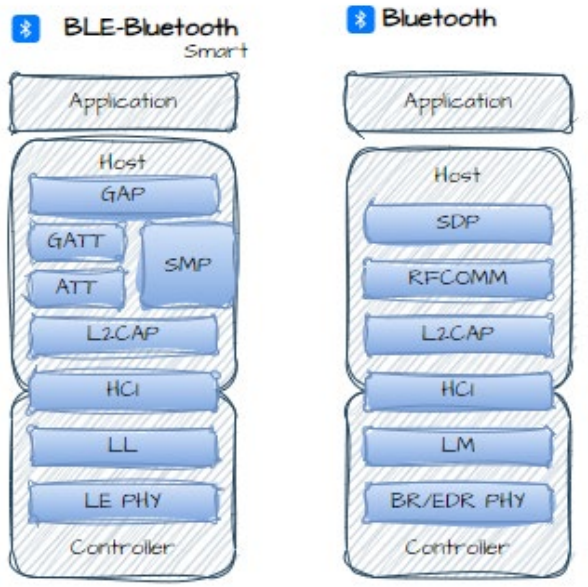
- Site Survey
  - RF Environmental Assessment
  - Electrical Noise
  - Mapping & Documentation
- Physical Location
  - Antenna placement, exterior to cabinet
- Environmental Considerations
  - Exposed hardware to environment

Bluetooth Evolution



Bluetooth Classic vs. Bluetooth Low Energy (BLE)

	Bluetooth Low Energy	Bluetooth Classic
Frequency Band	2.4 GHz ISM Band	2.4 GHz ISM Band
Channels	40 channels with 2 MHz spacing	79 channels with 1 MHz spacing
Data Rate	125 kb/s, 500 kb/s, 1 Mb/s, 2Mb/s	1 Mb/s, 2 Mb/s, 3 Mb/s
Range	50m	100m
Latency	6 ms	100 ms
Communication Topology	Mesh, Point-to-Point, Broadcast, Star	Point-to-point
Security	128-bit AES, user defined application layer	64b/128 bit, user defined application layer

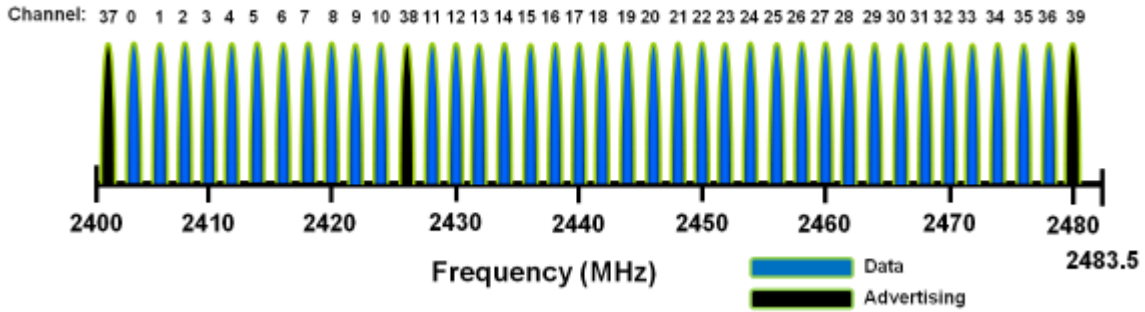


- BLE allows for enhanced security functionality, mesh networks, lower power consumption, and more recent specification enhancements by the BT SIG's.

BLE Reliability

Frequency Hopping and Frequency Shifting

- Shifts spectrum of channels at 1600 Hz.
  - 37 Channels for data, 3 for advertising
- Avoids poor signal
- Reduce bandwidth of transmitted signal
- Limit out-of-band interference



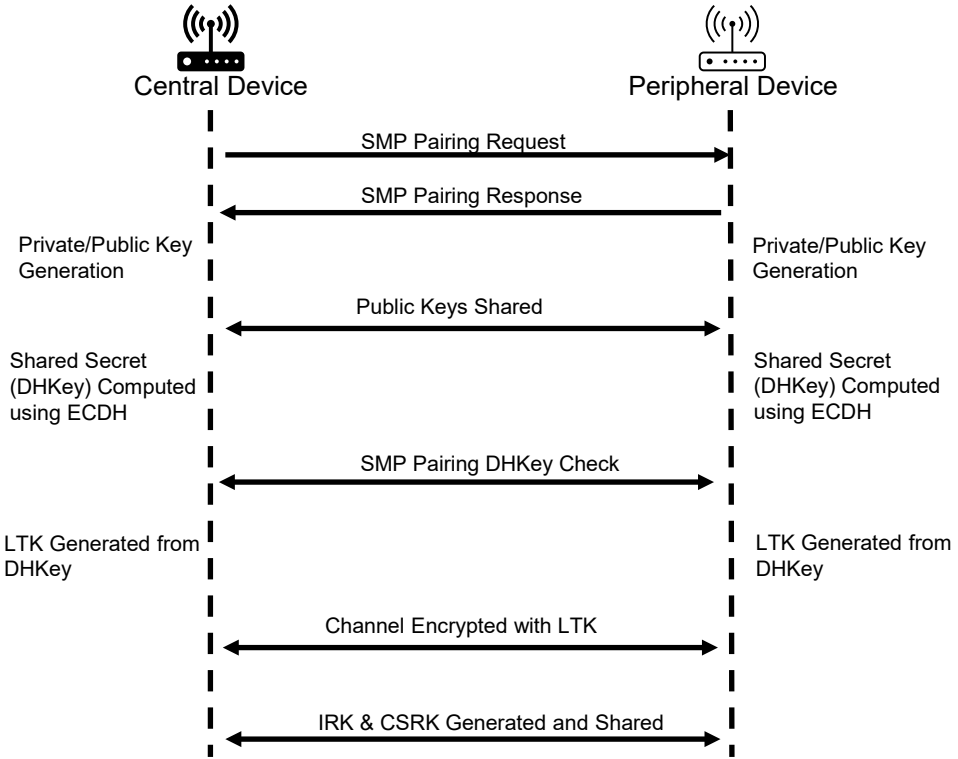
Secure Communications

LE Secure

- Bluetooth Core Specification version 4.2 (2014)
- Federal Information Process Standards (FIPS) Compliant
- Identity Resolving key (IRK) counters Identity tracking
- Encrypted communication counters passive eavesdropping (sniffing)
- Authentication of devices counters Active eavesdropping (man-in-the-middle)

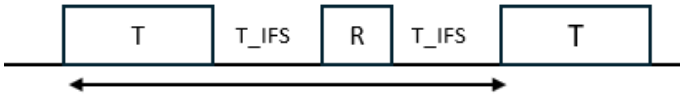
BLE Security Levels	
Level 1	No Security
Level 2	"Just Works" – Unauthenticated pairing with encryption
Level 3	Authenticated Pairing with Encryption through OOB or passkey
Level 4	Authenticated LE Secure Connection pairing with 128-bit encryption key

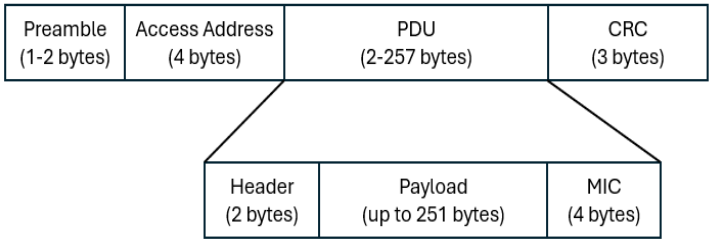
BLE Secure Connections (v4.2+) Pairing Sequence



BLE Throughput

- Time to transmit and Receive packet
  - T – Transmit Packet with Payload
  - T_IFS – Interframe time (150 µs)
  - R – Receive packet
- 1M PHY (BLE v4.2: 1Mbps)
  - 265-byte packet with payload**
  - T = 2120 µs | R = 80 µs
  - Throughput with CIP = .65 Mbps
- 2M PHY (BLE v5.0+: 2Mbps)
  - 266-byte packet with payload***
  - T = 1060 µs | R = 40 µs
  - Throughput with CIP = 1.16 Mbps

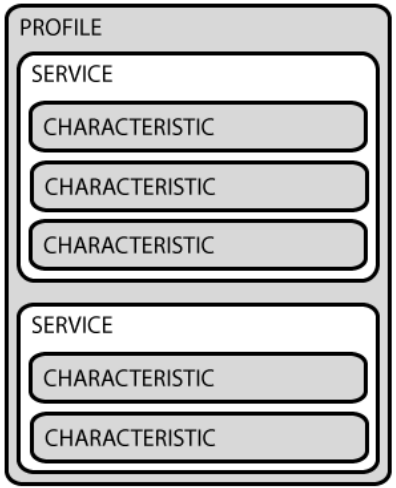




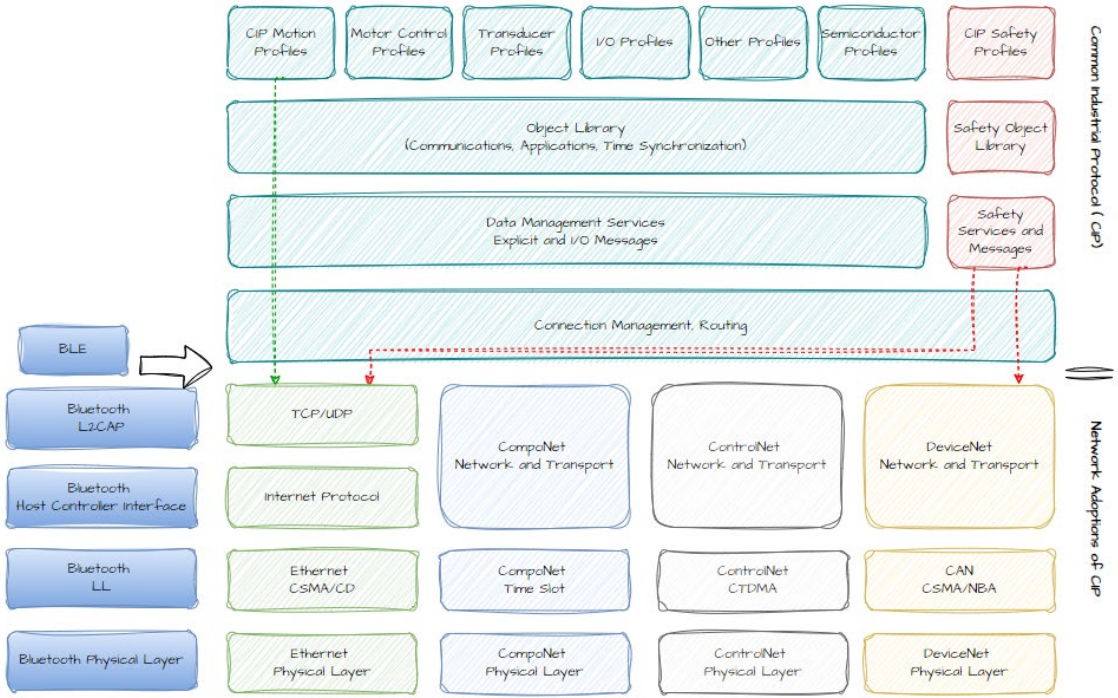
*CIP adds additional 48-byte header in Payload
**1M PHY utilizes 1 byte for Preamble
***2M PHY utilizes 2 bytes for Preamble

Bluetooth Profiles

- Each device has its own GATT Server Profile (Collection of Services)
- Service separates data logically and into characteristics
- Characteristics are the data itself.
  - Device name, manufacture name, values, permissions, etc.
- UUID and Handle for each Service and Characteristic
- GATT Client references Handle to read/write value.



Bluetooth Network Model with CIP



Bluetooth Interface Object Class

Bluetooth Interface Object

- Represents Interface and link-level security configuration

- Provides External Interface for:
  - Configuration
  - Monitoring
  - Network Commissioning

- BT Interface Object Class Attributes
  - Revision
  - Maximum Instance ID
  - Number of Instances

- Support Common Services:
  - Get_Attribute_Single(0x0E)
  - Set_Attribute_Single (0x10)

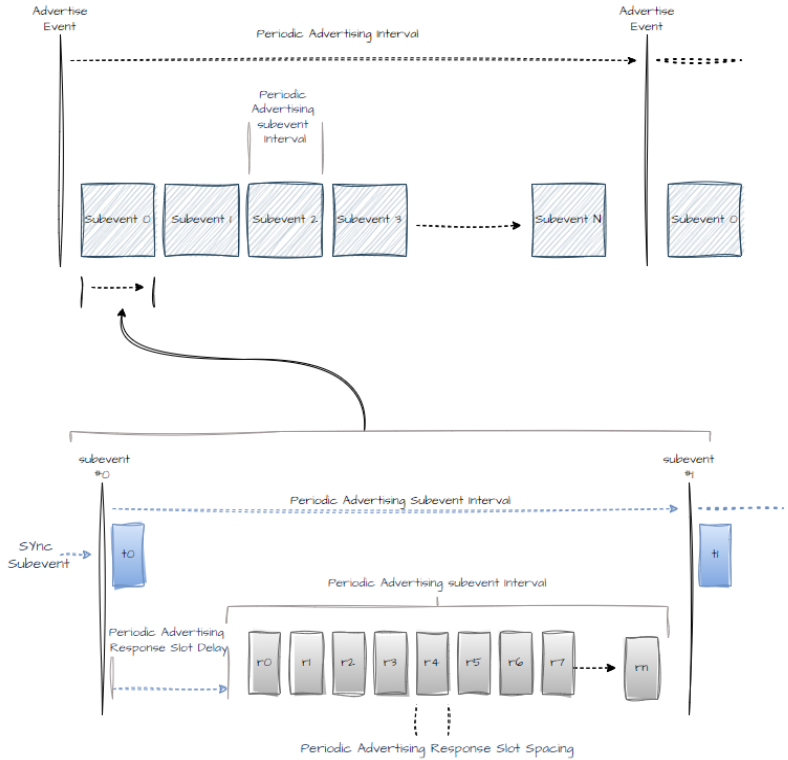
- Support Object Defined Services:
  - Clear Bonded Device List (0x4B-?)

Bluetooth Interface Object – Instance Attributes

- Enable
- Bluetooth Version
- Bluetooth Type
- Connection State
- Power Class
- Bonded Device List
- BLE Device Role
- Supported Profiles
- Connection Interval
- Slave Latency
- Supervision Timeout
- Supported Range
- Maximum Data Rate
- Supported Services
- Pairing Method
- Authentication Enable
- Encryption
- Resolvable Private Address
- Security Mode and Encryption Level
- Turn Off When Not In-Use
- Reject Unknown Pairing Request
- Use Strong Passkey
- Disable Unnecessary Services

Adapting to CIP – Combining with PAwR

- **Real-Time Monitoring**: Supports similar CIP Class 1 messaging for cyclic, time-critical data communication.
- **Low Power Consumption**: BLE PAwR's energy-efficient design ensures prolonged operation of battery-powered devices.
- **Scalability**: Manages thousands of devices using Group IDs and Response Slots, ideal for large-scale industrial deployments.
- **Deterministic Communication**: Collision-free data exchange enabled by Response Slots ensures reliable performance.
- **Explicit Messaging Support**: Facilitates non-cyclic tasks like configuration, calibration, and diagnostics using CIP services.
- **Mobile Device Integration**: BLE's ubiquity allows access via smartphones or tablets for flexible, on-the-go operations.
- **Enhanced Flexibility**: Unified framework supports both real-time monitoring and device management tasks.
- **Improved Operational Efficiency**: Enables centralized, scalable, and reliable process monitoring and control.



*PAwR - Periodic Advertising with Response

Use of CIP Safety, Security or CIP Motion?

CIP Safety Feasibility:

- BLE, with reliable frequency-hopping and sub-10 ms latencies,
- Can potentially support these safety applications at shorter distances.

CIP Motion Feasibility:

- Typically demands ultra-low latency and highly deterministic messaging.
- BLE solutions probably are not quite there, for synchronized axis motion control – At least not yet.
- However, BLE could be used in some non-critical motion diagnostics or configuration tasks.

CIP Security Feasibility:

Ensure confidentiality, integrity, and authenticity of industrial data

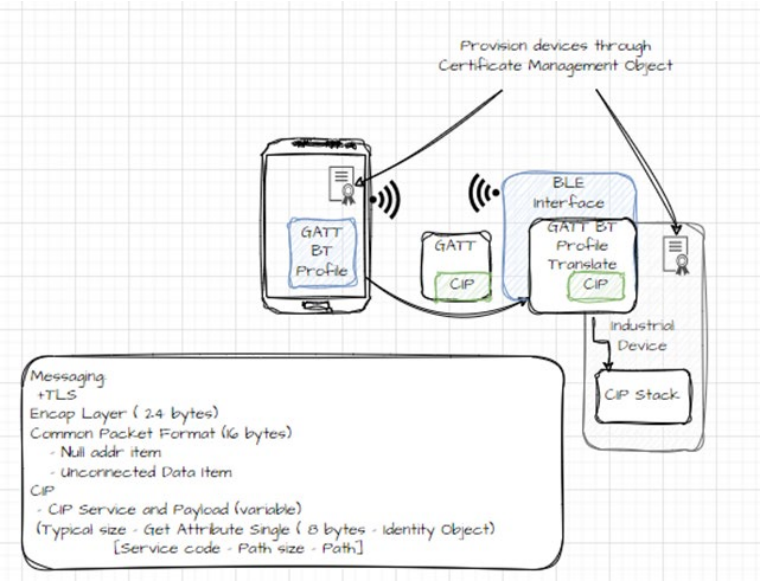
- AES-CCM encryption ensure secure data exchange
- Encapsulating CIP
- Resolvable Private Address (RPA) periodically change device's address
- Sets requirement for proper security mode and level

CIP Security Implementation Steps

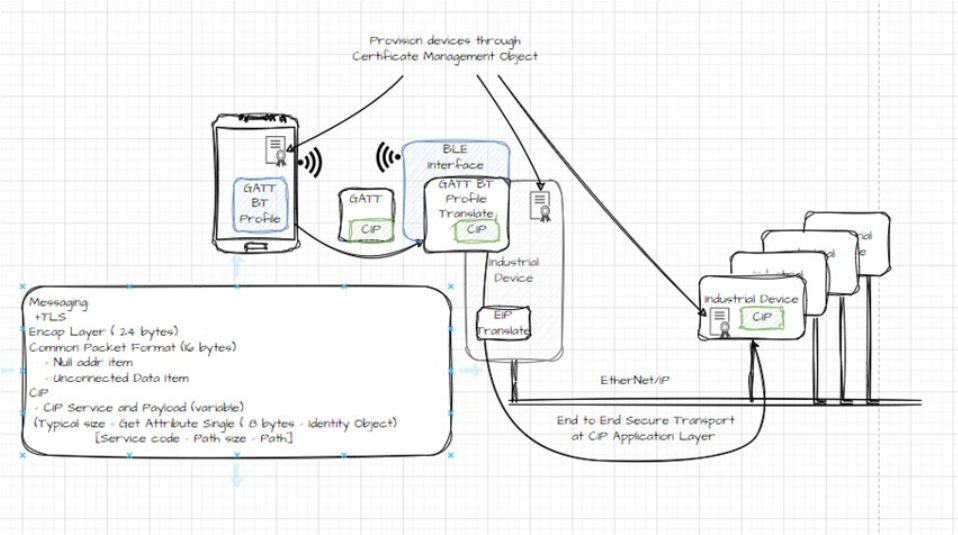
1. Device Pairing and Bonding
   - Bond devices to secure long-term keys for future reconnections
2. Enabling Encryption
   - Paired LTK's protect data in transit.
   - Only authenticated devices can decrypt and read.
3. Implementation of CIP Security Protocols
   - Incorporate message authentication to verify data integrity and legitimacy
4. Privacy Protection
   - Use Resolvable Private Address (RPA) - to rotate the BLE device address, making it harder for unauthorized parties to track devices.
5. Handling Security Modes and Levels
   - Leverage CIP Security's end-to-end encryption so sensitive information remains protected across the entire route

Connected Worker - CIP Security Examples

Originate CIP Message from BT Capable Device



Routing CIP to other devices on Ethernet/IP Network



Conclusion

- BLE proven technology in IoT applications through Bluetooth SIG supported by established vendors in the industry.
  - Reduced development costs over time.
  - Reliable medium through frequency hopping.
  - Continuous improvements in current and future releases.
- Wireless becoming more prevalent in industry with Connected Worker and Interoperability of devices growing.
- Recommendation to meet BLE Secure level 3 with encryption and authentication.
- Expansion of CIP ecosystem and interoperability to new mediums, applications, and industries.

Thank You – Questions?