Enabling CIP Communication over Bluetooth for Industrial Automation

Mark Trautman
Strategic Account Manager
HMS Industrial Networks, Inc.

Zach Farmer
Business Manager
HMS Industrial Networks, Inc.

Todd A. Wiese
Principal Software Systems Architect
Rockwell Automation, Inc.

Presented at the ODVA
2025 Industry Conference & 23rd Annual Meeting
March 19, 2025
Clearwater Beach, Florida, USA

Abstract

Wireless communication technology is becoming increasingly used in our daily lives and as such has found its way into industrial automation through a variety of mediums. Of these wireless technologies, Bluetooth is a respected technology for wireless communication in the consumer market due to its reliability, universal adoption, ease of use, and low cost. Bluetooth is a key communication technology driver behind the Internet of Things and with the increased adoption and implementation of the Industrial Internet of Things, Bluetooth technology expands the communication selection in the industrial automation ecosystem.

This paper aims to explore the potential for implementing Bluetooth for industrial use cases with CIP communications as the application layer interface for devices and software clients. It will examine the recent enhancements to the Bluetooth specifications that allow its potential use in the market, along with Bluetooth's security, stability, technical specifications, and the mapping of CIP onto Bluetooth transport with the exploration of implementing extensions of CIP onto Bluetooth. Additionally, feasibility by exploring use cases, industrial considerations, security at the application layer, and ODVA impact will be considered during this session’s content.

Keywords

Bluetooth (IEEE 802.15.1), CIP Security, Cybersecurity, Device Management, Gateway, Industrial Ethernet, Industrial Protocols, Transport Layer, Wireless.

Definition of terms (optional)

AES-CCM:	Advanced Encryption Standard with counter mode CBC-MAC
BLE:	Bluetooth Low Energy
BT:	Bluetooth
CBC-MAC:	Cypher Block Chaining – Message Authentication Protocol
CIP:	Common Industrial Protocol
CRC:	Cyclic Redundancy Check
CRSK:	Connection Signature Resolving Key
EMI:	Electro-magnetic Interference
FHSS:	Frequency Hopping Spread Spectrum
GAP:	Generic Access Profile
GATT:	Generic Attribute Profile
GFSK:	Gaussian Frequency Shift Keying
HCI:	Host Controller Interface
IRK:	Identify Resolving Key
ISM:	Industrial Scientific and Medical [2.4 gHz Band]
L2CAP:	Logical Link Control and Adaption Protocol
LAN:	Local Area Network
LL:	Link Layer
LTK:	Long-Term Key
MIC:	Message integrity Check
MTU:	Maximum Transmission Unit
OT:	Operational Technology
PAN:	Personal Area Network
PAwR:	Periodic Advertising with Response
PDU:	Protocol Data Unit
PHY:	Physical Layer Interface
SMP:	Security Manager Protocol
STK:	Short-Term Key
UUID:	Universal Unique Identifier

Introduction

Wireless technology as a medium represents 7% of the total market for industrial networks as of 2024 and has seen steady growth throughout the previous years.[9] Bluetooth, specifically Bluetooth Low Energy (BLE) has proven to be a key technology for short range wireless applications due to its reliability, ease of use, and low cost. By implementing CIP communications over BLE, industrial devices may be enabled to communicate wirelessly while maintaining commonality and compatibility when communicating with the existing CIP-based systems in today's market. The use cases in this paper, reference utilizing CIP over BLE in a system including scenarios for the connected worker through smart devices such as phones, tablets, and sensors and IO mesh networks.

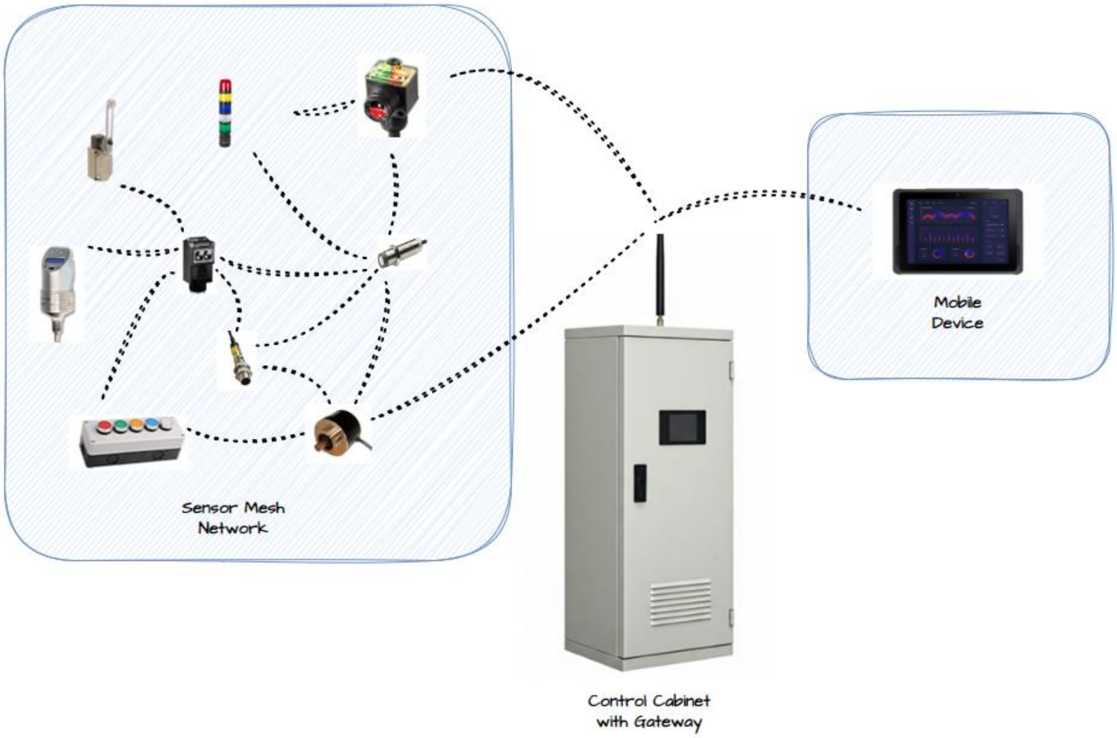
In the case of "the smart worker", personnel can be locally present on the plant floor with a tablet or phone, already utilizing BLE while connected to the machine, panel or device through a BLE enabled access point and view diagnostics, read/write parameters, and perform troubleshooting and commissioning procedures. If the device or network of devices which a mobile client is already connecting to, is utilizing CIP for communications, providing data over a BLE transport in CIP formatting will allow for a cohesive integration utilizing common familiar building blocks. Additionally, when commissioning the machine, there may arise a situation where a safe stop is needed in which case a virtual e-stop could be utilized on the application running on the mobile device by leveraging CIP Safety, thus completing CIP Safety over BLE.

Implementing BLE for sensor networks may also allow for alternative connectivity where wired connectivity is difficult, such as in hazardous areas, or situations that are not plausible for dynamic applications (Examples: slip rings and robotic end effectors). The mesh network feature of BLE may be leveraged to provide many-to-many (m:m) connections which optimize creating large scale device networks by enhancing the reliability and flexibility of the network. Implementing CIP transferred through BLE on these IO networks, the commonality of data used across the network will allow for a scalable and diverse solution to meet industry needs.

In many cases, there will be limitations that will be addressed in the sections below, some of which include range, data rates, and outlining the security concerns and recommendation to address these concerns such as introducing CIP Security to allow for continuous secure access throughout a network architecture. Additionally, these applications of BLE offer a personal area network (PAN) solution to the broader local area network (LAN) or wide area network (WAN) of the devices, machine, and plant. In order for data on the Bluetooth network to be utilized by the broader network, a gateway would need to be employed to facilitate this data transition. Some of the key reasons for utilizing a gateway in this context can include:

- Protocol translation – translate between BLE and various Ethernet protocols, in this case EtherNet/IP. Such as switching the transport mechanism from that of BLE to TCP/IP and UDP.
- Routing – Utilization of CIP Routing for gateway to route aggregated CIP data to the appropriate destination.
- Device Management – Gateway providing services to manage BLE connections including pairing, authentication, and maintaining these connections, as well as serve as the security manager.
- Network segmentation – Allow only the necessary data to pass to and from the Operational Technology (OT) networks, minimizing unnecessary data traffic.
- Security – Gateway to provide additional layer of security by serving as a firewall, controlling data flows and access to a machine network.
- Scalability – Ease of integration for adding more BLE nodes or a new network to a machine.

As an alternative approach to utilizing a gateway to segment the BLE PAN to a broader area network, functionalities described could be embedded into an IPC, edge computing device, or integrated directly into the firmware of an alternative device on a network such as a PLC or HMI. However, in comparison, a gateway provides a scalable and feasible approach to implementing a BLE interface into a broader CIP based network.



Industrial Considerations

When implementing a Bluetooth network in the industrial setting, the following considerations will need to be addressed for industrial implementations:

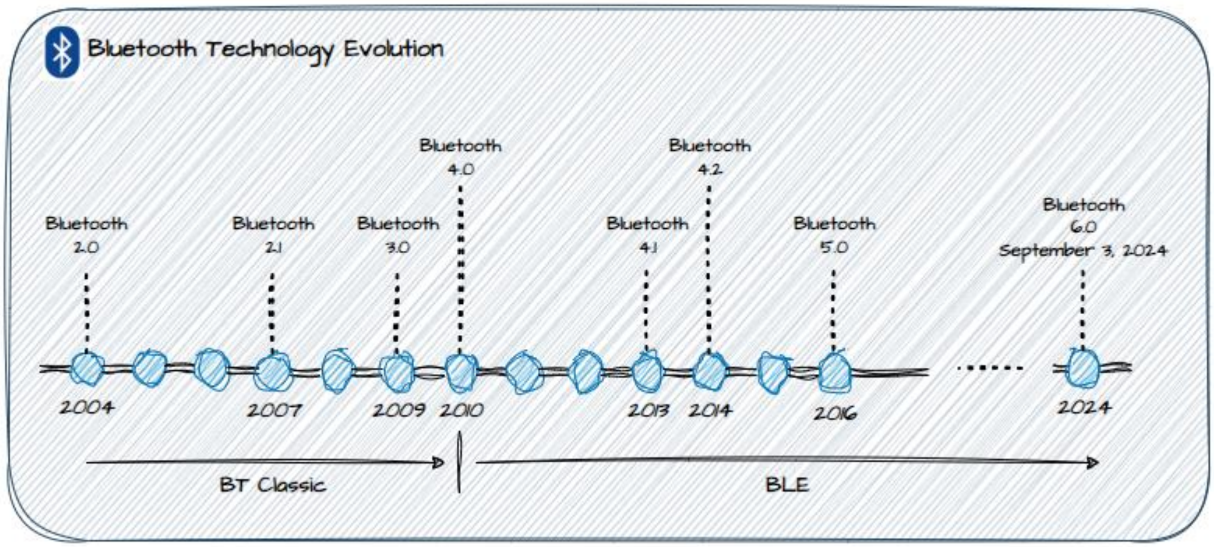
- **Site Survey** – providing a radio frequency (RF) environmental assessment, to understand if there is interference stemming from other 2.4 GHz networks such as Wi-Fi or Zigbee, electrical noise from motors and inverters, and additional metal structures that may interfere with Bluetooth signals. This can be completed via an RF spectrum analyzer by surveying the plant floor and testing the coverage. Additionally, a mapping and documentation summary is completed following the assessment. It is recommended to perform routine scans annually to proactively detect new interference as well as immediately after installing new machinery that could affect BLE performance.

- **Physical location** – understand where Bluetooth device(s), a gateway, or antenna(s) need to be placed on the machine or throughout the plant floor for optimal commissioning and integration. Ideally, wireless devices are placed externally to the cabinet enclosure.

- **Environmental considerations** – as the device is external to the cabinet, the environment must be accounted for to ensure the hardware is not being exposed to any caustic or corrosive gases that would cause failure in the device.

Bluetooth Primer

1.) General Background – BT Evolution:



2.) BT classic vs BLE

Bluetooth Classic and Bluetooth Low Energy (BLE), while stemming from the same underlying technology can be different in nature. BLE was introduced under Bluetooth v4.0 by the Bluetooth Special Interest Group (SIG) in the 2011 time-period and developed primarily for Internet of Things (IoT) applications. BLE technology uses a short burst of data transmission while Bluetooth Classic uses continuous data streaming, thus more appropriately lending itself to wireless streaming for audio and file transfer. Since BLE uses short bursts while in 'sleep mode' until a connection is initiated, it provides a solution of 1/10 the energy consumption of traditional Bluetooth devices. Table 1 below compares the technical specifications for BLE and Bluetooth Classic.

	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

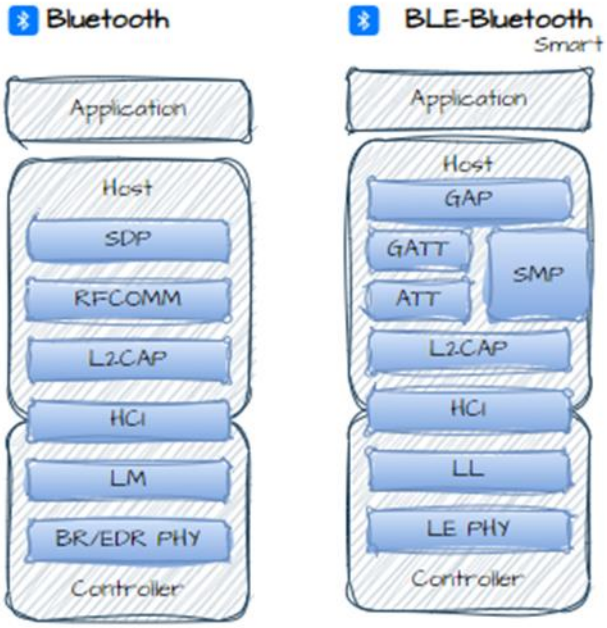
Table 1 BLE vs Bluetooth Classic Comparison[6]

The operating range of Bluetooth is highly variable depending on several conditions such as radio spectrum, transmit power, receiver sensitivity, obstacles, radio reflection, electromagnetic interference (EMI), and beacon orientation. It has been estimated for an industrial environment with a BLE transmission rate at 2 Mb/s, a 0 dBm transmit power configuration, using a 0 Transmitter Antenna Gain, and 0 dBm receiver gain, a probable range for appropriate communications can be expected to be 23-55m.[7]

3.) Bluetooth Stack Comparison

Bluetooth Classic and BLE (also referred to as Bluetooth SMART) protocol have two distinct stacks with the same three building blocks including Controller, Host, and Application blocks. The individual layers in the BLE stack starting at the bottom include:

- Physical Layer (PHY) – the physical radio interface that operates in the 2.4 GHz band, where the BLE packets are transmitted and received.
- Link Layer (LL) – the layer responsible for establishing and maintaining connections, advertising, scanning for devices.
- Host Controller Interface (HCI) – provides the interface between the host and controller layers, which is used to send and receive commands via USB, SPI, or UART.
- Logical Link Control and Adaptation Protocol (L2CAP) – Handles segmentation and reassembly of data packets for higher layers of message processing through logical channels.
- Security Manager Protocol (SMP) – responsible for device pairing, bonding, and key distribution and management.
- Attribute Protocol (ATT) – utilizes client-server model to define how data is represented in BLE server database, and how this data is read or written.
- Generic Attribute Profile (GATT) – Defines hierarchy of ATT attribute types so data is exchanged between devices in structured way.
- Generic Access Profile (GAP) - Responsible for how devices can discover and connect to each other.



4.) **Reliability**

Bluetooth's characteristic reliability features are twofold with its method for channel usage of Frequency Hopping Spread Spectrum (FHSS) and the type of frequency modulation it uses, Gaussian Frequency Shift Keying (GFSK).

BLE operates on 40 channels - 3 advertising and 37 data channels – in the 2.4 GHz ISM (Industrial, Scientific, and Medical) frequency band and uses FHSS as the method to hop between each of these channels within the frequency band. The BLE devices follow a pseudo-random hopping sequence that is dictated by the master device and communicated to slave device(s). These spectrum hops can occur up to 1600 times per second and during the time of hopping, the BLE devices continuously monitor the quality of communication on the present channel; if interference is present or poor signal quality is detected, the device will flag the channel to not use and continue with the remaining data channels. This frequency shifting also includes use of a Gaussian filter, as the name implies, allowing for smoother transitions between channel shifting by shaping the edges of the transmitted signals. This filtered keying helps reduce the bandwidth of the transmitted signals and reduces out-of-band interferences because the signal occupies less spectrum due to the Gaussian filtering.

5.) **Linking**

When establishing an encrypted link between two devices, the two devices will negotiate a suitable key length which each can support, and which is deemed acceptable for the application associated with the connection. This involves the central device sending a suggested key size to the peripheral device. The central device is typically a smartphone or tablet while the peripheral device would be a headset, fitness tracker, etc. In the use case for industrial automation and purpose of this paper, the central device would be the BLE gateway, and the peripheral device would be the sensors or a tablet. In either case, the central device initiates the connection, scans for advertising peripherals, and controls the data flow; where the peripheral device broadcasts its presence, waits for a connection request from a central device and provides data when connected. The suggested key size is always set to the maximum key size supported by the central device to begin with. If the peripheral device can accommodate the central device's suggested key size, it accepts it. If not, it replies with a suggestion of its own. This exchange of suggestions between central and peripheral continues until an agreement is reached or it is concluded that no mutually acceptable key length can be established, in which case the encryption setup is abandoned.

6.) Pairing

BLE offers two primary pairing methods: LE Legacy and LE Secure Connections. LE Legacy, part of Bluetooth v4.0 specification, uses less robust security, relying on pairing methods such as Just Works or Passkey Entry. LE Secure Connections, introduced in Bluetooth v4.2, provides enhanced securing using Elliptic Curve Diffie-Hellman (ECDH) cryptography for key generation and exchange.

In the BLE pairing process, there are various association models used to establish secure connection between the two devices . These include:

1. Just Works: This model does not provide protection against man-in-the-middle (MITM) attacks and is typically used when there is no user interface for entering or displaying a passkey.
2. Passkey Entry: This model involves the user entering a passkey for one or both devices. It provides MITM protection.
3. Numeric Comparison: Both devices display a number, and the user verifies that the numbers match, providing strong MITM protection.
4. Out of Band (OOB): Uses an external communication method (like NFC) to exchange cryptographic information, providing strong MITM protection.

LE Legacy Pairing Overview:

LE legacy supports the Just Works, Passkey entry and Out of Band association models for pairing. The pairing phases for LE Legacy are as follows:

1. Pairing Feature Exchange – The devices exchange information about their input/output capabilities and device which association model to use.
2. Short Term Key (STK) Generation: Depending on the chosen association model, the devices generate a temporary key (STK) that is used for encrypting the link during the pairing process.
3. Long Term Key (LTK) Generation and Distribution: Devices generate and exchange the LTK and other keys (such as Identity Resolving Key (IRK) and Connection Signature Resolving Key (CSRK)) that will be used for future secure connections. Security Capabilities:

Limitations of LE Legacy Pairing
Vulnerable to MITM Attacks, the "Just Works" association model is vulnerable to MITM attacks because it does not authenticate the devices. Limited to Bluetooth 4.0, LE Legacy Pairing is part of the Bluetooth 4.0 specification, and newer versions of Bluetooth (starting from Bluetooth 4.2) introduced LE Secure Connections, which provide stronger security features and mitigations against known vulnerabilities in LE Legacy Pairing.

LE Secure Connections Pairing Overview:

The key features of LE Secure Pairing include the following characteristics:
Elliptic Curve Diffie-Hellman (ECDH) Key Exchange:

- LE Secure Pairing uses the ECDH algorithm to generate a shared secret key, or Diffie-Hellman key, between the two devices. This key is then used to derive the Long-Term Key (LTK) and other encryption keys.
- ECDH provides a higher level of security by ensuring that the key is not transmitted over the air and is resistant to eavesdropping.

The association models LE Secure Connections supports are Just Works, Passkey Entry, Numeric Comparison, and Out of Band.

Pairing Phases:

1. Pairing Feature Exchange: Devices exchange information about their input/output capabilities and decide which association model to use.
2. Public Key Exchange: Devices exchange their public keys using the ECDH algorithm to generate a shared secret.
3. Authentication Stage: Devices authenticate each other using the chosen association model (e.g., Passkey Entry, Numeric Comparison).
4. Short Term Key (STK) Generation: Devices generate a temporary key (STK) using the shared secret key.
5. Long Term Key (LTK) Generation and Distribution: Devices generate and exchange the LTK and other keys, such as Identity Resolving Key (IRK) for resolving random private addresses and Connection Signature Resolving Key (CSRK)) for data signing to ensure authenticity of messages.

Security Capabilities:

- Protection Against Passive Eavesdropping: ECDH key exchange ensures that the shared secret is never transmitted over the air, making it resistant to eavesdropping.
- Protection against MITM Attacks: Depending on the association model used (e.g., numeric comparison, passkey entry), LE Secure Pairing provides strong protection against MITM attacks by authentication bot devices.

The advantages of LE Secure provide enhanced security features compared to LE Legacy Pairing, making it suitable for applications requiring high levels of security. These include improved user experience due to association models like Numeric Comparison and Passkey Entry which offer a balance between security and user convenience. Along with backward compatibility of devices which can still fall back to LE Legacy Pairing when communicating with older devices that do not support the newer method.

7.) LE Secure

The three common attack types that BLE must protect are as follows:

1.) Identity tracking which exploits the Bluetooth address to track a device on the network.
2.) Passive eavesdropping or sniffing, where the attacker is listening in to the data being transmitted between devices.
3.) Active eavesdropping or man-in-the-middle (MITM) where the attacker can impersonate a Bluetooth device on the network allowing them to listen in and potentially alter the data being transmitted.

As identity tracking exploits the Bluetooth address to track a device, protecting from such requires privacy protection. This can be done by enabling the LE Privacy feature provided by BLE to prevent the device information from being exposed during advertising mode. This feature functions by allowing the MAC address (Media Access Control) within the advertising packets to be changed to a random value thus disguising the real MAC address. This process is initiated during the pairing process where the devices exchange encryption keys so the underlying devices can understand the real MAC address which this random MAC address will be translated to. The encryption key that allows for this feature is the Identity Resolution Key (IRK), which allows for the first device to translate the random MAC address, which appear in the advertising packets from the second device to the real MAC address of the second device. Generally, the random private MAC address change in accordance with a timer the device manufacture implements in the product firmware, allowing the devices to know how often the MAC addresses will change.[8]

To prevent against actors listening in to the data exchange with passive eavesdropping, BLE encrypts the data being transferred using AES-CCM (Advanced Encryption Standard with CBC-MAC (Counter Mode Cipher Block Chaining Message Authentication Protocol)) cryptography while checking the integrity of the data itself. This cryptography specifically utilizes AES-128, Advanced Encryption Standard with 128-bit key, with it being a symmetric key meaning the same key is used for both encryption and decryption by the sender and receiver, all managed by the security manager protocol (SMP).

To protect the network from MITM attacks, the devices must adhere to security level 3 at a minimum of the security levels BLE defines for authentication and encryption. These levels are: security level 1 – no security with no authentication nor encryption, the devices simply connect without pairing; level 2 – unauthenticated pairing with encryption, the device requires pairing but in the notion of it 'just works'; level 3 – authenticated pairing with encryption, where the pairing mechanism could be out of band (OOB), such as through near field communication (NFC), or through passkey; level 4 – the most secure option utilizes authenticated LE secure connections pairing with encryption using a 128-bit encryption key.

8.) Throughput

In all network communications, the time it takes to send and receive data will dictate the throughput of the underlying technology. For BLE, a simplified diagram looks as shown in figure 1:

'T' is the transmission packet,
'R' is the receive packet from peer device acknowledging the packet has been received.
'T_IFS' is the inter frame space or time between two consecutive packets.

For any version of BLE 4.2 and above, the T_IFS will be 150µs and the length of time for transmission packet (T) and receive packet (R) will depend on the packet length and PHY used. The PHY used on the BLE device will dictate the baud-rate, the baud-rate of a LE 1M PHY would be 1 Mbps, while the baud rate of a LE 2M PHY is 2 Mbps. The LE 1M PHY is commonly used across BLE devices, while the 2M PHY is gaining market acceptance with its release in Bluetooth version 5.0.

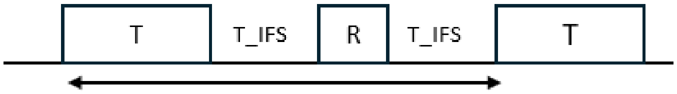


Figure 1 - Transmission Timing

The throughput of BLE depends on numerous factors such as the payload, Bluetooth version, mode used, and PHY. First regarding the payload of a BLE packet, the total packet length of BLE in v4.2 and above is 265 bytes total, with a payload of up to 251 bytes. To break this down further in the figure below, it is comprised of:

- Preamble (1-2 bytes) – used in the receiver to perform frequency synchronization, gain control, and symbol timing estimation. 1 byte for LE 1M PHY and 2 bytes for LE 2M PHY[10]. This results in a total packet of 265 bytes for LE 1M PHY and 266 bytes for LE 2M PHY.

- Access Address (4 bytes) – unique to each connection to avoid collisions.
- PDU (2-257 bytes) – Protocol Data Unit, consisting of header, payload, and MIC (Message Integrity Check), and can either be an advertising PDU to establish connection or as a data PDU to transmit the data with.
- CRC (3 bytes) – Cyclic Redundancy Check to detect errors in the packet.

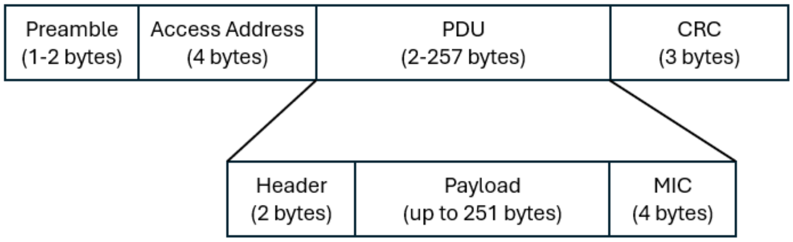


Figure 2 – Bluetooth Low Energy Packet

For the transmission packet as noted in figure 2, the maximum size with the largest payload will be 265 bytes and the receive packet length will be an empty payload to acknowledge receipt of data with just a preamble, access address, header, and CRC, thus a total of 10 bytes.
The version of BLE will impact the overall throughput attainable, as the maximum data rate of v4.2 is 1 Mbps with the corresponding LE 1M PHY, whereas the data rate of v5.0 and above is 2 Mbps with the LE 2M PHY. To illustrate how this will affect the overall throughput, in v4.2 the time it takes to send a transmission packet of 265 bytes at 1 Mb/s will be 2120 µs. Similarly, the time it takes to receive the receipt packet of 10 bytes at 1 Mb/s will be 80 µs. The total time to transmit a packet and receive the target device’s advertisement packet is 2500 µs. The payload to be transferred is 251 bytes; however, including CIP components of encapsulation layer (24 bytes), common packet format (16 bytes) and CIP services such as the Set Attribute Single (8 bytes), will leave the actual written data payload in CIP format to be up to 203 bytes. Therefore, the possible throughput for v4.2 of BLE utilizing the LE 1M PHY will be .65 Mb/s. In following similar logic for BLE v5.0 and above utilizing a 2M PHY with a maximum data rate of 2 Mbps, the time to transmit a packet would come down to 1060 µs, receive packet to 40 µs and therefore the resulting maximum throughput is 1.16 Mb/s.[11]

Within a BLE network, there may arise an instance where a CIP message is larger than the MTU (Maximum Transmission Unit) of BLE itself, or the 251-byte payload. In this case, messages can be separated into multiple packets through a fragmentation process which occurs within the L2CAP layer. This process occurs by way of the following:

1. Application Layer sends data to the L2CAP Layer.
2. If data is larger than the MTU, or 251 bytes, the L2CAP layer divides this message into multiple smaller fragments.
3. Each fragment is encapsulated into its own packet payload.
4. The receiving device’s L2CAP Layer receives these fragmented packets and reassembles into the original data stream.

This functionality will prove useful in the case where an EtherNet/IP packet, commonly much larger than the MTU of BLE, is needed to be fragmented into multiple smaller packets, and sent over a BLE network. For example, in the case of connected worker, if the mobile device connected to the machine via BLE needs to read an EtherNet/IP message on mobile device, the data read will be fragmented and sent over Bluetooth.

9.) Profiles

The host layer within the BLE stack sits below the application layer and above the control layer and is responsible for standardizing the method in which applications communicate with devices. The host layer provides the profiles which consist of a standard collection of services for a specific use case(s). Namely, the Generic Access Profile (GAP) defines the devices discovery and connections of the BLE network and Generic ATTribute (GATT) Profile which manages how attributes and data, are transferred once devices have established a dedicated connection.
The GAP defines how devices interact with each other at a high level such as how they advertise themselves, establish connections, and manage security of the connections. GAP dictates how devices discover and establish connections, as a result, there are four main roles a device can play on a BLE network. In the GAP, a device can be specified as a broadcaster – device that broadcasts data but does not allow connections; observer – device listens for broadcasted data without establishing connections; central – device actively scans for and connects to other devices; and peripheral – device that advertises its presence and allows other devices to connect to it. Regarding the aforementioned use cases, the primary GAP roles for industrial automation would be utilizing central and peripheral devices where a reliable, secure connection is made between devices. GAP is also responsible for managing the connection's security through the underlying Security Management Protocol (SMP) and setting the BLE device address, which is similar to that of the MAC address. The BLE device address is a unique 48-bit value comprised of 12 hexadecimal digits with the format: XX:XX:XX:XX:XX:XX.

Once the discovery and connection of devices has been achieved, the GATT profile manages and defines how the data is structured in the form of services, characteristics, and attributes, as well as how these items are read or written. There are two roles the device can serve defined by the GATT, the server or client. The GATT Server is implemented on the device side and contains one or more services which encapsulate functionality related to the characteristics, and attributes being the information transferred between devices. A typical characteristic may be comprised of the following attributes: characteristic value, characteristic value UUID (universal unique identifier), characteristic value handle, properties, and descriptors such as format or unit, all of which would be stored in the GATT server in an attribute table. In addition to the values of above attributes, also in the attribute table will be the handle – index of attribute in the table, type – indicates what the attribute data represents, and permissions – enforces if and how a GATT client device can access the attribute. The type for each attribute is represented by a UUID, some of which are defined by Bluetooth SIG and if not, can be custom generated. If the UUID is Bluetooth-SIG defined it will be 16-bits and if it is custom generated, or vendor specific, it needs to be 128-bits.

An example of a custom GATT Server profile for a simple temperature sensor is as below.

GATT Service: Temperature Sensor Service

Handle of Service: 0x0001 | UUID: 0x1234

Characteristics of Service:

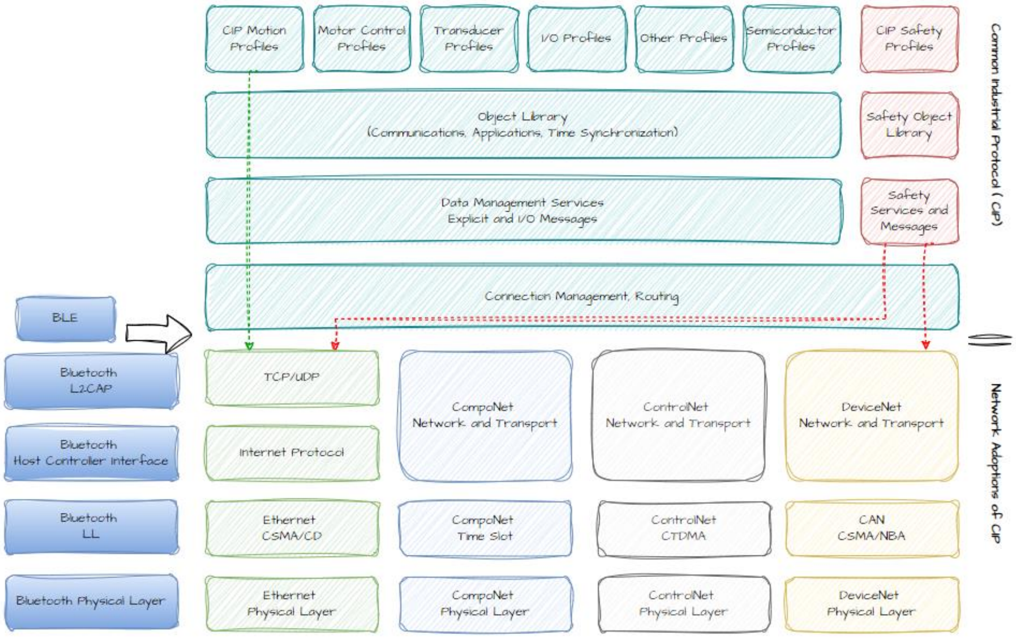
Handle	UUID	Description	Value	Permissions
0x0002	0x1235	Temperature Value (C)	22.2	Read
0x0003	0x1236	Temperature Threshold (C)	30	Write

In this example, the GATT client (mobile device or control system) can read the temperature value by referencing handle 0x0002 and set the temperature threshold by writing to handle 0x0003.

CIP Profile Mapping:

1.) CIP Model Representation:

As we are aware the Common Industrial Protocol (CIP) model representation is a comprehensive framework designed for industrial automation and control systems, facilitating seamless communication across various devices and networks. At its core, CIP integrates multiple layers, including the application, transport, network, and data link layers, to ensure robust and reliable data exchange. By incorporating Bluetooth technology, the CIP model can further enhance wireless communication capabilities, providing flexible, low-power, and cost-effective connectivity solutions for industrial applications.



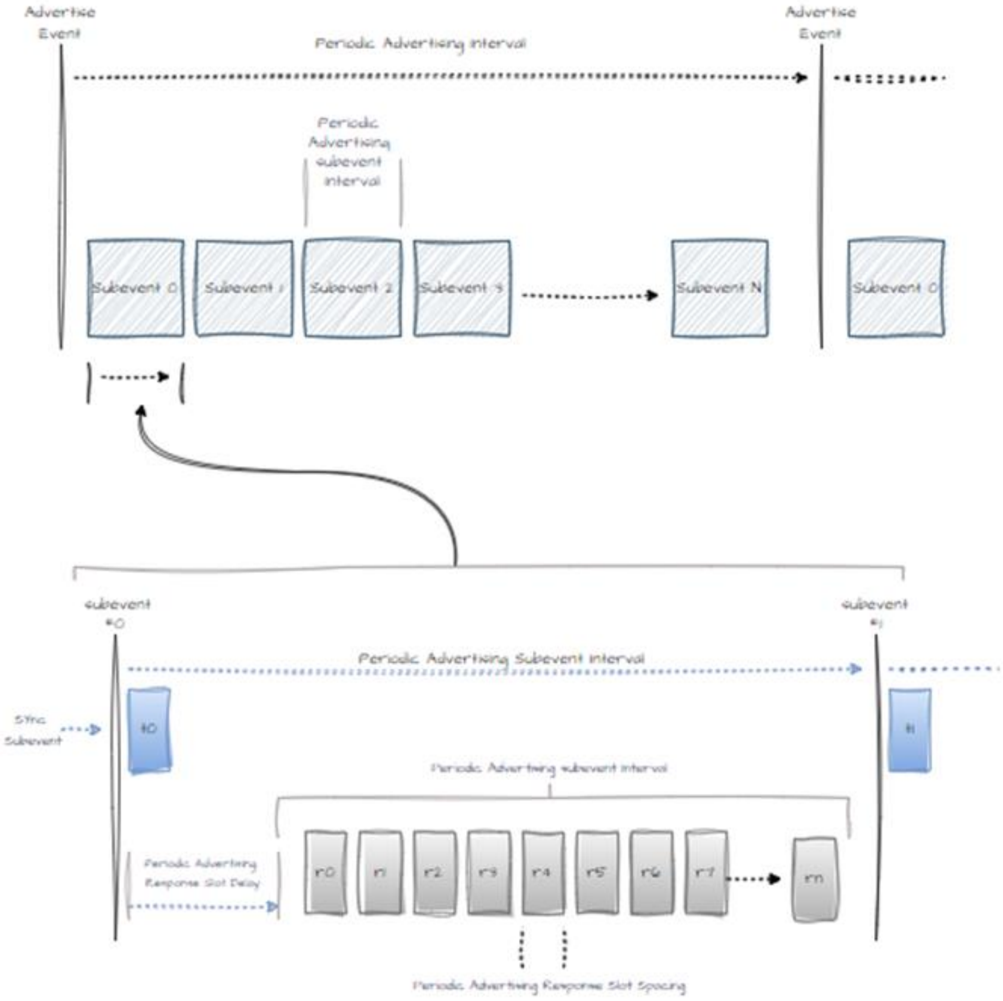
2.) Adaptability to CIP:

The integration of Bluetooth Low Energy (BLE) Periodic Advertising with Responses (PAwR) with the Common Industrial Protocol (CIP) may offer a scalable, low-power, and efficient communication framework for industrial devices. CIP, widely used in industrial automation and the process industry, organizes data into a hierarchical structure of Classes, Instances, and Attributes, with Services facilitating access and modification of these attributes. BLE PAwR, introduced in the Bluetooth 5.4 specification, provides a mechanism for managing large numbers of devices with minimal energy consumption, making it well-suited for industrial environments. By combining the two, process industries can achieve real-time monitoring, configuration, and diagnostics in a centralized and flexible manner.

Process industries, such as oil and gas, chemical manufacturing, and water treatment, rely heavily on continuous monitoring of critical parameters like pressure, temperature, flow rate, and pH levels. CIP’s Class 1 messaging, designed for cyclic and time-critical data exchange, can be implemented using BLE PAwR to enable real-time monitoring of these parameters. In this setup, a central device, referred to as the Access Point (AP), periodically broadcasts advertising packets to a group of devices (Responders) identified by Group IDs. Each device within the group is uniquely assigned an ESL ID (or a similar identifier) and a specific Response Slot for communication.

Sensors deployed across the process plant can aggregate multiple CIP attributes into an Assembly Object (e.g., Class 0x04), encapsulating real-time operational data. For example, a pressure sensor might aggregate readings such as Pressure = 150 psi, Temperature = 80°C, and Flow Rate = 50 L/min into an Assembly Object. The AP triggers data exchange by broadcasting periodic requests, and each sensor responds in its designated Response Slot with the latest data. BLE PAwR's short Periodic Advertising Intervals and support for multiple Subevents ensure low-latency, deterministic communication, making it ideal for real-time process monitoring where timely decisions are critical to maintaining operational efficiency and safety.

Reference the following diagram "PAwR operation"


Advertise Event
Periodic Advertising interval
Advertise Event
Periodic Advertising subevent interval
Subevent 0
Subevent 1
Subevent 2
Subevent 3
Subevent N
Subevent 0
subevent #0
subevent #1
Periodic Advertising Subevent interval
Sync Subevent
#0
#1
Periodic Advertising subevent interval
Periodic Advertising Response Slot Delay
r0
r1
r2
r3
r4
r5
r6
r7
rn
Periodic Advertising Response Slot Spacing

In addition to cyclic data exchange, BLE PAwR supports explicit messaging for non-cyclic tasks such as sensor configuration, calibration, and diagnostics. CIP's hierarchical structure allows specific attributes to be accessed or modified using services like Get_Attribute_Single or Set_Attribute_Single. BLE PAwR enables these operations by leveraging its targeted communication model. Devices periodically broadcast key attributes, such as Vendor ID, Product Type, or Product Code (from the CIP Identity Object, Class 0x01), in their advertising payloads. A mobile device or AP can query or configure a specific sensor by targeting its ESL ID and sending a request in the appropriate Response Slot. For instance, an operator might use a mobile application to recalibrate a pH sensor or update its operational range. Similarly, fault codes or diagnostic data can be retrieved to troubleshoot issues with a flow meter or temperature sensor. BLE’s ubiquity ensures seamless integration with mobile devices, enabling technicians to perform these tasks without requiring specialized hardware. This capability enhances flexibility and reduces downtime in process plants, where maintaining uninterrupted operations is critical.

Benefits:

The combination of CIP and BLE PAwR delivers several advantages for process industry applications. Scalability is achieved through PAwR’s ability to manage thousands of devices using Group IDs and Response Slots, enabling large-scale deployments in sprawling process plants. Low power consumption ensures that battery-operated sensors and devices can operate for extended periods, reducing maintenance overhead. The collision-free communication provided by Response Slots ensures deterministic and reliable data exchange, even in dense device environments. Furthermore, the ability to support both cyclic (real-time) and non-cyclic (configuration and diagnostics) communication provides a unified framework for diverse process monitoring and control applications.

Example Use Case: Water Treatment Plant

In a water treatment plant, multiple sensors are deployed to monitor critical parameters such as water pressure, flow rate, pH levels, and turbidity. Each sensor aggregates these readings into a CIP Assembly Object and communicates with the central AP using BLE PAwR. The AP periodically broadcasts requests to the sensor group (e.g., Group ID for water quality sensors), and each sensor responds in its designated Response Slot with real-time data. For example, a pH sensor might report pH = 7.2, while a turbidity sensor reports Turbidity = 5 NTU (Nephelometric Turbidity Units). If an anomaly is detected, such as a sudden drop in pH or an increase in turbidity, an operator can use a mobile application to connect to the specific sensor via BLE PAwR. The operator can retrieve diagnostic data, recalibrate the sensor, or adjust its operational parameters in real time. This approach ensures continuous process monitoring, reduces the risk of plant downtime, and improves overall operational efficiency.

Summary:

By mapping CIP’s hierarchical structure to BLE PAwR’s efficient communication model, process industries can achieve a new level of scalability, flexibility, and energy efficiency. This integration enables real-time monitoring, configuration, and diagnostics for thousands of sensors and devices, making it an ideal solution for some industry applications in the process sector. Whether it is for water treatment, chemical production, or oil and gas operations, the combination of CIP and BLE PAwR provides a robust foundation for modern industrial ecosystems.

3.) Bluetooth Interface Object:

The Bluetooth Interface Object represents the interface and link-level security configuration of Bluetooth Classic or Bluetooth LE (Low Energy) interfaces. This object provides the necessary external interface for devices capable of communicating through a close proximity wireless interface for configuration, monitoring, network commissioning, and additional functions. It also offers a structured representation of security configurations for Bluetooth devices, facilitating the management and implementation of security settings in industrial automation devices.

The Bluetooth Interface Object would include class attributes that define its general properties as normal for CIP Objects:

Class Attributes

Attribute Name:	Attribute Description:
Revision	Indicates the revision of the object class definition.
Maximum Instance Id	The highest instance number currently created.
Number of Instances	The count of instances currently created.

Instance attributes provide detailed information and control over the Bluetooth interface:

Instance Attributes

Attribute Name:	Attribute Description:
Enable	Allows the interface to be enabled or disabled.
Bluetooth Version	Specifies the version of the Bluetooth standard in use (e.g., Bluetooth Classic or Bluetooth LE, 2.0, 2.1, 3.0, 4.0, 4.1, 4.2, 5.0, 6.0. etc.). Note: Most recent versions of Bluetooth specifications are recommended for implementation due to reliable, robust, and secure operation.
Bluetooth Address	A unique 48-bit value identifying the Bluetooth device. The Upper Address Part (UAP): The UAP is the most significant byte of the 48-bit address. It typically represents the manufacturer of the device, or the Bluetooth module used in the device. The Lower Address Part (LAP): The LAP is the remaining 5 bytes of the 48-bit address, representing the unique identifier assigned to the specific device. The Bluetooth 48-bit address follows a specific format, usually represented as a series of 12 hexadecimal digits or six pairs of hexadecimal values separated by colons or hyphens. For example, a Bluetooth device address could be represented as "XX:XX:XX:XX:XX:XX" or "XXXXXXXXXXXX". It's important to note that the Bluetooth address is typically assigned by the manufacturer and cannot be changed by the user. This uniqueness of the Bluetooth address helps in device identification, pairing, and communication within Bluetooth networks.
Connection State	Indicates the operating state of the Bluetooth interface (e.g., Active Mode, Sniff Mode, Hold Mode, Park Mode).
Power Class	Defines the power class of the Bluetooth interface (e.g., Class 1, Class 2, Class 3).
Bonded Device List	Lists Bluetooth addresses currently associated with the interface.
BLE Device Roles	Specifies the device roles implemented. (e.g., Peripheral, Central, Broadcaster, Observer).
Supported Profiles	Lists supported Bluetooth profiles. GATT [Generic Attribute Profile]

	BNEP [Bluetooth Network Encapsulation Profile – BT Classic Only] PAN [Personal Area Network] DIP [Dev ID] SDAP [Service Discovery]
Connection Interval	The time between two connection events
Slave Latency	The number of skipped connection events allowed for a peripheral device.
Supervision Timeout	The timeout period from the last data exchange until a link is considered lost.
Supported Range	Describes the supported range of the Bluetooth interface.
Maximum Data Rate	Describes the maximum supported data rate.
Supported Services	Provides a bitmapped identification of supported Bluetooth services. Discoverable through SDAP profile: Examples Service Discovery Service - Allows a device to retrieve information on services offered by a neighboring device. Generic Access Service – Procedures related to discovery and link management aspects. Generic Attribute Service – Defines structure in which data is exchanged and how attributes are grouped to form services. Link Loss Service – Defines behavior when Link is lost between devices. Tx Power Service – Identifies current power transmit levels of a device while participating in a connection. Authorization Control Service – Enables authorization to access specific or protected GATT resources of server. Transport Discovery Service – Enables a device (BLE) to expose services that are available on another transport (Ethernet). Indoor Positioning Service – RTLS – Location tracking enabler.
Pairing Method	Specifies the pairing method used (e.g., SSP, Passkey Entry, Just Works).
Authentication Enable	Allows authentication to be enabled or disabled.
Encryption	Indicates the type of encryption used on the interface.
Resolvable Private Address	Enables privacy features for Resolvable Private Address.
Security Mode and Encryption Level	Defines the security mode and encryption levels supported by the Bluetooth interface.
Turn Off When Not In-Use	Allows the Bluetooth interface to be disabled when not in use to prevent unauthorized access.
Reject Unknown Pairing Request	Prevents pairing requests from unauthorized devices.
Use Strong Passkeys	Requires the use of strong passkeys for device access.
Disable Unnecessary Services	Provides a list of services to be enabled or disabled based on device requirements.

Common Services

Possible Bluetooth Interface Object supported common services:
• **Get_Attribute_Single (0x0E):** Retrieves a single attribute.
• **Set_Attribute_Single (0x10):** Sets a single attribute.

Object Specific:
Clear_Bonded_Device_List (0xXX): Clear the array of DB_ADDRs bonded to a device.

Summary

The Bluetooth Interface Object is a possible framework for managing Bluetooth interfaces in industrial automation devices. It offers robust security configurations, flexible interface management, and detailed control over Bluetooth communications, making it a vital component for modern industrial applications.

4.) Other CIP Extensions:

CIP Safety:

CIP Safety as an extension of the CIP suite provides safety critical communications in industrial environments and is typically used in high-availability, low-latency, and fault tolerant systems. In assessing the implementation of CIP Safety over BLE there are inherent benefits to BLE lending itself to this application such as its high reliability and stability from its frequency hopping mechanism. Some of the initial use cases for implementing CIP Safety over BLE can include:

- Remote E-Stop on a tablet in connected worker example, providing a safe stop mechanism when commissioning a machine from the remote device.
- Wireless E-stop local to the machine if dynamic application with rotating equipment.
- Additional stationary safety IO needed within close proximity of machine as part of mesh IO network.

Applications where CIP Safety would not be suitable over BLE would include where roaming is needed such as in AMRs/AGVs and applications with distances exceeding the limitations of BLE. For these use cases, BLE and the respective gateway necessary to connect to the LAN could act as a 'black channel' for the safety data that is being transmitted. CIP Safety has a relatively low payload of 74 bytes that would be able to fit within the BLE packet's payload. Additionally, as the latency can be as low as 6 ms on BLE, this would be suitable for most functional safe applications. However, more testing would need to be completed to understand the safety rated levels BLE can provide in terms of reliability, latency depending on payload and distance, as well as an understanding of the application and the risks posed.

CIP Motion:

In assessing CIP Motion over BLE, this is not something that would be feasible at the moment due to CIP Motion's requirement low-latency communication and determinism. One use case for utilizing BLE for motion applications in general could be to monitor or configure standalone motion applications that do not require real-time communication.

CIP Security:

Security (Routability) - General

CIP Security (Common Industrial Protocol Security) provides mechanisms to ensure confidentiality, integrity, and authenticity of data in industrial networks. Implementing CIP Security over BLE transport involves leveraging BLE's capabilities to secure communication channels between industrial devices. This section outlines the key considerations and steps for implementing CIP Security over BLE.

Implementing CIP Security over Bluetooth Low Energy (BLE) Transport

Possible Implementation Steps

Step 1: Device Pairing and Bonding

- Pairing: Initiate the BLE pairing process using a suitable method (e.g., Passkey Entry or Numeric Comparison) to establish a secure link between devices.
- Bonding: Store the long-term keys generated during pairing for future secure connections.

Step 2: Enabling Encryption

- Encryption Setup: Enable AES-CCM encryption on the BLE link to protect data during transmission. This ensures that all data exchanged between devices is encrypted and secure.
- Encryption Keys: Use the long-term keys generated during the pairing process to establish encrypted connections.

Step 3: Implementing CIP Security Protocols

- Secure Messaging: Implement CIP Security's secure messaging protocols over BLE transport. This involves encapsulating CIP messages within BLE's encrypted data packets.
- Message Authentication: Use cryptographic techniques (e.g., HMAC) to authenticate CIP messages. This ensures that messages are from legitimate sources and have not been tampered with.

Step 4: Privacy Protection

- Resolvable Private Address (RPA): Enable RPA to periodically change the device's address, enhancing privacy and making it difficult for unauthorized parties to track the device.

Step 5: Handling Security Modes and Levels

- Security Modes: Configure the BLE interface to operate in the appropriate security mode, as defined by CIP Security. This includes setting the security mode and encryption level to meet the required security standards.

- Security Levels: Ensure that the BLE transport meets the security level requirements specified by CIP Security, such as authenticated link keys and encryption.

Example/Possible Implementation could incorporate the following:

An example implementation of CIP Security over BLE transport could involve the following steps:

- Device Pairing: Use Numeric Comparison to pair two industrial devices, establishing a secure link.
- Bonding: Store the long-term keys generated during pairing for future connections.
- Encryption: Enable AES-CCM encryption on the BLE link to protect data during transmission.
- Secure Messaging: Encapsulate CIP messages within BLE's encrypted data packets, ensuring data integrity and confidentiality.
- Message Authentication: Use HMAC to authenticate CIP messages, verifying their authenticity.
- Privacy: Enable RPA to periodically change the device's address, enhancing privacy.

Implementing CIP Security over Bluetooth Low Energy transport involves leveraging BLE's built-in security features to ensure the confidentiality, integrity, and authenticity of data exchanged between industrial devices. By following the outlined steps and utilizing BLE's pairing, encryption, and privacy mechanisms, a secure communication channel can be established, meeting the requirements of CIP Security in industrial automation environments when there are point to point connections that are established. However, the consideration of including the mechanisms designed for CIP Security utilizing TLS should be used when transporting through multiple physical media segments, such as Bluetooth to Ethernet to provide an end-to-end security solution.

a. Originate CIP Message from BT capable clients.

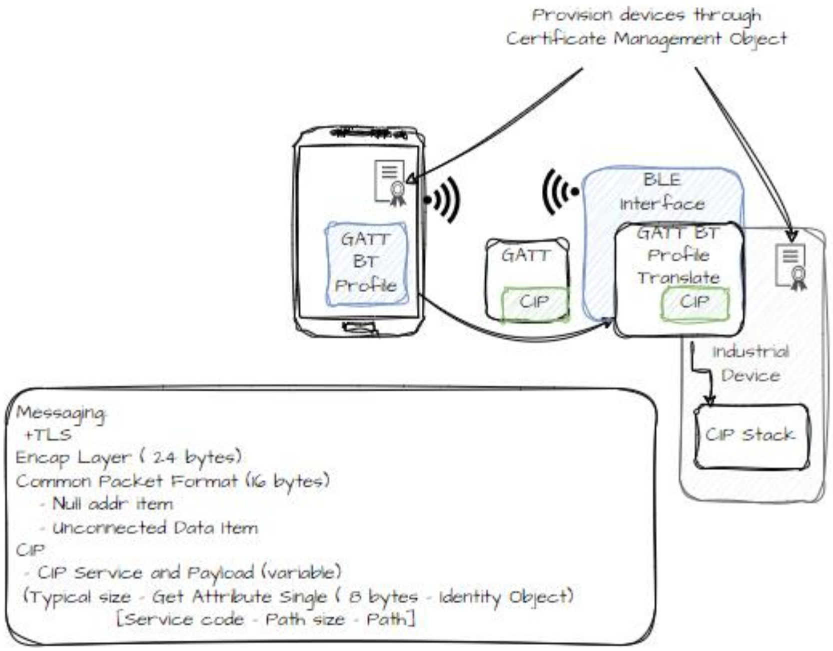

Provision devices through
Certificate Management Object
GATT
BT
Profile
GATT
CIP
BLE
Interface
GATT BT
Profile
Translate
CIP
Industrial
Device
CIP Stack
Messaging
+TLS
Encap Layer (24 bytes)
Common Packet Format (16 bytes)
- Null addr item
- Unconnected Data Item
CIP
- CIP Service and Payload (variable)
(Typical size - Get Attribute Single (8 bytes - Identity Object)
[Service code - Path size - Path]

Figure 32 Originate CIP Message from BT Capable Client

b. Securely Route to other devices on EIP network.

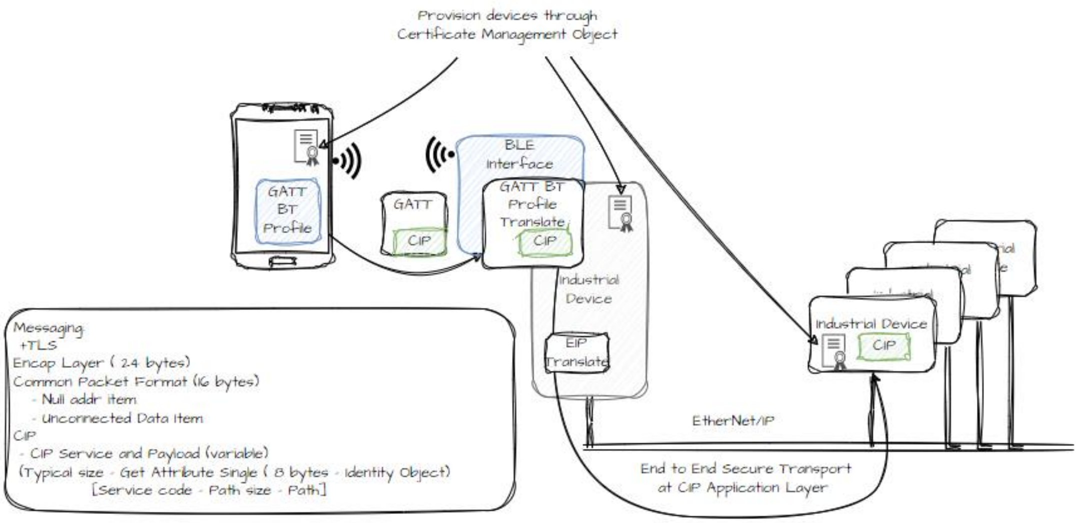

Provision devices through
Certificate Management Object
GATT
BT
Profile
GATT
CIP
BLE
Interface
GATT BT
Profile
Translate
CIP
Industrial
Device
EIP
Translate
Industrial Device
CIP
EtherNet/IP
End to End Secure Transport
at CIP Application Layer
Messaging
+TLS
Encap Layer (24 bytes)
Common Packet Format (16 bytes)
- Null addr item
- Unconnected Data Item
CIP
- CIP Service and Payload (variable)
(Typical size - Get Attribute Single (8 bytes - Identity Object)
[Service code - Path size - Path]

Figure 43 Securely Route to other devices on EIP network

Conclusion:

This whitepaper explored the feasibility and potential of implementing Bluetooth technology, more specifically Bluetooth Low Energy (BLE), for industrial automation by enabling Common Industrial Protocol (CIP) communications possibilities over BLE. It delves into recent enhancements in Bluetooth specifications, addressing aspects such as security, stability, and technical specifications. Therefore, it is strongly recommended to use the latest version of the BLE specification to take advantage of the most up to date capabilities. The paper discusses mapping CIP onto Bluetooth transport, extending CIP functionalities, and evaluates use cases including smart devices for connected workers and sensor networks in challenging environments. It also considered industrial considerations, security implications, and the role of gateways in integrating BLE with broader industrial networks, ultimately proposing a scalable and secure approach for adopting Bluetooth in industrial automation.

References

[1] ODVA, The CIP Networks Library, Volume 1: Common Industrial Protocol, Ann Arbor: ODVA, Inc., 2001-2024.
[2] ODVA, The CIP Networks Library, Volume 2: EtherNet/IP Adaptation of CIP, Ann Arbor: ODVA, Inc., 1999-2024.
[3] ODVA, The CIP Networks Library, Volume 5: CIP Safety, Ann Arbor: ODVA, Inc., 2005-2024.
[4] ODVA, The CIP Networks Library, Volume 8, CIP Security, Ann Arbor: ODVA, Inc., 2015-2024.
[5] ODVA, The CIP Networks Library, Volume 9, CIP Motion, Ann Arbor: ODVA, Inc., 2016-2024.
[6] BLE vs.BT, https://www.ezurio.com/resources/blog/bluetooth-low-energy-vs-bluetooth-classic-what-s-the-difference
[7] BT Range Estimator, https://www.bluetooth.com/learn-about-bluetooth/key-attributes/range/#estimator
[8] BT Protecting your Privacy, https://www.bluetooth.com/blog/bluetooth-technology-protecting-your-privacy/

[9] HMS, https://www.hms-networks.com/news/news-details/17-06-2024-annual-analysis-reveals-steady-growth-in-industrial-network-market.
[10] Bluetooth Packet Structure, https://www.mathworks.com/help/bluetooth/ug/bluetooth-packet-structure.html.
[11] Bluetooth Performance, https://www.bluetooth.com/blog/exploring-bluetooth-5-how-fast-can-it-be/.

****

The ideas, opinions, and recommendations expressed herein are intended to describe concepts of the author(s) for the possible use of ODVA technologies and do not reflect the ideas, opinions, and recommendation of ODVA per se. Because ODVA technologies may be applied in many diverse situations and in conjunction with products and systems from multiple vendors, the reader and those responsible for specifying ODVA networks must determine for themselves the suitability and the suitability of ideas, opinions, and recommendations expressed herein for intended use.