Simplified Asset Tracking Management With Wi-Fi®

ABSTRACT

This application report describes the development of Wi-Fi®-enabled Real-Time Location System (RTLS) tags. Specifically, the benefits of adding Wi-Fi® to an RTLS tag design are examined.

Different Wi-Fi® use cases and power modes are presented along with an estimate of system battery life for a typical use case. This application report demonstrates how SimpleLink™ Wi-Fi® makes it possible to create a battery powered RTLS tag design that can be tracked as well as be securely monitored and controlled from the cloud.

Contents

List of Figures

List of Tables

Trademarks

SimpleLink is a trademark of Texas Instruments.
Aruba Networks is a registered trademark of Aruba Networks, Inc.
Bluetooth is a registered trademark of Bluetooth SIG, Inc..
Cisco is a registered trademark of Cisco Systems, Inc. and its affiliates.
Wi-Fi is a registered trademark of Wi-Fi Alliance.
All other trademarks are the property of their respective owners.

1 Introduction

Location, tracking, RTLS and RFID are just few terms that are mentioned everywhere is the last few years, anytime that assets needs to be managed more efficiently, at all time. The technology used for tracking can vary from RADAR, infrared (IR), ultrasonic (USS), Bluetooth® Low Energy (BLE), and Wi-Fi®.

Since Wi-Fi® is almost everywhere these days, it was only a matter of time until the existing 802.11 infrastructure would be leveraged to provide location and asset tracking services. This helps businesses save costs associated with deploying and managing fully dedicated RTLS systems.

In addition to cost savings, integrating Wi-Fi® directly into an RTLS tag eliminates the need to use a bridge to connect the tag to the Internet. An integrated design provides an all-in-one product that reduces overall Bill of Material (BOM) cost and enables applications to connect to the internet directly and securely.

This document discusses multiple use cases and the benefits of integrating Wi-Fi® in an RTLS tag design, as well as some of the key requirements for tags with Wi-Fi® connectivity. Specifically, this document describes how SimpleLink™ Wi-Fi® enables the development of battery powered RTLS tag design that can be tracked as well as be securely monitored and controlled from the cloud.

1.1 Abbreviations

Table 1 lists the abbreviations used throughout this document.

Table 1. Abbreviations

Abbreviations	Meaning
AP	Access Point
BLE	Bluetooth® Low Energy
IC	Integrated Chip
IOT	Internet Of Things
IR	Infra-Red
LF	Low Frequency
LPDS	Low-Power Deep Sleep
OSI	Open Systems Interconnection model
OTA	Over-the-Air
PLCP	Physical Layer Convergence Protocol (for Wi-Fi®)
RF	Radio Frequency
RFID	Radio Frequency Identification
RTLS	Real-Time Location System
US	Ultra-Sonic
Wi-Fi	Wireless-LAN

1.2 Terminology

The following terminology is used throughout this document:

- **RTLS:** Real-Time Location System is the actual solution that provides location details of an asset. It is not the actual technology used which can vary from radar, infrared, ultrasonic, BLE, and Wi-Fi®.
- **Authenticity:** Authenticity ensures that assets or entities are genuine and authorized to perform a task or used as intended. The verification process usually involves cryptographic algorithms, which check that the entities are who they claim to be. Some predefined trust mechanism is always part of an authentication scheme.
- **Certificates:** Certificates are standard-formatted files. They typically contain the public key of the subject, and a CA signature of the header and public key. Anyone provided with the CA public key (or sub-CA in case of certificate chain) can verify the subject's identity.

- **Confidentiality:** Confidentiality ensures that an asset is not made available or disclosed to unauthorized entities. In most cases, confidentiality translates into encryption, while in other cases, obfuscation techniques are used to maintain confidentiality.
- **Integrity:** Integrity is an attribute describing an object that remains intact, in its entirety, compared to its original version.

2 Assets Tracking Tags

2.1 Types of Tags

RFID tags can be divided into two families, passive tags and active tags. Passive tags do not include an internal power source and instead are powered by the electromagnetic energy transmitted from an RFID reader. Active tags use an internal power source and continuously transmit their signal.

2.1.1 Passive RFID Tags

Passive tags wait for a signal from an RFID reader. The reader keeps sending electromagnetic waves into the air. Once the tag enters the cover zone, the RFID tag's internal antenna draws in energy from the RF waves. The energy moves from the tag's antenna to the IC and powers the chip which generates a signal back to the RF system. The signal is then detected by the reader.

Passive RFID tags operate at several possible frequencies. There are three main frequencies within which passive RFID tags operate. Table 2 lists the frequency, range and the typical application.

Table 2. Passive RFID Summary

Frequency	Low Frequency (LF) (125 kHz, 134.2 kHz)	High Frequency (HF) (13.56 MHz)	Ultra-High Frequency (UHF) (868 MHz, 902-928 MHz, 950-960 MHz)
Range	An extremely long wavelength with usually a short read range of about 1 to 10 cm	A medium wavelength with a typical read range of up to 1 meter	A short, high-energy wavelength with a typical read range of about 5 to 6 meters
Typical Application	Animal tracking, pallet level tracking	Item / Case level tracking	Item / Case level tracking, pallet tracking

2.1.2 Active RFID Tags

Active RFID tags possess their own internal power source that enables them to have extremely long read ranges. Typically, active RFID tags are powered by a battery which lasts a few years depending on the use case. Hence, power consumption is one of the most important requirements that active tags vendors insist on.

Essentially, there are two different types of active RFID tags available:

- Transponders: like in passive systems, the active transponder needs to enter the cover zone to detect the signal coming from the reader and only then sends a signal back with the relevant information. Transponder tags are very efficient because they conserve battery life when the tag is out of range of the reader.
- Beacons: the active tag will 'beacon', or send out its specific information periodically regardless of its position. Active tag's beacons can be read from a long distance but consume more power than the transponders.

Active RFID tags operate at several possible frequencies. There are three main frequencies within which active RFID tags operate. Table 3 lists the frequency, range and the typical application.

Table 3. Active RFID Summary

Frequency	Proprietary / 802.15.4f (UHF) (433.92 MHz)	Bluetooth® Low Energy (BLE) (UHF, 2.4 GHz)	Wi-Fi® (UHF, 2.4 GHz, 5 GHz)
Range	Up to 400 meters	Up to 100 meters or up to 1.6 km	Local network range: 30 to 100 meters
Typical Application	Long range, high value item, harsh environments	Long range, low to medium value item, indoor and outdoor	Indoor RTLS, enterprise network based

2.2 RTLS Systems

The typical RTLS system includes several components:

- **The LAN infrastructure:** in most cases the infrastructure uses well known enterprise vendors like Cisco® and Aruba Networks® that already have designated modules and software that supports RTLS. Nevertheless, it is also possible to have a proprietary deployment. The infrastructure includes Access Points (AP), controllers and location engines as well as end-equipment that monitor, control and manage the tags.
- **Exciters:** an optional hardware component that assists in getting a more accurate location of the asset. Exciters are deployed in several locations across the building; usually in tightly-defined areas (for example, a gate, doorway) or in choke points. The exciters use low-frequency signals in technologies like Low Frequency (LF), Infra-Red (IR), Ultra Sonic (US) and others. A tag receiving signals from one or several exciters can either include the information in the periodic RTLS packet or send it over Wi-Fi® instantly.
- **Sensors:** mainly refers to those that can assist in improving the location accuracy. Some of the sensors include accelerometer, gyroscope, altimeter, magnetometer, and others. For example, an altimeter can assist in understanding at what height/shelf an asset is located in a warehouse.
- **Tags:** active tags that are battery powered and operate in various technologies. Tags usually do not need strong computing power and only collect samples and measurements and transmit it to the infrastructure where the actual location calculation takes place. Tags can also include other functionalities like an emergency button for immediate alert or non-telemetric sensors like temperature and humidity sensors if required by the assets.

Figure 1 illustrates an example for hospital environment.

The ordered process of locating an asset in the hospital is:

1. Typical enterprise infrastructure in hospitals and some RF exciters for location assistance.
2. Locating resources - a tag is attached to an equipment (monitor equipment in this case) or a personnel (surgeon, nurse) that needs to be located at all time, within the hospital.
3. The tag may also be equipped with optional telemetry sensors for location assistance.
4. The tag receives a signal from exciters (along with their ID and signal strength) and either includes the information in the periodic RTLS packet or send it over Wi-Fi® instantly.
5. The tag periodically sends an RTLS packet which may include sensors samples, exciters samples and some proprietary payload.
6. The location engine in the infrastructure gets all the measurements, interpolates and estimates the tag location.
7. The operator can monitor, control and manage the tags.

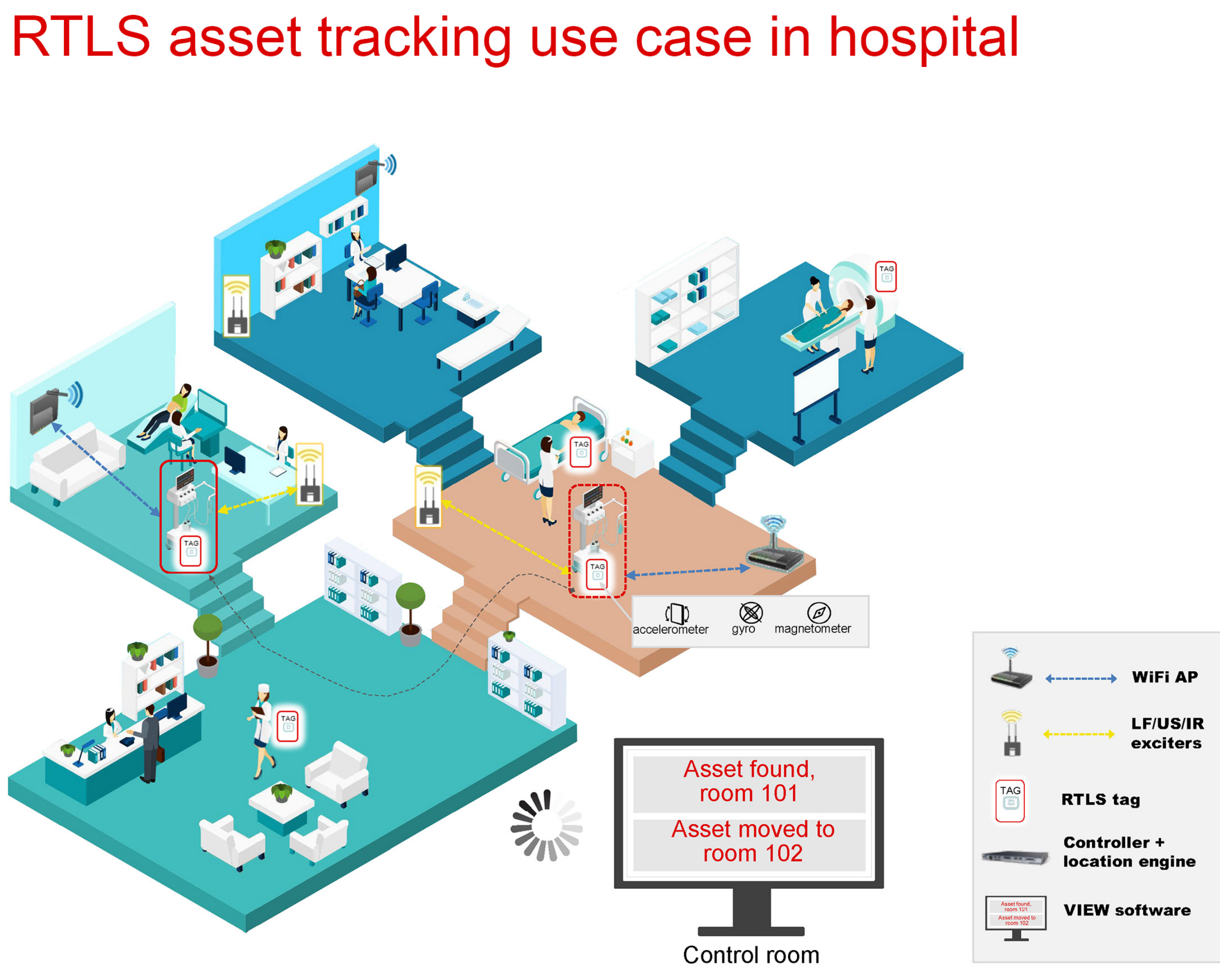


Figure 1. RTLS Asset Tracking Use Case In Hospital

Figure 1 shows a monitor equipment that is moved between rooms. The monitor equipment receives a signal from exciters in the surrounding rooms and also sample its sensors. The monitor equipment includes the sensors samples and the exciters readings in an RTLS packet and either sends the packet periodically or instantly. The location engine in the infrastructure gets the measurements, interpolates and estimates the location or the monitor equipment.

2.3 Key Requirements

An active Wi-Fi® tag that communicates with an enterprise infrastructure should follow the listed system requirements.

- **Low power consumption:** The power consumption is the most important factor for an active tag since it is powered with batteries and should last for several years. This is challenging because an active Wi-Fi® tag has several working modes, connected and non-connected, interacting with several radio technologies and peripherals. To save as much power as possible, all procedures also need to be short in time.
- **Non-connected, radio layer access:** For localization purposes, the Wi-Fi® tag communicates while not connected to the enterprise infrastructure. Thus, an access to the radio layer is mandatory. The user must have the option to set the working channel frequency, the output transmit power and the payload.
- **Wi-Fi Enterprise compatibility:** There are other purposes other than localization that are also expected from the tag. The tag should be able to trigger an immediate alert, send periodic reports, support scheduled upgrades and enable remote management and control. These tasks require connection via the enterprise infrastructure.
- **Fast secured transport connection:** All the procedures like triggering an immediate alert, sending periodic reports, supporting scheduled upgrades and enabling remote management and control, requires higher level support. The tag should connect to a server or a peer device fast and securely.
- **Over-the-Air (OTA) capabilities:** The tag must also have the option to get upgraded once in a while when new software is available. The update procedure should be secured and fail-safe, while keeping the integrity of the system and enabling rollback in case of error.
- **Integrated telemetric sensors for location assistance:** Location accuracy can be further improved by integrating telemetric sensors such as accelerometer, gyroscope, altimeter, magnetometer, and others.
- **Other radio technologies for location assistance:** Location accuracy can be further improved by integrating exciters using other radio technologies like Low Frequency (LF), Infra-Red (IR), Ultra Sonic (US) and others.

2.4 Location Accuracy

In general, location tracking systems can be classified according to the measurement techniques employed to better sense and measure the position of an RTLS asset. These techniques may include one or combination of distance estimation (lateration), angle estimation (angulation), and pattern recognition. Other factors that improve tracking and positioning of an asset include sensors and exciters. As described earlier in the document, adding such integrated components to the RTLS tag and transmitting the samples to the main infrastructure may further improve the location accuracy.

To get a good impression of the accuracy performance, Cisco® LBS solution can be taken as an example. It is important to understand that location accuracy should also include an indication of the percentage probability of successful location detection, otherwise, there is no real value if the level of accuracy is not consistence. Cisco® LBS solution reaches an accuracy of less than or equal to 10 meters, with 90 percent precision and less than or equal to 5 meters, with 50 percent precision. These numbers do not take into account any of the additional integrated components that can further improve precision but only the Wi-Fi® related algorithm.

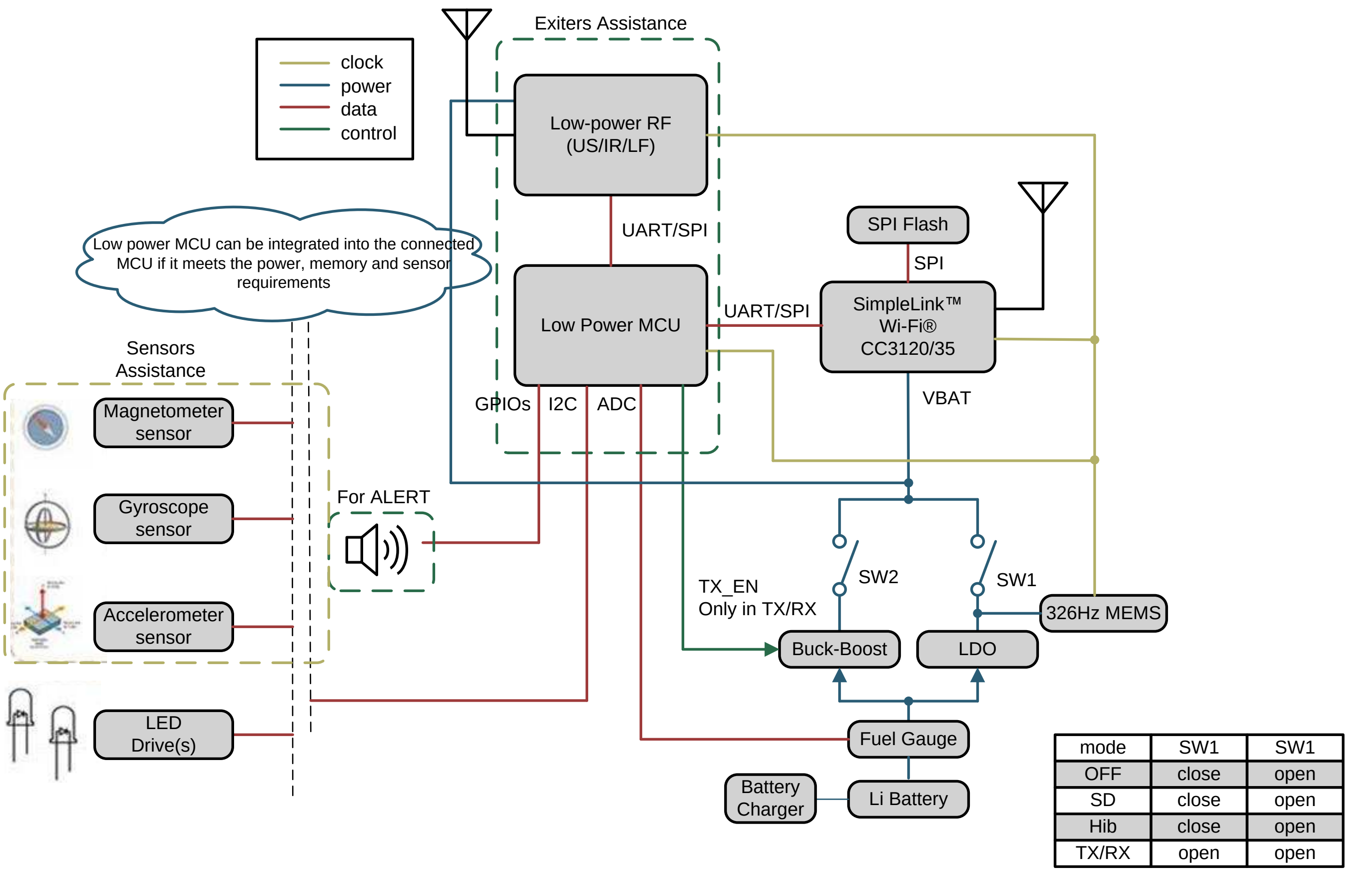
To summarize, the level of accuracy depends on many techniques and algorithms deployed by the infrastructure and not solely on Wi-Fi®. Therefore, location accuracy is not covered in this document.

2.5 Block Diagram

Figure 2 shows a typical block diagram for an active Wi-Fi® tag.

- **Low Power MCU:** This is the host controller and is responsible for processing inputs from the user, sensors, and the low-power RF. The host controller periodically triggers sending an RTLS message to the infrastructure, triggers immediate connection when manually alerted from a GPIO or unsolicited event from the exciters or executes a scheduled OTA.

- **SimpleLink™ Wi-Fi® CC3120 Device:** This block provides the wireless connectivity to the outside infrastructure. The various tasks include sending RTLS packets for location purposes, triggering alerts or emergency events, remote control and monitoring of the tag and wireless transfer of software updates.
- **Power subsystem:** This subsystem is responsible to get the best battery life achieved by the system for all use cases. For achieving optimal power performance, a designer must choose the right components and configure the system accordingly.
- **Low-power RF:** Various other radio technologies like Low Frequency (LF), Infra-Red (IR), Ultra Sonic (US) may be used to assist in improving the location accuracy. A tag receiving signals from one or several exciters can either include the information in the periodic RTLS packet or send it over Wi-Fi® instantly.
- **Sensors:** Various sensors can be used in a Wi-Fi® tag and assist in improving the location accuracy. Some of the sensors include accelerometer, gyroscope, altimeter, magnetometer, and others. Other sensors such as a temperature and humidity sensors can also be used for other specific purposes (not location related).



mode	SW1	SW1
OFF	close	open
SD	close	open
Hib	close	open
TX/RX	open	open

Figure 2. Wi-Fi® Tag Block Diagram

There are two kinds of data that can be triggered by the low-power MCU: RTLS data that is triggered in non-connected mode, and non-RTLS data that is triggered in connected mode. Figure 3 shows a typical block diagram that illustrates the data flow.

As illustrated, sending RTLS data (which usually is triggered periodically) is directly applied over the Radio layer. This means that the low power MCU is responsible to build the payload and send it to the NWP, which encapsulate it over the Wi-Fi® physical layer.

Sending a non-RTLS data is sent over a socket, which means that the internal network stack is used and the packet is built while moving in all layer of the NWP.

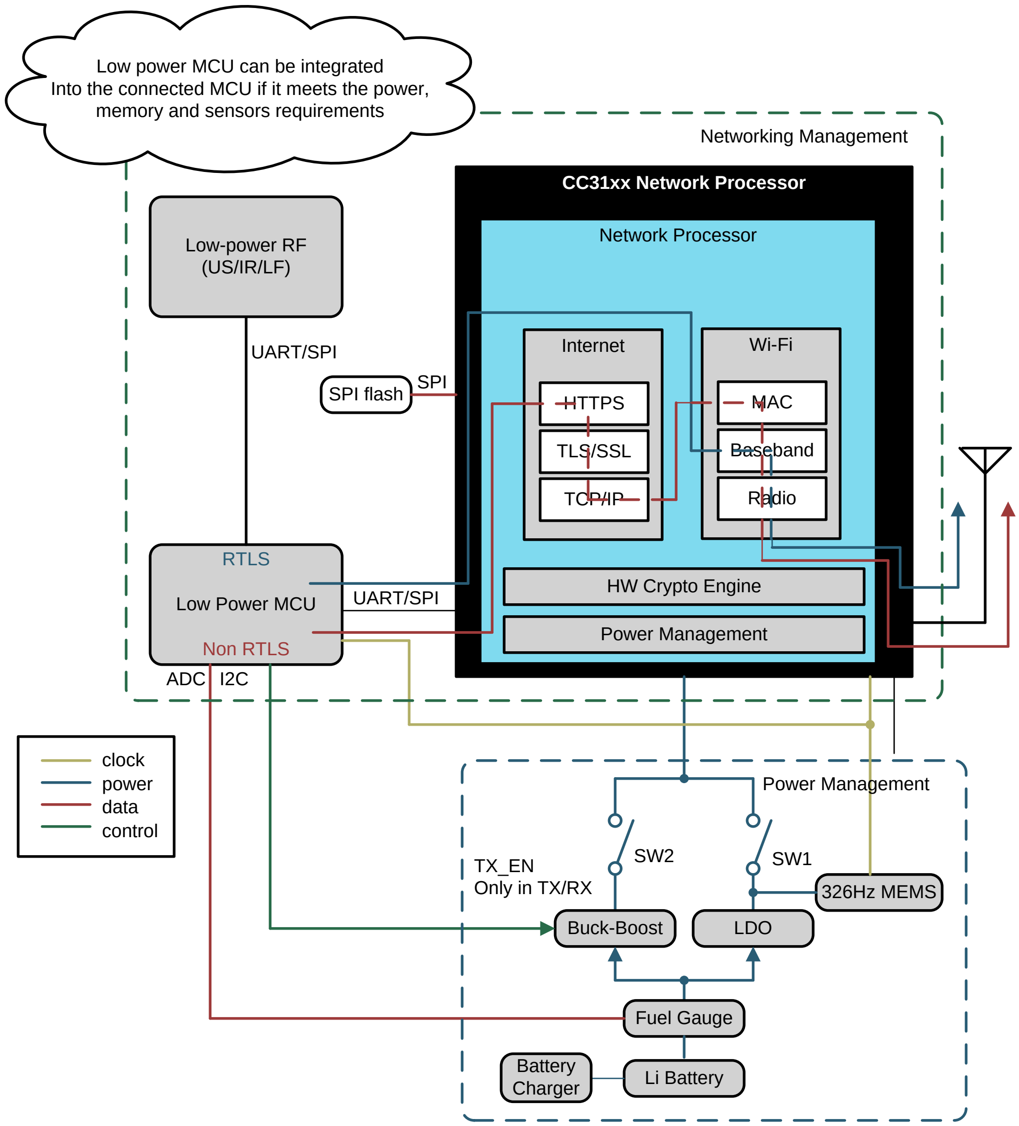


Figure 3. Data Flow in Wi-Fi® Tag Block Diagram

3 Wi-Fi® Use Cases and Benefits

Integrating Wi-Fi® into an active RFID tag makes it possible to:

- Know where your asset is within the controlled area
- Know when the asset crosses a predefined boundary
- Get an alert when a button is pressed manually
- Perform an OTA update

3.1 Know Where Your Asset Is

Knowing where the asset is, staff or equipment, has major implications on many applications. In terms of operations and workflow, manufacturing vendors can track the work-in-process inventory as it moves through the production process. This provides real-time view of which and how many items have progressed through the production line. In a hospital environment for example, knowing the location and status of clinical staff, patients, beds, and critical clinical equipment is essential to improving patient care and departmental workflow. Additionally, real-time inventory management becomes automated and efficient with no need for manual scanning.

3.2 Know When the Asset Crosses a Boundary

Knowing when the asset crosses a boundary has many advantages that directly translates into cost savings. The main applications relate to security and safety.

- In terms of safety, an immediate alert is triggered when the asset enters a hazardous area. In hospital environment for example, patient elopement of at-risk patients will trigger an alert.
- In terms of security, the system can alert when trying to steal equipment, especially an expensive one.

3.3 Get a Manual Alert

Tags can also include a push button to manually alert when needed. The main application relates to safety. In hospital environment for example, distress call of elderly patients, wearing tags with call buttons can trigger panic or distress alerts. Also, staff members carry call-button tags, which can be triggered to alert other staff upon encountering an emergency or in duress situations.

3.4 Perform Over-the-Air (OTA) Updates

It is necessary to have a method for updating the system files and software. Examples of files that must be replaced over time are device certificates and keys that are used to identify and establish secure connections. Software updates may also be required to enable new features, fix existing issues, or address security flaws. Implementing a wireless update mechanism, known as an over-the-air (OTA) update, provides a simple way to keep the system up-to-date.

4 Wi-Fi®Connectivity and Power Use Cases

There are many distinct ways that Wi-Fi® connectivity can be used in RTLS tags. The number of features enabled and the power budget required depends on how the Wi-Fi® connectivity is used. The most common Wi-Fi® connectivity use cases are:

- Wi-Fi® scheduled wake-up for location updates
- Wi-Fi® scheduled wake-up for periodic updates
- Wi-Fi® wake-up on sensor or exciter event

The first use case is when the Wi-Fi® is turned on periodically to send location updates to the server. The RTLS data does not require a Wi-Fi® connection to an AP but instead only using the Wi-Fi® radio layer. This mode is known as transceiver mode and described as detailed in Section 5.1.2. The RTLS data is usually short in length and transmitted on a few Wi-Fi® channels. The Wi-Fi® infrastructure is capable of detecting the RTLS transmissions, decoding those and send it to the service engine for further processing.

Another use case is when the Wi-Fi® is turned on only for periodic updates. A wake-up that is scheduled to occur periodically can be used to turn on the Wi-Fi® and check for an update such as delivering new software in the form of OTA updates. The device can also wake up periodically and send status report to the server. The last use case is when the Wi-Fi® is triggered to wake up on a sensor or exciter event (such as a button press, or another low frequency exciter). A triggered wakeup can be useful to optimize power consumption while also enabling the system to respond to a user. When a user pushes an alert button or enters an exciter's cover zone that implements this scheme for Wi-Fi® activity, it can securely connect to the server and send a push notification.

Following the last two use cases, it is clear that the Wi-Fi® solution must have a short wakeup and connection cycle to provide the best user experience and lowest power consumption. SimpleLink™ Wi-Fi® has multiple built-in mechanisms to optimize wakeup and connection times including Fast Connect, Fast DHCP Renew, and hardware acceleration of TLS/SSL handshakes. When used together, SimpleLink™ Wi-Fi® can wake up from hibernate or shutdown mode, establish a WPA2 secured connection to an AP, and create a TLS/SSL connection to a server in approximately 0.5 seconds.

5 TI Offering

5.1 Radio Layer Access

5.1.1 Open Systems Interconnection (OSI) Layer Model

The OSI model characterizes and standardizes the communication functions without regard to its underlying internal structure or technology. The model is partitioned into seven abstraction layers. Each layer serves the layer above it and is served by the layer below it. Two connected peer devices communicate with each other such that each layer on one device communicates with its parallel layer on the other device.

Every communication technology can be represented by the OSI layer model. Wi-Fi® technology is for local area network (LAN) and as such, covers the first two layers. Figure 4 illustrates Wi-Fi® technology in OSI layer model.

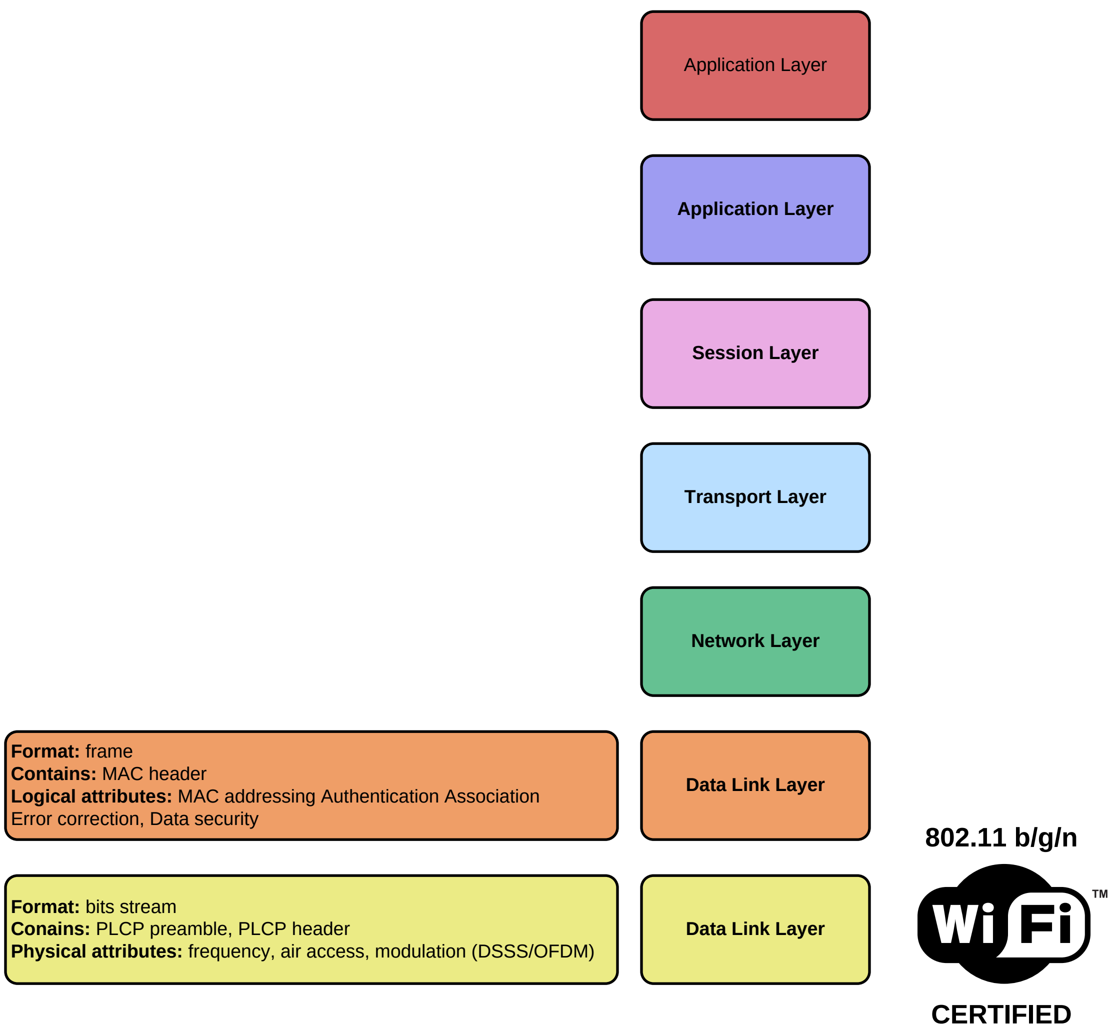


Figure 4. OSI Layer Model in Wi-Fi®

5.1.2 Transceiver Mode

Transceiver mode is a special mode where most of the communication layers of the OSI model are bypassed and direct access to the radio layer is provided. Figure 4 details what the physical layer and the data link layer contain and what attributes these layers fulfill.

When working in transceiver mode, the host application opens a socket directly on top of the radio layer. The user should configure the Wi-Fi® channel, the back off from maximal power, the Wi-Fi® rate (which implies the modulation) and the payload data.

Since the Wi-Fi® radio layer is used, it means that any implementation or protocol must be based on standardized Wi-Fi®. Standardized Wi-Fi® defines the radio frequency of each channel, the channel bandwidth, the maximum transmit power and the modulation. Additionally, the PLCP preamble and header precedes any transmission and cannot be altered. This means that the Radio layer is not fully configurable and any standardized or proprietary implementation should take into account that the Radio layer is based on standardized Wi-Fi®.

Tag vendors that are working in an enterprise security network (for example, Cisco, Aruba, and others), do not connect to the AP but only transmit the packets over Wi-Fi® radio. The infrastructure, which is equipped with RTLS extensions, is able to decode these packets according to the MAC address and direct it to a location engine service for further processing.

5.2 Low-Power Architecture

5.2.1 Power Modes

Typical tag use case includes transmission of short packets on several channels and then returns to low power mode. There are three different low-power modes available in the SimpleLink™ device, LPDS, Hibernate, and Shutdown. Choosing which low-power mode is best depends on the use case and more importantly on the cycle period. The longer the cycle period is, the better it would be to use a power mode that consumes less current on the average.

In addition to the power consumption, it is also important how fast the device wakes up to transmit. A combination of fast wakeup and low power consumption is desired. The lower the power mode consumes, the longer the wake-up time gets.

According to this logic, shutdown mode consumes the least amount of power but takes longer to wake up, versus Hibernate and LPDS In shutdown mode, it takes over 1 second to wake up the device due to the long stabilization time of the internal slow clock. To accelerate the wake-up time of shutdown mode to almost that of hibernate mode, an external slow clock oscillator (RTC) can be used.

Table 4 lists the various powers modes parameters for SimpleLink™ Wi-Fi® CC3120 device.

Table 4. CC3120 Power Modes Measurements

Power Mode	Wake-up Time (ms)	LPDS (µA)	Hibernate (µA)	Shutdown (µA)
LPDS	0	115		
Hibernate	60		4.5	
Shutdown – internal slow clock	1160			1
Shutdown – external slow clock	80			1

5.2.2 Typical Power Profiles Use Cases

5.2.2.1 RTLS Only

5.2.2.1.1 Wake-up From LPDS

The setup configuration includes:

- Power up from LPDS
- Transmit one packet on channels #1, #6, #11
- Packet is 100 bytes
- 6 Mbps OFDM
- Transmit at maximum power. For 6 Mbps OFDM, the typical value is 17.3dBm.

The measured charge per TAG cycle is 540 [uC], which is 150 [µAh], measured with 3.3V power supply and including the serial flash power.

Figure 5 illustrates the current over time chart for this LPDS profile.

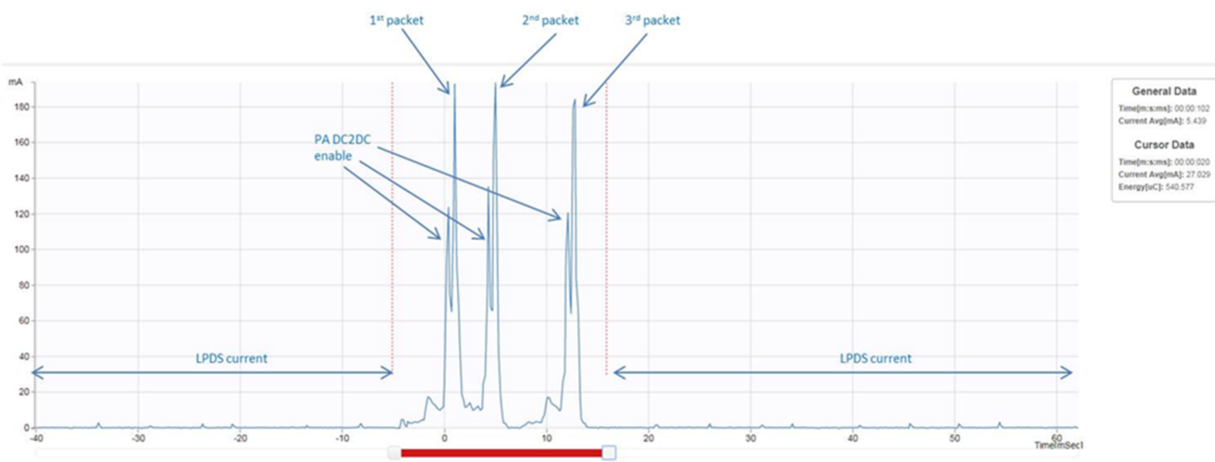


Figure 5. Current Over Time Profile Chart - LPDS

5.2.2.1.2 Wake-up From Hibernate

The setup configuration includes:

- Power up from hibernate
- Transmit one packet on channels #1, #6, #11
- Packet is 100 bytes
- 6 Mbps OFDM
- Transmit at maximum power

The measured charge per TAG cycle is 2170 [uC], which is 603 [µAh], measured with 3.3V power supply and including the serial flash power.

Figure 6 illustrates the current over time chart for this LPDS profile.

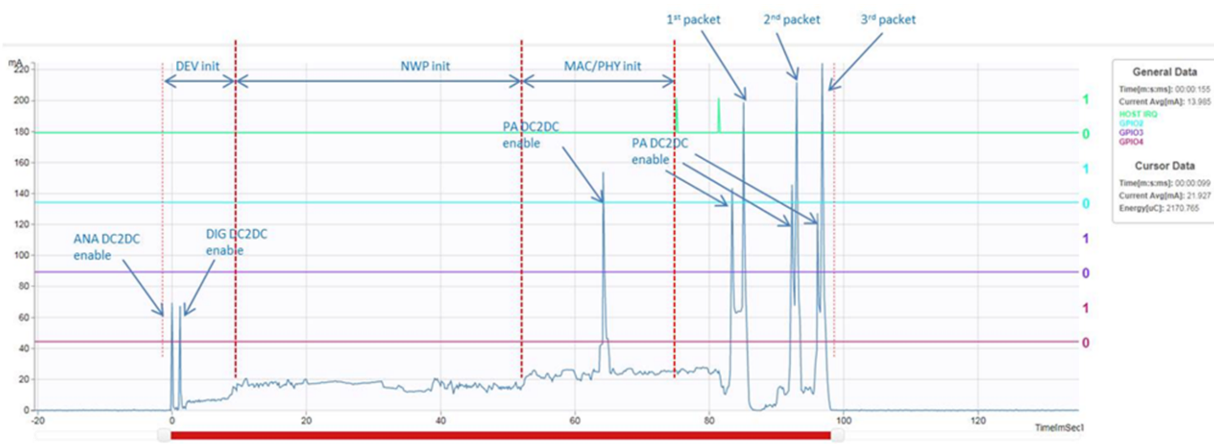


Figure 6. Current Over Time Profile Chart - Hibernate

5.2.2.1.3 Wake-up From Shutdown – Internal Slow Clock

The setup configuration includes:

- Power up from shutdown, internal slow clock
- Transmit one packet on channels #1, #6, #11
- Packet is 100 bytes
- 6 Mbps OFDM
- Transmit at maximum power

The measured charge per TAG cycle is 2556 [uC], which is 710 [µAh], measured with 3.3V power supply and including the serial flash power.

Figure 7 illustrates the current over time chart for this LPDS profile.

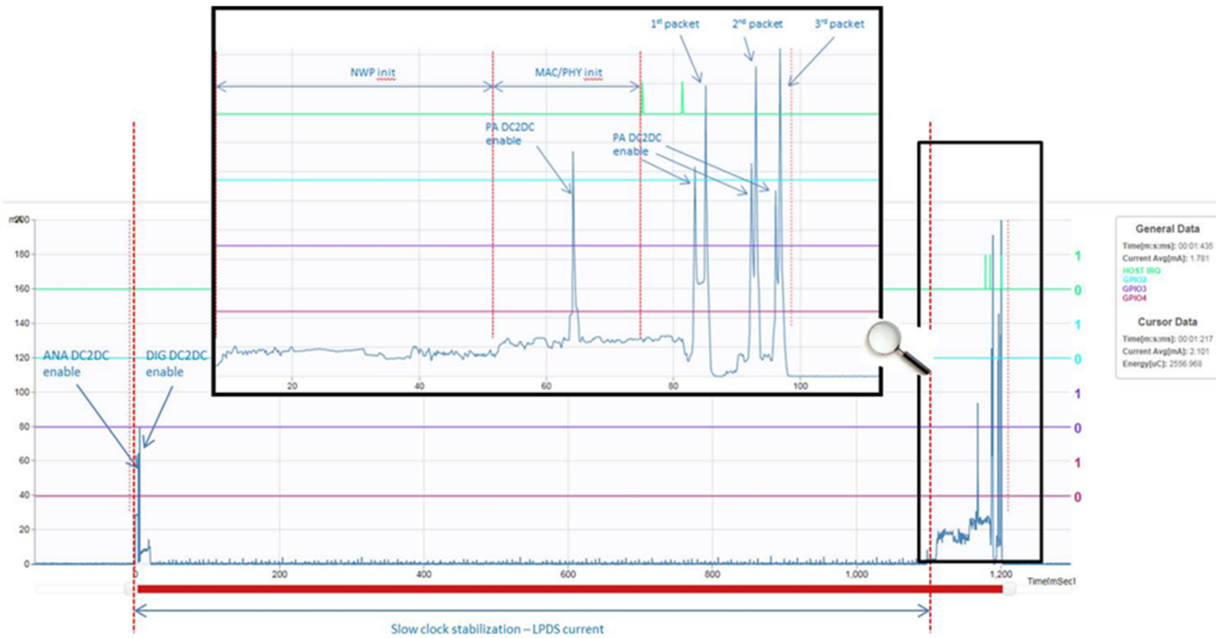


Figure 7. Current Over Time Profile Chart - Shutdown With Internal Clock

5.2.2.1.4 Wake-up From Shutdown – External Slow Clock

The setup configuration includes:

- Power up from shutdown, external slow clock
- Transmit one packet on channels #1, #6, #11
- Packet is 100 bytes
- 6 Mbps OFDM
- Transmit at maximum power

The measured charge per TAG cycle is 2370 [uC], which is 658 [µAh], measured with 3.3V power supply and including the serial flash power.

Figure 8 illustrates the current over time chart for this LPDS profile.

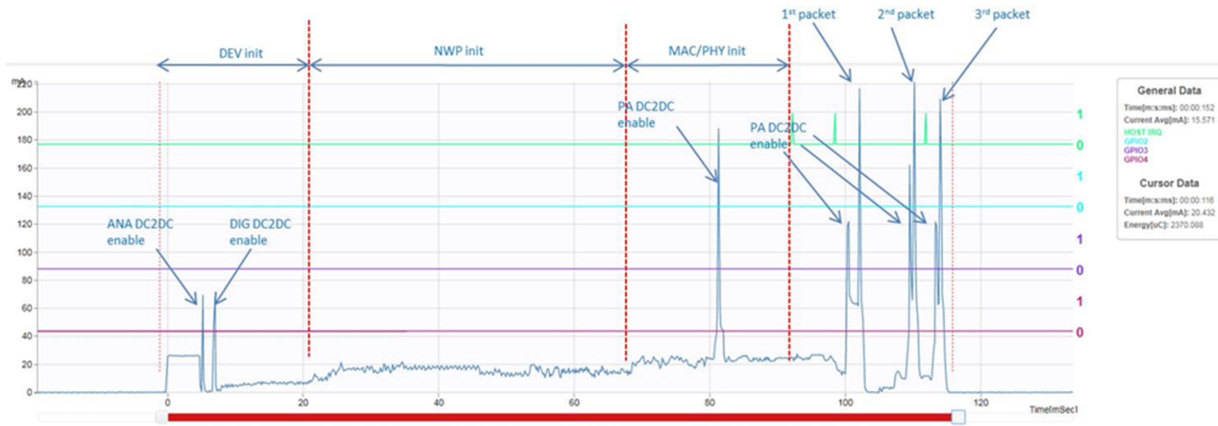


Figure 8. Current Over Time Profile Chart - Shutdown With External Clock

5.2.2.1.5 Preferred Power Mode

Choosing the preferred mode is mainly done according to the estimated battery life. The longer the battery life is, the better is the power mode. Nevertheless, most likely the device had other tasks to perform that involve Wi-Fi® connectivity and not RTLS only. Users should take all factors into account when calculating the aggregated power budget.

Looking from the RTLS use case only, and taking into account the suggested profile of transmitting one 100 bytes packet on channels #1, #6, #11 in 6 OFDM modulation and maximal power, it is possible to calculate the preferred power mode over time. Note that the calculated crossing point is highly dependent on the configured profile.

Figure 9 illustrates the average current versus the cycle time for LPDS, hibernate, and shutdown with internal slow clock (for external, extra power of the slow clock should be considered but this is part number dependent). It is observed that the crossing point for moving between LPDS power mode and hibernate/shutdown is approximately 15 seconds. This makes sense as the power consumed during full initialization takes more effect if the cycle time is short.

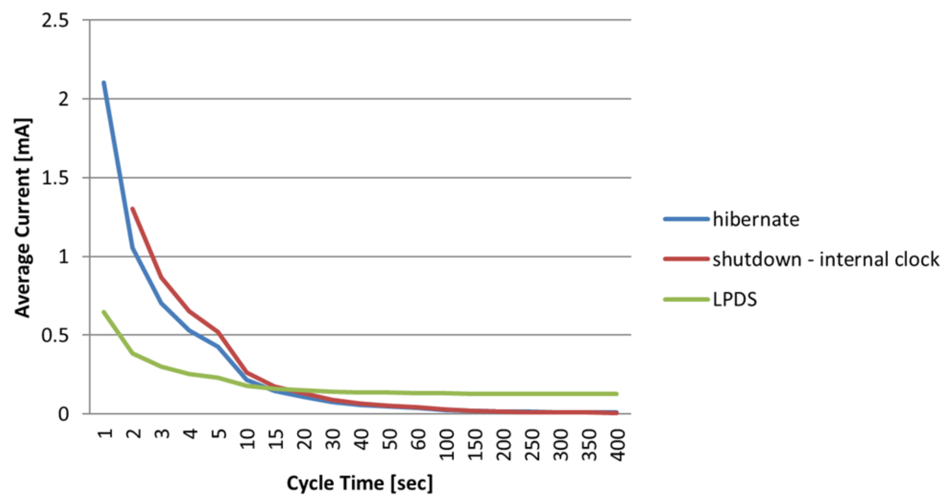


Figure 9. Average Current vs. Cycle Time - Zoom Out

Figure 10 zooms in on the average current versus the cycle time for hibernate and shutdown only.

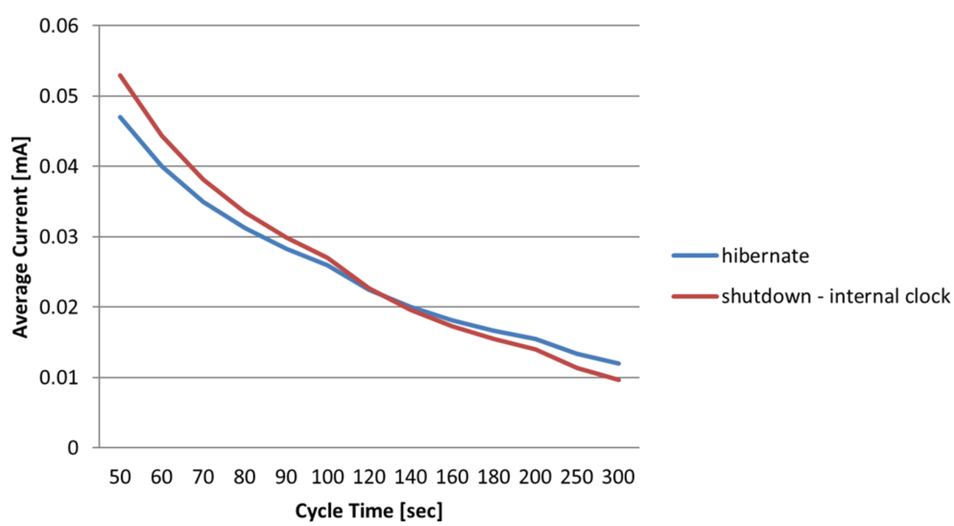


Figure 10. Average Current vs. Cycle Time - Zoom In

5.2.2.2 Intermittently Connected

As described in Section 4, a Wi-Fi® enabled tag could be designed to only turn on the Wi-Fi® interface when it must transmit data to or receive data from a remote server. The Wi-Fi® interface could be turned on either based on a scheduled wakeup or from a sensor or exciter trigger. In this case, the system will be intermittently connected to the local network and server. It is assumed for the intermittently connected use case that the system will remain in hibernate or shutdown mode when it is not connected to the network. In hibernate or shutdown mode, the application processor and the network subsystem memory is not retained. The following steps are required for each wake-up cycle before sending data:

1. Initialize the system (load the network processor).
2. Reconnect to the local network.
3. Establish a secure socket session.
4. Transmit and receive data.
5. Return to hibernate or shutdown.

5.3 RTLS Tag Security

Because RTLS tags are personal ID cards attached to assets or people, they must be designed with security in mind. RTLS tags must address the following security challenges:

- **Connecting to the local infrastructure securely:** The infrastructure environment used with RTLS tags is of enterprise type. It means that on top of the personal WPA2 Wi-Fi® security, additional level of security is required. The Enterprise infrastructure includes Radius servers that authenticate the clients. The enterprise connection can require up to three files to complete the process, depending whether client authentication is required in addition to server authentication.
- **Connecting to a remote server securely:** The RTLS tag is rendered compromised if connection to a remote server is not secured and authenticated. RTLS tags should be protected against malicious attacks when connecting and transferring data with servers on the network.
- **Protecting against malicious or invalid OTA updates:** The RTLS tag is rendered useless if it becomes locked out by having its software changed by an attacker or by performing an update to a new version with a bug. Ensure the RTLS tag operates when needed by protecting the system integrity through guarding against malicious or invalid updates. Providing a way to roll back to the last valid image in case of corruption is also mandatory.
- **Securing end-user private data:** End-user data must be secured during transfer over the Wi-Fi® interface, transfer through the internet, and any time it is stored in non-volatile memory on the RTLS tag.
- **Protecting intellectual property (IP):** It is important to protect the confidentiality of the intellectual property (IP) on the system, such as the RTLS tag software. Keeping the IP protected helps ensure that attackers are unable to copy the design or learn how the system works in order to exploit potential flaws.

5.3.1 Wi-Fi® Security – Enterprise

Wi-Fi® security refers to security on the local area network. The SimpleLink™ Wi-Fi® device supports Wi-Fi® enterprise connection according to 802.1x authentication process. Enterprise connection requires an authentication of the STA by the radius server behind the AP. The SimpleLink™ Wi-Fi® device includes a rich set of authentication methods to choose from. The user can connect to the enterprise network through a manual connection or through a dedicated profile on the file system. Enterprise configuration also requires up to three files to complete the process, depending whether client authentication is required in addition to server authentication. These files can be securely stored on the SimpleLink™ Wi-Fi® device file system.

5.3.2 Secured Internet Connection – TLS/SSL

Secured internet connection refers to security on the public network. A key step in protecting data that is transferred through the internet is using secure sockets (TLS/SSL). Use of a secure socket makes it possible for both the server and the client to verify identity and negotiate a cryptographic protocol to use for securing the transferred data.

The CC3120 device supports up to six simultaneous secure sockets out of the 16 total sockets that are available. The SimpleLink™ Wi-Fi® device includes a rich set of cipher suits that can be used and negotiated with the server during connection.

When it comes to design, the SimpleLink™ Wi-Fi® device is unique in the following aspects:

- For common systems, the SSL is a layer on top of the transport layer. To simplify the use, the TLS/SSL is embedded into the BSD layer in the SimpleLink™ Wi-Fi® device. TLS/SSL operations are easily done by using the BSD commands with unique parameters and options.
- Hardware accelerators are also used to offload the main MCU in arithmetic calculation of cryptography algorithms.
- To verify and validate the peer device, the SimpleLink™ Wi-Fi® device uses a trusted root-certificate catalog. The trusted root-certificate catalog is a file containing a list of known and trusted root CAs, as well as a list of revoked certificates. The trusted root-certificate catalog gives the user the confidence that the CA is trusted and known by TI. This file gets updated periodically through the OTA update procedure and is available in the SDK - .

5.3.3 User Data and Code Protection

User data and code protection refer to security on the local device file system. Securely storing private user files as well as the user IP is a top priority in the IOT world. Secure storage helps protect against both direct and indirect attempts to read nonvolatile memory.

The SimpleLink™ Wi-Fi® device uses an external nonvolatile memory in the form of a serial flash. The content stored on the serial flash is organized by the network processor into a file system. Many features are built into the file system that can be used to:

- Encrypt data: use onboard crypto hardware to keep data confidential.
- The authenticity is validated every write: the certificate chain is validated against a trusted root-certificate catalog in ROM.
- Check data integrity: apply a signature to the file when changed and verify the content when opened for read.
- Control access to data: use file tokens to set access permissions.
- Alert the system about tampering: detect invalid and potentially malicious attempts to access to files.

6 Summary and Conclusions

Wi-Fi® connectivity provides key benefits over other RF technologies in RTLS tags by leveraging an existing 802.11 infrastructure and providing a direct method to remotely monitor, manage and control the tag. Wi-Fi® also improves the user experience by enabling automatic delivery of software updates. The SimpleLink™ Wi-Fi® CC3120 Network Processor makes it possible to integrate Wi-Fi® connectivity directly into the tag design without compromising battery life. SimpleLink™ Wi-Fi® also provides the key security features and the high level of interoperability necessary for a robust tag design.

7 References and Related Documentation

Product Pages on TI.com

[1] Asset tracking application for SimpleLink™ Wi-Fi®, http://www.ti.com/wireless-connectivity/simplelink-solutions/wi-fi/applications.html

[2] RTLS asset tracking with SimpleLink™ Wi-Fi® devices: Enabling smart management inventory

[3] SimpleLink™ Wi-Fi® CC3120 SDK Plugin

User's Guides

[4] CC3120, CC3220, SimpleLink™ Wi-Fi® and Internet of Things Network Processor Programmer's Guide

Application Reports

[5] SimpleLink™ CC3120, CC3220 Wi-Fi® Internet-on-a chip™ Solution Built-In Security Features Application Report