



# The Latest in HADM using Bluetooth LE



# Agenda

- 01** Target Markets and Applications
- 02** Demand for HADM – Beyond RSSI
- 03** HADM & Channel Sounding
- 04** Performance Results
- 05** Early Access & Sample Applications
- 06** Next Steps

---

# High Accuracy Distance Measurement (HADDM) Applications

# Target Markets & Applications



HOME

**Item Finding**  
**Keyless Entry**  
**Pet Tracking**



COMMERCIAL

**Access Control**  
**Inventory management**  
**Asset Tracking**



# Demand for Improved Distance Measurement – Beyond RSSI



## Accuracy & Reliability

RSSI is sensitive to indoor multipath environment



## Simplicity

Enable design of low-cost devices  
Single antenna design  
Reduce system resources



## Security

Attacker manipulation of RSSI via RF signal amplification



## Interoperability

Standards Based Feature

# HADM & Channel Sounding

## LOCATION SERVICES

### Drivers for Tomorrow

#### Bluetooth® high-accuracy distance measurement will set a new bar for performance of location services solutions

Bluetooth® technology will soon add high-accuracy distance measurement (HADM), enabling item finding solutions to provide greater precision as users get closer to an item being located, allowing passive keyless entry solutions to add another layer of authentication and accuracy, and improving the performance of real-time locating systems.

**260**  
MILLION

Bluetooth® asset tracking devices  
will ship in 2027

**338**  
THOUSAND

Bluetooth® RTLS implementations  
by 2027



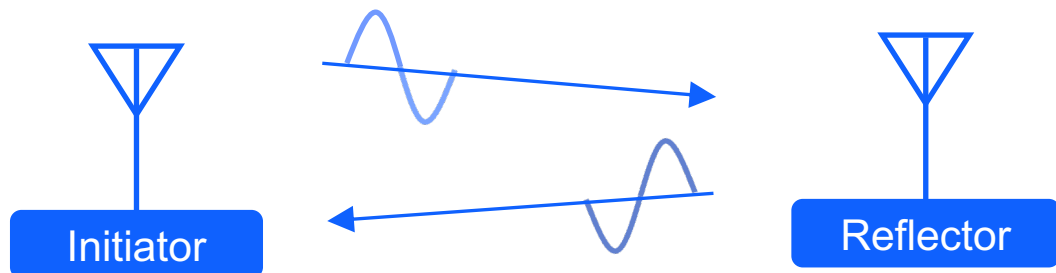
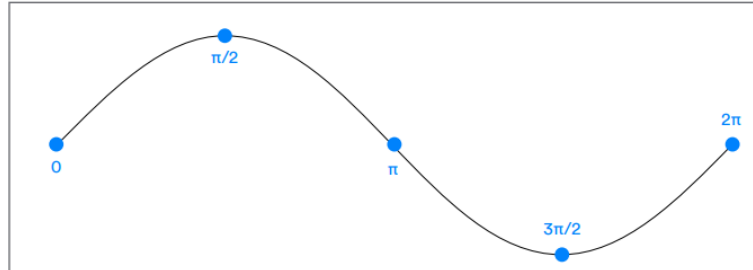
#### Channel Sounding (CS) is the Bluetooth feature that enables HADM.

- CS is currently being defined by the Bluetooth SIG
- Draft Specifications publicly available at <https://www.bluetooth.com/specifications/specs/channel-sounding/>
- Defines support for phase based ranging (PBR) tone exchange and/or round trip timing (RTT) packet exchange
- Also defines procedures, events, sub-events etc to enable distance estimation

# Phase Based Ranging (PBR)

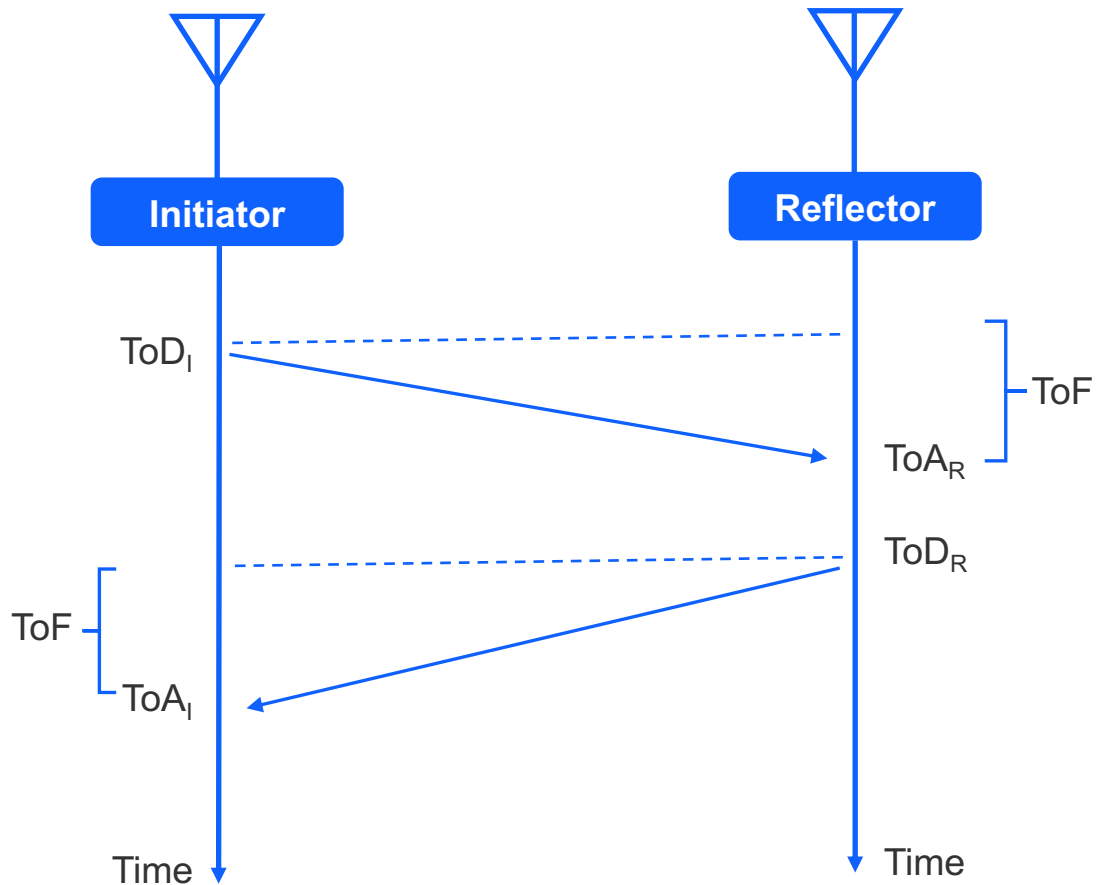
## Phase

A specific point in a wave cycle, perhaps measured as the wave passes over an antenna, is known as its *phase*. Phase is measured as an angle from 0 at the start of the wave cycle to 360 degrees or  $2\pi$  radians at the end of the wave cycle. Figure 8 illustrates the concept of phase.



- **Tone exchange between two devices**
- **Phase of RF signals is a function of frequency of the carrier and the distance traveled**
  - Phase rotation due to spatial propagation determined
  - Measurements at multiple RF frequencies to resolve distance ambiguity
- **Distance is calculated using the phase difference between transmitted and received signal**
- **Security**
  - Manipulation of phase is more complex than RSSI
  - IQ sample quality
- **Much more accurate than RSSI**
- **Key Considerations**
  - Antenna radiation patterns
  - Board design specific calibration

# Round Trip Timing (RTT)

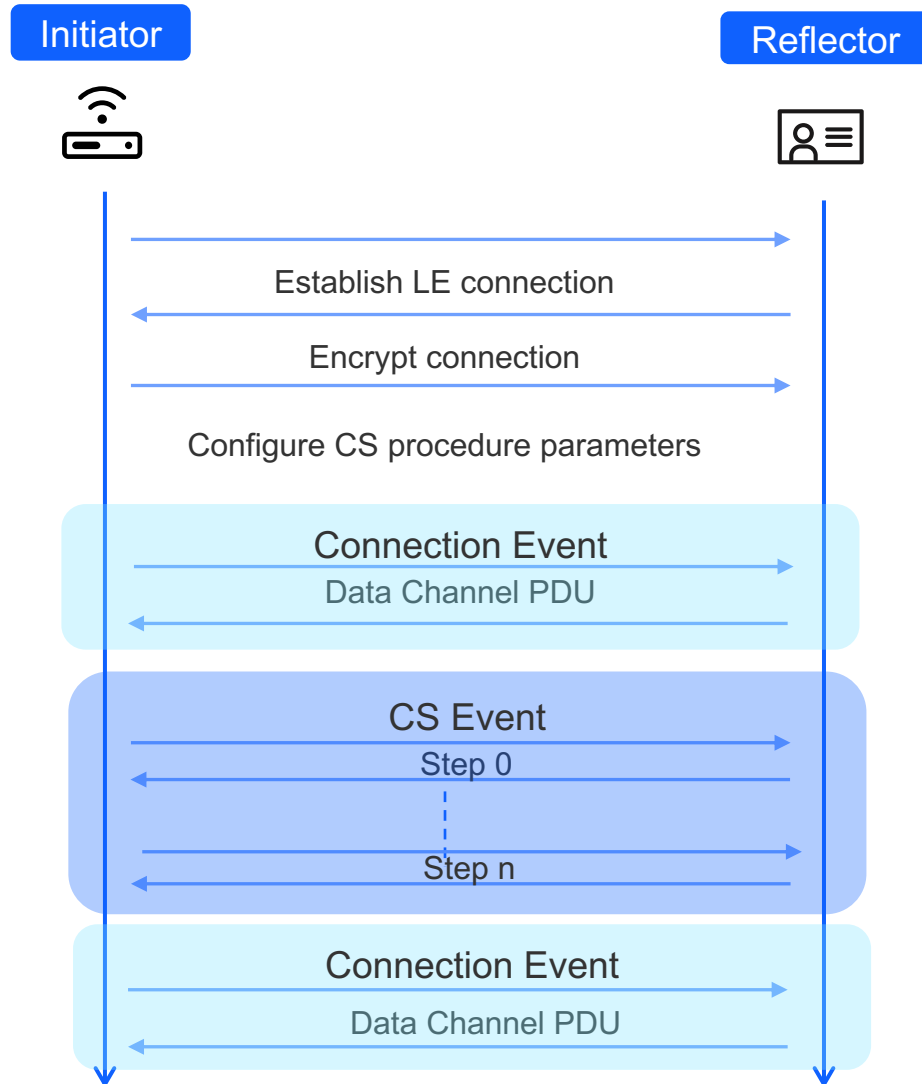


$$RTT = 2 ToF = (ToA_I - ToD_I) - (ToD_R - ToA_R)$$

- **Packet transmission time (ToF) is measured on both initiator and reflector side using Time-of-Arrival (ToA) and Time-of-Departure (ToD)**
  - Modulated packets exchanged over multiple channels to determine ToF and estimate distance
  - Fractional timing techniques used to resolve sampling uncertainty and improve resolution
- **Time cannot be reversed -> RTT increases security**
- **Less accurate than PBR**



# Measurement Procedure Explained



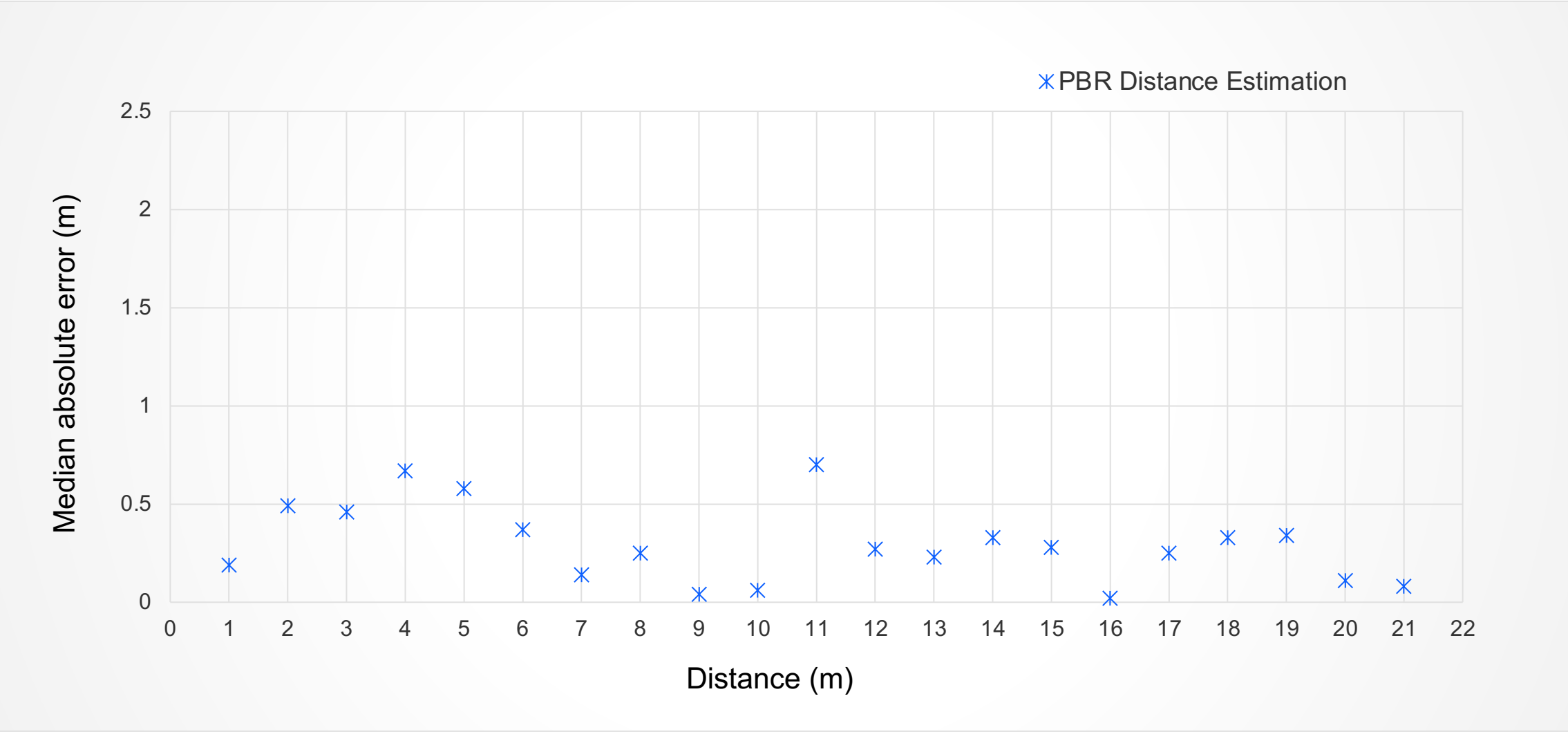
- **Connection-based 2-way ranging with encrypted Bluetooth LE connection events and secure CS events**
  - Reflector sends received signal info via GATT indications during connection events
- **Interchangeable device roles (central, peripheral) and CS roles (initiator, reflector)**
- **Initiator configures CS procedure parameters**
  - Number of channels, channel map(randomized), TX power
  - Allowed duration of connection interval, CS event
  - Measurement modes – RSSI, PBR, RTT
  - Trade-offs between accuracy, duration, and power
- **CS Event**
  - Calibration – frequency offset
  - Modulated packets or tones exchanged over multiple channels
  - Channel mapping is randomized to prevent attackers
- **Distance Estimation**
  - Initiator parses the measured data - IQ samples, time
  - Signal processing – averaging, filtering outliers, detecting multipath, etc.

# Performance in Indoor Office Environment



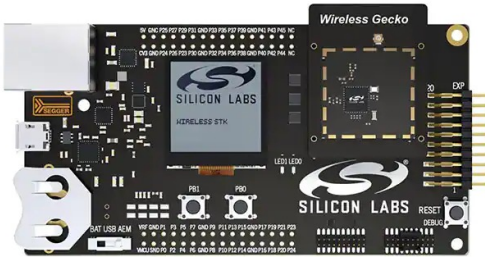
- **Ceiling rail infrastructure**
  - Internal test environment
  - Multiple stationary EFR32 devices placed at different locations
  - Mobile EFR32 device for controlled measurements (repeatability)
- **Challenges - heavy multi-path in an indoor office setting**
  - Line of Sight (LOS), Non-Line of Sight (NLOS)
  - Physical obstacles (metal, plastic, glass, etc.) in NLOS configurations
- **Statistical analysis**
  - Static measurements at multiple distances up to 30 meters
  - Hundreds of measurements per distance to determine min/max, mean, median, std, absolute error

# Indoor Office Performance Results



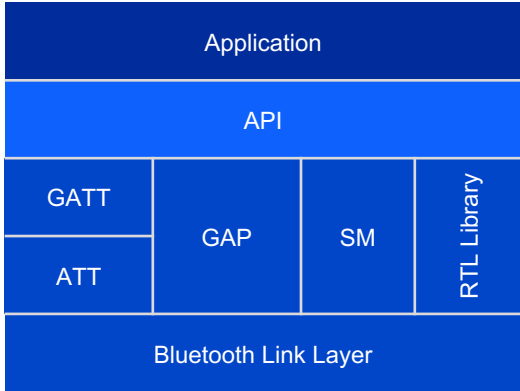
# Early Access and Application Development

Early Access integrated into 23Q2 GSDK release



## SOC, DEV KITS

- 2x BRD4198A
- 2x Dipole Antennas
- Wireless Pro Kit
- EFR32MG24 + 10dBm OPN



## STACK SOFTWARE

- In-house developed stack
- Supports Bluetooth 5.4 features
- All security features supported
- New and improved Ranging features

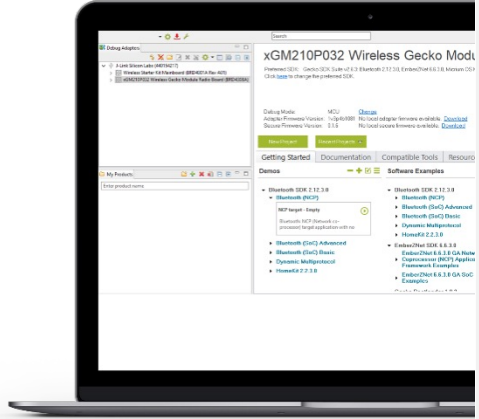
```

exe -- -zsh -- 80x49
vevarati@mac0015025 bt_abr_host_initiator % cd exe
vevarati@mac0015025 exe % ./bt_abr_host_initiator -u /dev/tty.usbmodem0004402801
515
[E] Invalid operation mode selected. Please select either 1 (RTT) or 2 (PBR)
vevarati@mac0015025 exe % ./bt_abr_host_initiator -u /dev/tty.usbmodem0004402801
515 -# 2 -#
[I] Accepting any suitable reflector.
[I] NCP host initialised.
[I] Resisting NCP target...
[I] Press Ctrl+C to quit

[I] Initialising RTL...
[W] abr_report_PBR.json already exist!
[W] Renaming abr_report_PBR.json --> abr_report_PBR.json_bkp31-5-2023-17_13_43
[I] Renamed successfully.
[I] File logger initialized.
[I] Bluetooth stack booted: v6.0.0-b37
[I] Bluetooth public device address: 34:25:84:A8:D8:15
[I] Scanning...
[I] Opening connection to Reflector
[I] Connection opened to the Reflector
[I] Encryption connection
[I] Connection encrypted
[I] Service found
[I] Service discovered
[I] Found remote value characteristic
[I] Characteristic discovered
[I] Creating ABR config...
[I] RTL process 49 channels
[I] Open file abr_report_PBR.json to write header...
[I] Config created
[I] Log measurement cycle 0000 ...
[I] Measurement result: 2051 mm | RSSI distance: 56 mm
[I] Log measurement cycle 0001 ...
[I] Measurement result: 1056 mm | RSSI distance: 40 mm
[I] Log measurement cycle 0002 ...
[I] Measurement result: 1076 mm | RSSI distance: 107 mm
[I] Log measurement cycle 0003 ...
[I] Measurement result: 1068 mm | RSSI distance: 56 mm
[I] Log measurement cycle 0004 ...
[I] Measurement result: 1082 mm | RSSI distance: 78 mm
[I] Log measurement cycle 0005 ...
[I] Measurement result: 1103 mm | RSSI distance: 107 mm
[I] Log measurement cycle 0006 ...
[I] Measurement result: 1115 mm | RSSI distance: 56 mm
[I] Log measurement cycle 0007 ...
[I] Measurement result: 1114 mm | RSSI distance: 56 mm
    
```

## HADM DEMO

- Python based Visualization tool
- RTL Library (GATT, IQ reporting)
- EFR32xG24 NCP/SoC
- RSSI, PBR, RTT modes



## DEVELOPMENT TOOLS

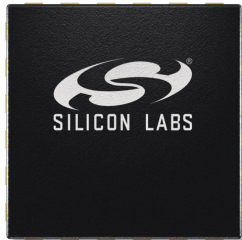
- Simplicity Studio
- Initiator & Reflector Example
- Energy Profiler + Network Analyzer
- Application Note
- Salesforce Support

# BG24 and BGM241S: 2.4 GHz SoC Ideal for Bluetooth Location Services

## SOCS AND MODULES



BG24 SoC



BGM241S SiP Module

## SOC DEVICE SPECIFICATIONS

### High-Performance Radio

- Up to +19.5 dBm TX
- -97.6 dBm RX @ LE 1 Mbps
- -105.7 dBm RX @ Bluetooth LE 125 kbps

### Efficient ARM® Cortex®-M33

- 78 MHz
- 1536kB Flash, 256kB RAM

### Low Power

- 33.4  $\mu$ A/MHz
- 5.0 mA TX @ 0 dBm
- 5.1 mA RX (802.15.4)
- 4.4 mA RX (LE 1 Mbps)
- 1.3  $\mu$ A EM2 sleep

### Multiple protocol support

- Bluetooth (1M/2M/LR)
- Bluetooth mesh
- Proprietary 2.4 GHz

### SoCs and Modules

- 5x5 QFN40
- 6x6 QFN48
- 7x7 SiP Module
- 12.9x15.0 PCB Module

## DIFFERENTIATED FEATURES

### +20 dBm output power

- Eliminates need for external power amplify

### High Accuracy Distance Measurement

- Measures distance between connected LE devices w/ sub-meter accuracy

### AI/ML accelerator

- Accelerates inferencing while reducing power consumption

### Secure Vault High

- Protects data and devices from local and remote attacks

### 20-bit ADC

- 16-bit ENOB for advanced sensing

### Antenna Diversity

- Provides 6-8 dBm better link budget

### Improved Coexistence

- Ideal for gateways and hubs

### PLFRCO

- Eliminates need for 32 KHz xtal

## SEGMENTS AND APPLICATIONS

### Smart Home

- HVAC
- Locks
- LED Lighting
- Switches
- Sensors
- Gateways, Hubs and Panels

### Connected Health

- Portable Medical

### Industrial and Smart Buildings

- Access Control
- HVAC
- Predictive Maintenance
- Asset Tracking

### Smart Cities

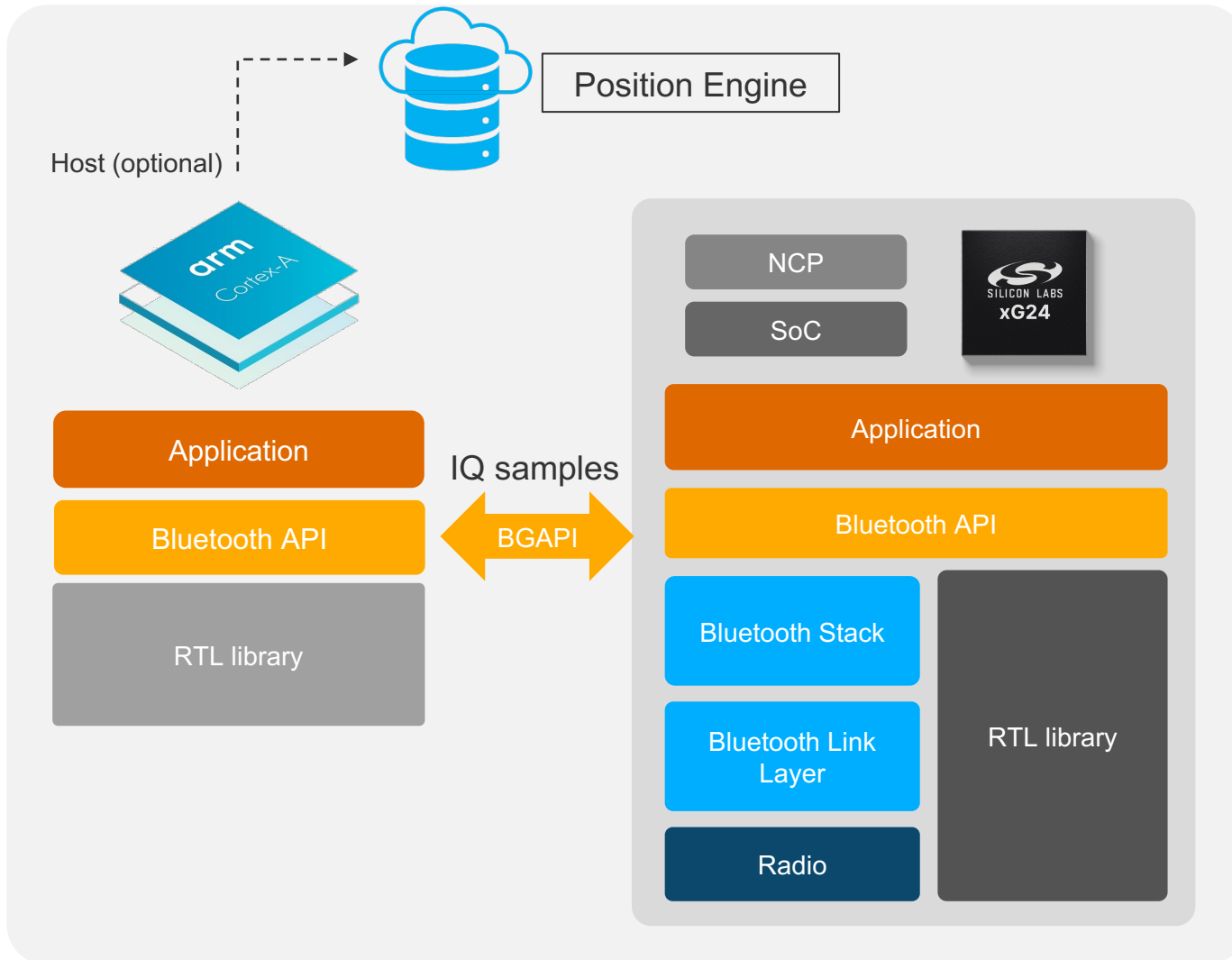
- EV Charging

### Commercial

- Lighting
- Access Points
- Clinical Medical
- Indoor Real Time Location Services



# Software Stack Architecture



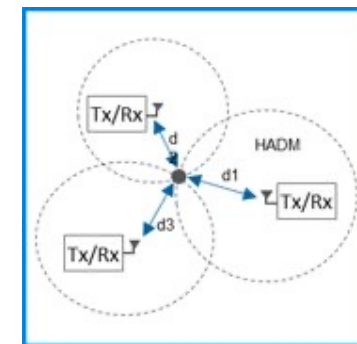
## Flexible mode of operation

- Host-NCP mode – RTL library runs on host
- SoC mode - RTL Library runs on xG24
- Supported host platforms - Windows x64, Ubuntu x64, Raspbian (Cortex A), Darwin x64

## GATT Ranging Service

- Measurement results sent via GATT indications

## Extend ranging application to other location services via trilateration



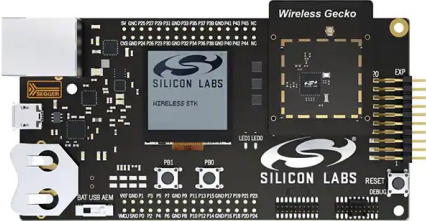


# Sample Applications – Out-of-Box Experience

The image displays three overlapping components related to a radio board application:

- Web Application (Left):** Titled "BG24 Ranging Radio Board (BRD419)", it features a navigation menu with "OVERVIEW", "EXAMPLE PROJECTS & DEMOS", and "DOCUMENTATION". A search bar contains "abr". A sidebar on the left lists categories like "Wireless Technology", "Device Type", "Ecosystem", "MCU", "Capability", "Project Difficulty", and "Quality". A filter for "EXPERIMENTAL (3)" is selected.
- Terminal Window (Middle):** Shows a shell prompt "vevarati@mac0015025 exe % ./bt\_abr\_host". The output logs the process of accepting a reflector, initializing NCP, scanning for services, and establishing a Bluetooth connection. It also displays a series of "Log measurement cycle" entries with results ranging from 507 mm to 596 mm.
- Graph (Right):** A line graph titled "Distance (m)" showing a blue line fluctuating around a mean value of 1.08 m. A legend indicates "HADM : 1.08 m". The y-axis ranges from 0.0 to 3.0 meters.

# What's Next?



2023

tech **talks**  
WEBINAR SERIES

# Thank You



BLUETOOTH SERIES

Watch **ON DEMAND**

2023



WEBINAR SERIES

# Wi-Fi 6 Benefits for IoT Applications

February 2<sup>nd</sup> at 10 AM CT

[Register Today](#)



WI-FI SERIES