Welcome

Explore Bluetooth Channel Sounding

Rajendra Mohan Goswami – Sr. Field Application Engineer

Agenda

01 Target market and Applications

02 Channel Sounding Overview & Use Cases

03 Performance data

04 Silicon Labs Offerings

05 Q&A

Target Applications for Bluetooth Ranging

PROXIMITY AWARENESS

Door locks

Keyless entry

Building access systems

Geofencing - security alerts

LOCALIZATION

Indoor asset management - hospitals, warehouses

Pet tracking inside home

Item finding - wallet, keys

Overview

Channel Sounding Overview

- **Measure distance between two devices using**
  - Phase-based Ranging (PBR)
  - Round Trip Time (RTT)
- **RTT and PBR operates across 2.4 GHz band**
  - Standard specifies up to 72 channels
  - Random hopping pattern
- **Connection-Oriented 2-way ranging with two roles**
  - Initiator: device that wishes to calculate distance from itself to another device
  - Reflector: device responding to initiator
- **Supports up to 4 antenna paths between devices**
  - 8 possible antenna combinations
- **Multiple security features included in the standard**
- **Can be combined with Angle of Arrival / Departure (AoA/AoD)**
  - Enables position estimation with single initiator/reflector pair
- **Bluetooth SIG Specification adoption expected in 2024**
  - Draft Channel Sounding specification at: https://www.bluetooth.com/specifications/specs/channel-sounding-cr-pr/

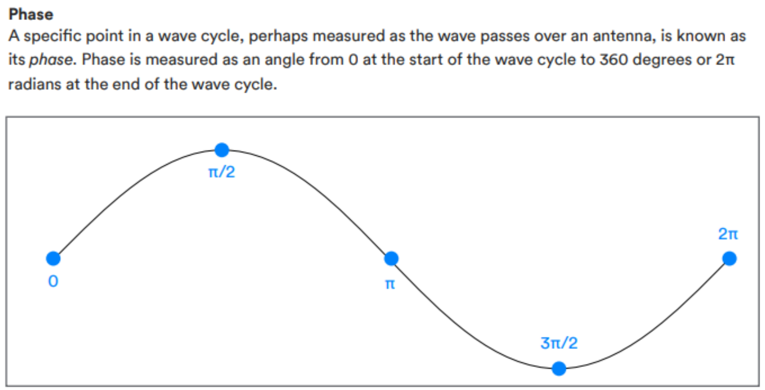
What's included in the spec

- RF and link layer timing and functional requirements
- Mandatory vs. optional features and modes
- Guidance on antenna configurations and security features

What's not included in the spec

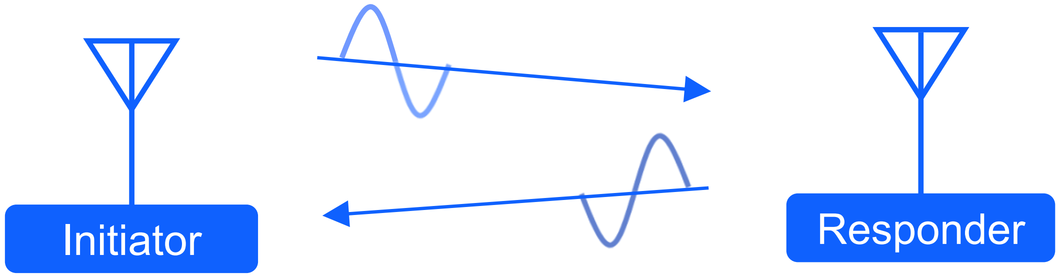
- Distance measurement algorithm recommendations and optimizations

Phase-Based Ranging (PBR) Measurement



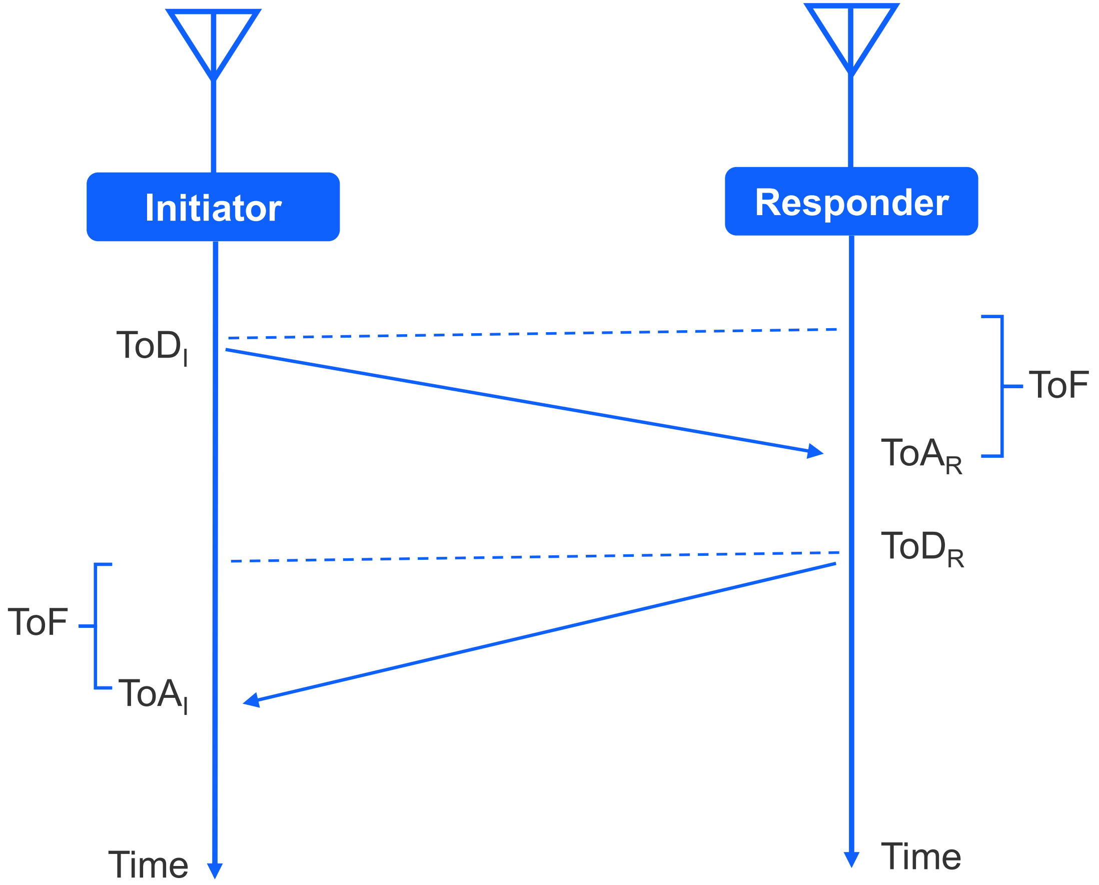
Phase

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 2π radians at the end of the wave cycle.



- **Phase of RF signals is a function of frequency of the carrier and the distance traveled**
  - Phase rotation due to spatial propagation desired
  - Measurements at multiple RF frequencies to resolve distance ambiguity
- **Distance is calculated using the phase difference between transmitted and received signal**
- **Distance measurement process**
  - Calibration phase
  - Measurement phase where both devices transmits a packet and calculates the phase difference
  - Signal processing and distance calculation algorithm
- **Security benefits**
  - Difficult for an attacker to manipulate phase
  - Random transmission length and channel map makes sniffing difficult

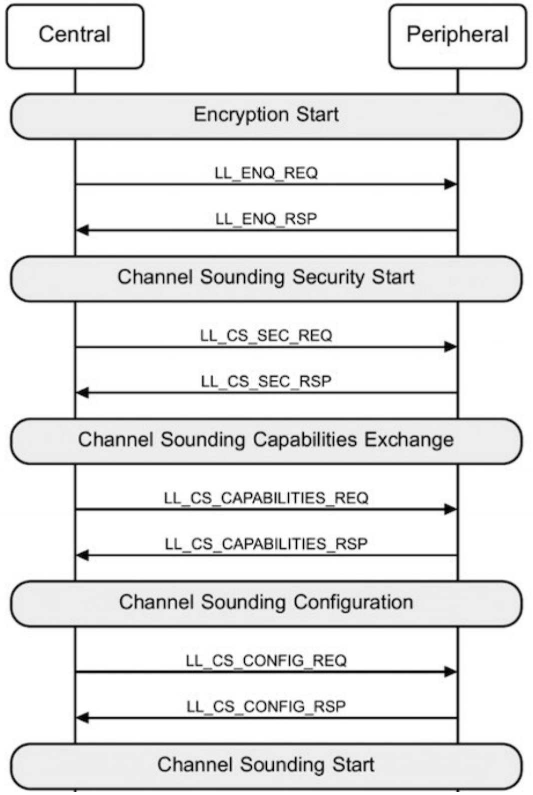
Round Trip Time (RTT) Measurement



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

- **Time of Flight (ToF) is measured on both initiator and reflector side using Time-of-Arrival (ToA) and Time-of-Departure (ToD)**
  - Distance is estimated from exchanged measurements on multiple channels
  - Fractional techniques used to resolve sampling uncertainty and increase accuracy
- **Duration of measurement procedure is variable**
  - Procedures can be split across multiple intervals
  - Multiple measurements in longer connection interval
  - Number of channels
- **Security benefits**
  - Time cannot be reversed, preventing reflector from appearing closer than it is
  - Random bits as sync word guard against packet sniffing
  - Random tone length prevents attackers from altering toning sequence

Channel Sounding setup between central and peripheral



LE ACL encryption start

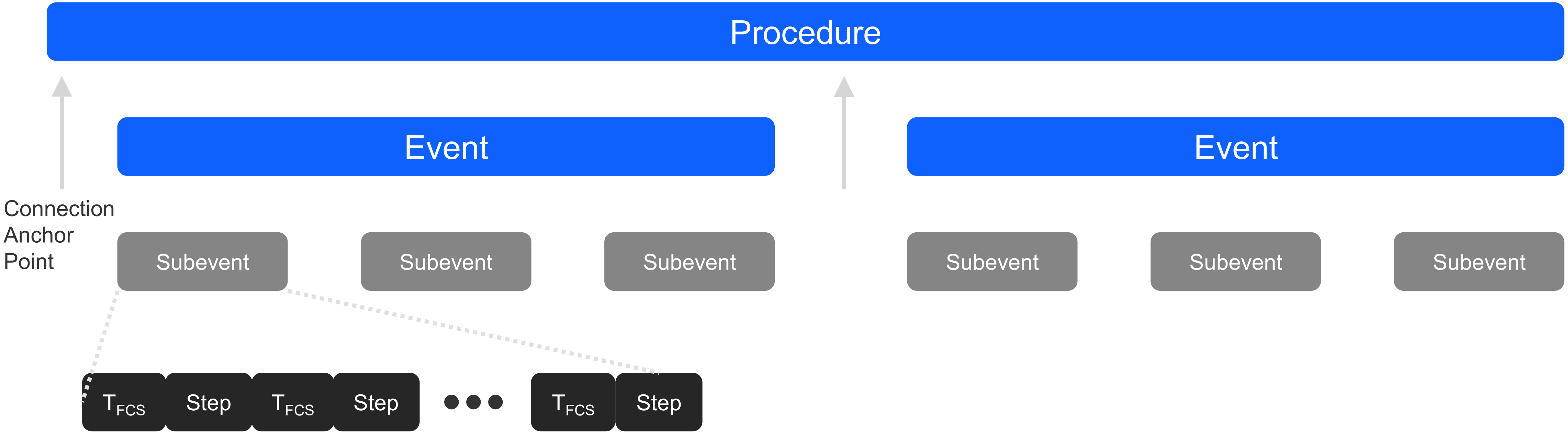
DRBG secret exchange for randomized bit streams

Define all possible antenna configs and supported modes/submodes, supported PHYs, and more

Defines antenna config, PHY, and who acts as initiator, with decisions based on capabilities exchange

Note: While this exchange occurs before every channel sounding procedure start, some of these steps can be skipped during setup if information has been cached previously

Channel Sounding Procedure -> Events -> Subevents -> Steps



- **Procedures**, composed of **events**, can span multiple connection intervals
- **Subevents** are required to complete within single connection interval
- **Steps** correspond to setup, PBR, or RTT ranging, defined as **4 modes**

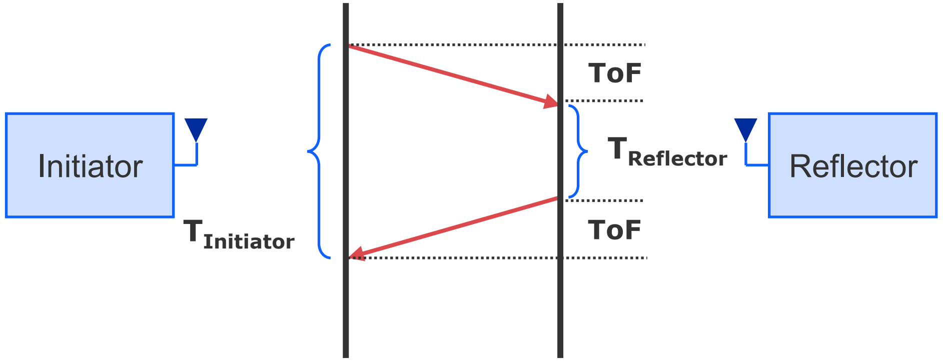
Channel Sounding Step Modes

Mode-0: Calibration

- Compensates for clock drift and frequency offset
- Results in fractional frequency offset table

Required

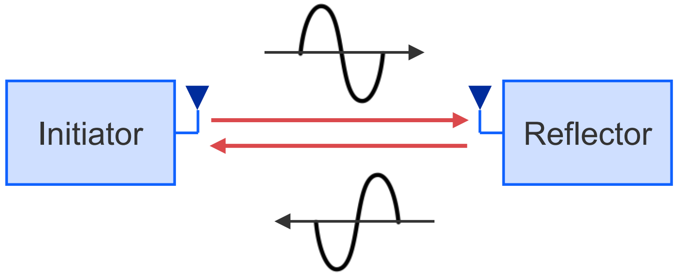
Mode-1: Round trip time



- CS SYNC packets exchanged between initiator and reflector

Required

Mode-2: Phase based ranging



- CS Tone exchanged between initiator and reflector
- Each antenna path exercised in each step

Required

Mode-3: PBR+RTT

- Combined PBR and RTT in each step
- RTT distance measurement can be cross-checked with PBR results
- Provides higher security as a mismatch in distance estimation can indicate relay attack

Optional

Channel Sounding security features

- **Potential vulnerabilities**
  - Spoofing
  - Man in the middle (MITM) or relay attacks

- **Deterministic random bit generator (DRBG)**
  - Initialized during security start data exchange
  - Scrambles bit sequences between initiator and reflector
  - Randomizes payloads in tone extensions, antenna path selection, and more

- **Cross-checking PBR with RTT**
  - Can be done in Mode 1 steps with mode 2 as submode or using Mode 3
  - Mismatch in distance estimation indicates relay attack

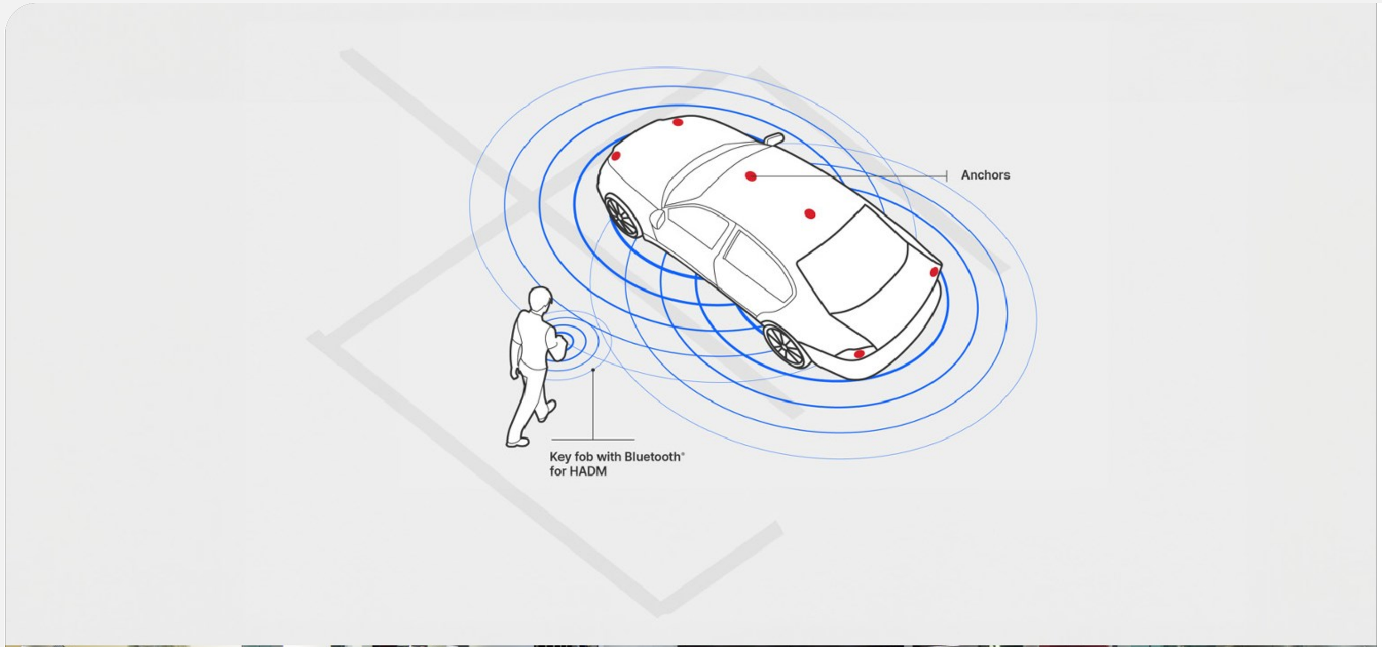
- **Normalized Attack Detector Metric (NADM)**
  - Detects unexpected bit transitions or phase changes in received signals
  - Standard does not include implementation requirements,
  - Prescribes scale for now anomalies are classified
  - Optional feature

Bluetooth® LE Location Services Comparison

	RSSI	Angle of Arrival	Channel Sounding
Localization metric	Resolve distance estimation from transmitter signal strength	Resolve relative angle between two points	Resolve distance between two points using time of flight and phase-based ranging
Antenna requirements	Single antenna	Multi-antenna required by spec	Multi-antenna not required, but useful for optimal position resolution
Bluetooth® LE connectivity	Connection-oriented and connectionless	Connection-oriented and connectionless	Connection-oriented
Performance metrics	+/- 5 m, high susceptibility to multipath interference	+- 3 degrees accuracy – azimuth +- 5 degrees accuracy – elevation	+- .3 m < 5m with PBR ranging +- 0.5 m > 5m with PBR ranging
Solution advantages	• Ubiquitous support for RSSI measurements in existing Bluetooth LE products	• Scalable solution for real time position tracking • Supports 5-10 year battery life	• Small form factor with flexible antenna design • Feature-add for security by proximity

Use cases

Channel Sounding for Geo-Fencing Applications



Unlock on Approach:

- Remote Keyless Entry
  - Zonal detection through ranging for secure vehicle access
  - User enhancement with wake/welcome response
- Proximity-based locking and unlocking
  - Automatic door lock & unlock at a certain distance from it

- **Loss Prevention**
  - Retail theft prevention
    - Tracks the location of high-value items within the store and triggers alarms if they are moved outside designated areas.
  - Geofenced Notifications for Unauthorized Movement
    - Sends alerts upon detection of unauthorized movement or movement of goods outside a certain defined boundary.

Channel Sounding in an Indoor Facility

Access Control

- Restrict access to unauthorized personnel
- Send alerts to local servers/cloud if anyone dwells in the area for too long

Entry access

Authenticate and grant access to authorized workers when they approach the door

Asset management

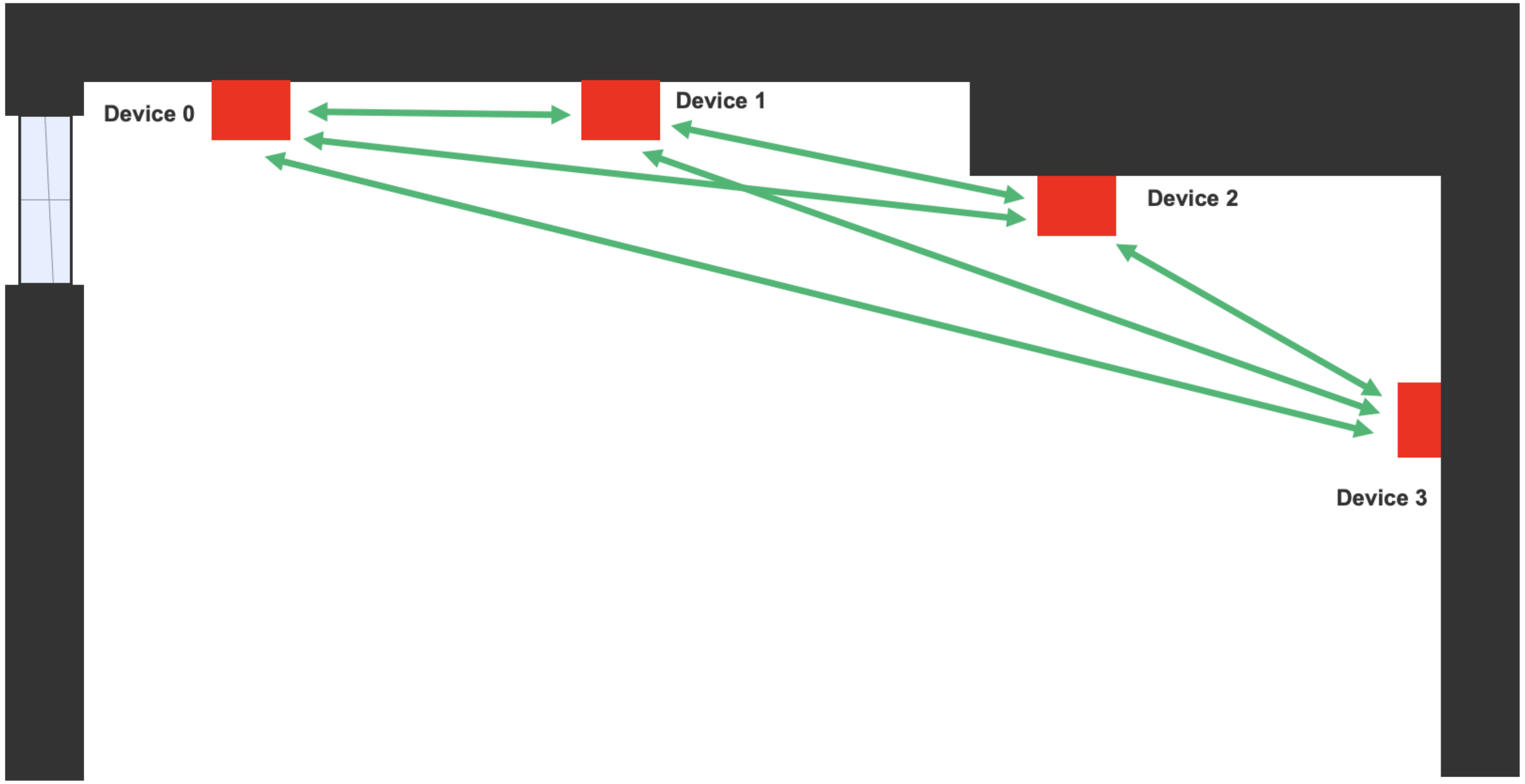
- Coarse localization of inventory inside the facility
- Increase worker efficiency

Distance Measurement Demo

SILICON LABS

Distance Measurement Demo

Channel Sounding for Static Device Positioning



- Enables device positioning for static devices like luminaries or access points.
- The devices act as initiators and reflectors to calculate the distance from each other to create a geometric map.

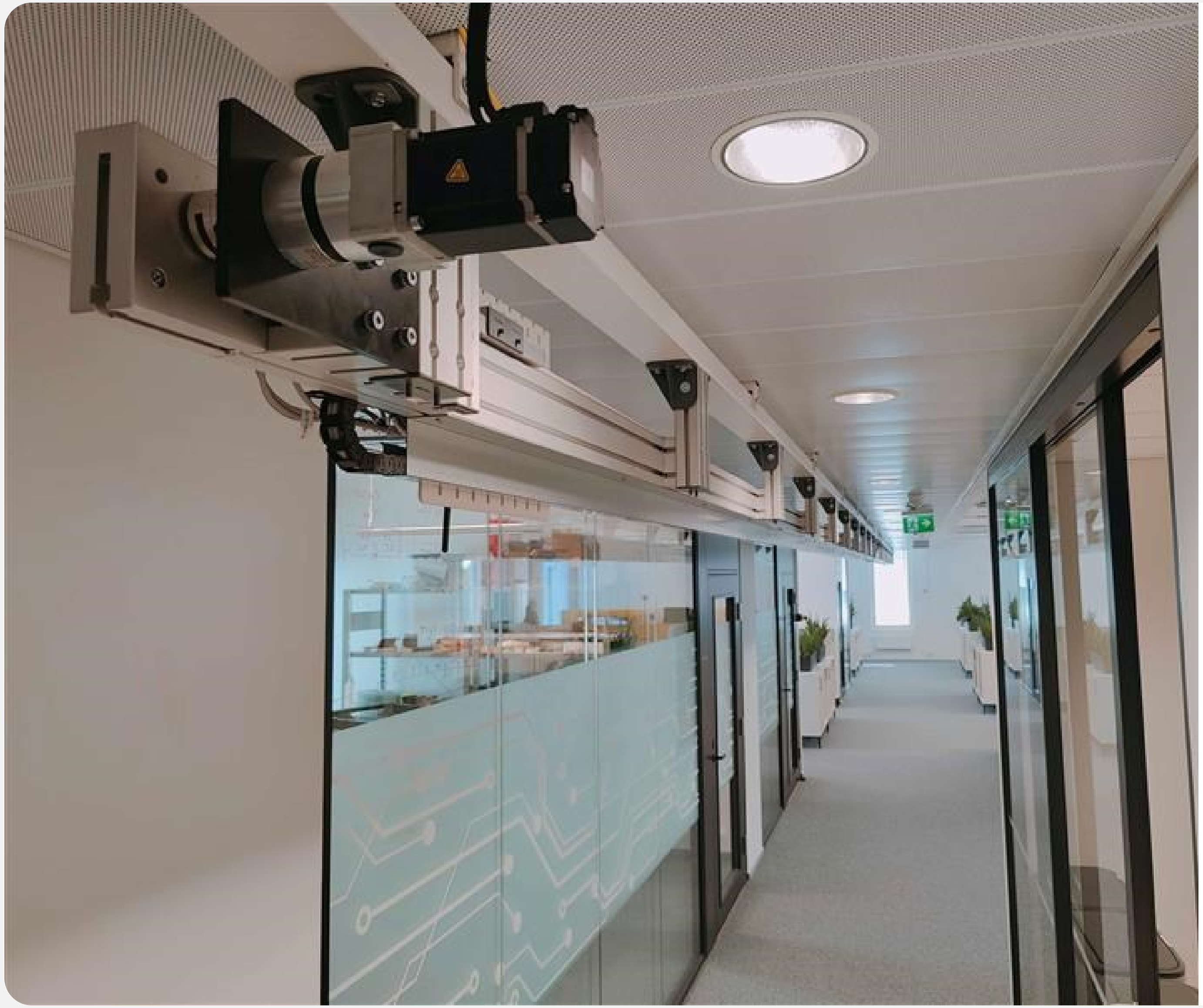
Static Device Positioning Demo

SILICON LABS

Static Device Positioning

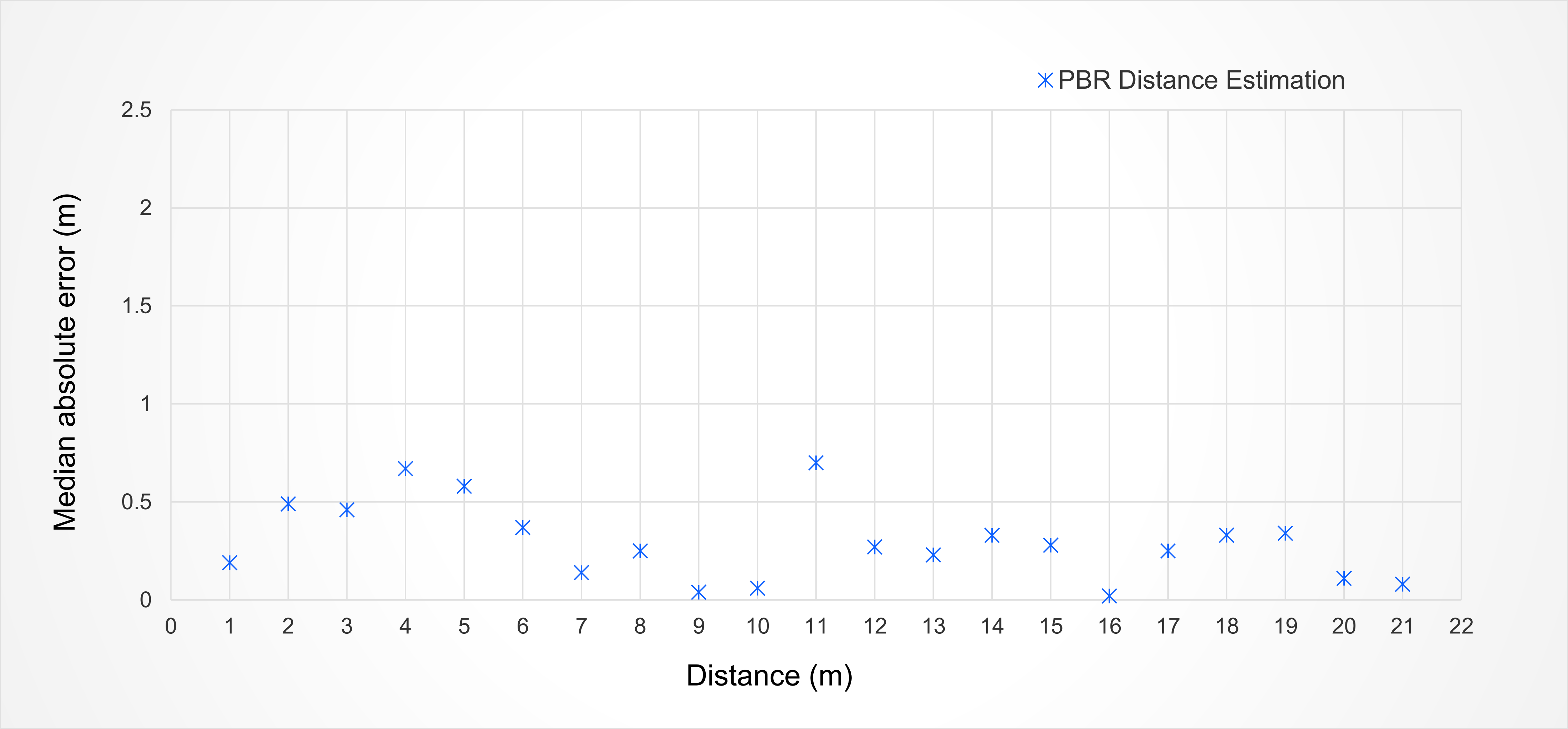
Performance

Performance in Indoor Office Environment

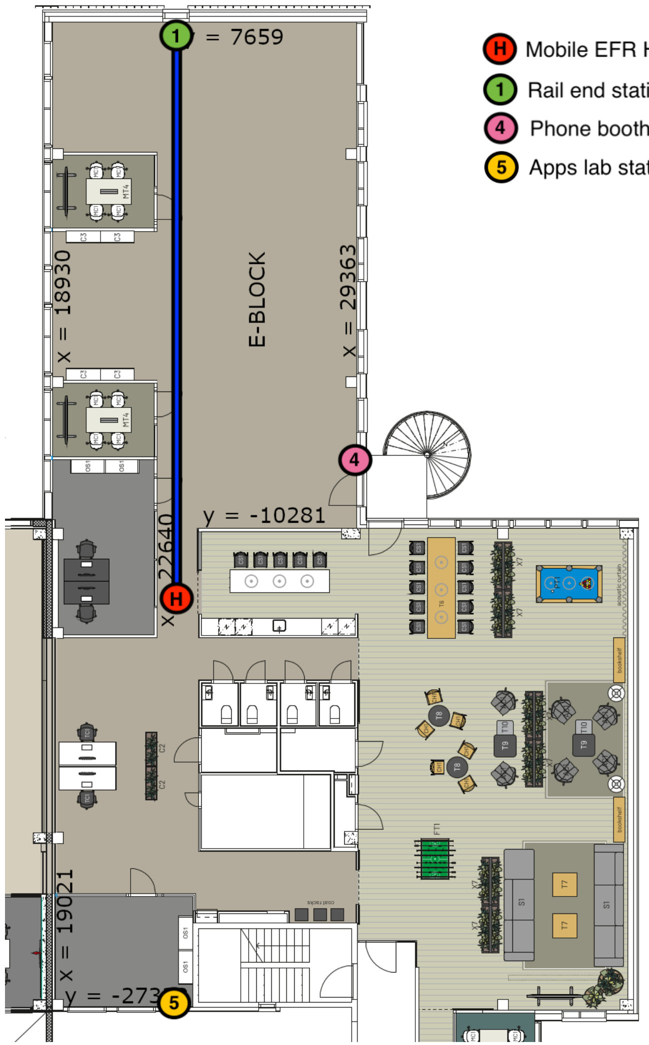


- **Ceiling rail infrastructure**
  - Internal test environment
  - Multiple stationary EFR32 devices placed at different locations
  - Mobile EFR32 device for controlled measurements (repeatability)
- **Challenges - heavy multi-path in an indoor office setting**
- **Statistical analysis**
  - Static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

Indoor Performance Result – Line of Sight

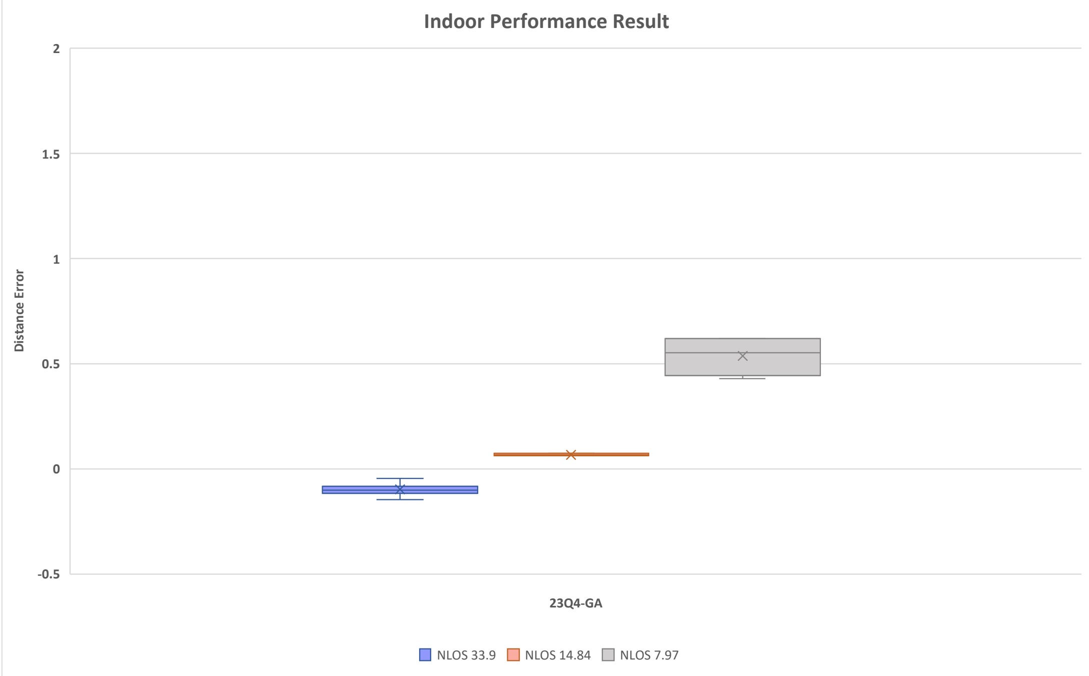


Indoor Performance Result – Non - Line of Sight



H Mobile EFR HOME
1 Rail end static EFR
4 Phone booth static EFR
5 Apps lab static EFR

1 – 5 = NLOS 33.9m
1 – 4 = NLOS 14.84m
H – 4 = NLOS 7.9m



Silicon Labs Offerings

BG24: Optimized for Battery Powered, Channel Sounding-enabled IoT Devices

Bluetooth® Proprietary

- 5x5 QFN40 (26 GPIO)
- 6x6 QFN48 (32 GPIO)
- 3.1x3.0 WLCSP42

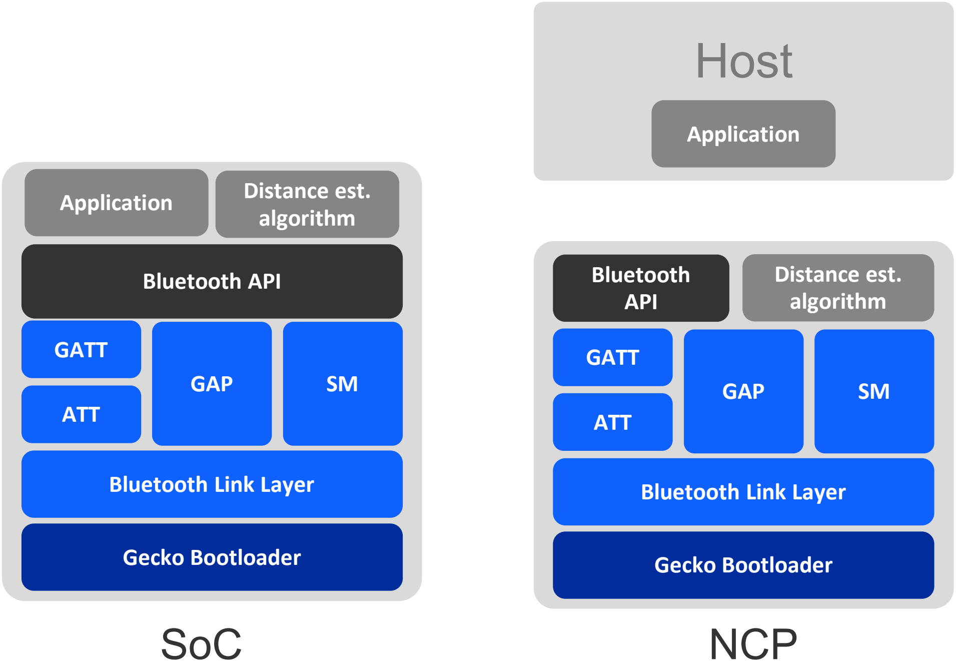
DIFFERENTIATED FEATURES

- **Ultra small form-factor**
  - 3.1 x 3.0 WLCSP package
- **+20 dBm output power**
  - Eliminates need for external power amplify
- **AI/ML accelerator**
  - Accelerates inferencing while reducing power consumption
- **Secure Vault High**
  - Protects data and device from local and remote attacks
- **20-bit ADC**
  - 16-bit ENOB for advance sensing
- **Improved Coexistence**
  - Ideal for gateways and hubs
- **PLFRCO**
  - Eliminates need for 32 KHz xtal

DEVICE SPECIFICATIONS

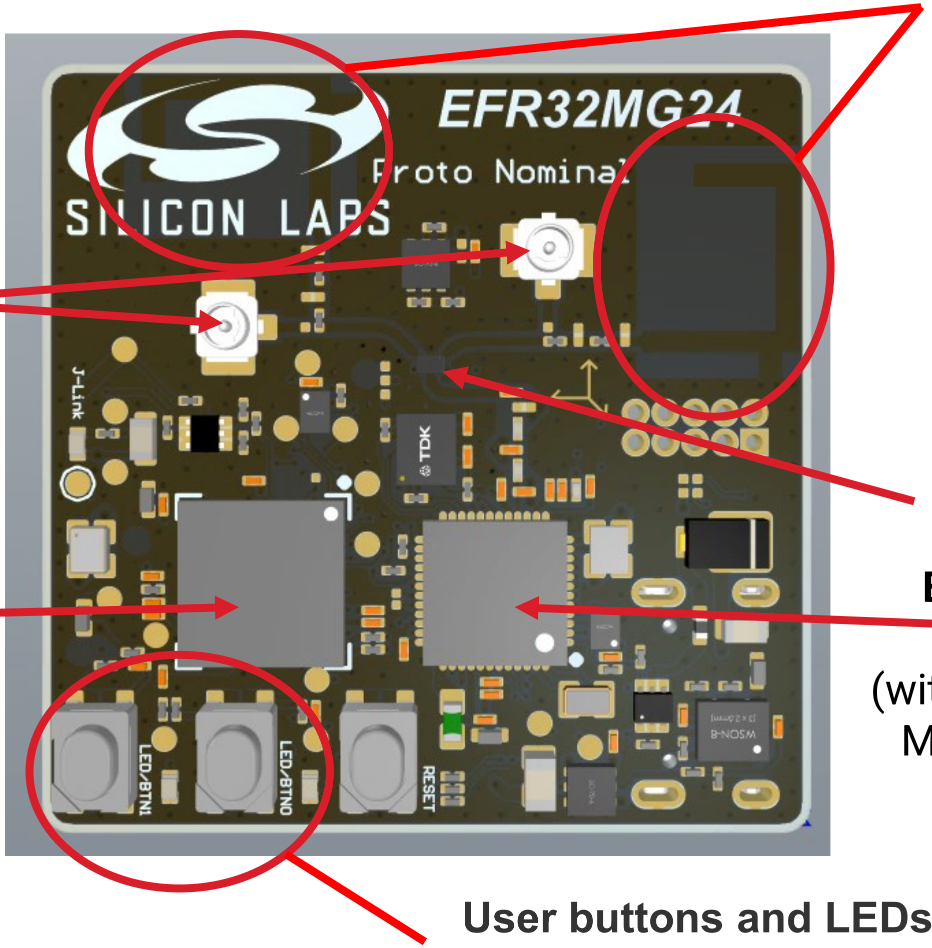
- **High Performance Radio**
  - Up to +19.5 dBm TX
  - -97.6 dBm RX @ BLE 1 Mbps
- **Efficient ARM® Cortex®-M33**
  - Up to 78 MHz
  - 1536kB Flash, 256kB RAM
- **Low Power**
  - 49.1 µA/MHz (CoreMark)
  - 5.0 mA TX @ 0 dBm
  - 5.1 mA RX (802.15.4)
  - 4.4 mA RX (BLE 1 Mbps)
  - 1.3 µA EM2 sleep
- **Multiple protocol support**
  - Bluetooth 5.4 (1M/2M/LR), Bluetooth mesh, Proprietary 2.4 GHz

Bluetooth Software for Channel Sounding



- **Bluetooth 6.0 support for Channel Sounding**
  - All mandatory channel sounding features supported
  - Distance estimation algorithm included
- **SoC and NCP modes**
  - Channel Sounding data over BGAPI and distance estimation calculated on-chip
- **Supported by BG24 SoCs and Modules**
- **Software components included in Simplicity Studio**
- **Example applications available for alpha customers**
- **Typical Channel sounding application with stacks is 500K**
  - Leaves 60%+ for user applications
- **Documentation: http://docs.silabs.com/**

Dual antenna Channel Sounding board - front



2x PCB antenna for antenna diversity and dual polarization

2x U.FL connector for optional external antenna support

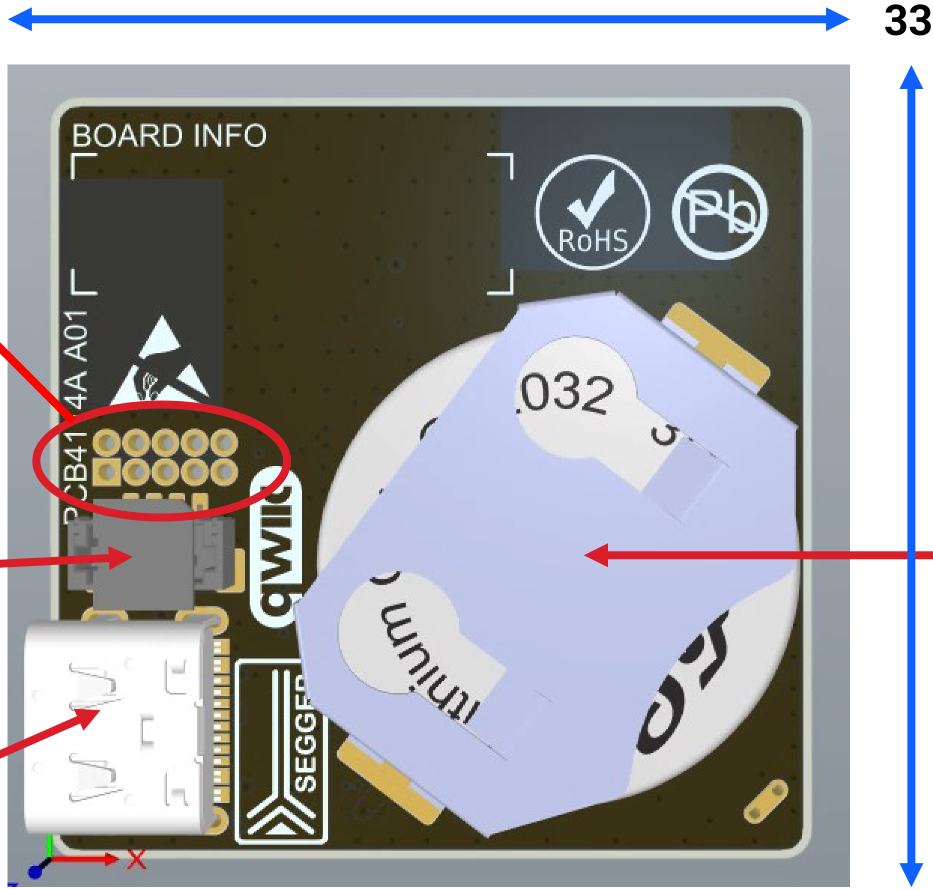
1-to-2 RF switch

On-board debugger for easy programming and debugging

EFR32MG24B210F1536IM48-B
our most capable xG24 part
(with 1.5MB flash, Channel Sounding, MVP, Secure Vault High, +10dBm)

User buttons and LEDs
for demo firmware support

Dual antenna Channel Sounding board - back



33x33mm overall size

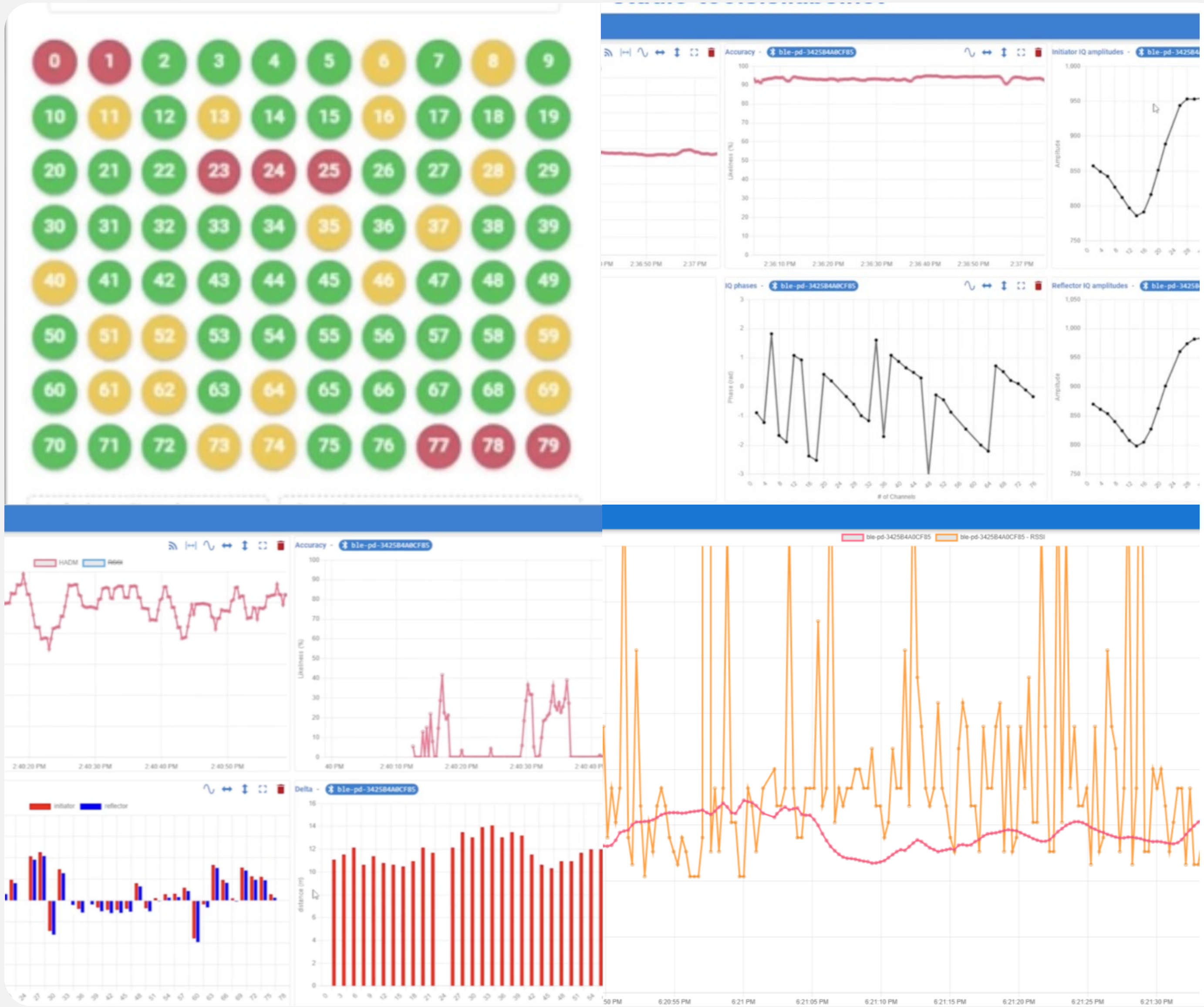
Mini Simplicity header for Wireless Main Board connectivity. Provides Advanced Energy Monitoring and Packet Trace Interface options.

Qwiic connector for extendibility

USB-C connector for easy PC connectivity. Provides both debugger and virtual UART interfaces

CR2032 for portability

Visualizer Tool



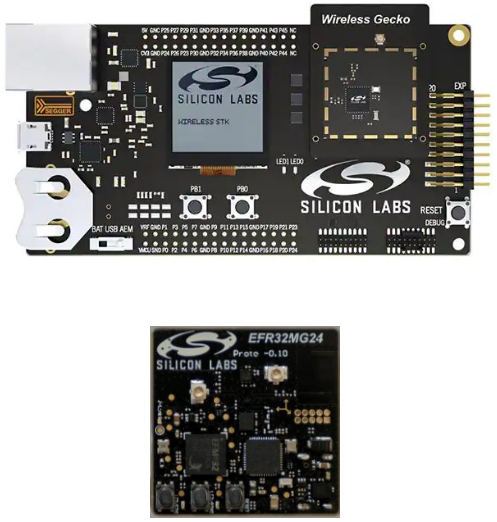
Visualizer Tool displays realtime data

- Channel sounding data with RSSI readings for comparison
- Interfaces with Channel Sounding-enabled EVKs

Upcoming features

- Data logging
- Confidence metric display
- Channel map selection

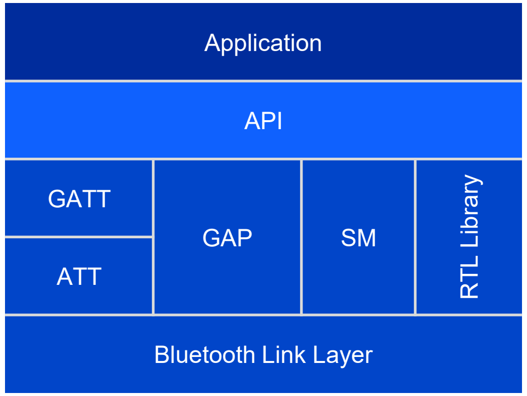
Silicon Labs Channel Sounding – Complete Offering



DEVELOPMENT KITS

BRD4198A with Single Antenna
Wireless Pro Kit
EFR32MG24 + 10dBm OPN
BRD2606A with Dual Antennas

Bluetooth®



STACK SOFTWARE

In-house developed stack

Supports Bluetooth 5.4 features + Channel Sounding

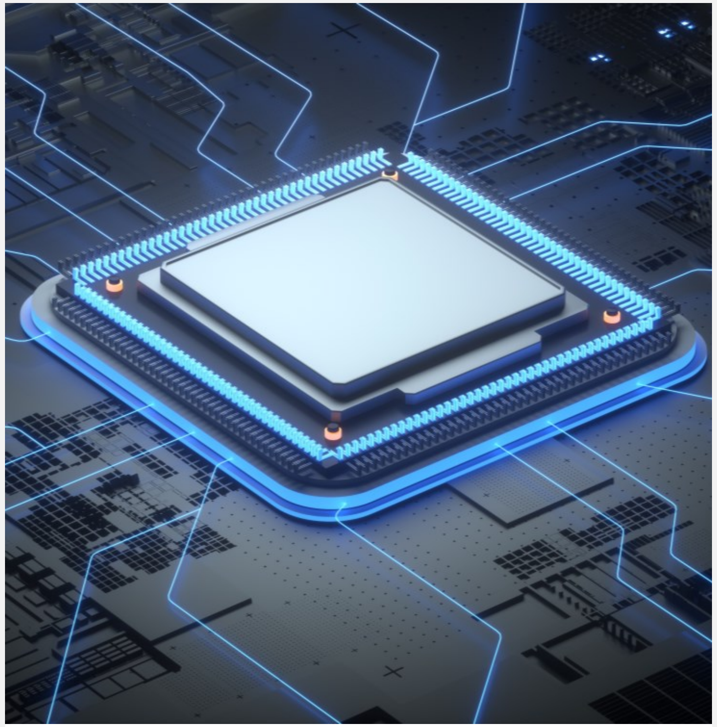
New and improved Ranging features

Simplicity Studio 5

DEVELOPMENT TOOLS

Real-time visualization tool
PBR, RTT modes
CS Sample projects
CS Analyzer + Energy Profiler + Network Analyzer
App note + Salesforce Support

Call to Action!



GET EARLY ACCESS

Become a part of our ongoing Channel Sounding Early Access Program to get access to our development tools.

CONTACT US

For any questions or to join our Early Access Program, please contact our sales team.

LEARN MORE

To learn more about Channel Sounding and SiLabs offerings, please visit our website.

Q&A

BLUETOOTH

Welcome

Unboxing Silicon Labs’ Latest Bluetooth SoC for Energy Harvesting

Koichi Matsuo – Senior FAE, Silicon Labs Japan

BLUETOOTH

Agenda

01 The Problem with Batteries..

02 Ambient IoT’ for ‘Energy Harvesting’

03 Unboxing xG22E

04 Resources: xG22E Explorer Kit e-peas Shields

05 Q&A

The problem with batteries...

Koichi Matsuo

The Problem with Batteries for IoT

15 billion

batteries are thrown in land-fills every year

More than 15 billion batteries are thrown in land-fills around the world every year (900,000 tons of hazardous waste)

The average household purchases over 90 batteries annually most have much less than 10-year lifetime

Batteries are slowing down the growth of IoT

- 25 billion IoT devices predicted by 2025 would require 6 million battery replacements every day
- In industrial setting with 1,000 sensors, the annual replacement of over 350 batteries—typically exceeding one per day—incurs significant recurring costs, often surpassing the batteries' own price.
- IoT is compromised when sensor polling rate, payload size, transmission rate and range are lowered due to lack of power.
- Systems need to integrate energy awareness decision making

Battery regulations

- National Electric Code (**NEC**) is introducing **new requirements on battery collection and recycling** as well as mandating the **elimination of batteries** in certain devices.

- **More and more countries** are following the movement (NEC US, NEC Europe, Japan, Australia, Canada)

- [17 AUG 2023] – **European Commission – Batteries Regulation**
- **Biden-Harris Administration Announces $62 Million to Lower Battery Recycling Costs Across the Nation**

- These upcoming regulations impact IoT device design.

  This is the beginning of a new era of IoT product development

Source:

https://www.lightnowblog.com/2023/05/2023-nec-prohibits-battery-only-wall-light-switches/

https://environment.ec.europa.eu/news/new-law-more-sustainable-circular-and-safe-batteries-enters-force-2023-08-17_en

Energy Harvest – Application Profiles

SOLAR - OUTDOOR

LOGISTICS / LIVESTOCK TRACKING

- Bluetooth /Bluetooth Long Range
- 802.15.4 Mesh

- 10 mW/cm²

SOLAR - INDOOR

ASSET TRACKING / SMART BUILDING SENSORS

- Bluetooth
- 802.15.4 Mesh

- 10 µW/cm²

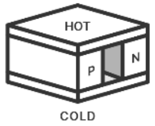
KINETIC PULSE

SMART SWITCHES

- Bluetooth / Bluetooth Mesh
- 802.15.4 Mesh

- 120~300 µJ/press

Energy Harvest – Application Profile

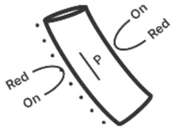


THERMAL

MACHINE MONITORING

- Bluetooth / Bluetooth Mesh
- 802.15.4 Mesh

- 1-10 mW/cm²

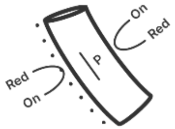


VIBRATION / PIEZO

FACTORY AUTOMATION / AGRICULTURE / TPMS

- Bluetooth
- 802.15.4 Mesh

- 100 μW/cm²



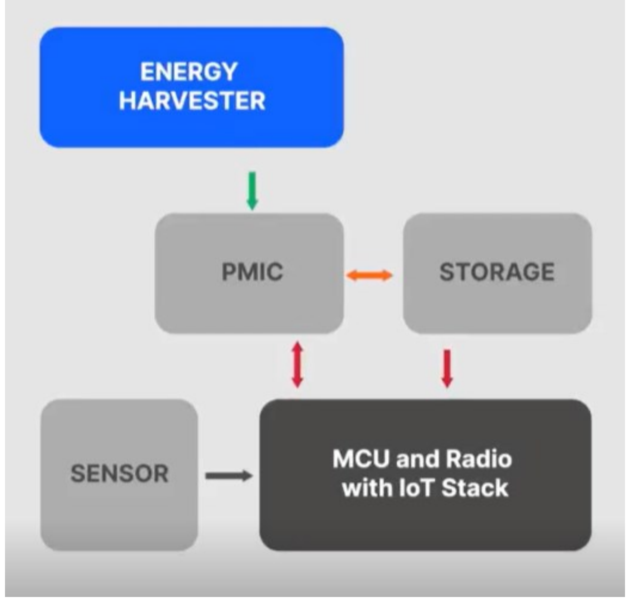
INDUCTION

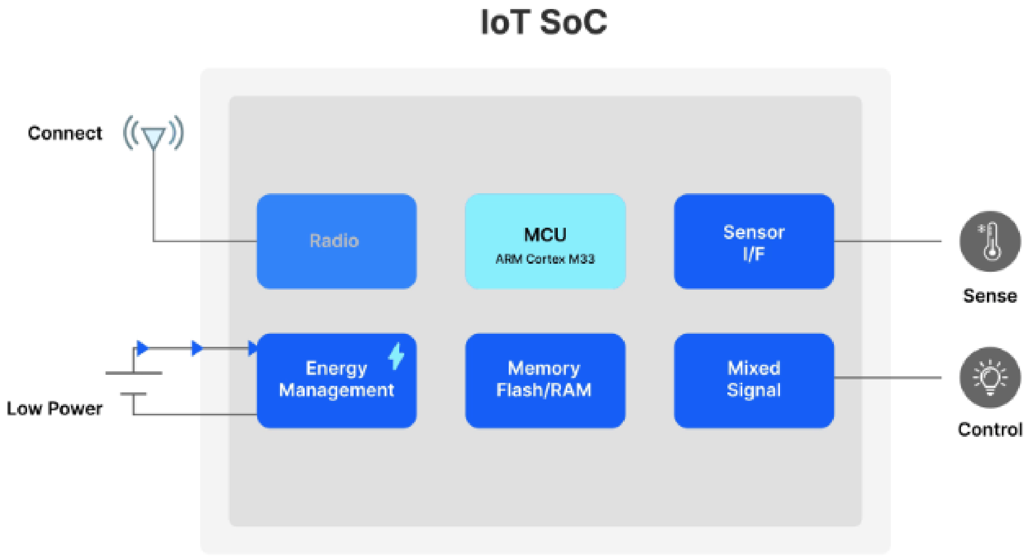
ELECTRIC SUB-METERING

- Zigbee Green Power
- 802.15.4 Mesh

- 100 μW/cm²

Understanding IoT Architectures for Energy Harvesting





- **Energy Harvester:** harness ambient energy
- **Storage:** energy bank
- **PMIC:** power management and transformation
- **MCU and Radio:**
  - Application and communication
  - energy-based decision making ; sleep and wake control

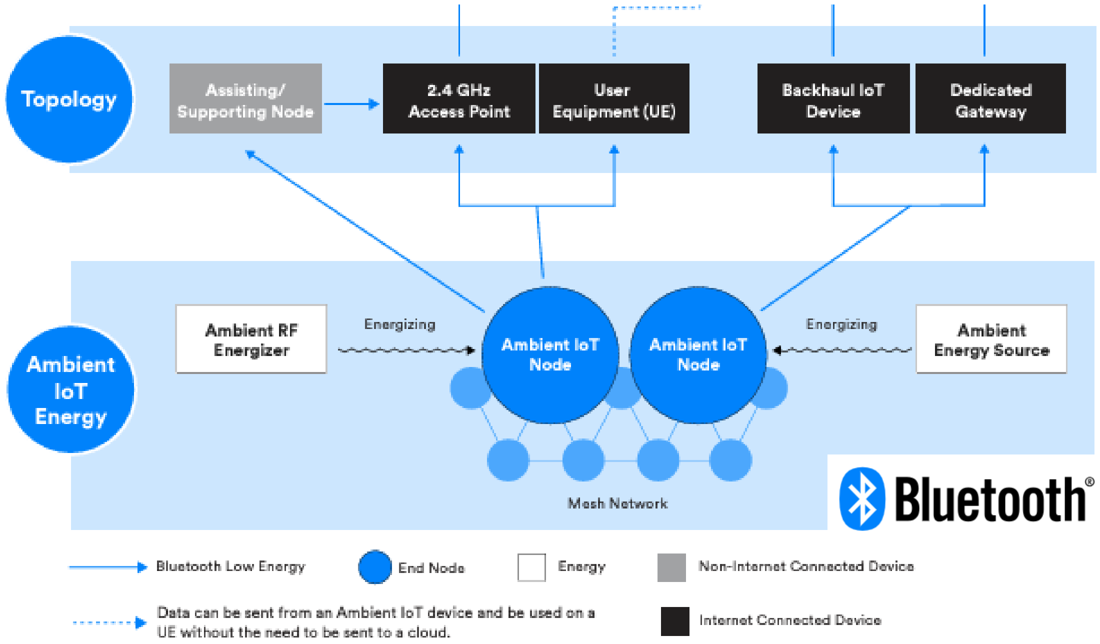
The IoT SoC Platform is responsible for:

- assessing available energy
- determining when to wake up peripheral systems
- executing system actions...or remain asleep.
- Managing communication payload and transmitting

Ambient IoT’ for ‘Energy Harvesting’

Koichi Matsuo

‘Ambient IoT’ for ‘Energy Harvesting’



The Connectivity Standards Alliance Releases Green Power 1.1.2 for Zigbee-based Energy-harvesting Technology
green power
certified by connectivity standards alliance
csa connectivity standards alliance

- BTSIG preparing for battery-less, energy-harvested IoT
  - FEB, 2024 – *The Role of Bluetooth Technology in the Ambient IoT*
  - Reference link

- CSA launching ZGP 1.1.2 - 24Q2 GSDK
  - MARCH, 2024 – *CSA Releases Green Power 1.1.2 for Zigbee-based Energy-Harvesting Technology*
  - Reference link

Unboxing xG22E

Koichi Matsuo

xG22E: Ideal for Ultra-low Energy, Ambient IoT, and Energy-Harvesting

Bluetooth® Proprietary

zigbee

- **5x5 QFN40 (26 GPIO), AEC-Q100**
- **4x4 QFN32 (18 GPIO)**

DIFFERENTIATED FEATURES

- **Efficient, Low-Energy Cold Start**
  - Boot-up time less than 8ms
  - Energy consumption under 150uJ
- **Low-Energy Deep Sleep wake-up**
  - Consuming less than 17uJ
- **Power-efficient energy mode transition**
  - Optimized to smoothly transition out of energy modes
  - Mitigates current spikes or inrush
- **RFSense with OOK mode**
  - Ultra low-power receive mode to wake-up MCU from EM2 or EM4
  - Results in longer battery life
- **PLFRCO**
  - Eliminates need for 32 KHz XTAL and lowers overall system cost
- **16-bit ADC**
  - Up to 14-bit ENOB for better analog sensing

DEVICE SPECIFICATIONS

- **High Sensitivity 2.4 GHz Radio**
  - -Up to +6 dBm TX
  - -98.9 dBm RX @ BLE 1 Mbps
  - -106.7 dBm RX @ BLE 125 kbps
  - -102.3 dBm RX @ 15.4
- **Efficient ARM® Cortex®-M33**
  - Operating Frequency: Up to 76.8 MHz
  - 512kB Flash, 32kB RAM
  - Low Power
  - 27 µA/MHz
  - 3.4 mA TX @ 0 dBm
  - 2.5 mA RX (BLE 1 Mbps)
  - 1.4 µA EM2 sleeps
  - 0.17 µA EM4
- **Secure**
  - Secure Vault Base
  - ARM ® TrustZone
- **Wide Operating Range**
  - 1.71 to 3.8 volts
  - +125ºC operating temperature
- **PLFRCO**
  - 500 PPM LFRCO

xG22E Optimizations

COLD START

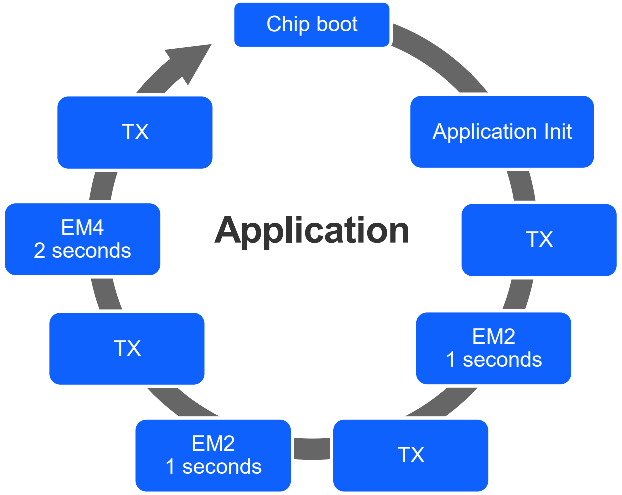
- **Efficient, Low-Energy Cold Start**
  - Boot-up time less than 8ms
  - Energy consumption under 150uJ

- **For energy-harvest devices that require booting up from *zero-power level***

ENERGY MODE SLEEP WAKE-UP

- **Low-Energy Deep Sleep wake-up ; Smooth energy mode transitions**
  - Consuming less than 17uJ
  - Current in-rush spikes mitigated between rapid energy mode transition to protect batteries and capacitors

- **For devices that spend extremely lengthy periods in deep sleep with *frequent* wake-ups between Tx**
  - Extends battery-life
  - Allows for energy-based wake decision making for energy-harvesting
  - Multi-source wake-up (RF Sense, GPIO, RTC)

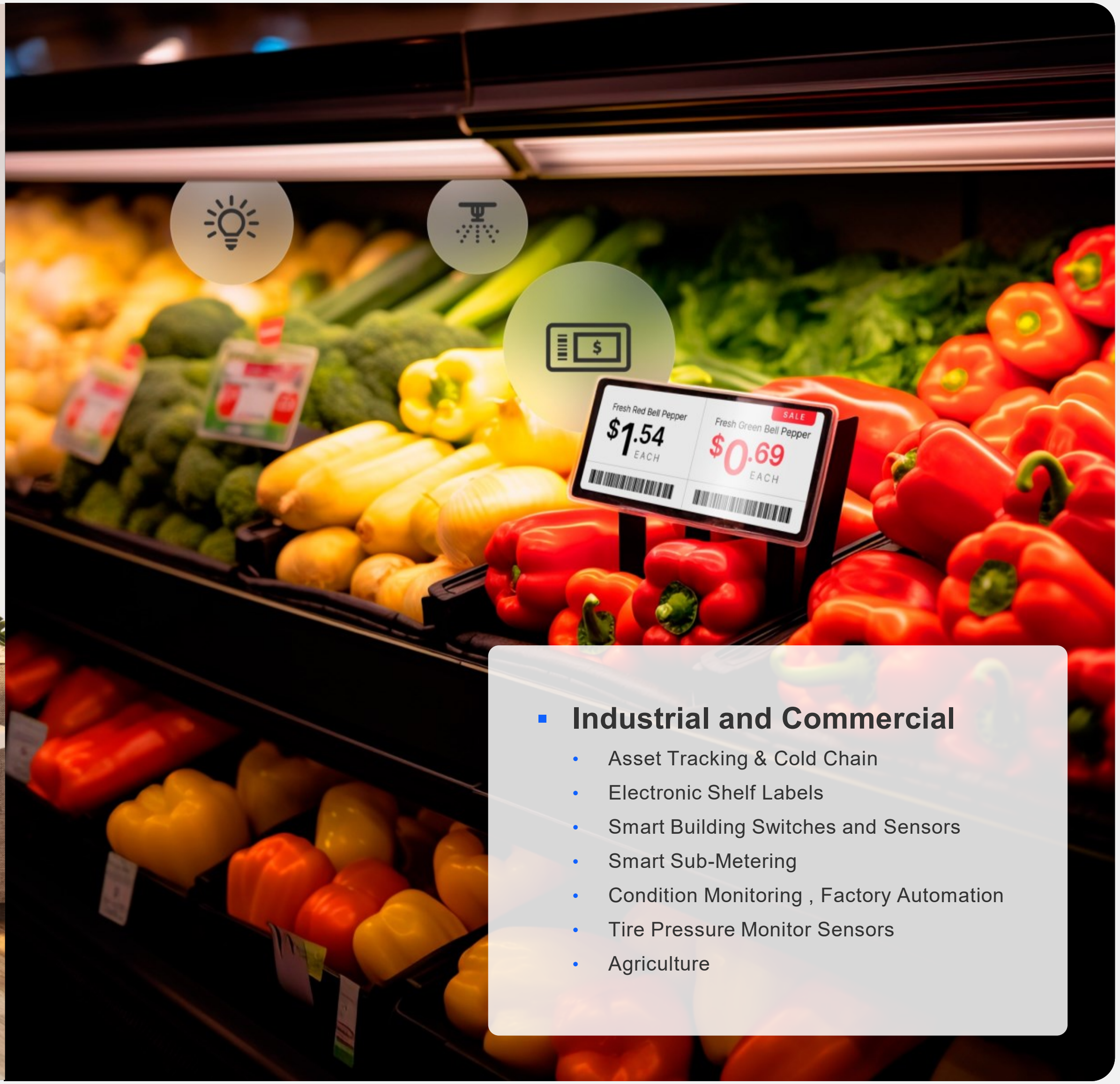


xG22
Startup time: 18.8 ms
Startup Energy: 185 uJ
EM4 wake-up: 9.2 ms
EM4 energy: 76.7 uJ

xG22E
Startup time: 8.01 ms *(-42%)*
Startup Energy: 150 uJ (*-19%)*
EM4 wake-up: 1.83 ms *(-80%)*
EM4 wake-up energy: 16.6 uJ (*-78%)*

Target Markets and Applications

- **Home and Life**
  - Smart Home Doors & Switches
  - Smart Sensors
  - Smart Appliances
  - Gaming Electronics
  - Remote Controllers



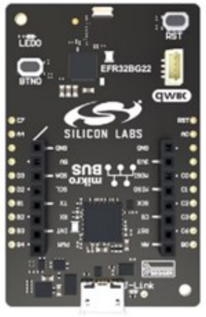
- **Industrial and Commercial**
  - Asset Tracking & Cold Chain
  - Electronic Shelf Labels
  - Smart Building Switches and Sensors
  - Smart Sub-Metering
  - Condition Monitoring , Factory Automation
  - Tire Pressure Monitor Sensors
  - Agriculture

xG22E Value Proposition

- **Minimize Battery Replacement and Recharging**
  - Low run-time and wake-up currents in sleep modes
  - Extended battery life for ultra-low power beacon applications and sensors
- **Compatibility with variety of power sources, power management and harvesters**
  - Exploration into new battery technologies and super-capacitors
  - Compatible with multitude of power management IC's (built-in DC-DC Converter and Voltage Regulator)
  - Integration with energy-harvesting hardware
- **Silicon Lab's first part in Ambient IoT and energy-harvesting**
  - Multiple configurations for energy – DC-DC bypass, LFRCO, Radio PA, etc.
  - Based on existing Series 2 catalogue – pin-to-pin compatible. Short turnaround time to market!
  - Compliant with CSA's energy-harvesting protocol Zigbee Green Power 1.1.2
- **Multiple deep sleep wake-up options**
  - RFSense, GPIO and RTC wake-up sources from deepest EM4 sleep mode.
- **Silicon Labs' Proven Application Expertise**
  - Partner reference designs
  - Simplicity Studio streamlines the development process, reducing costs and accelerating time-to-revenue

Resources

Getting Started with EFR32xG22E



- **NEW Explorer Kit – June 2024**
  - Isolated debug circuit for lowest power
  - mikroBus socket
  - Qwiic connector
- **Contents**
  - 1x Explorer board

Part Number	Description
EK2710A- BRD2710A	EFR32MG22E Explorer Kit

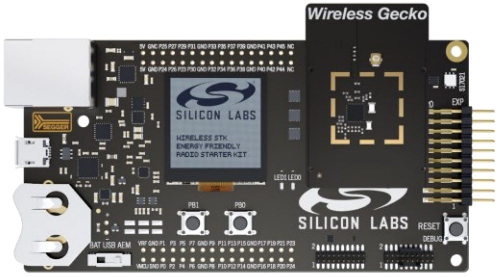
NEW Explorer Kit Shield – TBA (24Q3)

- mikroBus socket
- Qwiic connector
- E-peas PMIC shields

Contents

- 1 Explorer board
- 3x Energy Shields

Part Number	Description
EK8200A	EFR32xG22E Explorer e-peas shield
BRD8201A	Alternate battery and super-capacitors
BRD8202A	AEM0300 PMIC for kinetic pulse sources
BRD8203A	AEM13920 PMIC for dual energy source



Radio Board kits – May 2024

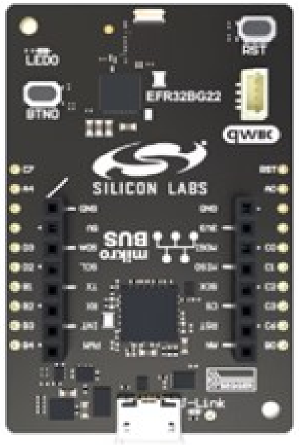
- Uses existing WSTK boards
- Uses existing software tools

Contents

- 1x radio board

Part Number	Description
xG22E-RB4415A	EFR32xG22E 2.4 GHz +6 dBm Radio Board (QFN40)
SLWRBRD4415A	

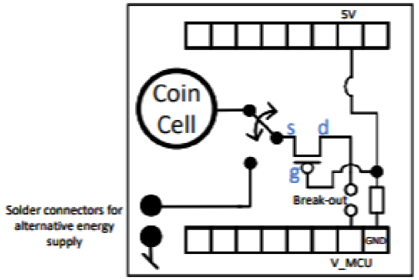
Introducing xG22E Explorer Kit e-peas Shields for energy-harvesting



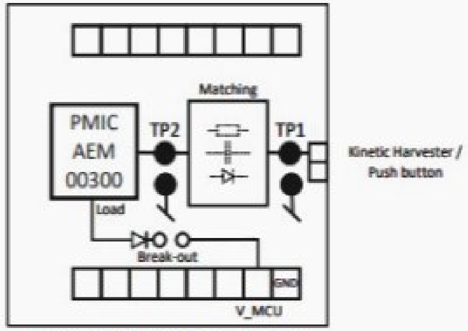
NEW Explorer Kit: redesigned to minimize leakage and isolation of debugger circuit

Shield interface expansion boards:
A: Transistor rectifier
B: Diode rectifier
C: Over-voltage protection
D: Additional input capacitance

Shield #1 for alternative battery technologies and storage options with measurements



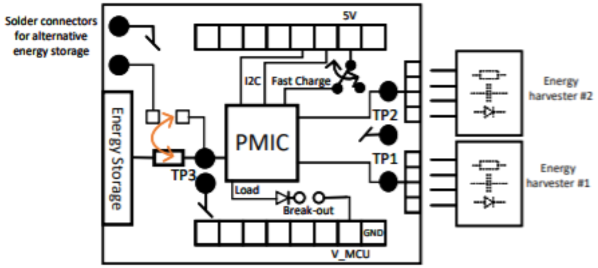
Battery Supply Shield



Kinetic Harvester Shield

Shield #2 dedicated for evaluating kinetic/pulse harvest generators with measurements.

Shield #3 for dual harvest sources (PV, Thermal, Vibration, bricks) with measurements



Dual Harvester Shield

Reference Materials

Website / Announcements:

- silabs.com/wireless/energy-harvesting
- silabs.com/blog/building-a-more-sustainable-connected-world-with-xg22e

WorksWith:

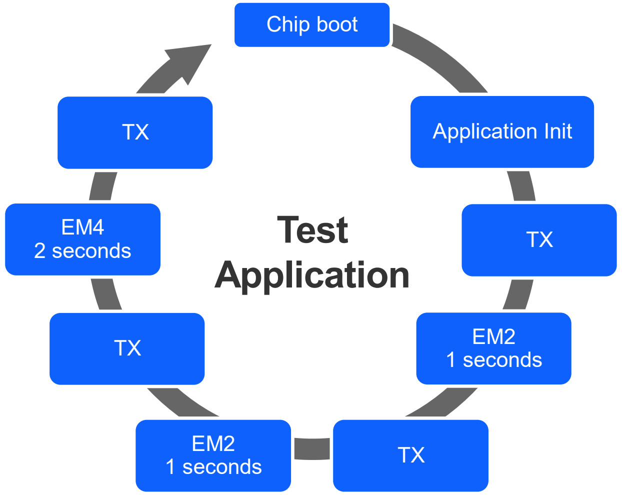
□ 2023 – IOT104 – *Energy Harvesting for Low Power Wireless*
- 2022 – APP104 – *Factory Monitoring with Thermal Harvesting*
- 2020 – EH202 – *Building Energy Harvest Devices*

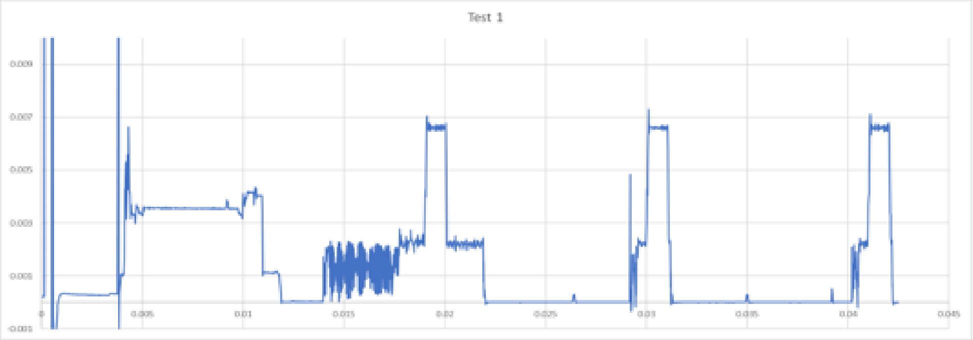
Reference Designs / White-papers:

- Thermal Energy example
- Kinetic Switch example
- PV Cell example

Additional resources:

□ resources.mouser.com/energy-harvesting
□ Power Electronics News – energy harvesting





REFERENCE EXAMPLES:

- Zigbee Green Power for kinetic push buttons - github
- Bluetooth for solar asset tags - github

Q&A

BLUETOOTH

Thank you

tech talks

BLUETOOTH