

# STM32WB

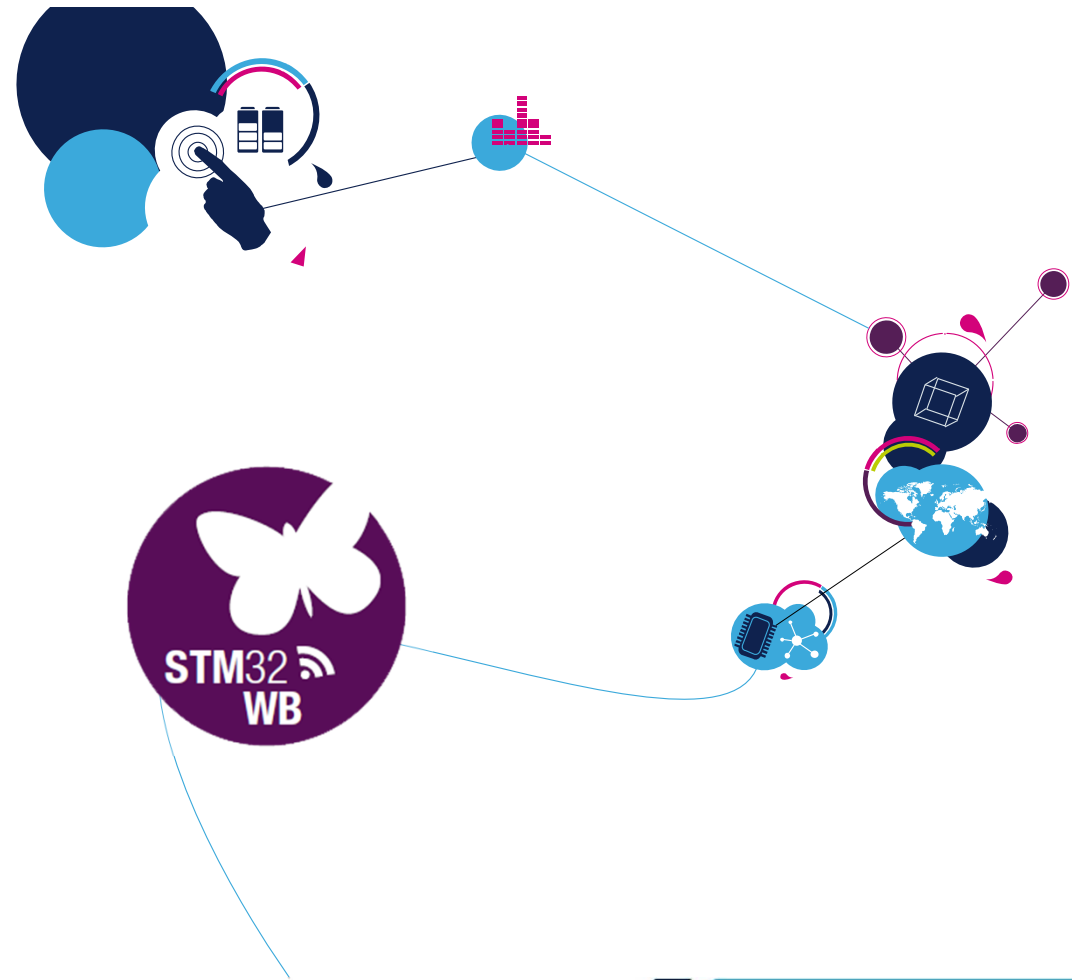
## Wireless MCUs

### BLE 5 and IEEE 802.15.4

Joe Tijerina  
Field Applications Engineer

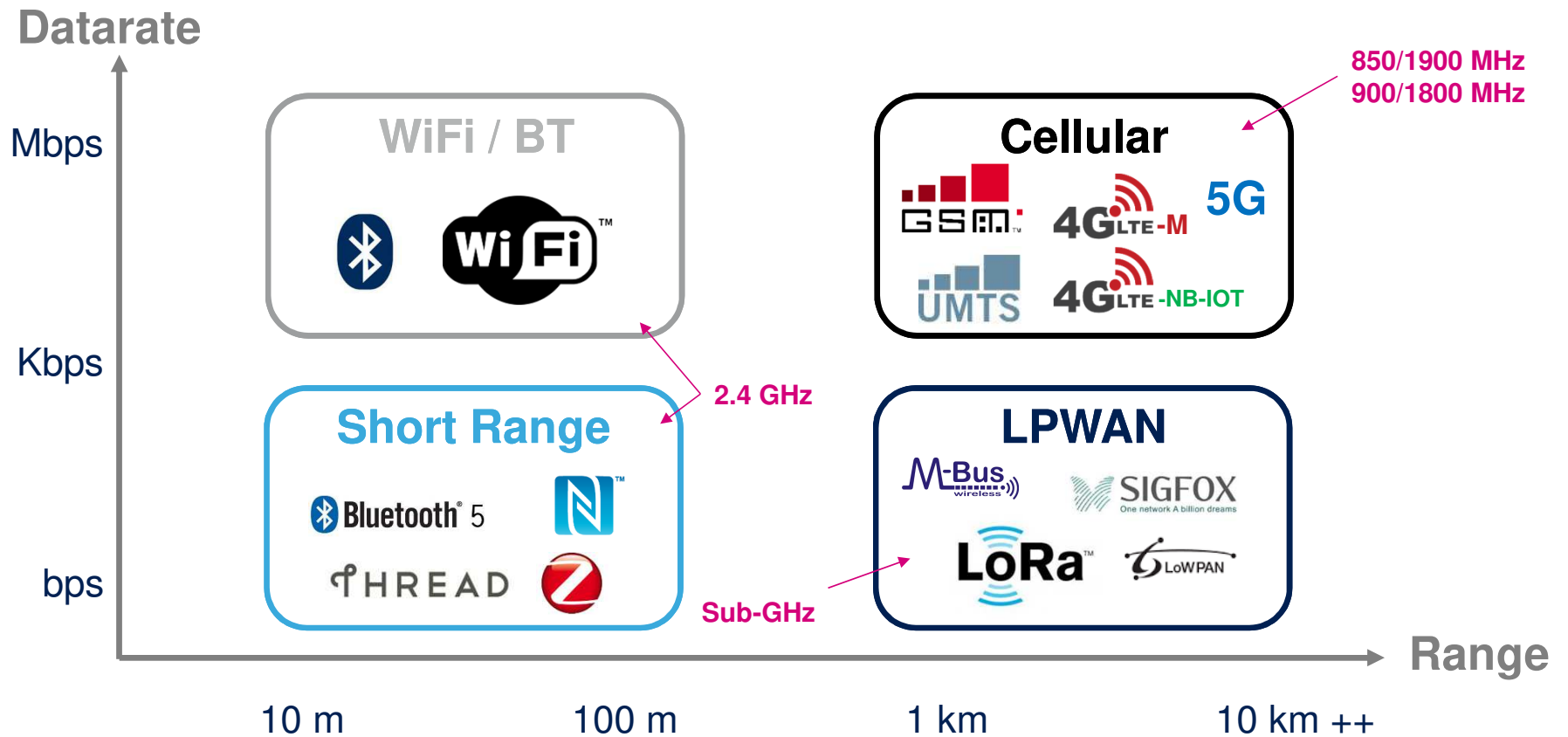


Technology Tour 2019  
Anaheim, CA | March 26





# Communication Technologies





# Low-data rate apps



Insulin Pump



Hearing aid



Watches



Glasses



Tag locator



Fitness



Alarm



Heating/Cooling



Door lock



White goods



Smoke detectors



Lighting



## Bluetooth LE

Point-to-point communication with smartphones and other wireless devices



## BLE Mesh / 802.15.4

Home automation with Mesh network need



# Your Smartphone is your GUI!



# BLE & 802.15.4





# STM32WB Key Takeaways



**Multi-protocol**



**Dual-core**



**Secure**



# Multiprotocol



 **Bluetooth  
5**

- Fully certified
- 2Mbps
- BLE Mesh



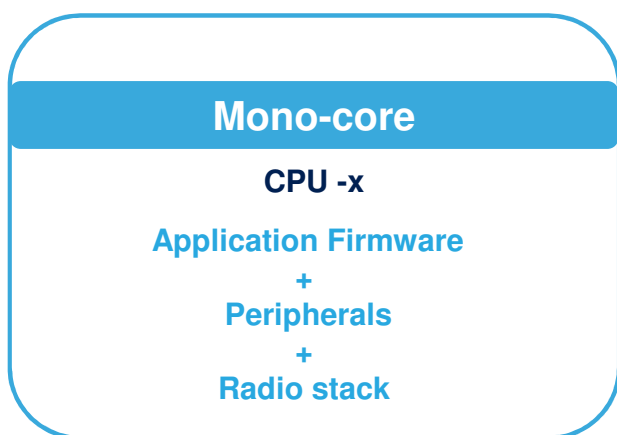
- Zigbee 3.0
- OpenThread
- Concurrent BLE + OpenThread

**2.4 GHz  
Open**

- OpenMAC

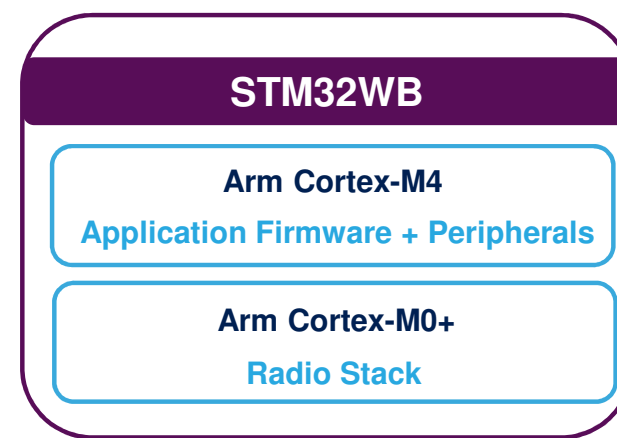


# Dual-Core



- **Drawbacks**

- Time sharing
- Companion MCU?



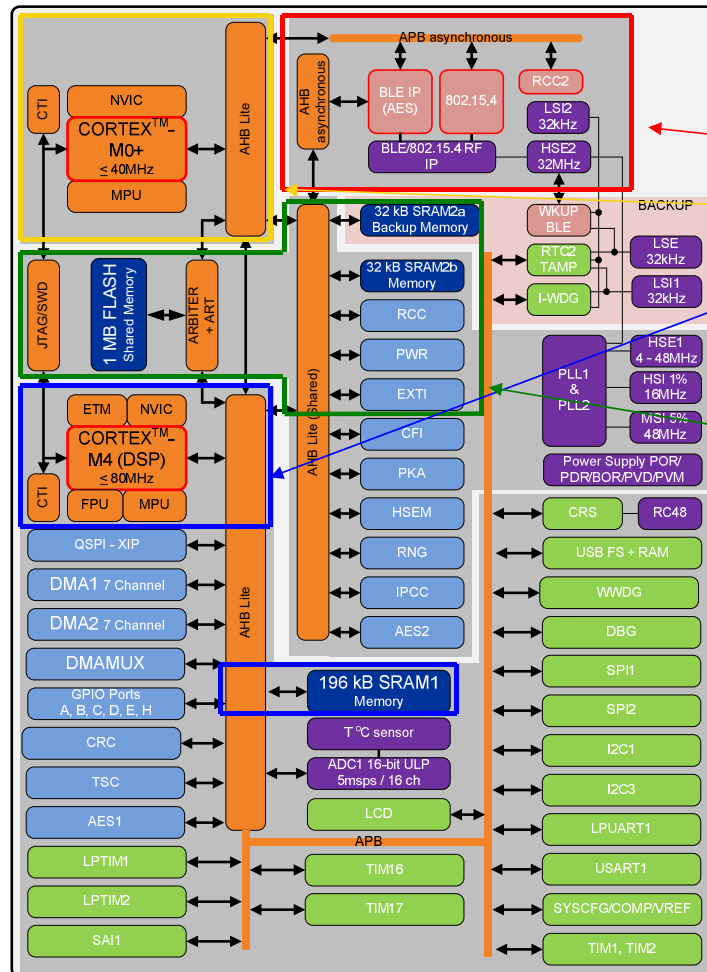
- **Benefits**

- Single-die SoC solution
- Lower power
- Cost
- Time-to-market





# Architecture

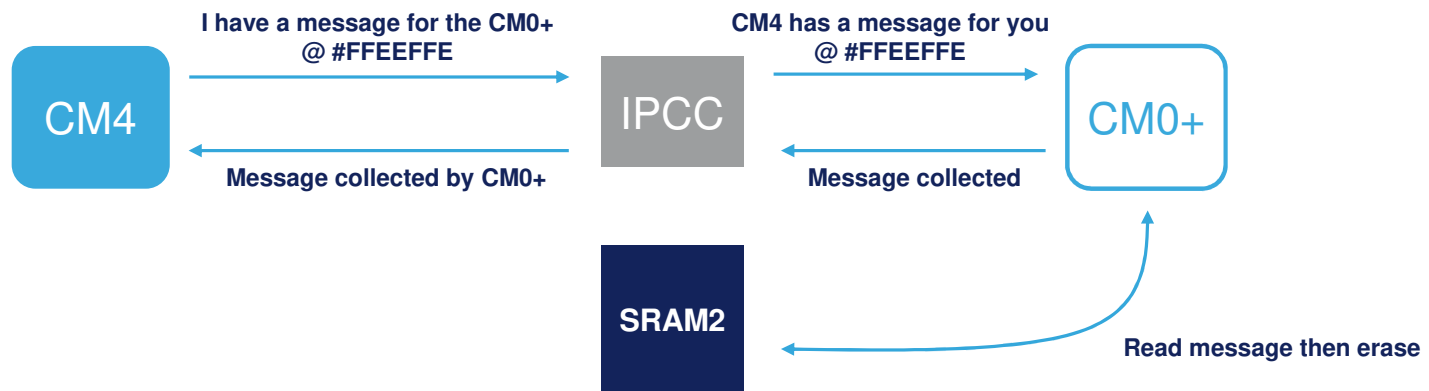


- 3 autonomous sub-systems
  - Radio sub-system
  - Cortex-M0+ (CPU2)
  - Cortex-M4 (CPU1)
- Common run domain
  - Flash, SRAM2, RCC, PWR, EXTI



# Dual core – How does that work?

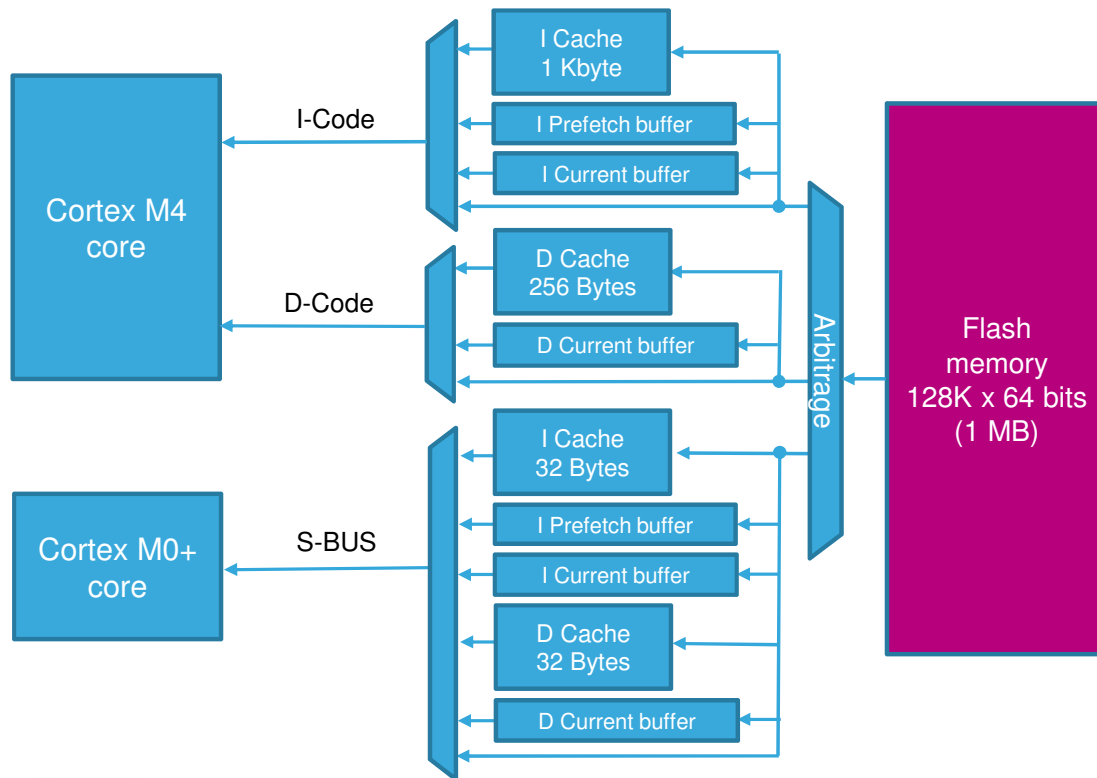
- HSEM: Hardware Semaphore – prevent shared resource access conflicts
- IPCC: Inter Processor Communication Controller



*IPCC works in both directions*



# ART Accelerator™



- **Cortex-M4**

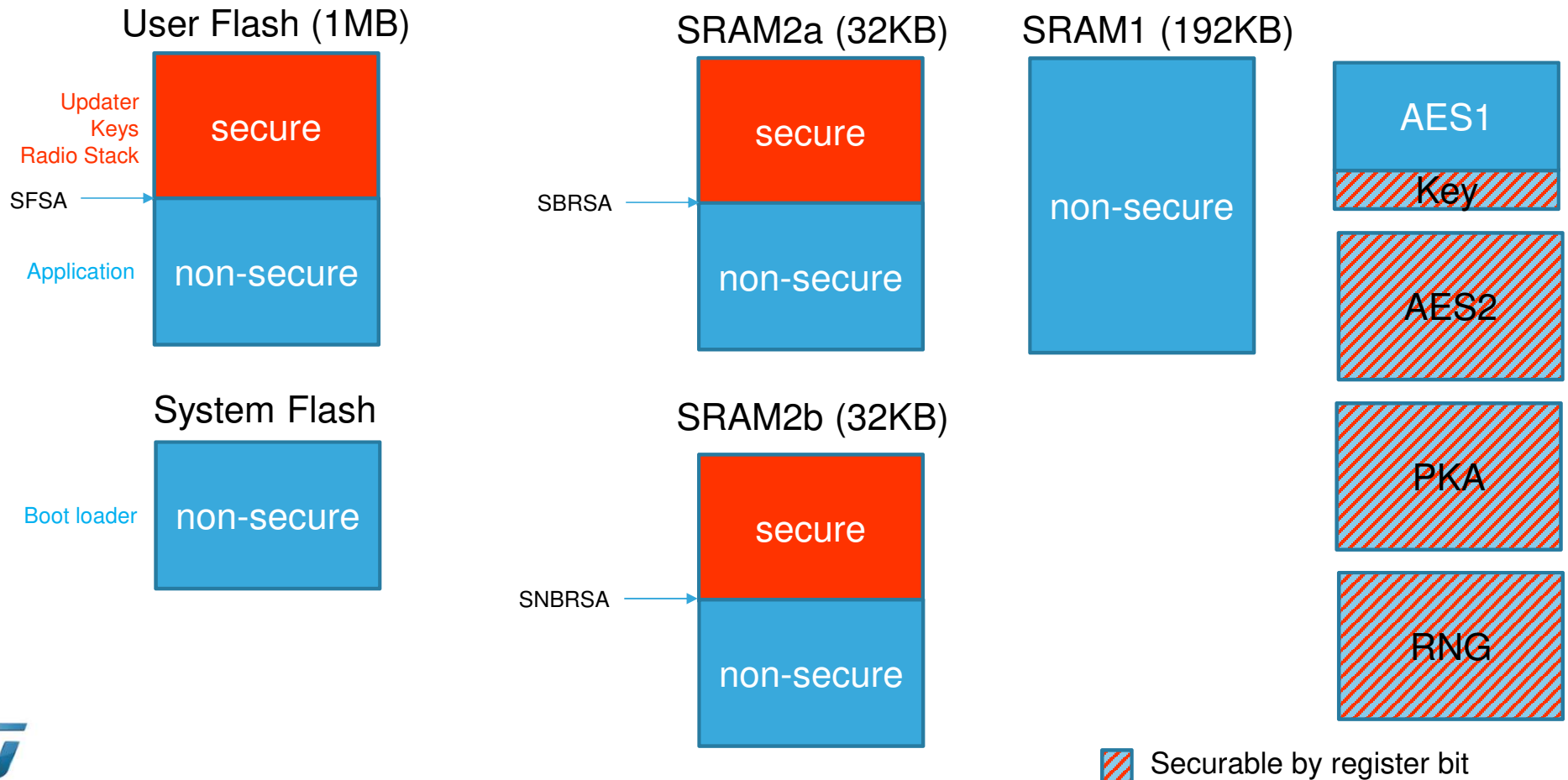
- **Instruction cache** = 32 lines of 4x64 bits
- **Data cache** = 8 lines of 4x64 bits
- **Pre-fetch buffer**

- **Cortex-M0+**

- **Instruction cache** = 4 lines of 1x64 bits
- **Data cache** = 4 lines of 1x64 bits
- **Pre-fetch buffer**

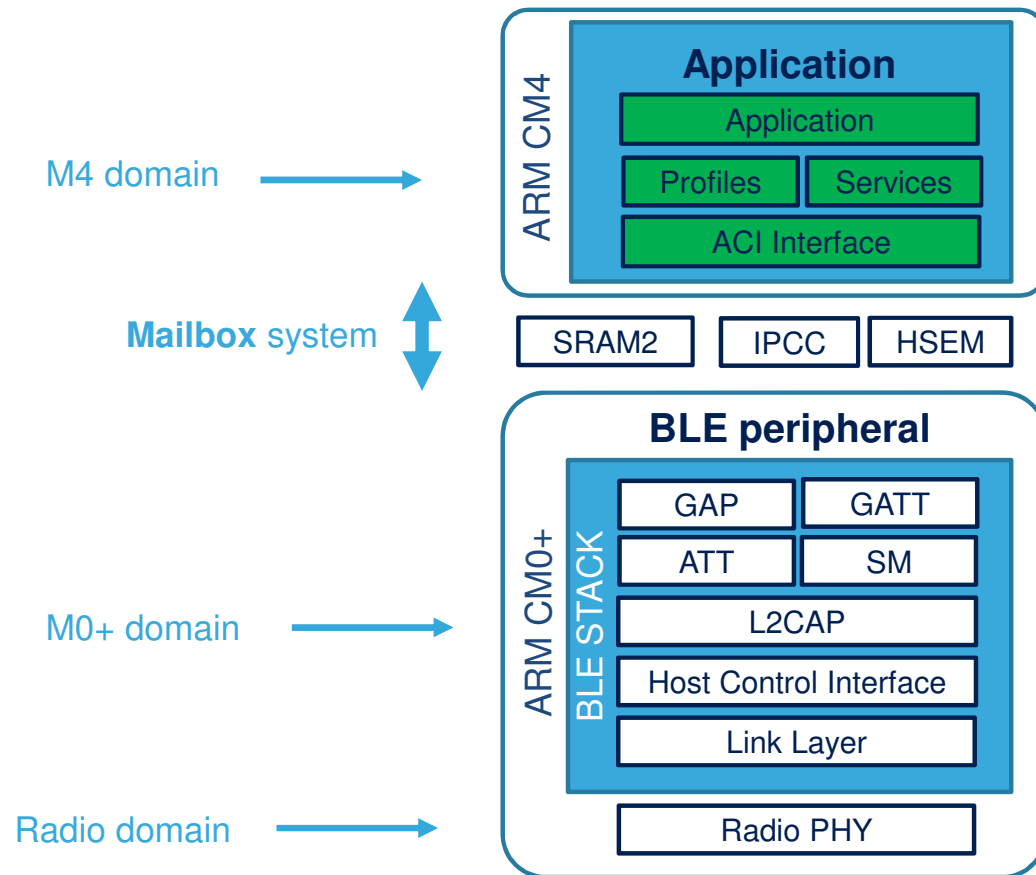


# Security





# Protocol Stack layers



# Classic vs Low Energy

Comparison of Classic and Low Energy		
	Classic (BR/EDR)	Low Energy (LE)
Application	Cell phones, headsets, stereo/audio streaming, automotive (handsfree), PCs, etc.	Smartwatches, sport & fitness, home electronics, automation, industry, healthcare, smartphones, etc.
Voice	Yes	No
RF band ISM	2.4 GHz	2.4 GHz
Energy consumption	Reference	0.5...0.01 times Classic as reference
Coverage	10 m	≥ 10 m
Power	3 classes (max.): <ul style="list-style-type: none"> <li>+20 dBm</li> <li>+4 dBm</li> <li>0 dBm</li> </ul>	max. +20 dBm four informative classes
Connection	Inquiry Yes, always hopping	Advertising Connection only if necessary, then hopping
Connection setup	100 ms	6 ms
RF channels	79 with 1 MHz spacing	40 with 2 MHz spacing <ul style="list-style-type: none"> <li>3 advertising</li> <li>37 data (+ secondary advertising)</li> </ul>
Modulation	GFSK <ul style="list-style-type: none"> <li>BT = 0.5</li> <li>Deviation = 160 kHz</li> <li>Mod index = 0.28...0.35</li> </ul> π/4-DQPSK 8DPSK	GFSK <ul style="list-style-type: none"> <li>BT = 0.5</li> <li>Deviation = 250 kHz or 500 kHz</li> <li>Mod index = 0.45...0.55</li> <li>Stab Mod index = 0.495...0.505</li> </ul>
Gross data rate	1...3 Mbit/s	1...2 Mbit/s
Application data rate	0.7...2.1 Mbit/s	0.2...0.6 Mbit/s

100X lower power

Longer range

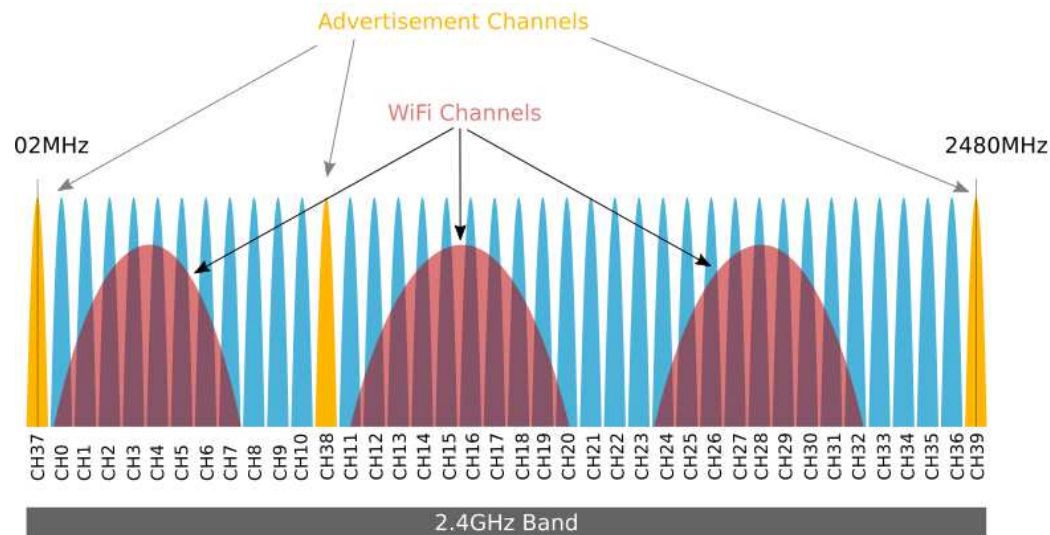
Fast connection (only 3 advertising channels to scan)

Relaxed RF requirements

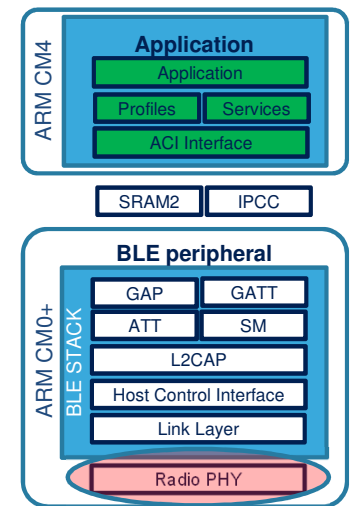
# PHY

Strategically placed advertising channels

Remaining 37 channels are data channels



	BLE	Classic	
	BLE	BR	EDR
Modulation	GFSK 0.45 to 0.55	GFSK 0.28 to 0.35	DQPSK / 8DPSK
Data Rate	1 Mbit/s	1 Mbit/s	2 and 3 Mbit/s
Channels	40	79	79
Spacing	2MHz	1MHz	



# Basic RF System Front-End

**Balun** – Combine TX and RX signals

**Matching Network** – 50  $\Omega$  impedance transformation

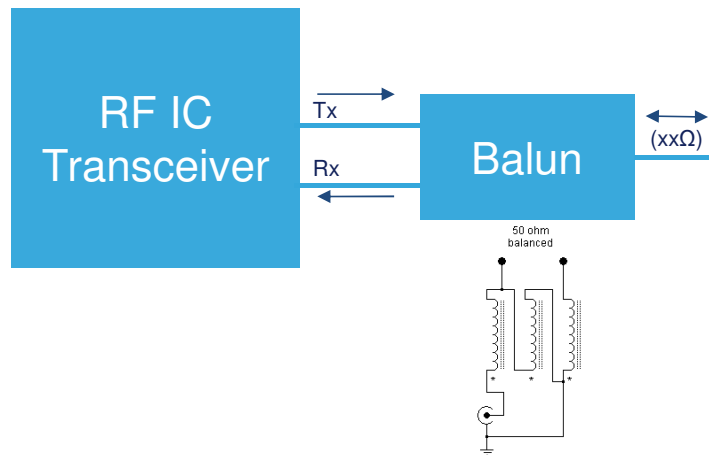
**Harmonic Filter** – Reduce out-of-band harmonics

# Basic RF System Front-End

**Balun** – Combine TX and RX signals

**Matching Network** – 50  $\Omega$  impedance transformation

**Harmonic Filter** – Reduce out-of-band harmonics

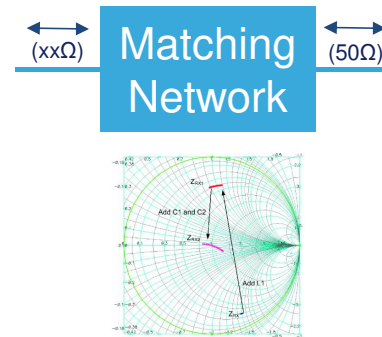


# Basic RF System Front-End

**Balun** – Combine TX and RX signals

**Matching Network** – 50  $\Omega$  impedance transformation

**Harmonic Filter** – Reduce out-of-band harmonics

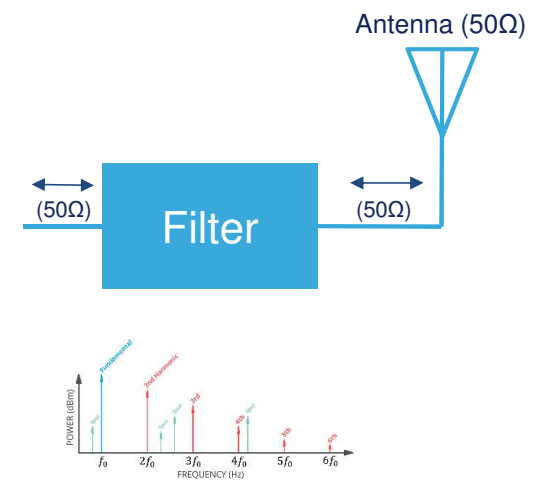


# Basic RF System Front-End

**Balun** – Combine TX and RX signals

**Matching Network** – 50  $\Omega$  impedance transformation

**Harmonic Filter** – Reduce out-of-band harmonics

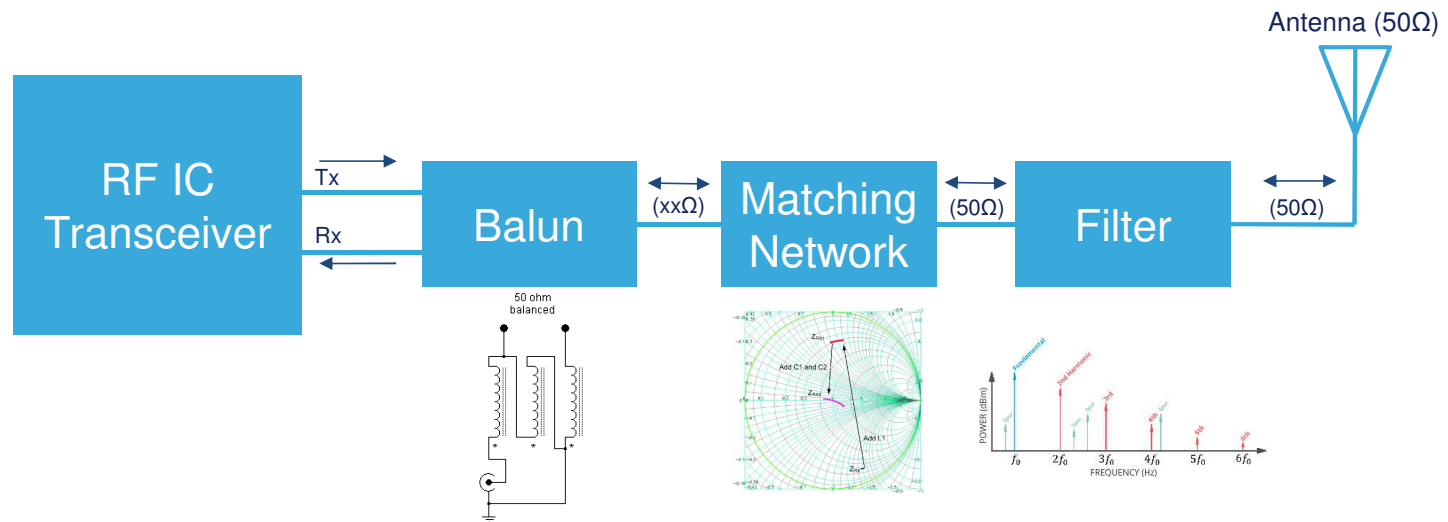


# Basic RF System Front-End

**Balun** – Combine TX and RX signals

**Matching Network** – 50  $\Omega$  impedance transformation

**Harmonic Filter** – Reduce out-of-band harmonics

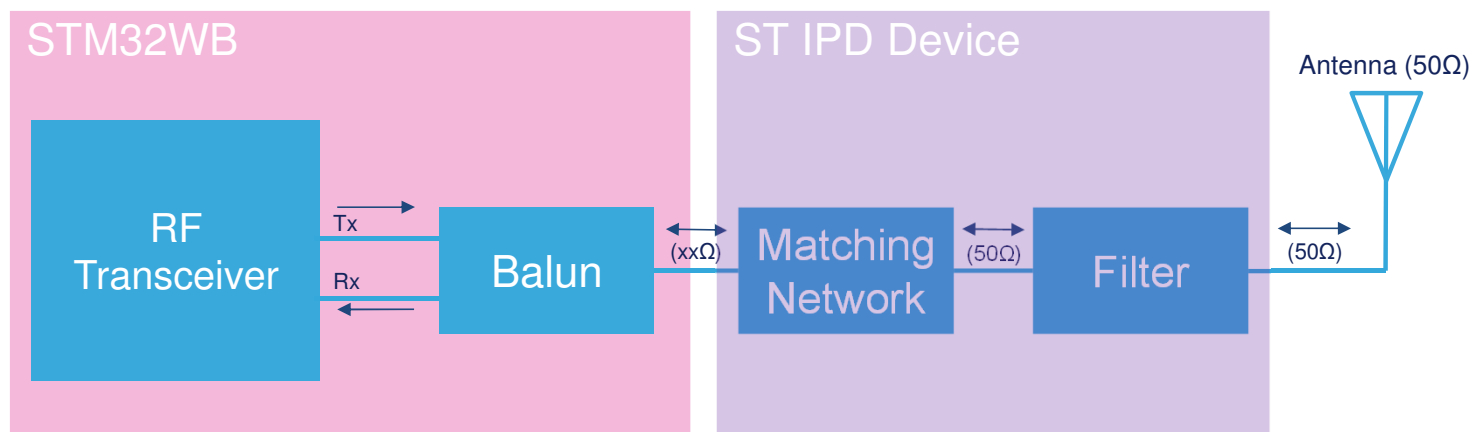


# Basic RF System Front-End

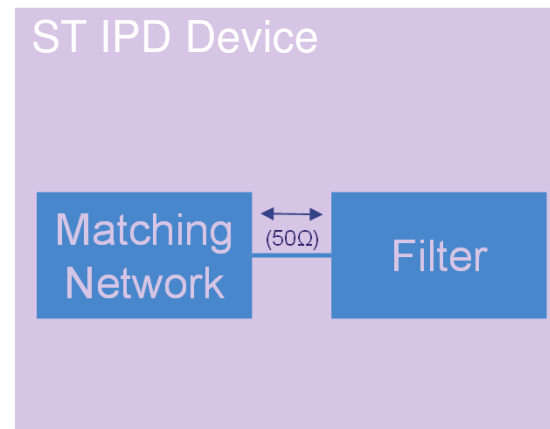
**Balun** – Combine TX and RX signals

**Matching Network** – 50  $\Omega$  impedance transformation

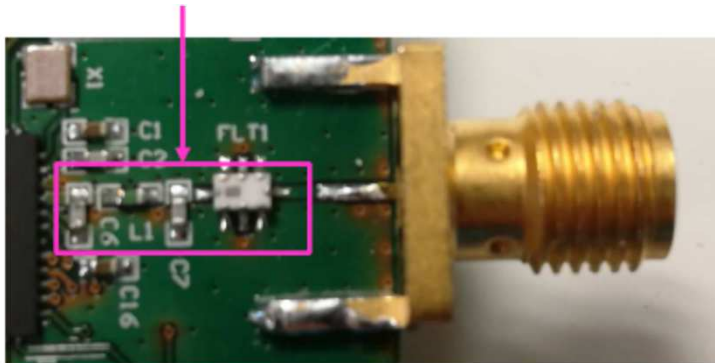
**Harmonic Filter** – Reduce out-of-band harmonics



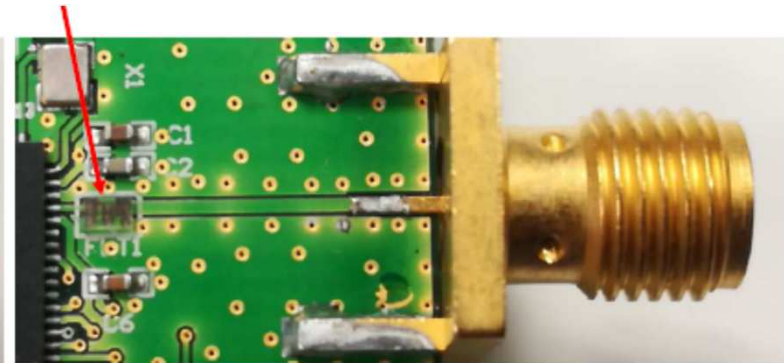
# Matching Network + Harmonic Filter



Discrete network & filter in STM32WB ref design



MLPF-WB55-01E3 IPD device



Sampling NOW

Production in March

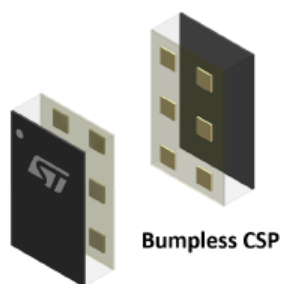


# IPD Filter

MLPF-WB55-01E3

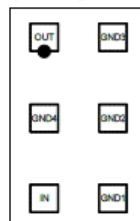
Datasheet

2.4 GHz low pass filter matched to STM32WB55Cx/Rx



Bumpless CSP

Top view (pads down)



## Features

- Integrated impedance matching to STM32WB55Cx and STM32WB55Rx
- LGA footprint compatible
- 50  $\Omega$  nominal impedance on antenna side
- Deep rejection harmonics filter
- Low insertion loss
- Small footprint
- Low thickness  $\leq 450 \mu\text{m}$
- High RF performance
- RF BOM and area reduction
- ECOPACK®2 compliant

## Applications

- Bluetooth 5
- OpenThread
- Zigbee®
- IEEE 802.15.4
- Optimized for STM32WB55Cx and STM32WB55Rx

1mm x 1.6mm CSP

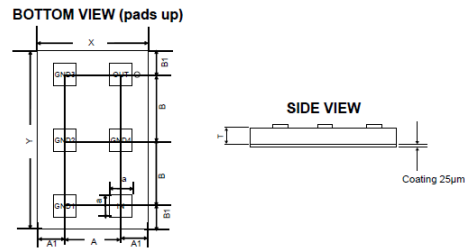
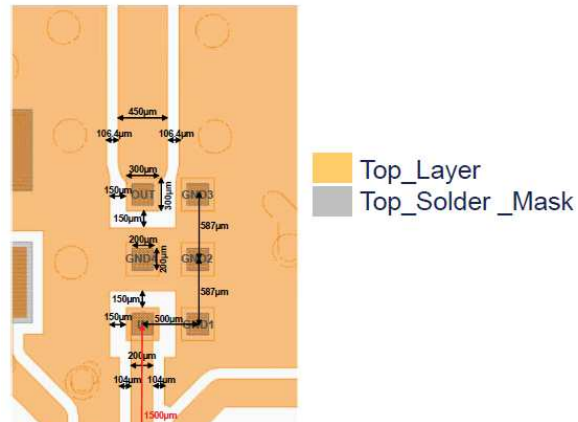


Table 4. Bumpless CSP package mechanical data

Parameter	Description	Min.	Typ.	Max.	Unit
X	X dimension of the die	975	1000	1025	µm
Y	Y dimension of the die	1575	1600	1625	µm
A	X pitch		500		µm
B	Y pitch		587		µm

Figure 13. PCB land pattern recommendations



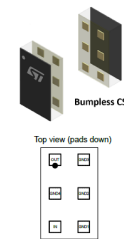
# IPD Filter



MLPF-WB55-01E3

Datasheet

2.4 GHz low pass filter matched to STM32WB55Cx/Rx



## Features

- Integrated impedance matching to STM32WB55Cx and STM32WB55Rx
- LGA footprint compatible
- 50 Ω nominal impedance on antenna side
- Deep rejection harmonics filter
- Low insertion loss
- Small footprint
- Low thickness ≤ 450 µm
- High RF performance
- RF BOM and area reduction
- ECOPACK<sup>®</sup>2 compliant

## Applications

- Bluetooth 5
- OpenThread
- Zigbee<sup>®</sup>
- IEEE 802.15.4
- Optimized for STM32WB55Cx and STM32WB55Rx

# Link Layer State Machine

- **Standby** state: Sleep, Stop, Standby
- **Advertising** is the key to initiating all BLE communications!
- As an **Initiator** and **Advertiser** negotiate a **Connection**, the Initiator becomes a “*Master*” and Advertiser becomes a “*Slave*”
- In a Connection
  - The Link-Layer **Master** is also the GAP **Central**
  - The Link-Layer **Slave** is also the GAP **Peripheral**

Up to 8 simultaneous State Machines!

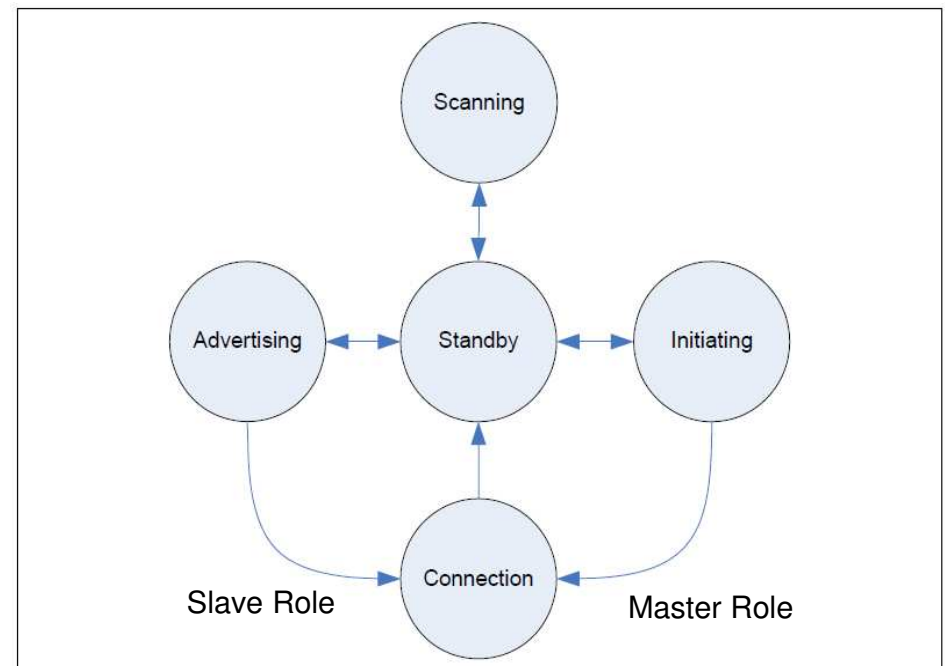
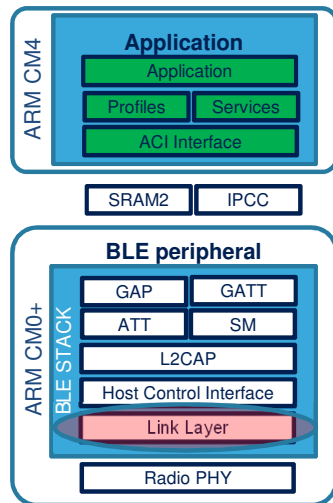
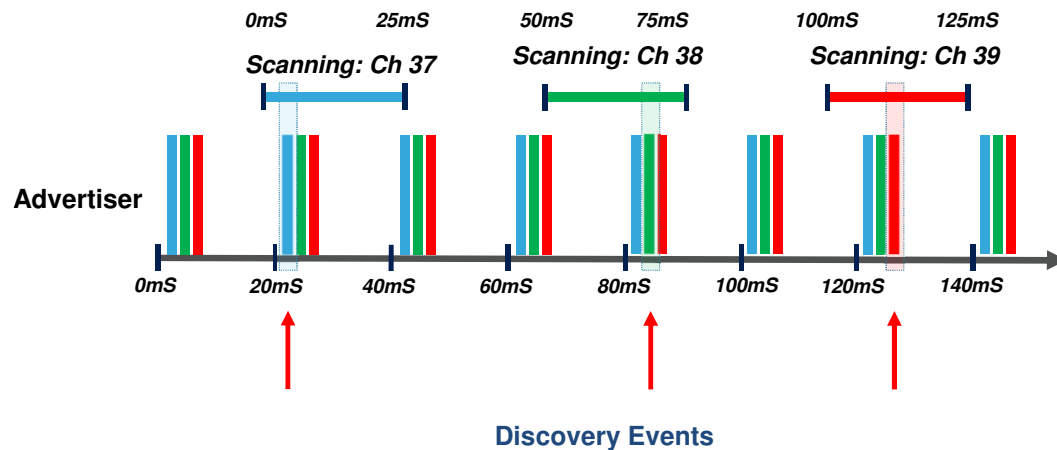



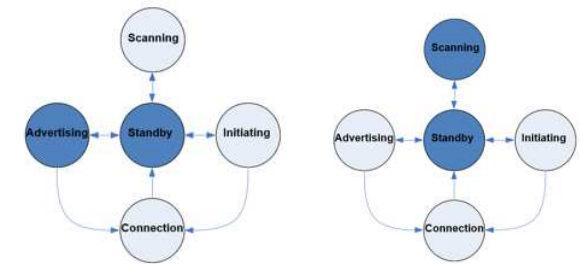


Figure 1.1: State diagram of the Link Layer state machine

# Discovery: Advertising & Scanning



Advertising on Ch 37:   
Advertising on Ch 38:   
Advertising on Ch 39: 



## Advertiser Settings:

- Advertising Interval: 20mS

## Scanner Settings:

- Scan Interval: 50mS
- Scan Window: 25mS

# GAP (Generic Access Profile)

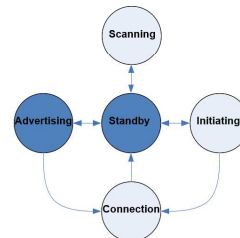
- Roles and Modes

- Advertising Mode
- Connected Mode



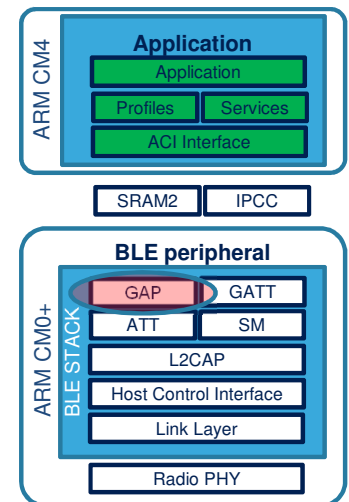
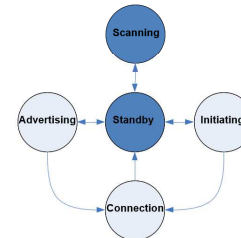
**Broadcaster**

Sends advertising events  
Can include characteristics and service data  
Doesn't need receiver  
Can be discoverable if it does have receiver



**Observer**

Receives advertising events  
Listens for characteristics and service data  
Doesn't need transmitter  
Can discover devices if it does have transmitter



# GAP (Generic Access Profile)

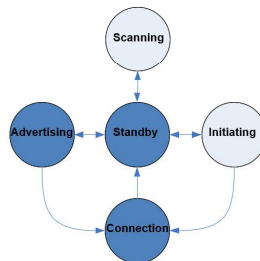
- Roles and Modes

- Advertising Mode
- Connected Mode



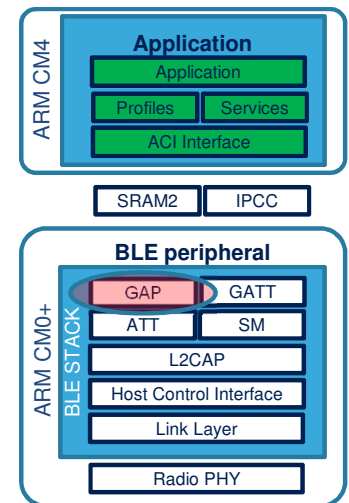
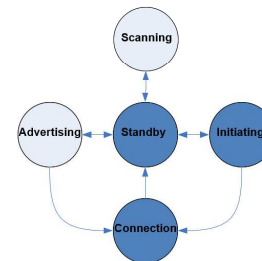
**Peripheral**

Has transmitter and receiver  
Always slave  
Connectable advertising



**Central**

Has transmitter and receiver  
Always master  
Never advertises



# GATT (Generic Attribute Profile)

GAP Central is also a “GATT Client”

GAP Peripheral” is also a “GATT Server”

- Central queries the Services available
  - Peripheral **Services** and **Characteristics** are exposed via its’ **GATT** database

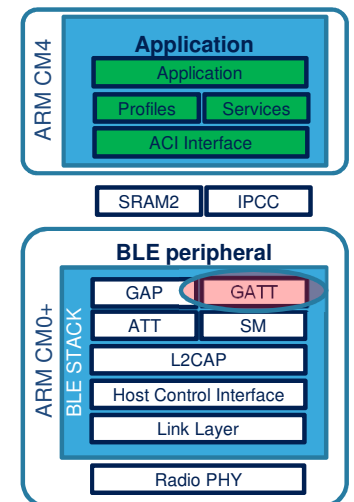


What is my heartrate?

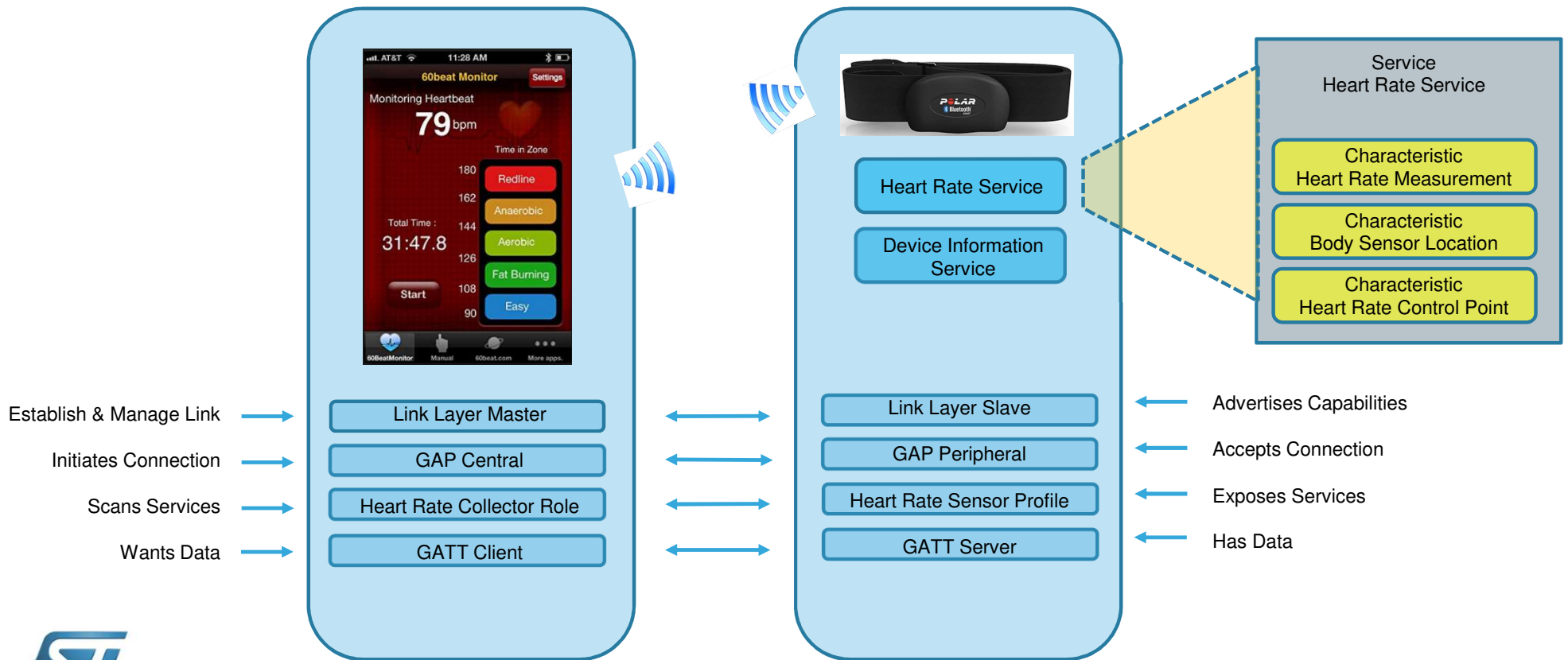
147 bpm

What is your Mfr ID?

Polar



# GATT: Profiles, Services and Characteristics



# Bluetooth SIG

[Help & Support](#)[Join the SIG](#)[TECHNOLOGY](#)[MARKETS](#)[DEVELOP WITH BLUETOOTH](#)[SPECIFICATIONS](#)[RESOURCES](#)

## All signs point to blue

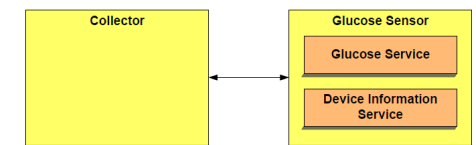
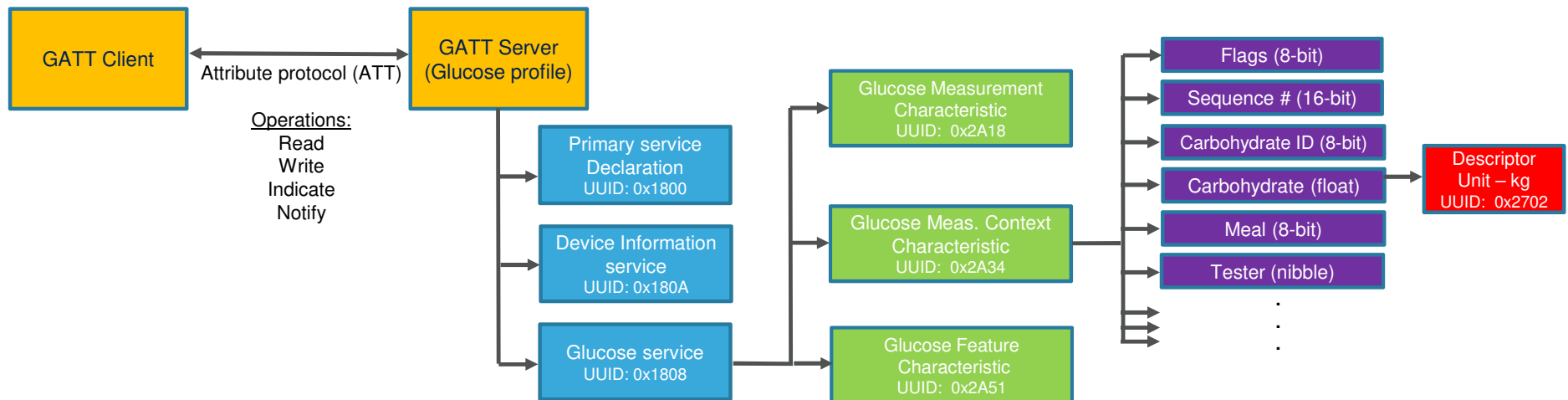
Introducing Bluetooth direction finding

[Read More](#)

[www.bluetooth.com](http://www.bluetooth.com)

# GATT Glucose Profile

GLP Profile defines two roles: Collector & Glucose Sensor





# Bluetooth MESH

- MESH is application on top of BLE stack
  - “Managed-flood-based” mesh network
- Mesh vs BLE
  - Mesh offers unlimited end-points vs 8 with standard BLE
- Apps:
  - Building automation : Lighting, HVAC, Security
  - Asset tracking
  - Smart waste management
- <https://www.bluetooth.com/specifications/mesh-specifications>



## 2 Mesh system architecture

This section provides an overview of the mesh network operation and layered system architecture.

### 2.1 Layered architecture

The Mesh Profile specification is defined as a layered architecture as shown in Figure 2.1.





# Thread

**WHAT IS THREAD?**

Thread was designed with one goal in mind: to create the best way to connect & control products in the home.

[WATCH VIDEO](#)

The banner is framed by a series of white line-art icons on an orange background. The top row includes icons for a power outlet, a light bulb, a window blind, a coffee maker, a smartphone, a battery, a fan, and a smart plug. The bottom row includes icons for a house, a smartphone, a thermostat, a door handle, a washing machine, a radiator, a door, and a faucet.

The video player shows a woman sitting on a couch in a modern living room, with the text "Built on Thread" in the top left corner of the video frame.



# Thread

## THREAD What it delivers

### A secure wireless mesh network for your home and its connected products

Built on well-proven, existing technologies

Uses 6LoWPAN and carries IPv6 natively

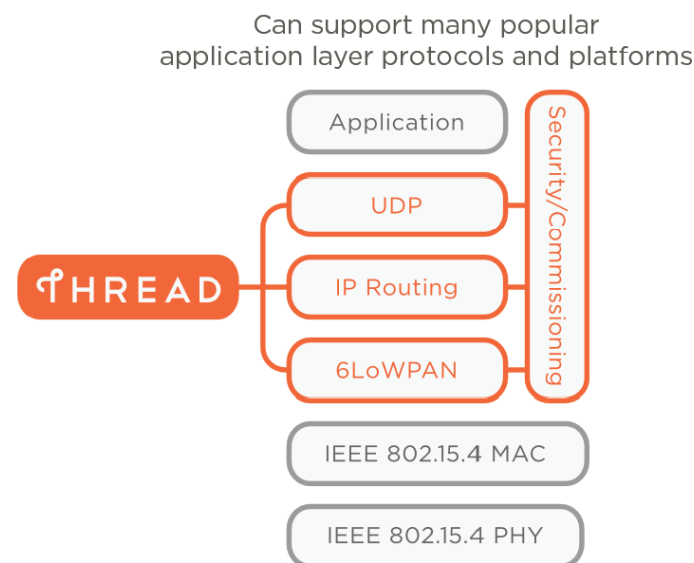
Runs on existing 802.15.4 silicon

New security architecture to make it simple and secure to add / remove products

250+ products per network

Designed for very low power operation

Reliable for critical infrastructure



A software upgrade can add Thread to currently shipping 802.15.4 products



# Thread

## THREAD Direct Addressability of devices

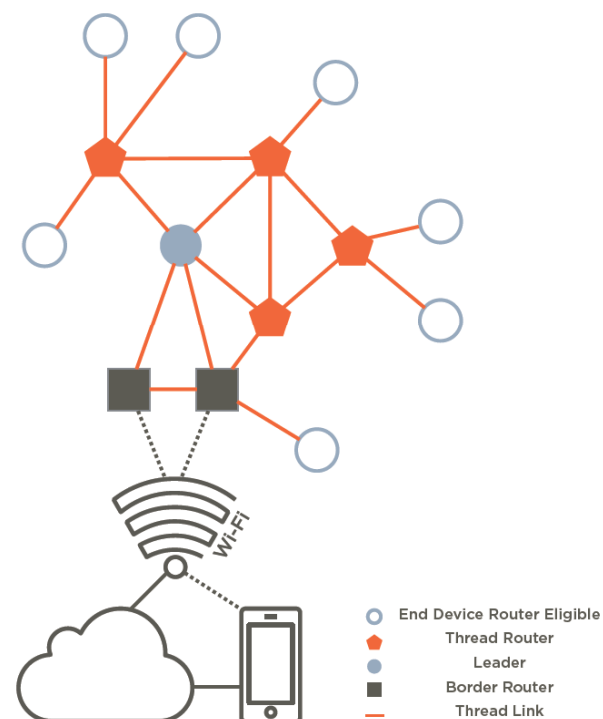
All devices have IPv6 addresses plus short address on HAN

DHCPv6 used for router address assignment

Home Network can directly address devices through Border Routers

Cloud Services can address devices from the Internet

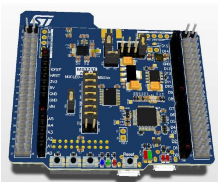
Devices can address local devices on HAN or off network devices using normal IP addressing



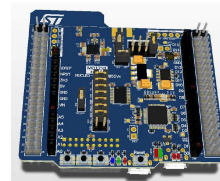


# COAP based

Push Button



*COAP request (LED on)*



- Msg Type: { CON/**NON**/ACK/RST }
- Msg Code: { GET/**PUT**/POST/ACK }

kCoapTypeNonConfirmable  
kCoapRequestPut

- Dest Addr:
- Port
- UriPath :

FF03::1  
5683  
"light"



# BLE / Thread Concurrent modes

## Static Concurrent Mode

→ Switching from BLE to Thread as two **exclusive** modes

## Dynamic Concurrent Mode

→ Switching from BLE mode to Thread mode within **polling loop**



# BLE / Thread Concurrent modes

## Static Concurrent Mode

→ Switching from BLE to Thread as two **exclusive** modes

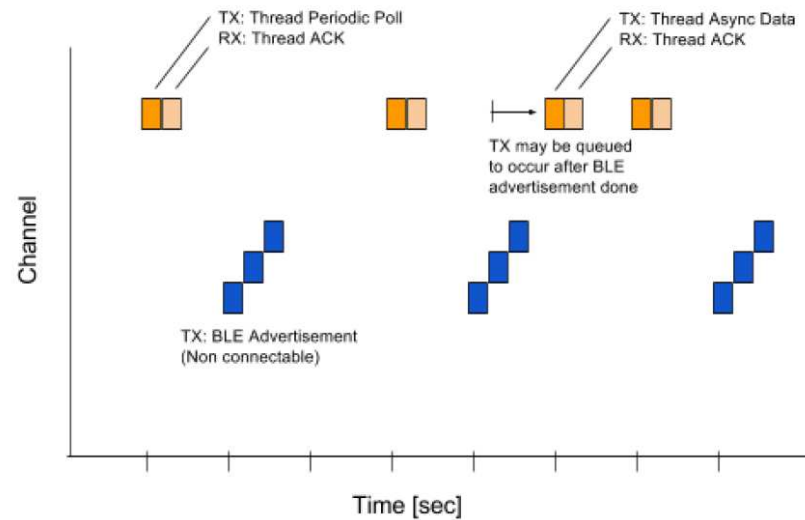
## Dynamic Concurrent Mode

→ Switching from BLE mode to Thread mode within **polling loop**

### Thread + BLE Beacon

Thread

Bluetooth





# BLE / Thread Concurrent modes

## Static Concurrent Mode

→ Switching from BLE to Thread as two **exclusive** modes

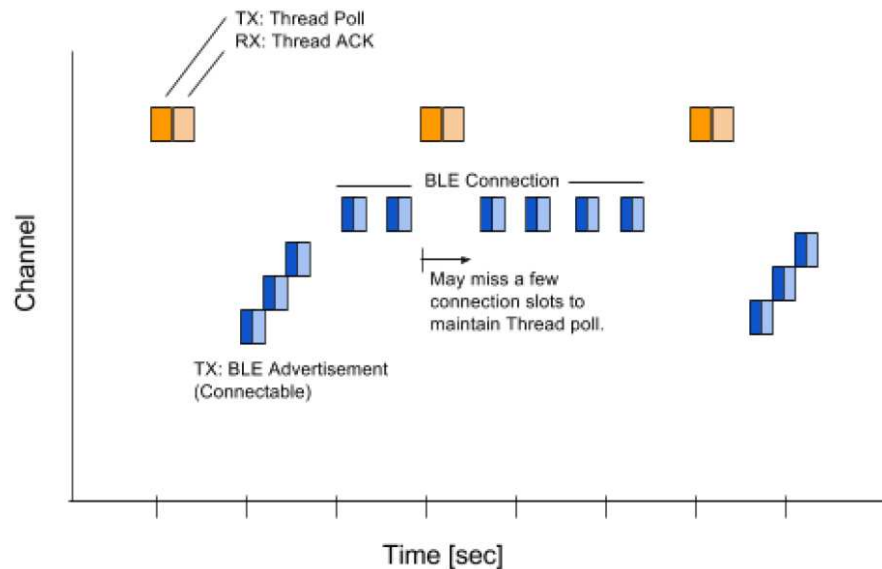
## Dynamic Concurrent Mode

→ Switching from BLE mode to Thread mode within **polling loop**

### Thread + BLE Connection

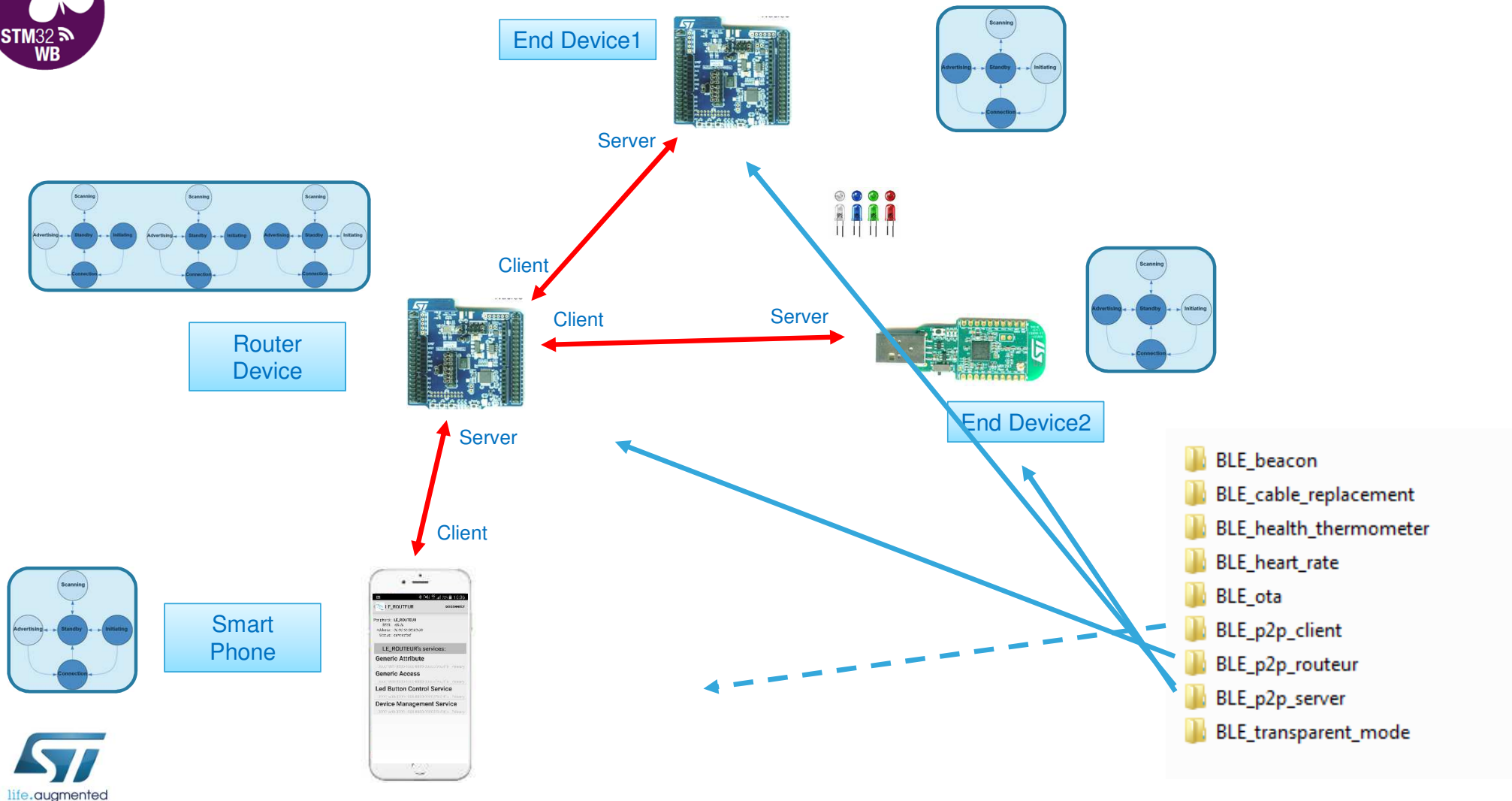
Thread

Bluetooth



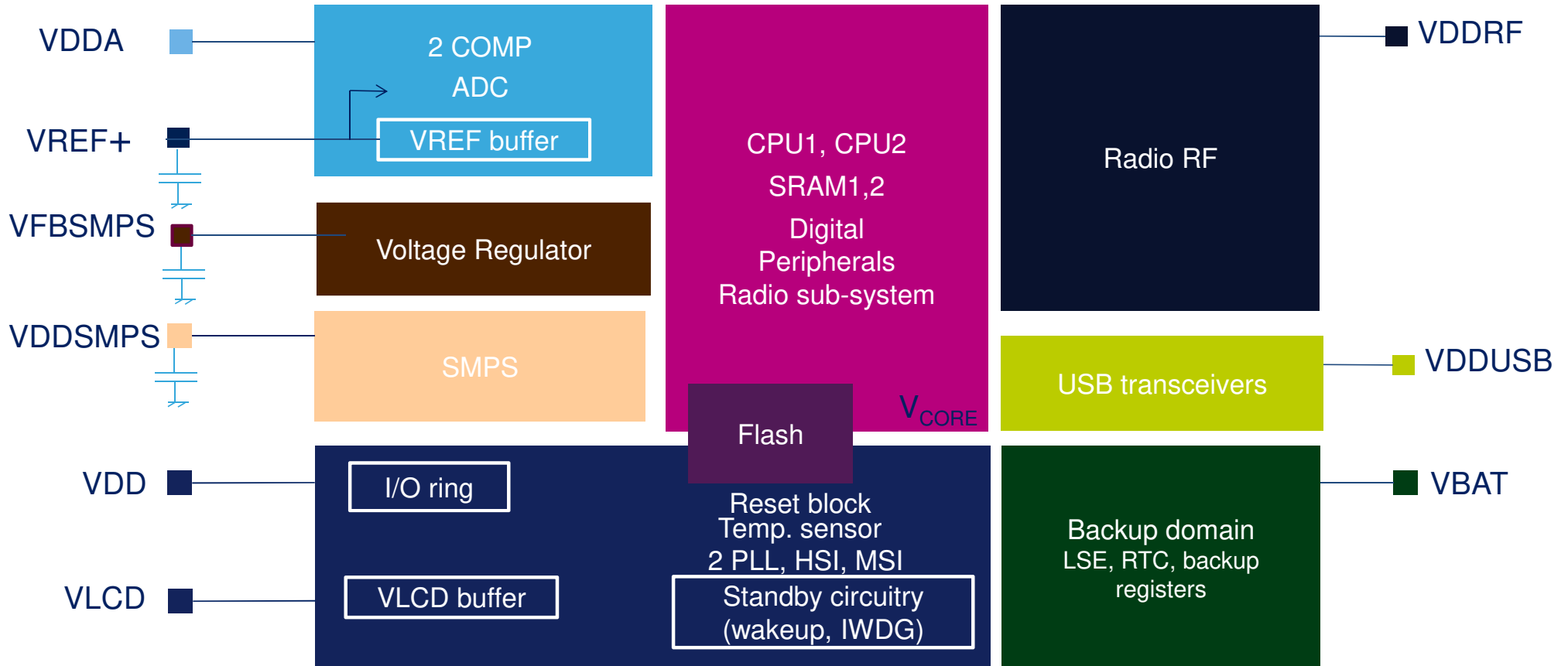


# BLE Multi-Role Topology





# Power schemes



# Overview

43

## FlexPowerControl

Wake-up time

9 cycles
9 cycles
1.7 $\mu$ s
4 $\mu$ s (19 $\mu$ s)
5 $\mu$ s (20 $\mu$ s)
14 $\mu$ s (25 $\mu$ s)
14 $\mu$ s (25 $\mu$ s)
50 $\mu$ s

() Typ. value for SMPS mode



RUN (Range1) at 64 MHz	117 (73) $\mu$ A / MHz**
RUN (Range2) at 16 MHz	109 $\mu$ A / MHz**
LPRUN at 2 MHz	103 $\mu$ A / MHz**
SLEEP at 64 MHz	41 $\mu$ A / MHz
LPSLEEP at 2 MHz	45 $\mu$ A / MHz
STOP 0 (full retention)	100 $\mu$ A
STOP 1 (full retention)	9.2 $\mu$ A / 9.6 $\mu$ A*
STOP 2 (full retention)	1.8 $\mu$ A / 2.2 $\mu$ A*
STANDBY + 32 KB RAM	320 nA / 600 nA*
STANDBY	110 nA / 440 nA**
SHUTDOWN	30 nA / 315 nA*
VBAT	2 nA / 300 nA*

RF Operation

Typ @ VDD = 1.8 V @ 25 °C

\* with RTC

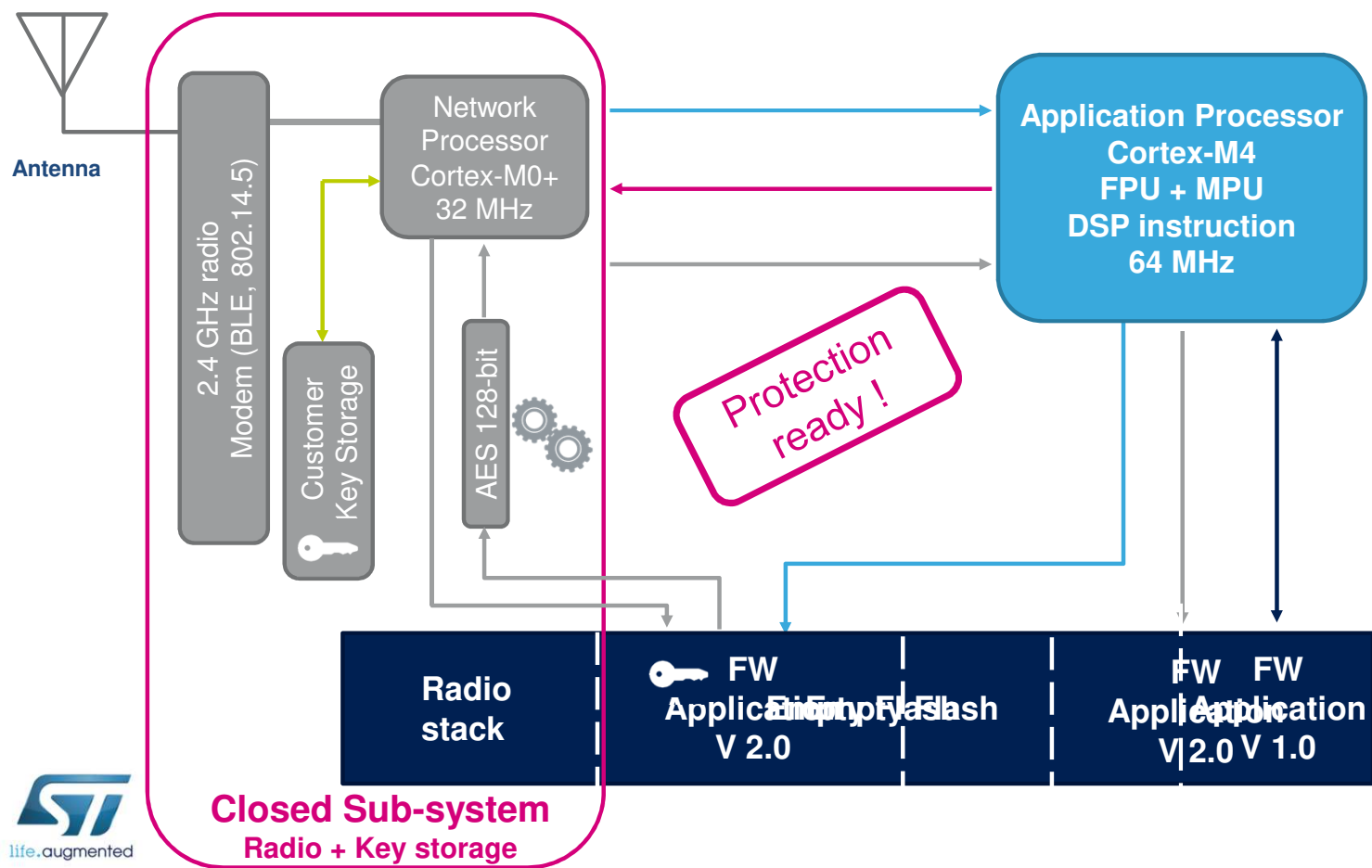
\*\* from SRAM1

- High performance  
→ CoreMark score = 215
- Outstanding power efficiency  
→ ULPBench score = 175



# IoT Protection Ready

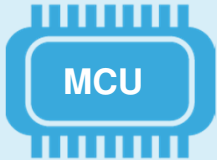

Radio stack or Application firmware updates



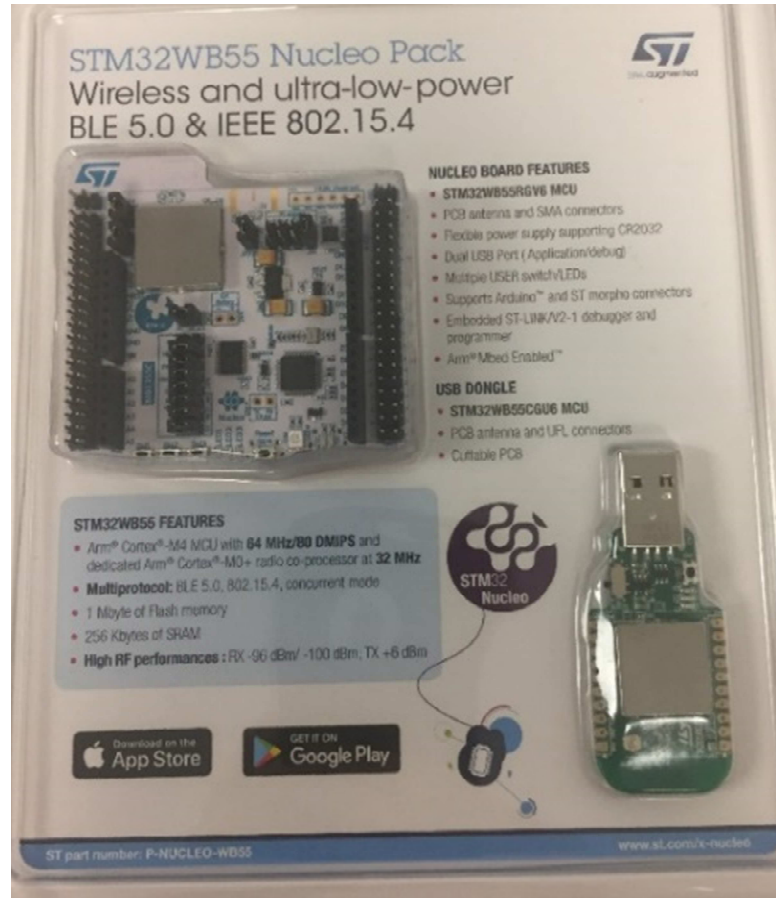
- 1 New FW package received
- 2 New FW detected Update is launched
- 3 M4 sends firmware signature and key for authentication
- 4 Authentication signature matches preprogrammed key
- 5 New firmware is decrypted with proprietary key



# IoT Protection Ready

Attacks	Attacks description	STM32WB Countermeasures
<p>Non Invasive</p> 	<ul style="list-style-type: none"><li>• Environment<ul style="list-style-type: none"><li>• Temp / Voltage / Clocks</li></ul></li><li>• Fault injection</li><li>• Exploit debugger</li><li>• Side channel</li><li>• Power Analysis</li></ul>	<ul style="list-style-type: none"><li>• Temp sensor</li><li>• Power supply monitor</li><li>• Clock security system</li><li>• Tamper pads</li><li>• ECC, Parity check</li><li>• SRAM mass erase</li><li>• Read out protection</li><li>• Flash-only boot</li></ul>
<p>Software</p> 	<ul style="list-style-type: none"><li>• Break the encryption</li><li>• Extract keys</li><li>• Exploit debugger / test modes</li><li>• Malware</li><li>• Replay</li></ul>	<ul style="list-style-type: none"><li>• Customer Key Storage</li><li>• RNG, Crypto accelerator, CRC</li><li>• Readout / Write memory protections</li><li>• Memory Protection Unit</li><li>• Root Security Service</li><li>• Secure Firmware Update (SFU)</li><li>• 96-bit Unique ID</li></ul>

# Nucleo Pack



# Nucleo

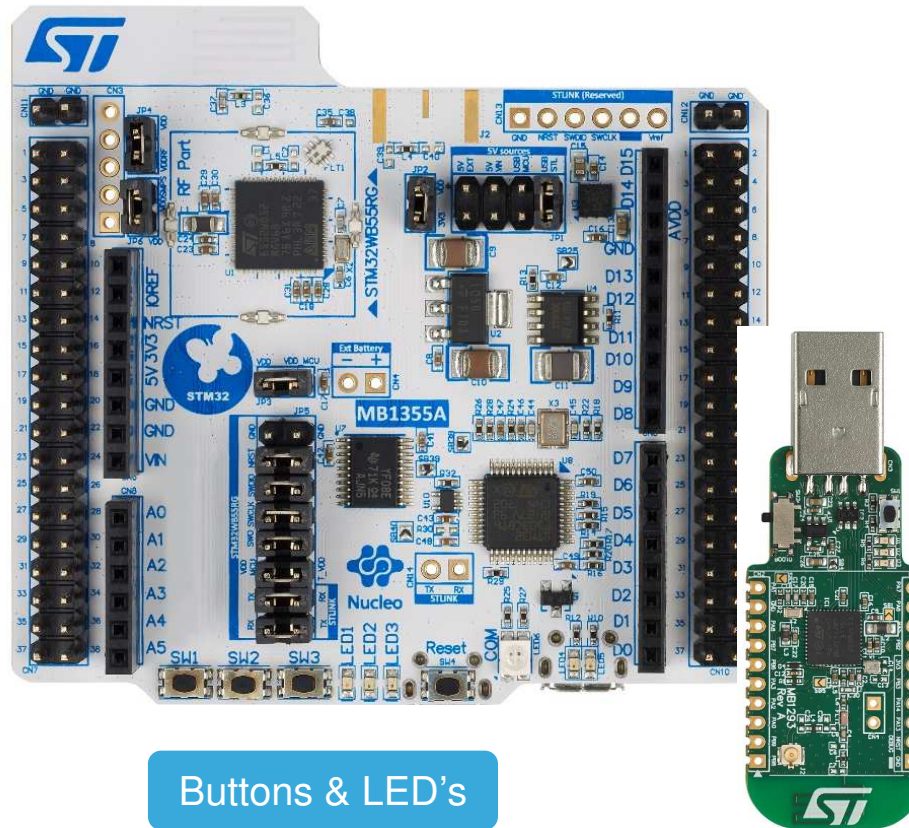
2.4GHz PCB antenna

STM32WB55RGV6  
(VQFPN68)

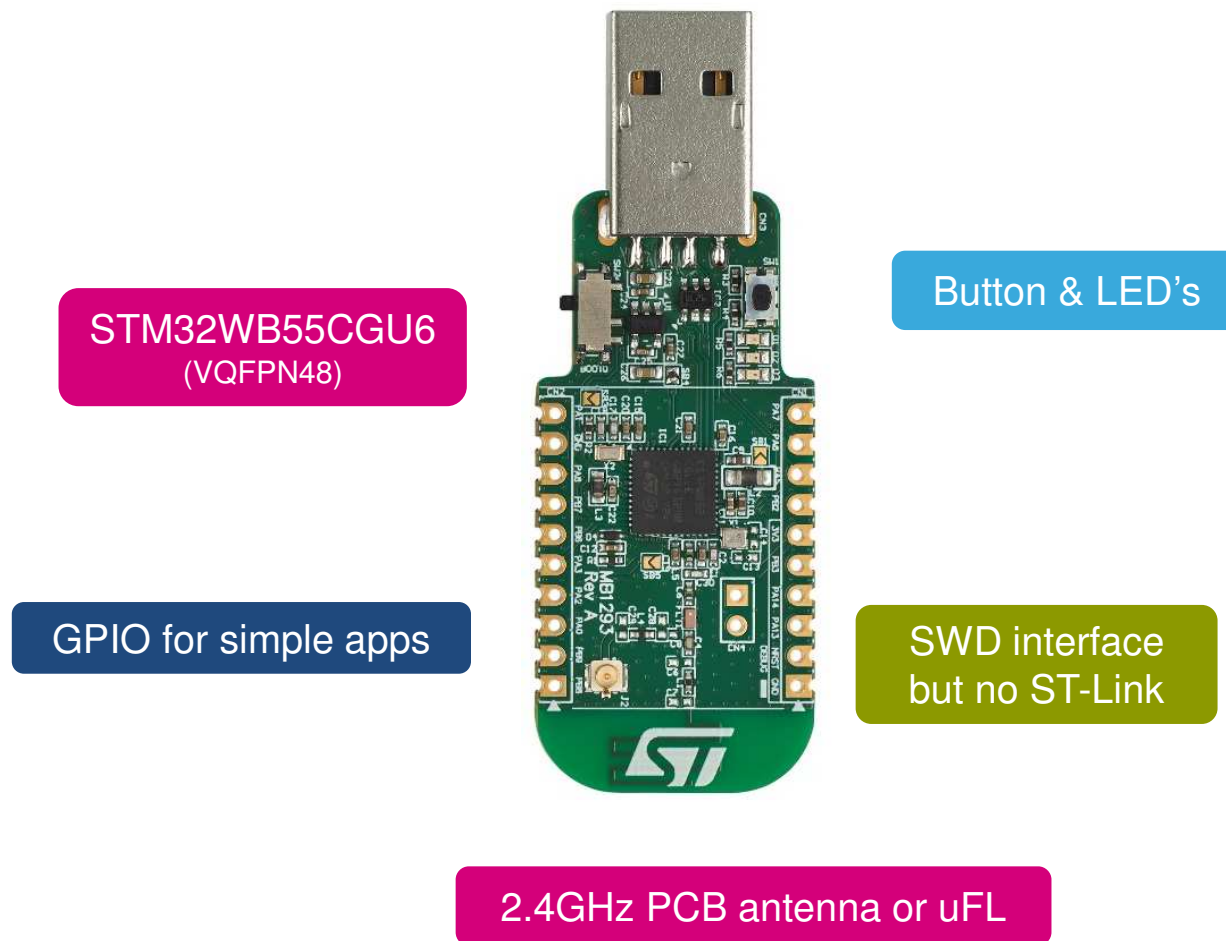
Arduino & Morpho  
Headers

Buttons & LED's

ST-Link/V2-1  
(for programming and  
debugging)



# Dongle

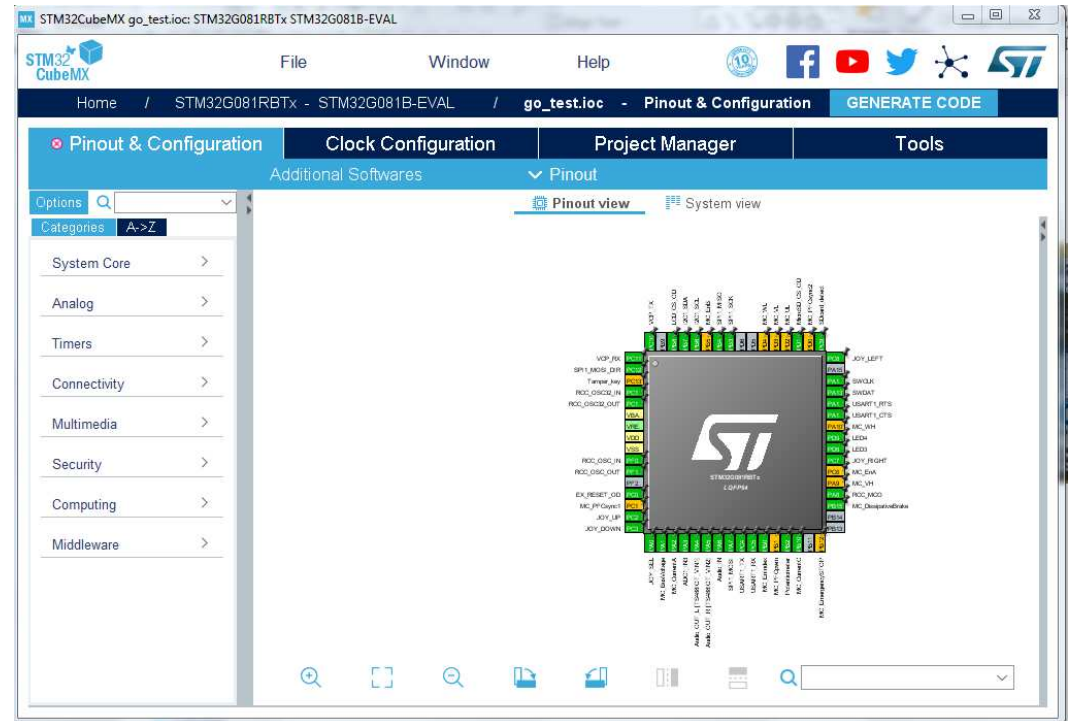


# Cube Tools

- STM32CubeMX
- STM32CubeProgrammer
- STM32CubeMonitorRF
- CubeWB HAL Firmware

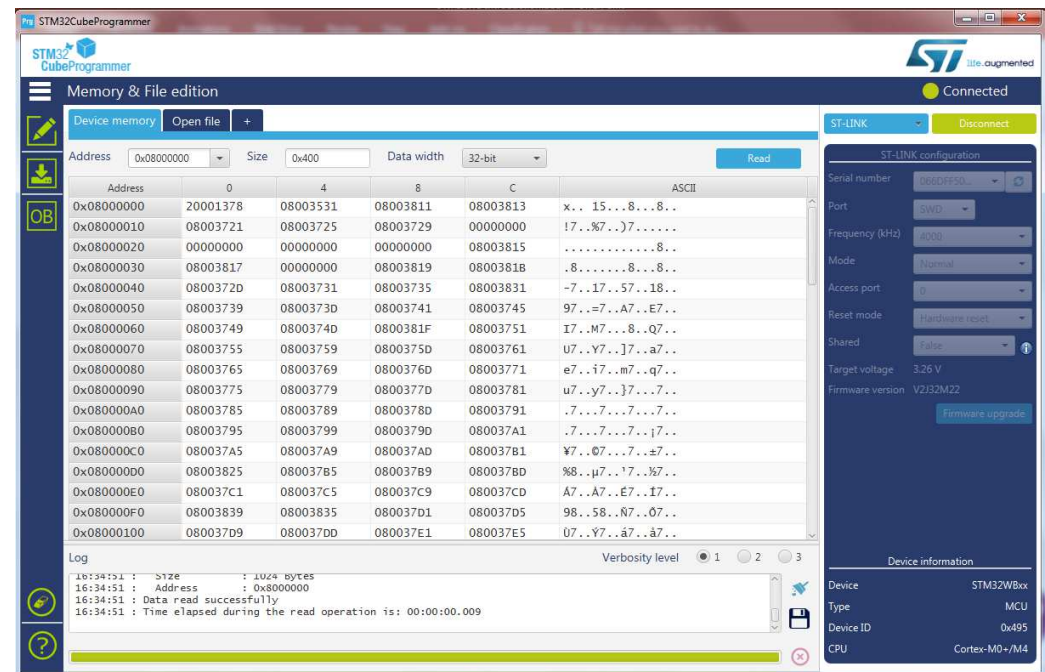
# Cube Tools

- STM32CubeMX
- STM32CubeProgrammer
- STM32CubeMonitorRF
- CubeWB HAL Firmware



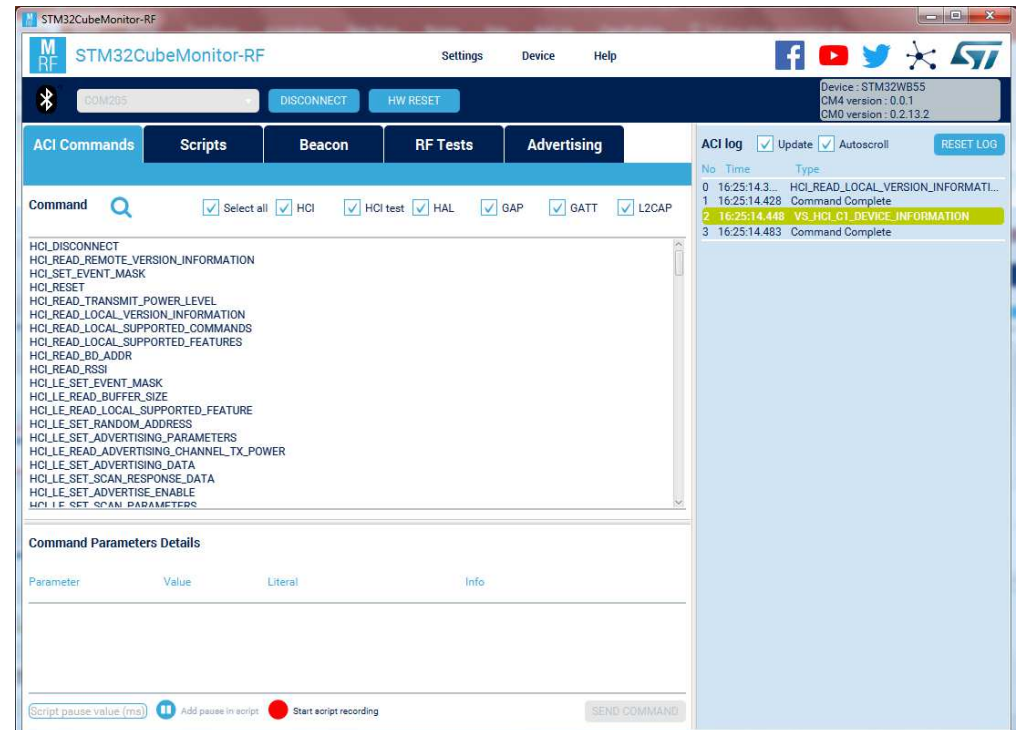
# Cube Tools

- STM32CubeMX
- STM32CubeProgrammer
- STM32CubeMonitorRF
- CubeWB HAL Firmware



# Cube Tools

- STM32CubeMX
- STM32CubeProgrammer
- STM32CubeMonitorRF
- CubeWB HAL Firmware



# Bonus Cube Tool!

- STM32CubeMX
- STM32CubeProgrammer
- STM32CubeMonitor-Power
- CubeWB HAL Firmware



X-NUCLEO-LPM01A

# Cube Tools

- STM32CubeMX
- STM32CubeProgrammer
- STM32CubeMonitorRF
- CubeWB HAL Firmware

ADC  
BSP  
COMP  
Cortex  
CRC  
CRYP  
DMA  
FLASH  
GPIO  
HAL  
HSEM  
I2C  
IWDG  
LPTIM  
PKA  
PWR  
RCC  
RNG  
SPI  
TIM  
UART  
WWDG

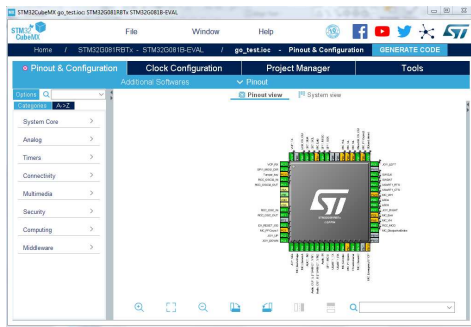
Thread\_Cli\_Cmd  
Thread\_Coap\_DataTransfer  
Thread\_Coap\_Generic  
Thread\_Coap\_MultiBoard  
Thread\_Commissioning  
Thread\_FTD\_Coap\_Multicast  
Thread\_SED\_Coap\_Multicast  
Thread\_Coap\_Generic.zip

FreeRTOS\_Mail  
FreeRTOS\_MPU  
FreeRTOS\_Mutexes  
FreeRTOS\_Queue  
FreeRTOS\_Semaphore  
FreeRTOS\_SemaphoreFromISR  
FreeRTOS\_Signal  
FreeRTOS\_SignalFromISR  
FreeRTOS\_ThreadCreation  
FreeRTOS\_Timers

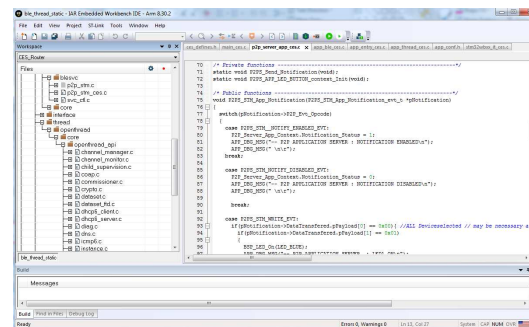
ble\_beacon  
ble\_blood\_pressure  
ble\_cable\_replacement  
ble\_data\_throughput  
ble\_health\_thermometer  
ble\_heart\_rate  
ble\_heart\_rate\_freertos  
ble\_hid  
ble\_ota  
ble\_p2p\_client  
ble\_p2p\_routeur  
ble\_p2p\_server  
ble\_proximity  
ble\_transparent\_mode

# Iterative Design Process

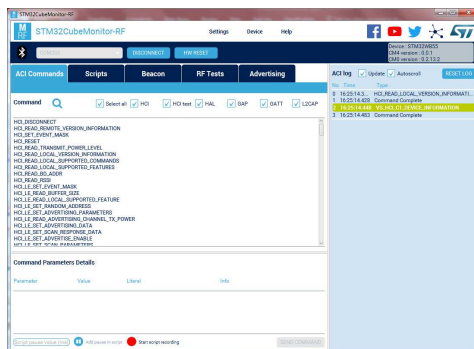
## Configure



## Code & Debug



## Test



## Measure





# BOM cost

## Silicon cost

- Embedded RF balun
- Few external components
- Simple RF front-end
- Embedded USB crystal
- Capacitive touch controller
- Simple 2-layer PCB

## Ecosystem cost

- BLE 5 stack
- OpenThread stack
- Open 802.14.5 MAC stack
- Zigbee 3.0 (coming soon!)
- STM32CubeMX
- STM32CubeMonitorRF
- Atollic C-compiler IDE



# STM32CubeMonitorRF

STM32CubeMonitor-RF

Help

BlueNRG-MS HW v3.1  
BlueNRG-MS FW v7.2c

COM5

Close

HW Reset

ACI Commands

ACI Utilities

Scripts

Beacon

RF Tests

☒ Select all ☒ HCI ☒ HAL ☒ HCI test ☒ GAP ☒ GATT ☒ L2CAP

Command

Send

ACI\_GATT\_DISC\_CHARAC\_BY\_UUID  
ACI\_GATT\_DISC\_ALL\_CHARAC\_DESCRIPTOR  
ACI\_GATT\_READ\_CHARAC\_VAL  
ACI\_GATT\_WRITE\_CHARAC\_DESCRIPTOR  
ACI\_GATT\_READ\_CHARAC\_DESC  
ACI\_GATT\_READ\_HANDLE\_VALUE  
ACI\_HAL\_GET\_FW\_BUILD\_NUMBER  
ACI\_HAL\_WRITE\_CONFIG\_DATA  
ACI\_HAL\_READ\_CONFIG\_DATA  
**ACI\_HAL\_SET\_TX\_POWER\_LEVEL**  
ACI\_HAL\_DEVICE\_STANDBY  
ACI\_HAL\_LE\_TX\_TEST\_PACKET\_NUMBER  
ACI\_HAL\_TONE\_START  
ACI\_HAL\_TONE\_STOP  
ACI\_HAL\_GET\_LINK\_STATUS

Command Packet

Parameter	Value	Literal	Info
HCI packet indicator	0x01	HCI Command Packet	
Op_Code	0xFC0F	ACI_HAL_SET_TX_POWER_LEVEL	
Parameter_Total_Length	0x02		
EN_High_Power	<input type="text" value="0x01"/>		Can be only 0 or 1. Set high power bit on or off.
PA_Level	<input type="text" value="0x05"/>		Can be from 0 to 7. Set the PA level value.

ACI log ☒ Update ☒ Autoscroll

Reset log

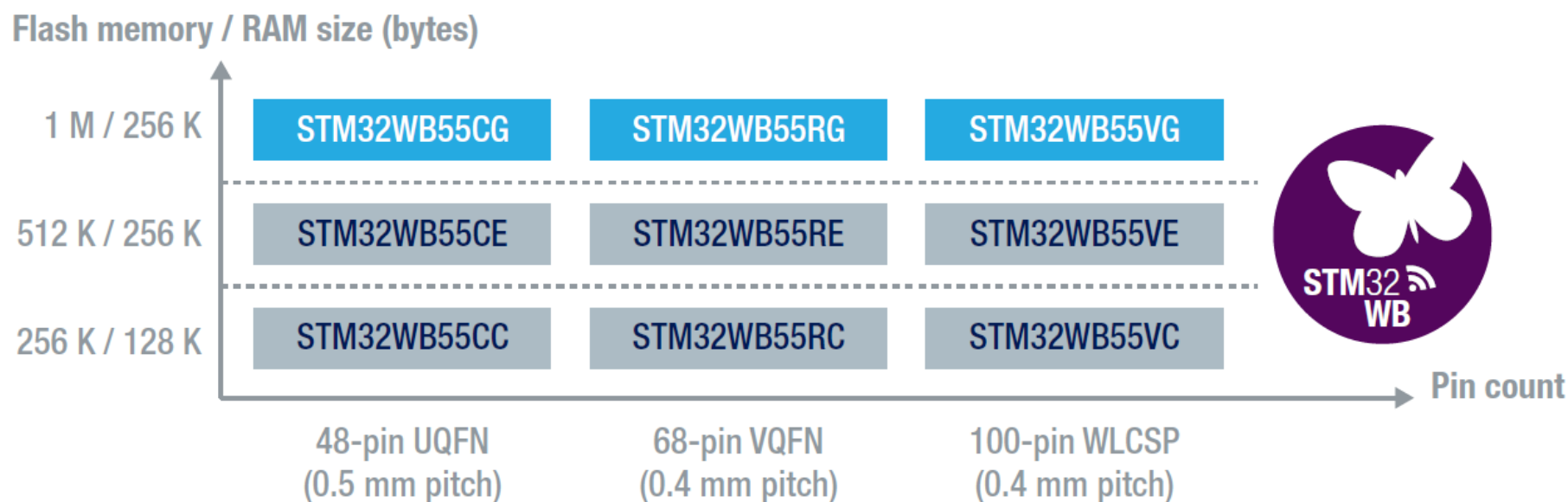
No.	Time	Type
12	09:12:25.389	Command Complete
13	09:12:28.013	HCI_RESET
14	09:12:28.047	Command Complete
15	09:12:28.077	HCI_VENDOR_EVENT
16	09:12:28.576	ACI_HAL_SET_TX_POWER_LEVEL
17	09:12:28.612	Command Complete
18	09:12:28.638	ACI_HAL_TONE_START
19	09:12:28.672	Command Complete
20	09:12:31.690	ACI_HAL_TONE_STOP
21	09:12:31.726	Command Complete
22	09:12:43.192	ACI_HAL_SET_TX_POWER_LEVEL
23	09:12:43.228	Command Complete

Packet details

Parameter	Value	Literal	Info
HCI packet indicator	0x04	HCI Event Packet	
Event_Code	0x0E	Command Complete	
Parameter_Total_Length	0x04		
Num_HCI_Command_Pac...	0x01		The number of HCI command packets which ...
Command_Opcode	0xFC0F	ACI_HAL_SET_TX_POWER_LEVEL	Opcode of this command which caused this e...
Status	0x00	SUCCESS	command succeeded or failed



# STM32 offering



# Releasing Your Creativity



f /STM32

t @ST\_World

ST community



[www.st.com/stm32wb](http://www.st.com/stm32wb)