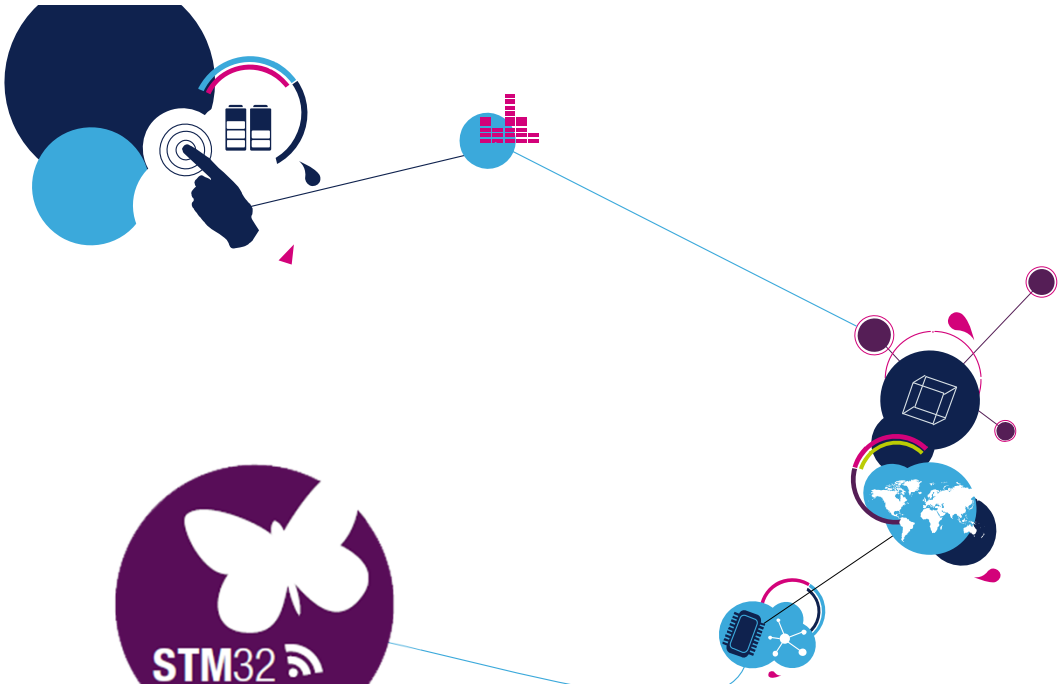
STM32WB Wireless MCUs

BLE 5 and IEEE 802.15.4

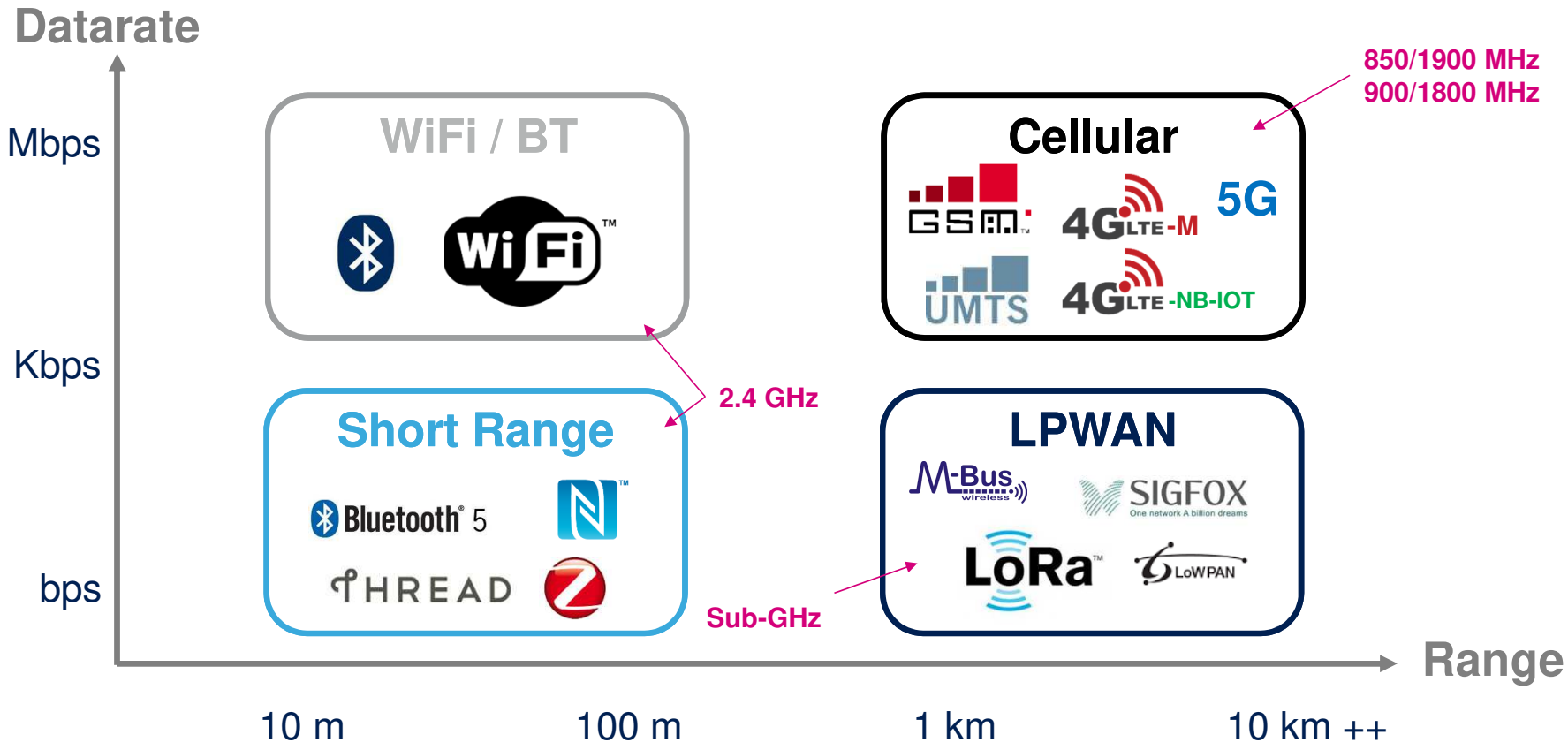


Joe Tijerina
Field Applications Engineer

life.augmented

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

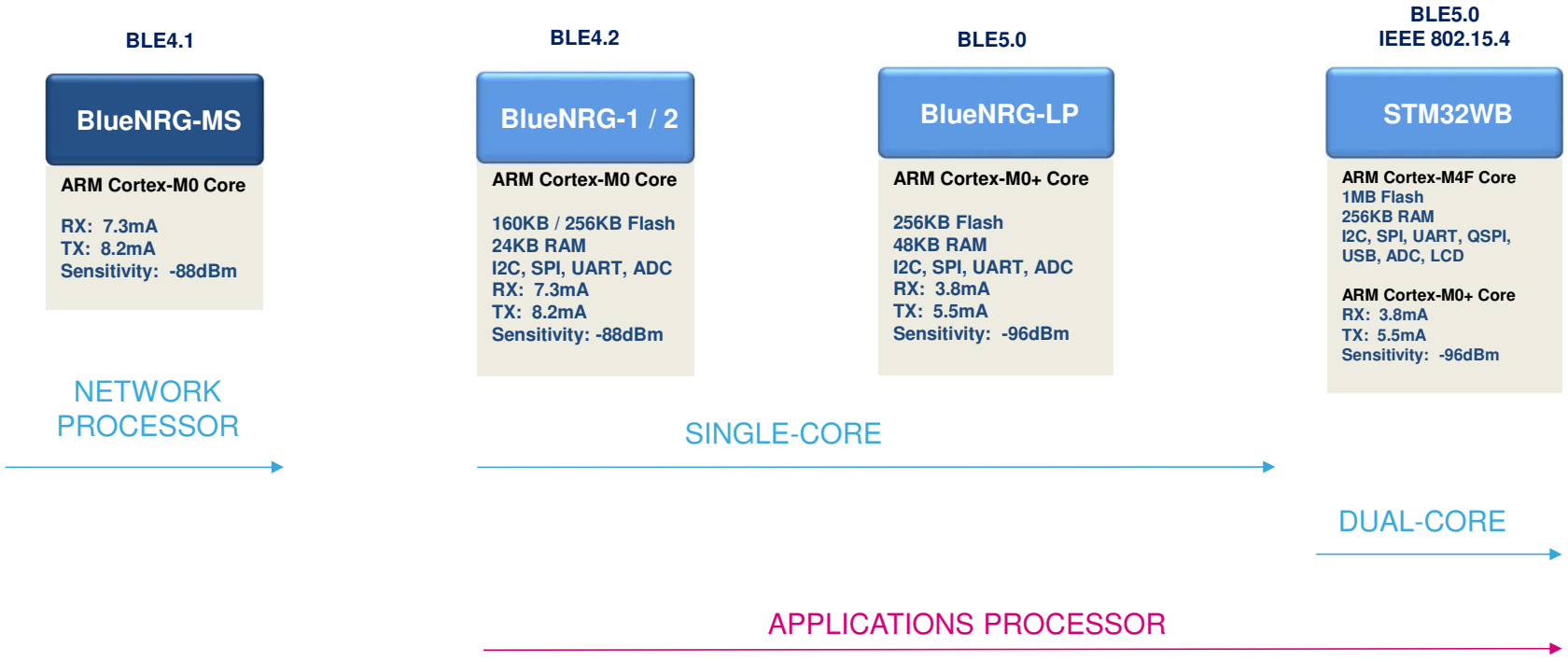
Bluetooth LE
Point-to-point communication with smartphones and other wireless devices

BLE Mesh / 802.15.4
Home automation with Mesh network need

Your Smartphone is your GUI!

life.augmented

BLE & 802.15.4



life.augmented

STM32WB Key Takeaways

Multi-protocol

Dual-core

Secure

life.augmented

Multiprotocol

Bluetooth 5

- Fully certified
- 2Mbps
- BLE Mesh

THREAD ZigBee

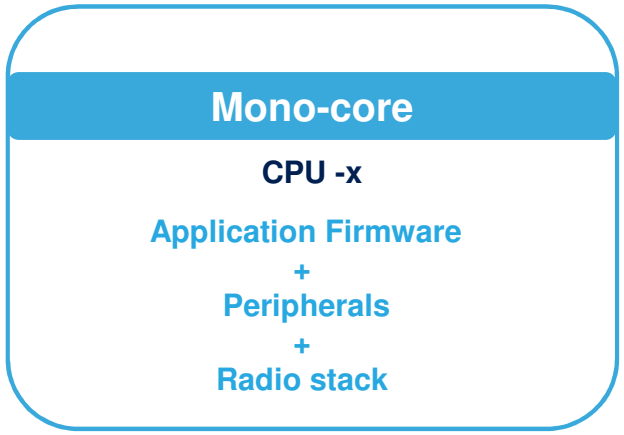
- Zigbee 3.0
- OpenThread
- Concurrent BLE + OpenThread

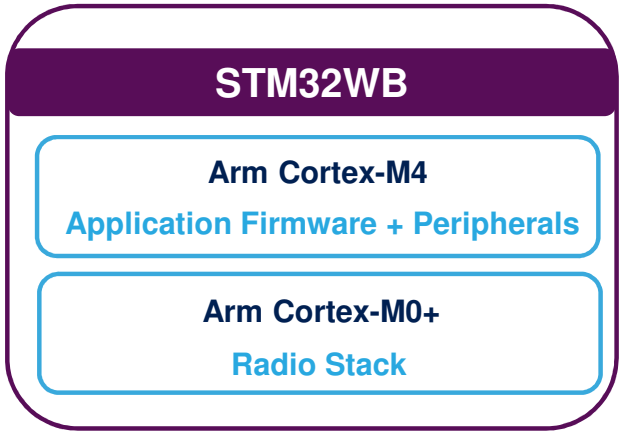
2.4 GHz
Open

- OpenMAC

life.augmented

Dual-Core

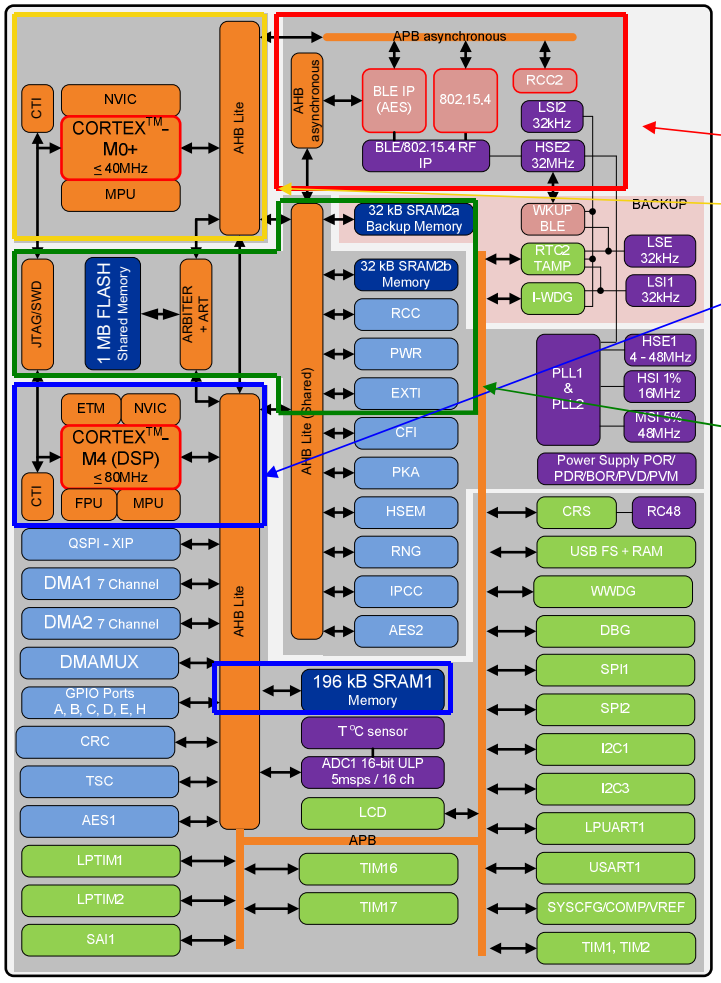




- **Drawbacks**
  - Time sharing
  - Companion MCU?

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

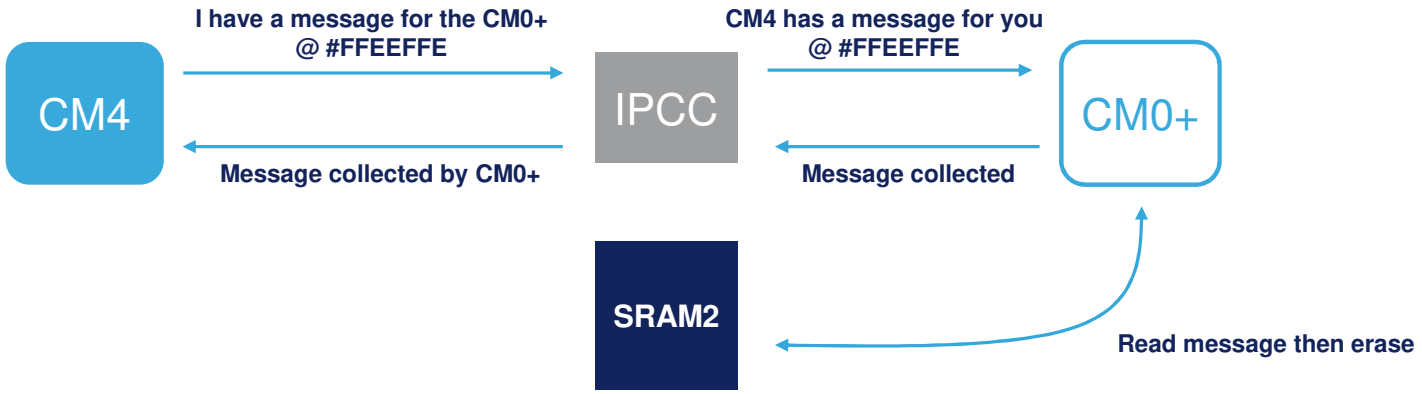
Architecture



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

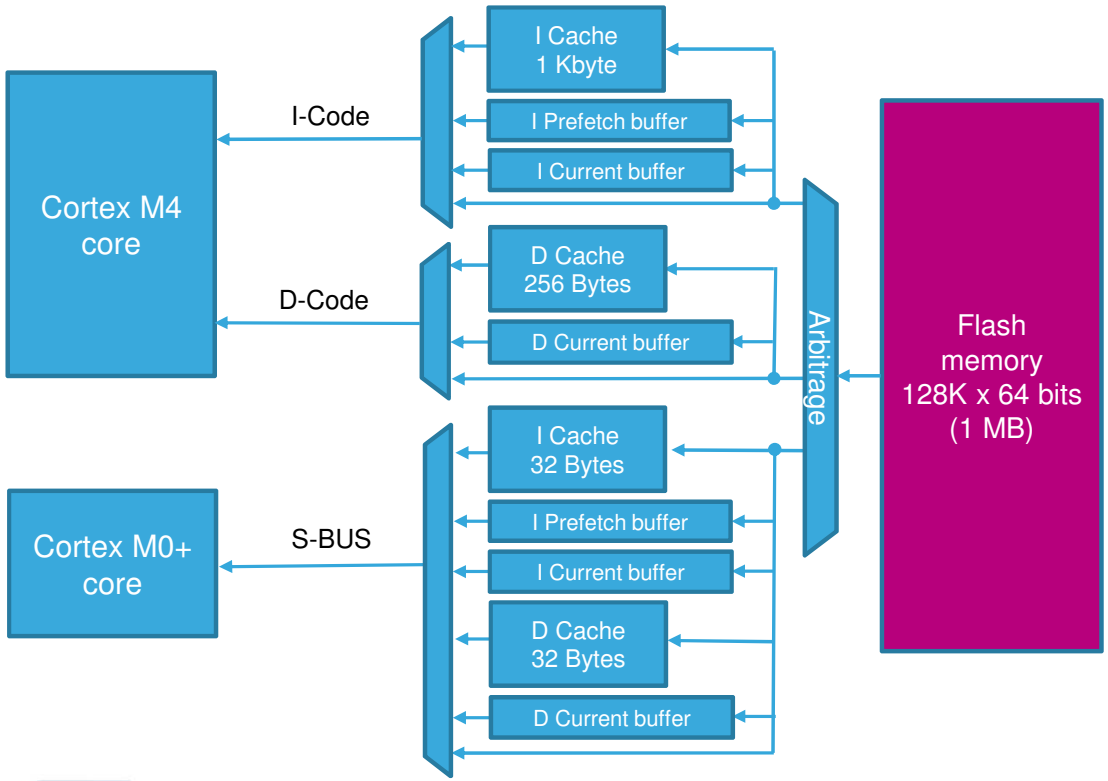
Dual core – How does that work?

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



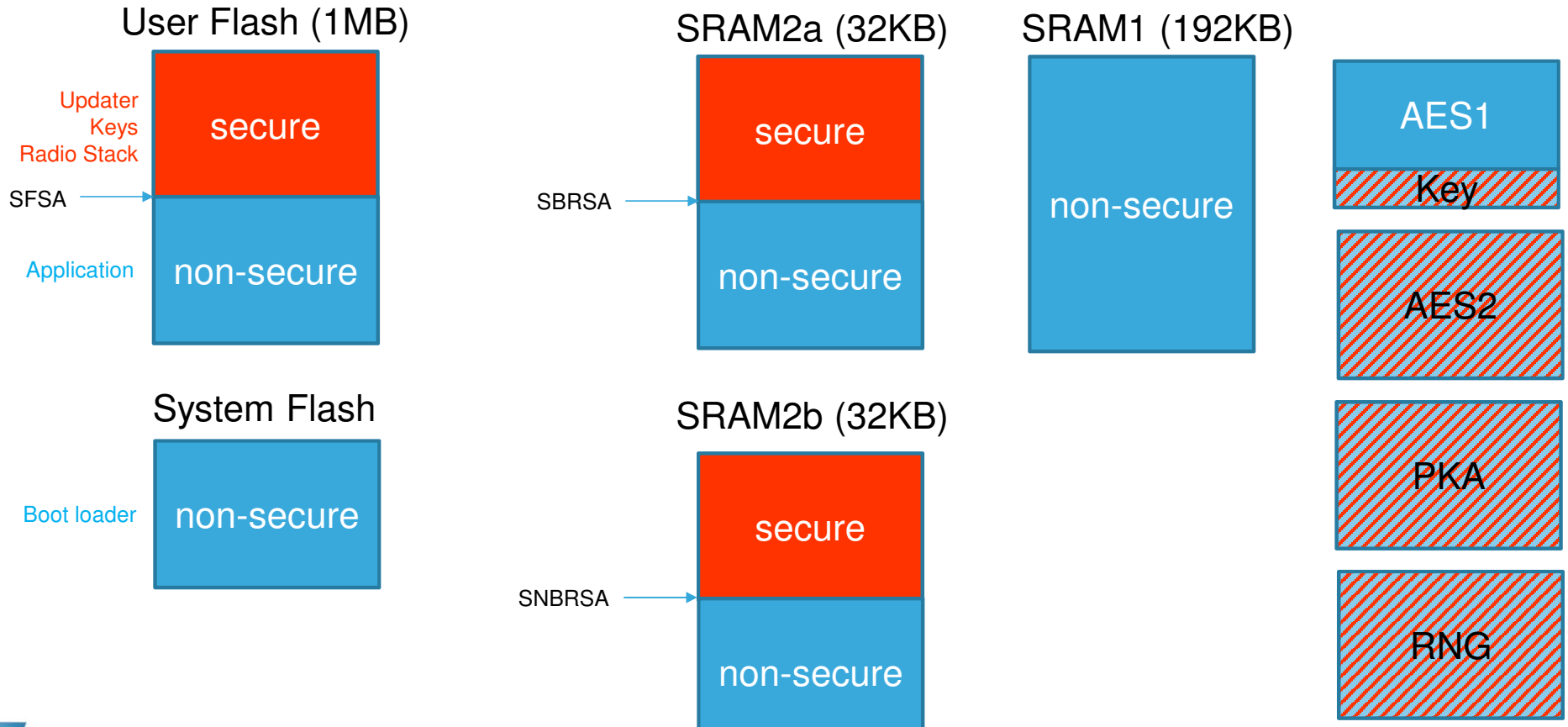
IPCC works in both directions

ART Accelerator™

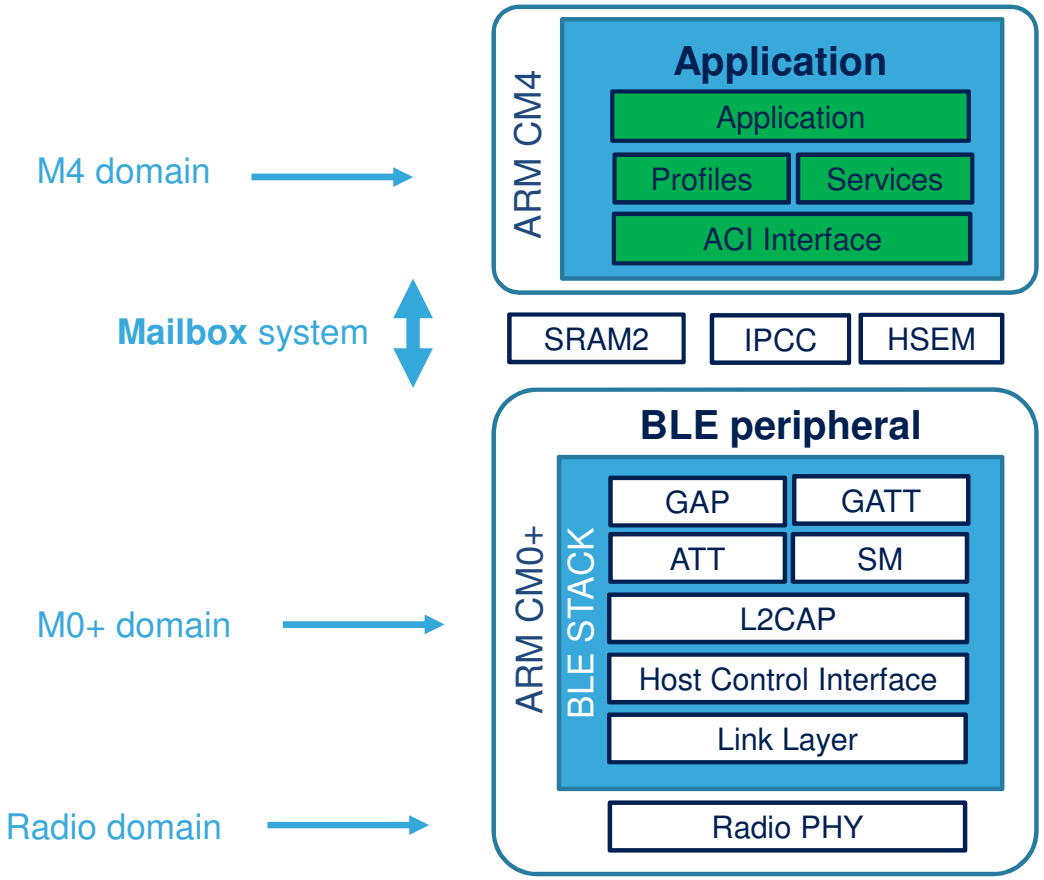


- **Cortex-M4**
  - **Instruction cache** = 32 lines of 4x64 bits
  - **Data cache** = 8 lines of 4x64 bits
  - **Pre-fetch buffer**
- **Cortex-M0+**
  - **Instruction cache** = 4 lines of 1x64 bits
  - **Data cache** = 4 lines of 1x64 bits
  - **Pre-fetch buffer**

Security


User Flash (1MB)
Updater
Keys
Radio Stack
secure
SFSA
Application
non-secure
System Flash
Boot loader
non-secure
SRAM2a (32KB)
SBRSA
secure
non-secure
SRAM2b (32KB)
SNBRSA
secure
non-secure
SRAM1 (192KB)
non-secure
AES1
Key
AES2
PKA
RNG
Securable by register bit

Protocol Stack layers



Classic vs Low Energy

100X lower power

Longer range

Fast connection (only 3 advertising channels to scan)

Relaxed RF requirements

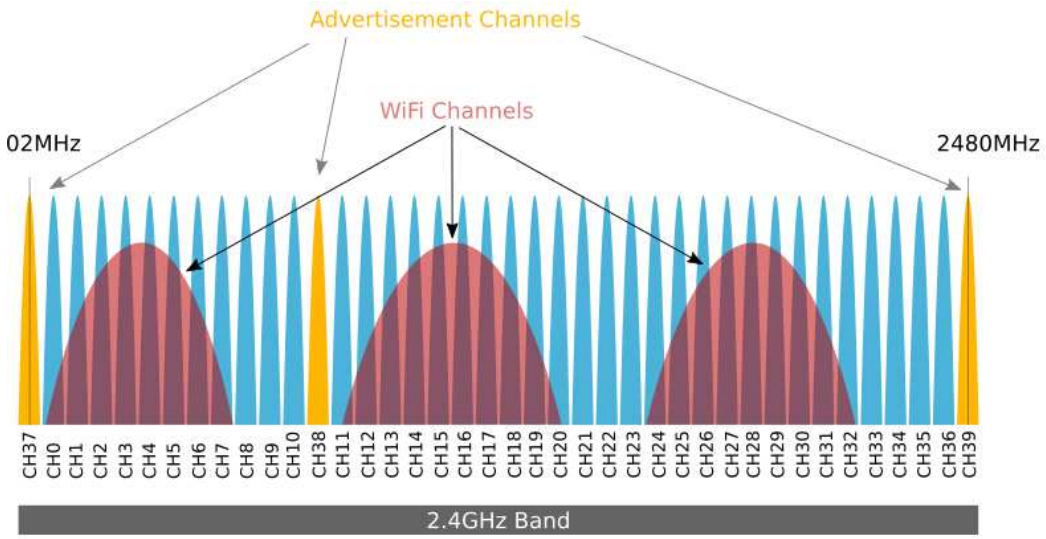
Comparison of Classic and Low Energy		
	Classic (BR/EDR)	**Low Energy (LE)**
Application	Cell phones, headsets, stereo/audio streaming, automotive (handsfree), PCs, etc.	Smartwatches, sport & fitness, home electronics, automation, industry, healthcare, smartphones, etc.
Voice	Yes	No
RF band ISM	2.4 GHz	2.4 GHz
Energy consumption	Reference	0.5…0.01 times Classic as reference
Coverage	10 m	≥ 10 m
Power	3 classes (max.): • +20 dBm • +4 dBm • 0 dBm	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 • 3 advertising • 37 data (+ secondary advertis-ing)
Modulation	GFSK • BT = 0.5 • Deviation = 160 kHz • Mod index = 0.28….0.35 π/4-DQPSK 8DPSK	GFSK • BT = 0.5 • Deviation = 250 kHz or 500 kHz • Mod index = 0.45…0.55 • Stab Mod index = 0.495…0.505
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

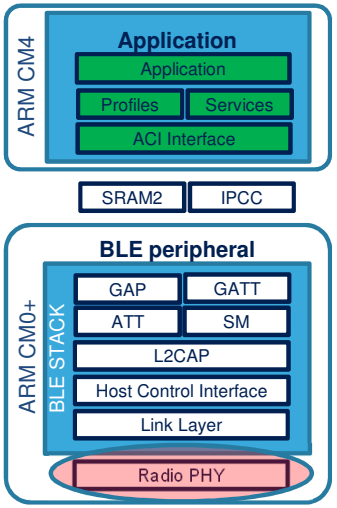
life.augmented

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 / 8DSPK
Data Rate	1Mbit/s	1 Mbit/s	2 and 3 Mbit/s
Channels	40	79	79
Spacing	2MHz	1MHz	-

life.augmented

Basic RF System Front-End

Balun – Combine TX and RX signals

Matching Network – 50 Ω impedance transformation

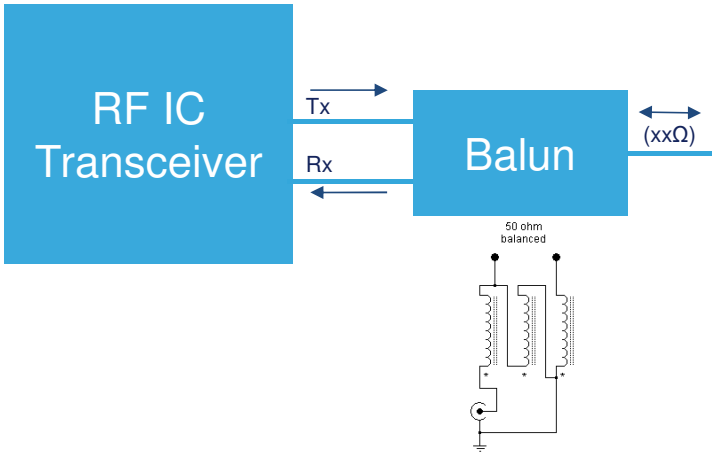
Harmonic Filter – Reduce out-of-band harmonics

Basic RF System Front-End

Balun – Combine TX and RX signals

Matching Network – 50 Ω impedance transformation

Harmonic Filter – Reduce out-of-band harmonics



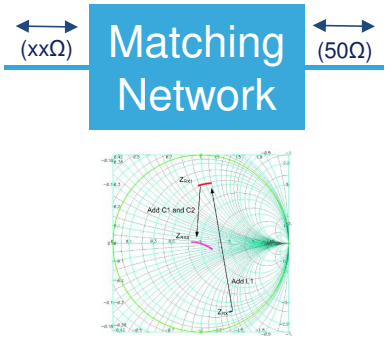
life.augmented

Basic RF System Front-End

Balun – Combine TX and RX signals

Matching Network – 50 Ω impedance transformation

Harmonic Filter – Reduce out-of-band harmonics



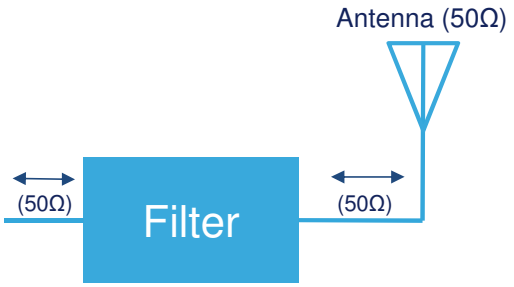
life.augmented

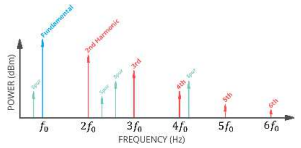
Basic RF System Front-End

Balun – Combine TX and RX signals

Matching Network – 50 Ω impedance transformation

Harmonic Filter – Reduce out-of-band harmonics





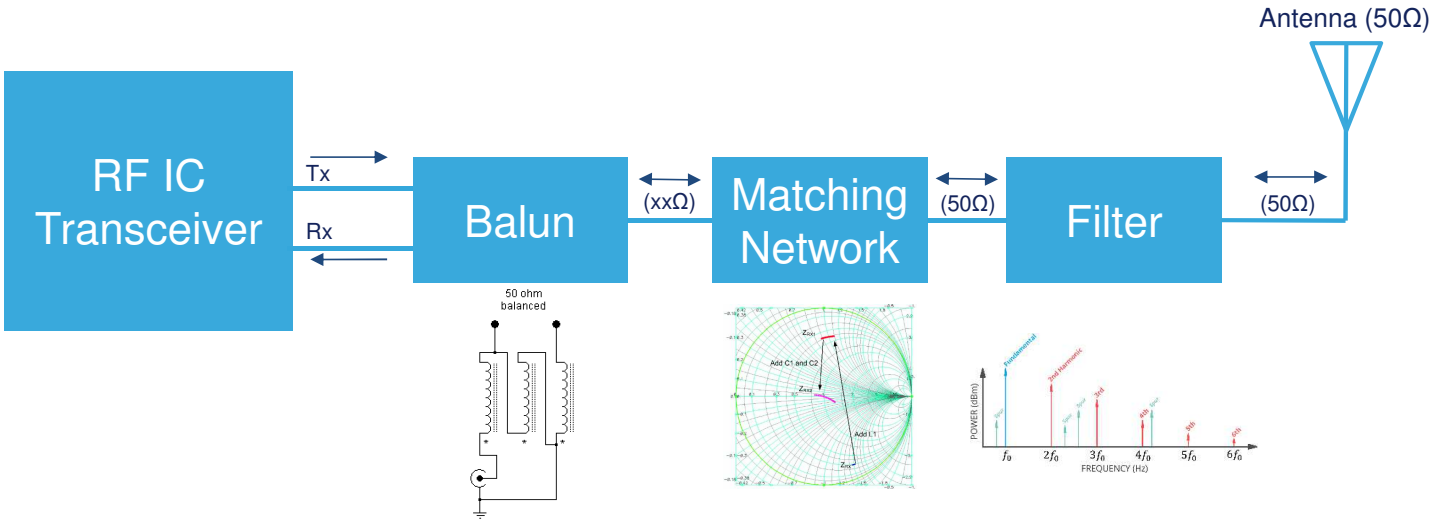
life.augmented

Basic RF System Front-End

Balun – Combine TX and RX signals

Matching Network – 50 Ω impedance transformation

Harmonic Filter – Reduce out-of-band harmonics



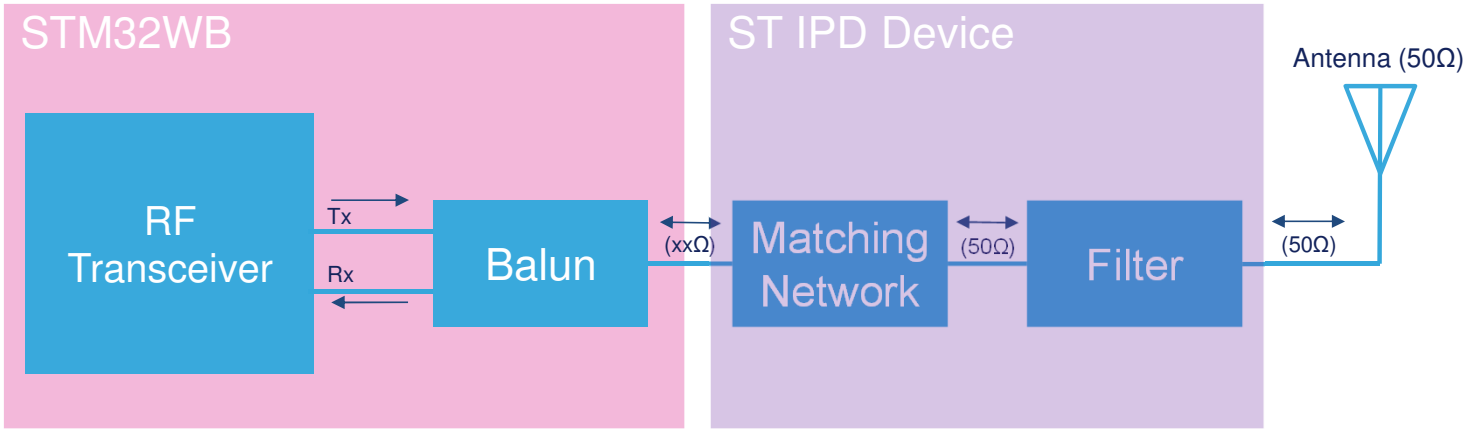
life.augmented

Basic RF System Front-End

Balun – Combine TX and RX signals

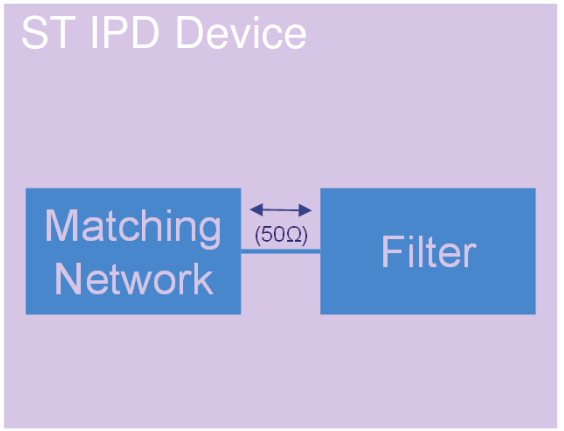
Matching Network – 50 Ω impedance transformation

Harmonic Filter – Reduce out-of-band harmonics

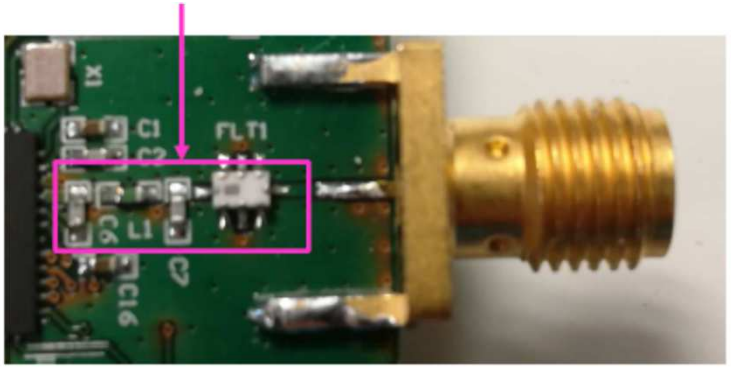


life.augmented

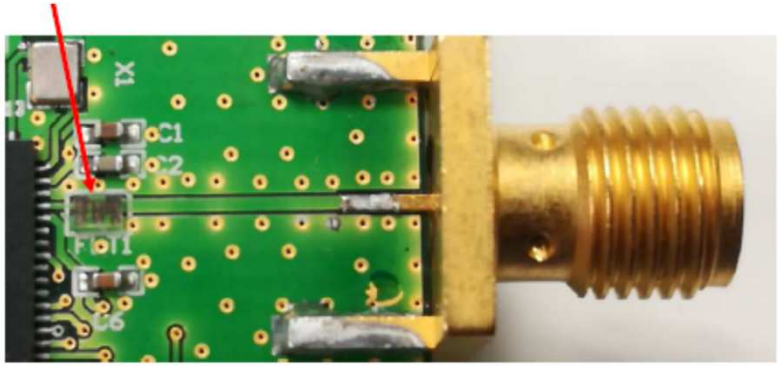
Matching Network + Harmonic Filter



Discrete network & filter in STM32WB ref design



MLPF-WB55-01E3 IPD device



life.augmented

Sampling NOW

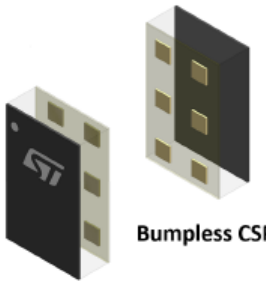
Production in March

IPD Filter

MLPF-WB55-01E3

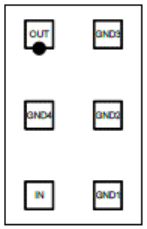
Datasheet

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 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®2 compliant

Applications

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

IPD Filter

1mm x 1.6mm CSP

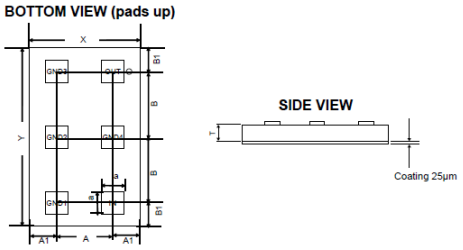


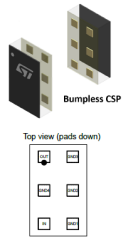
Table 4. **Bumpless CSP package mechanical data**

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

MLPF-WB55-01E3

Datasheet

2.4 GHz low pass filter matched to STM32WB55Cx/Rx



Features

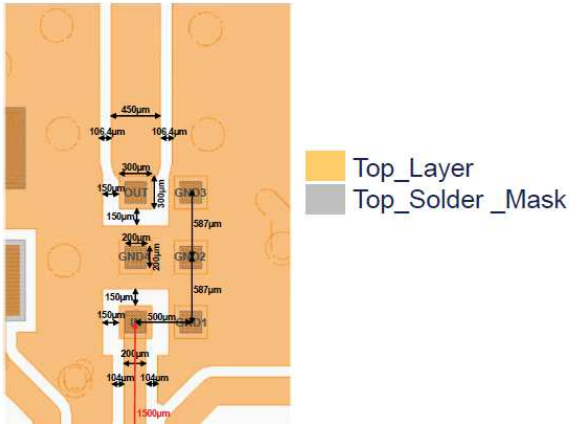
- Integrated impedance matching to STM32WB55Cx and STM32WB55Rx
- LGA footprint compatible
- 50 Ω nominal impedance on antenna side
- Deep rejection harmonics filter
- Low insertion loss
- Small footprint
- Low thickness ≤ 450 µm
- High RF performance
- RF BOM and area reduction
- ECOPACK®2 compliant

Applications

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

PCB recommendations included in datasheet

Figure 13. **PCB land pattern recommendations**

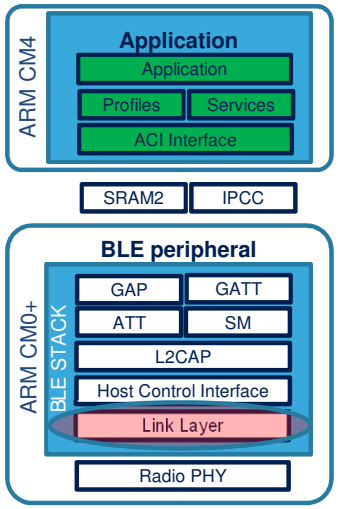


life.augmented

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!



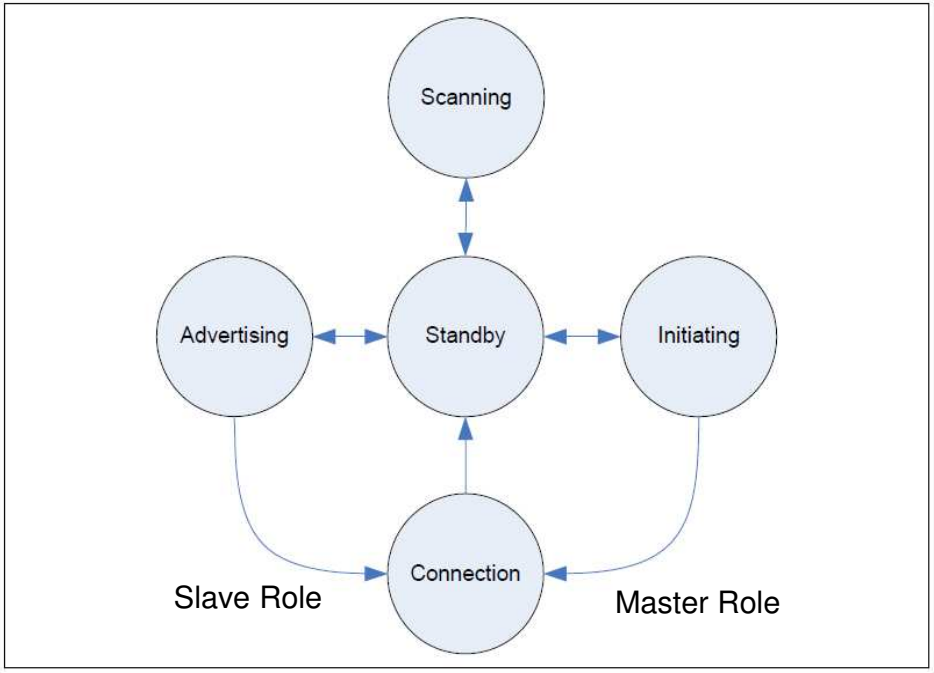
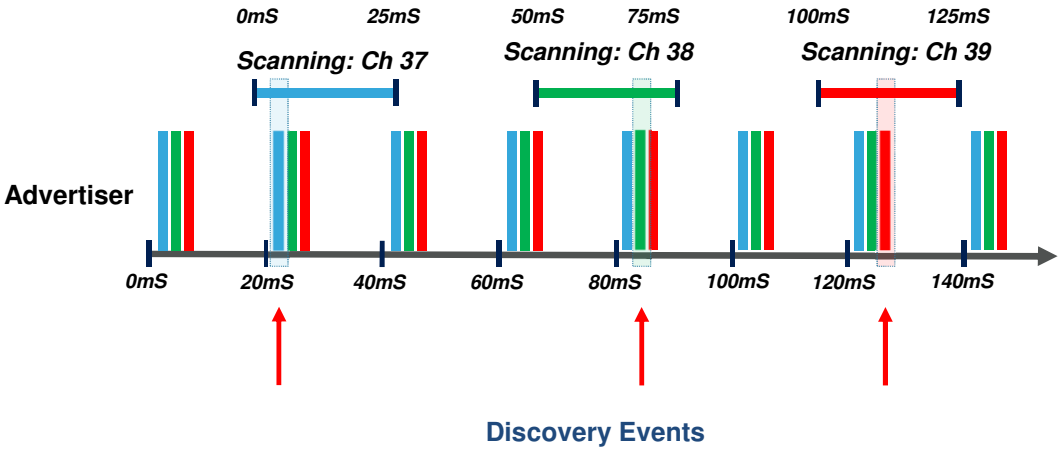
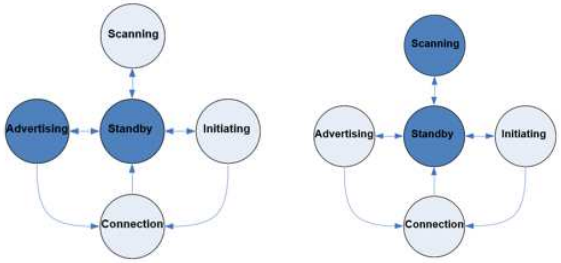


Figure 1.1: State diagram of the Link Layer state machine

life.augmented

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**

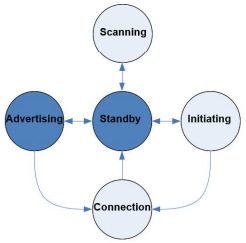
life.augmented

GAP (Generic Access Profile)

- Roles and Modes
  - Advertising Mode
  - Connected Mode

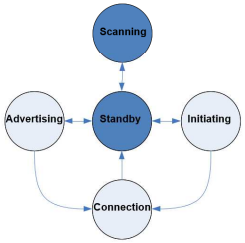
Broadcaster

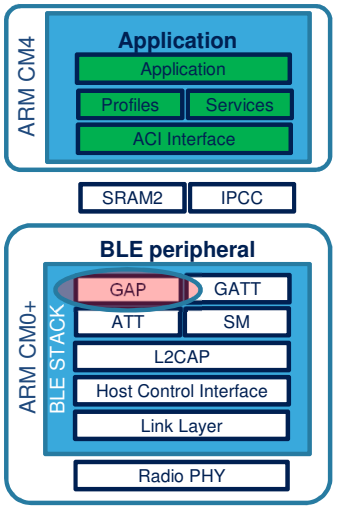
Sends advertising events
Can include characteristics and service data
Doesn't need receiver
Can be discoverable if it does have receiver



Observer

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





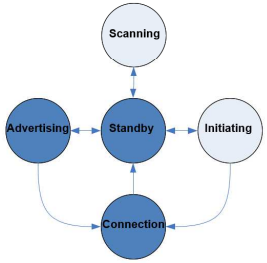
life.augmented

GAP (Generic Access Profile)

- Roles and Modes
  - Advertising Mode
  - Connected Mode

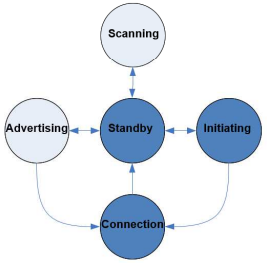
Peripheral

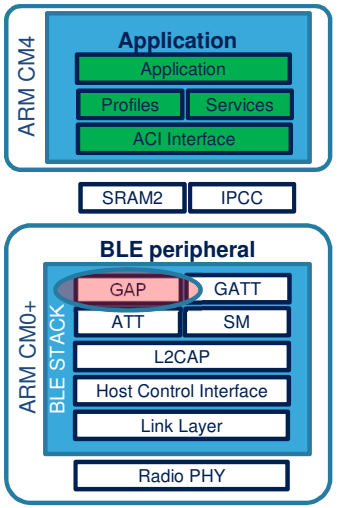
Has transmitter and receiver
Always slave
Connectable advertising



Central

Has transmitter and receiver
Always master
Never advertises





life.augmented

GATT (Generic Attribute Profile)

GAP Central is also a “GATT Client”
GAP Peripheral” is also a “GATT Server”

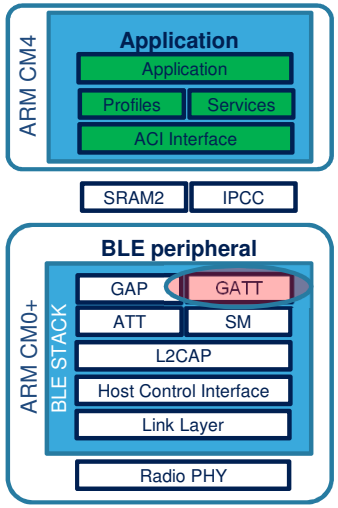
- Central queries the Services available
  - Peripheral **Services** and **Characteristics** are exposed via its’ **GATT** database

What is my heartrate?

147 bpm

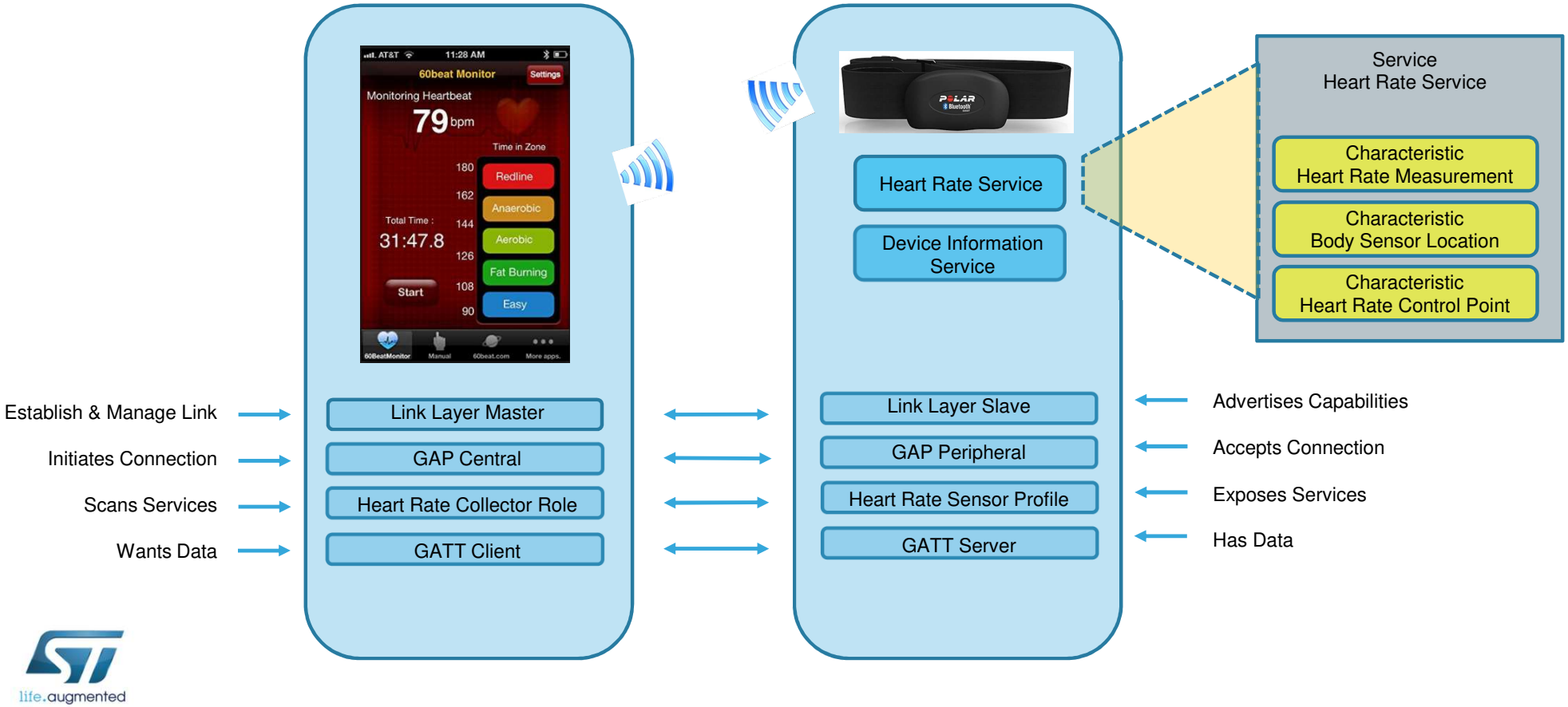
What is your Mfr ID?

Polar



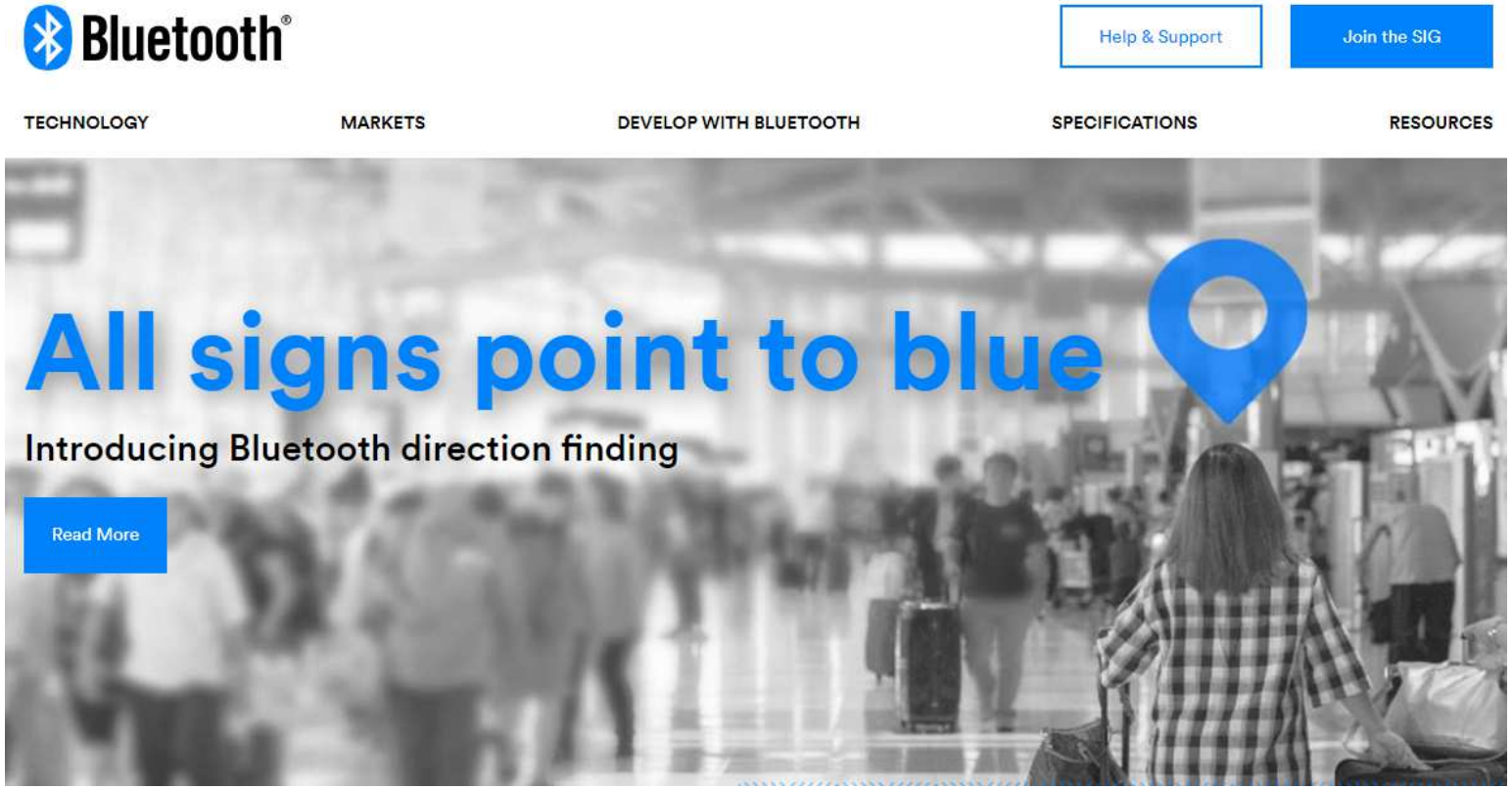
life.augmented

GATT: Profiles, Services and Characteristics



life.augmented

Bluetooth SIG

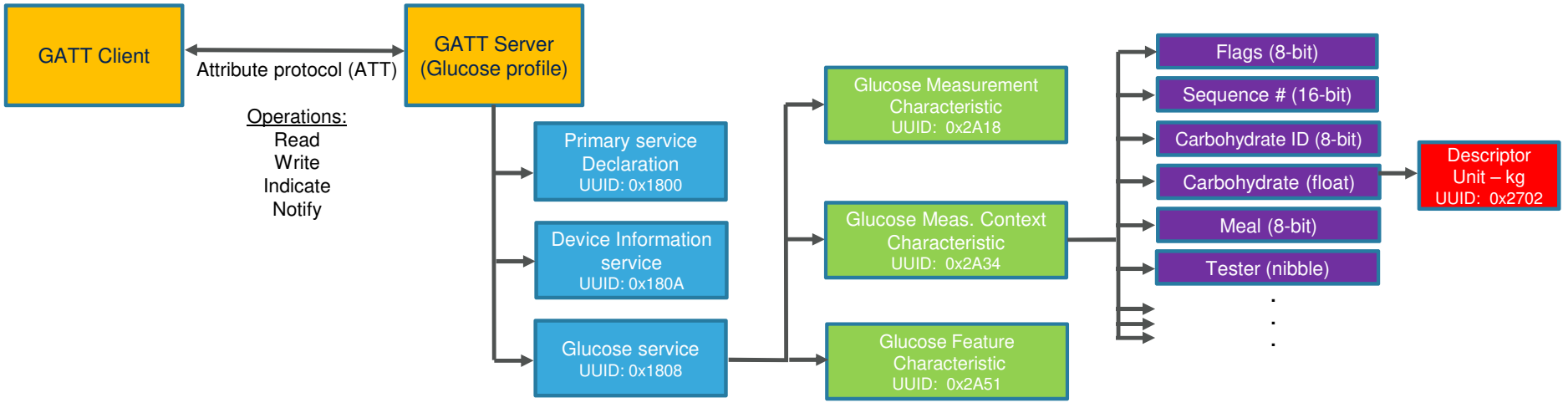


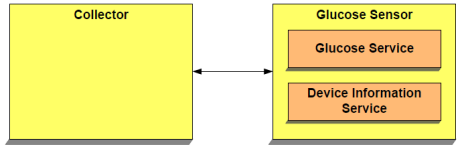
www.bluetooth.com

life.augmented

GATT Glucose Profile

GLP Profile defines two roles: Collector & Glucose Sensor

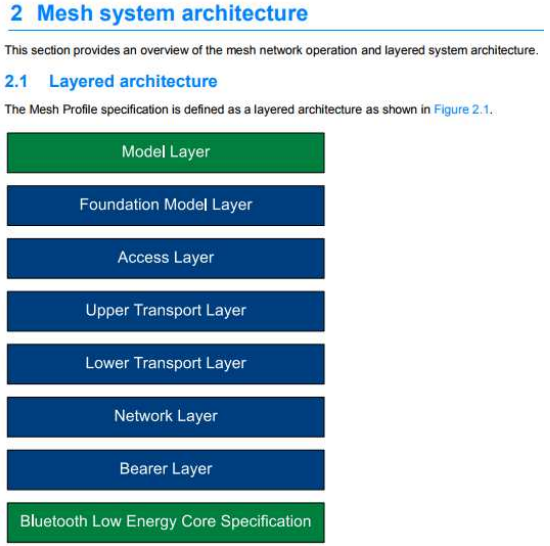




life.augmented

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



Thread


WHAT IS THREAD?
Thread was designed with one goal in mind: to create the best way to connect & control products in the home.
Built on Thread
WATCH VIDEO

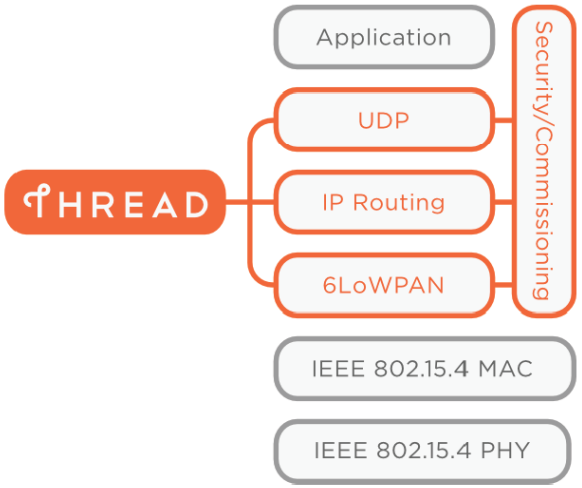
Thread

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

Can support many popular application layer protocols and platforms



A software upgrade can add Thread to currently shipping 802.15.4 products

Thread

THREAD Direct Addressability of devices

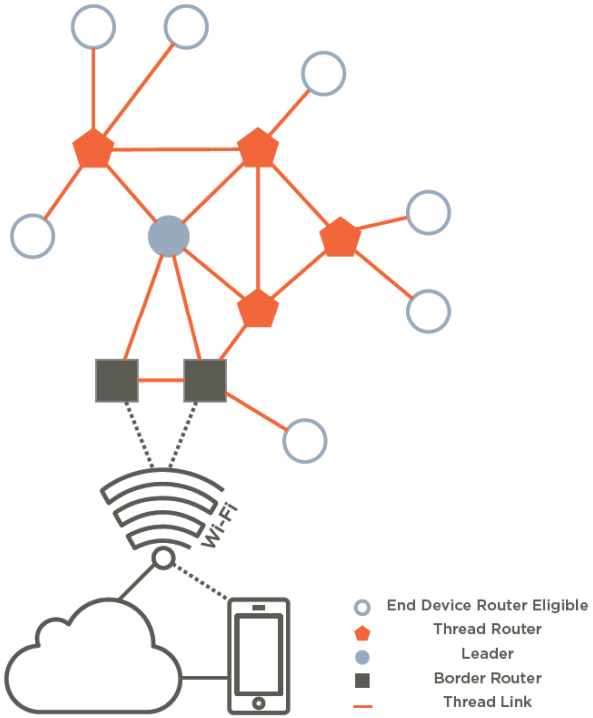
All devices have IPv6 addresses plus short address on HAN

DHCPv6 used for router address assignment

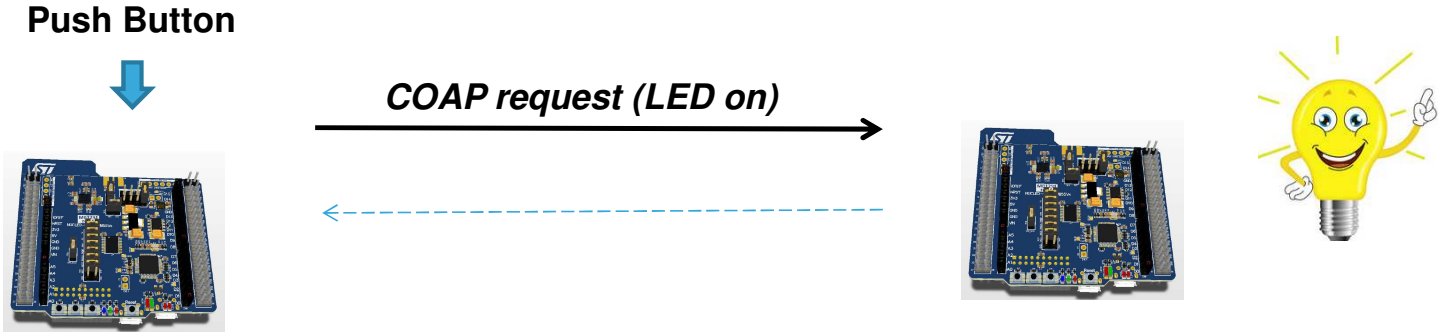
Home Network can directly address devices through Border Routers

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



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

- Dest Addr: FF03::1
- Port 5683
- UriPath : “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

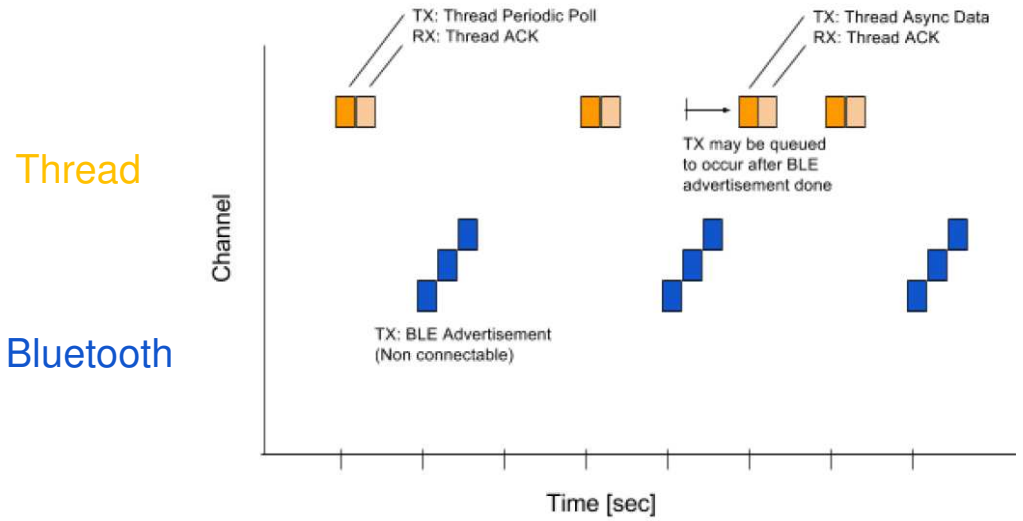
Static Concurrent Mode

➔ 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



BLE / Thread Concurrent modes

Static Concurrent Mode

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

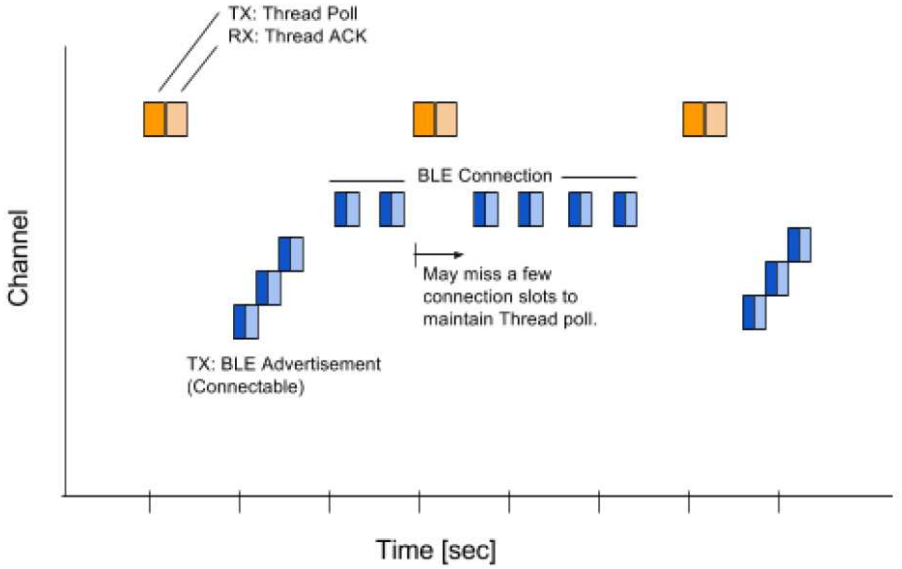
Dynamic Concurrent Mode

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

Thread + BLE Connection

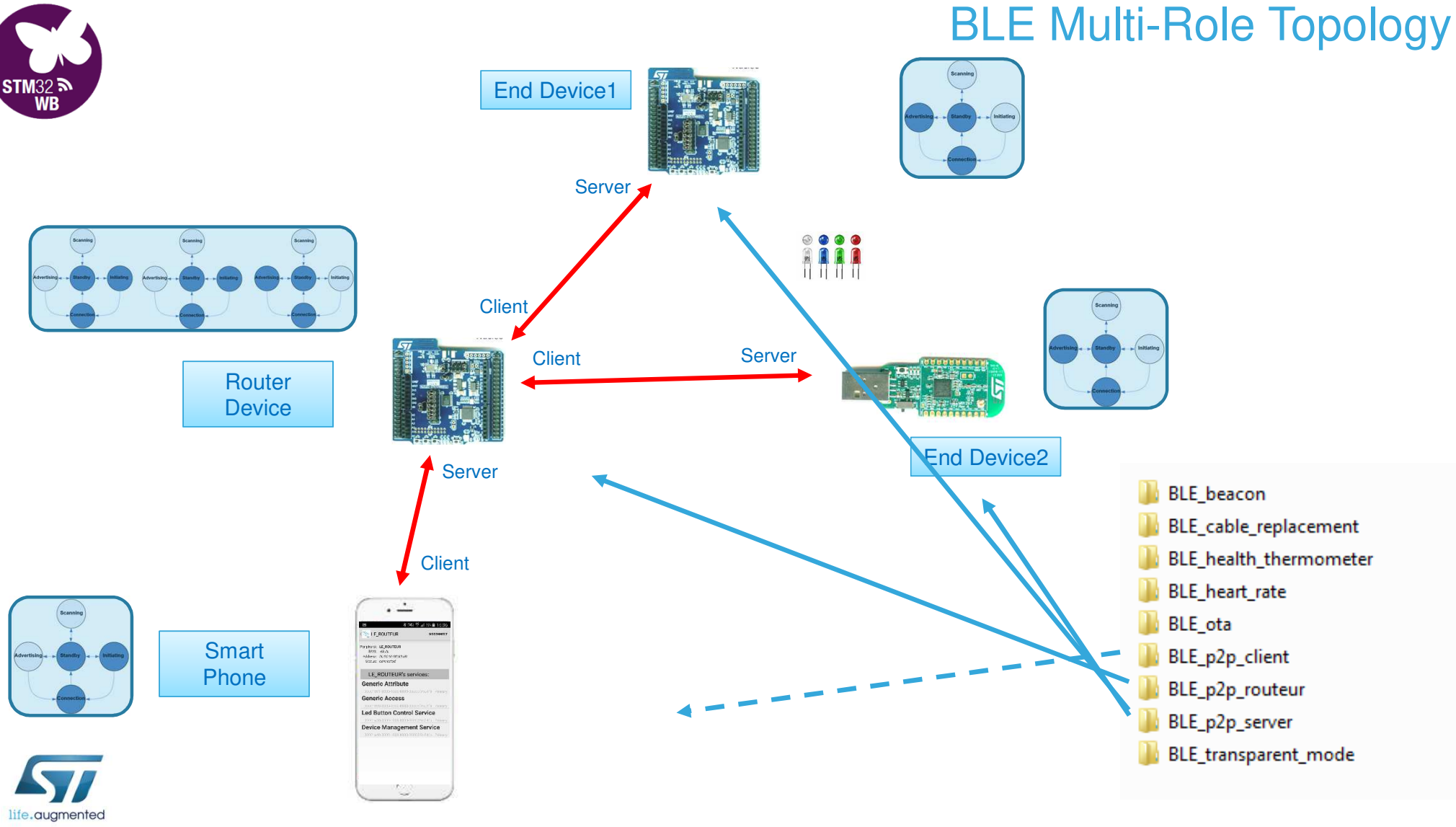
Thread

Bluetooth

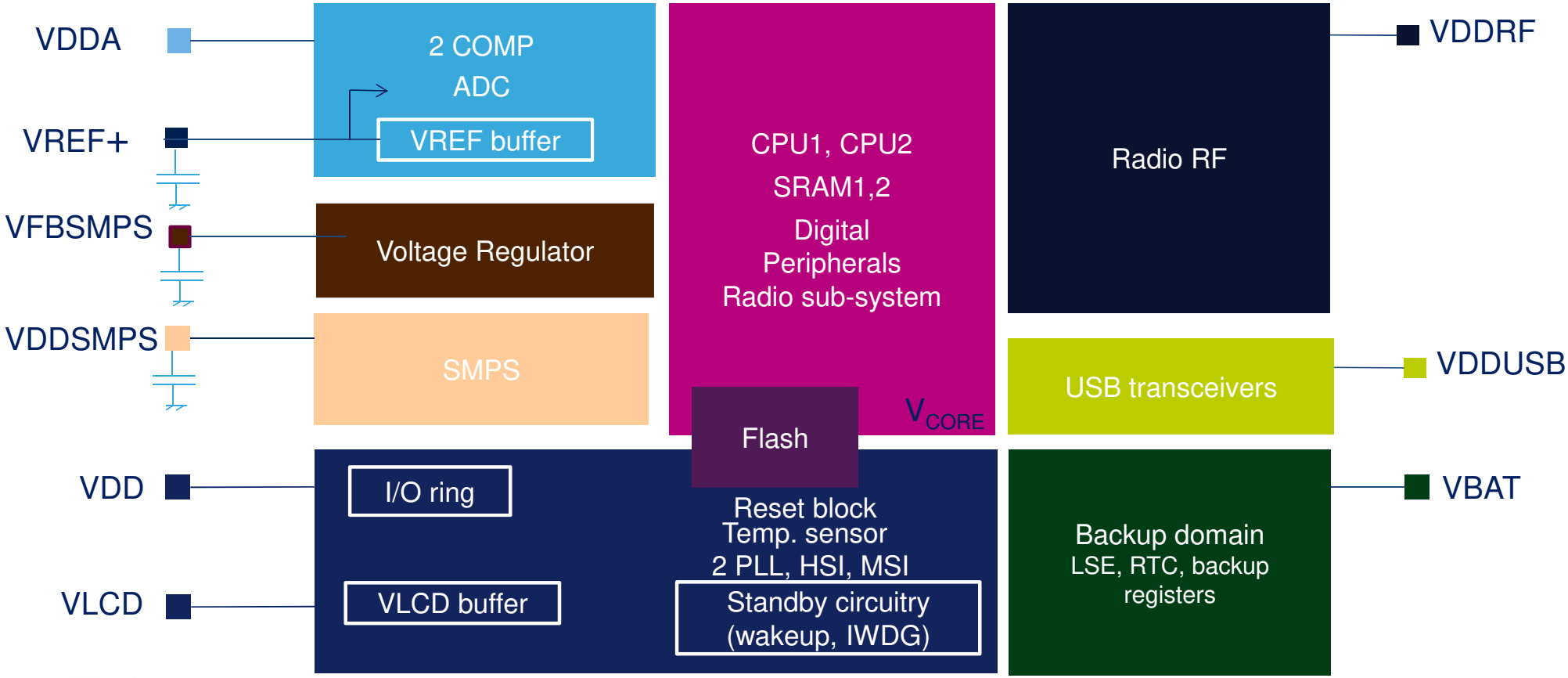


life.augmented

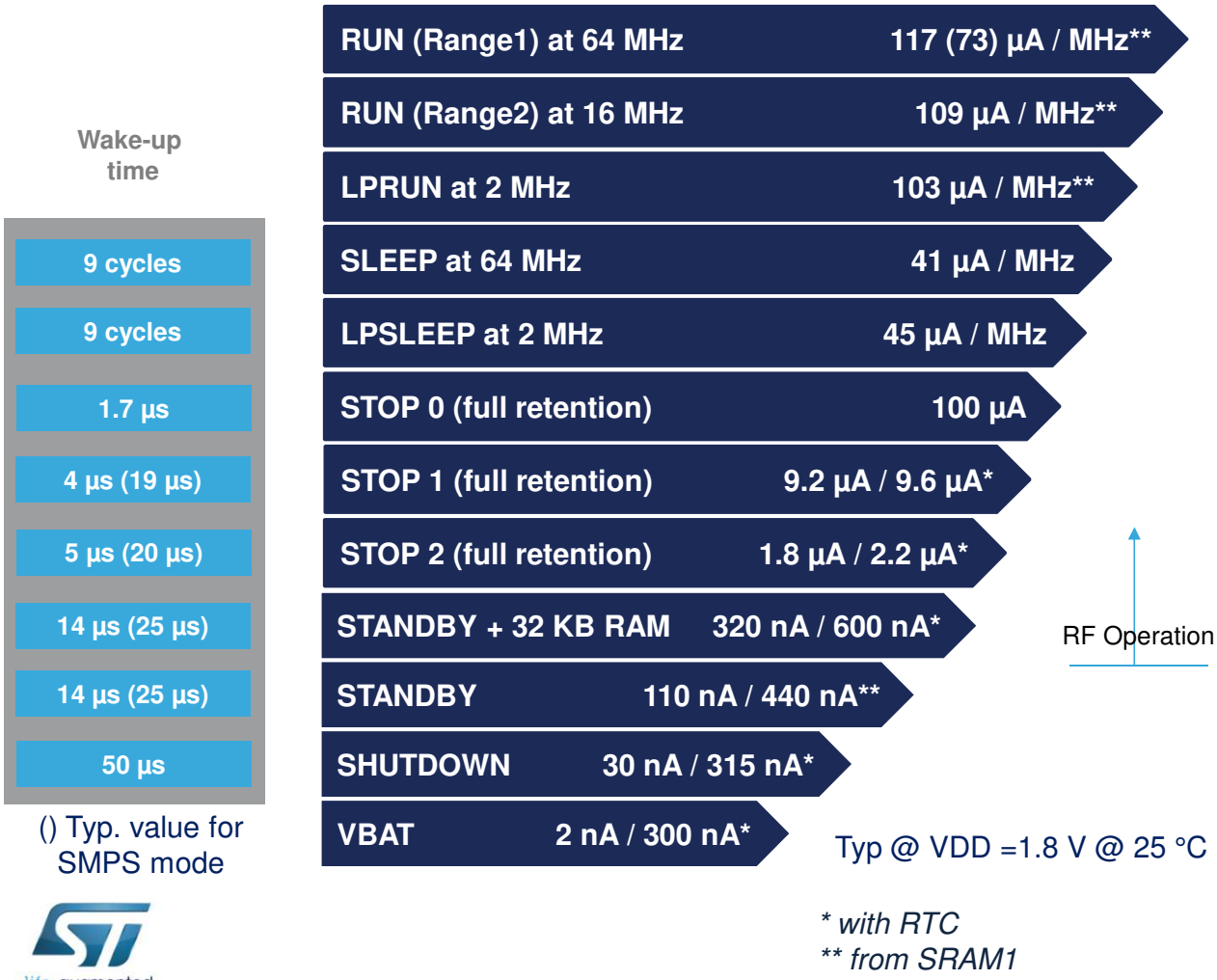
BLE Multi-Role Topology



Power schemes



Overview



() Typ. value for SMPS mode

Typ @ VDD =1.8 V @ 25 °C

** with RTC*
*** from SRAM1*

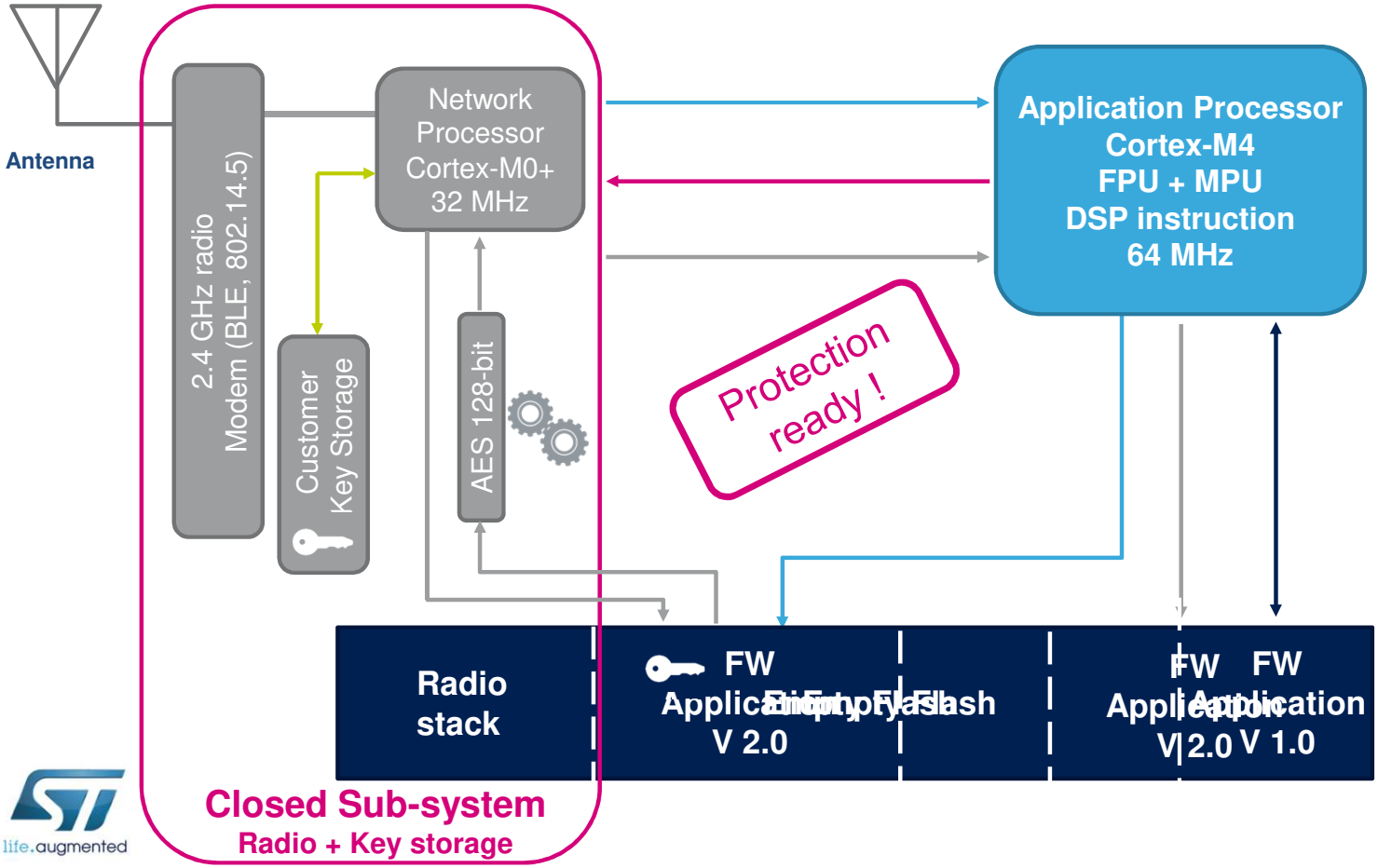
FlexPowerControl

- High performance
  - ➔ CoreMark score = 215
- Outstanding power efficiency
  - ➔ ULPBbench score = 175

life.augmented

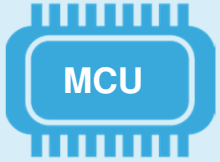
IoT Protection Ready

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
Non Invasive 	• Environment • Temp / Voltage / Clocks • Fault injection • Exploit debugger • Side channel • Power Analysis	• Temp sensor • Power supply monitor • Clock security system • Tamper pads • ECC, Parity check • SRAM mass erase • Read out protection • Flash-only boot
Software 	• Break the encryption • Extract keys • Exploit debugger / test modes • Malware • Replay	• Customer Key Storage • RNG, Crypto accelerator, CRC • Readout / Write memory protections • Memory Protection Unit • Root Security Service • Secure Firmware Update (SFU) • 96-bit Unique ID

life.augmented

Nucleo Pack

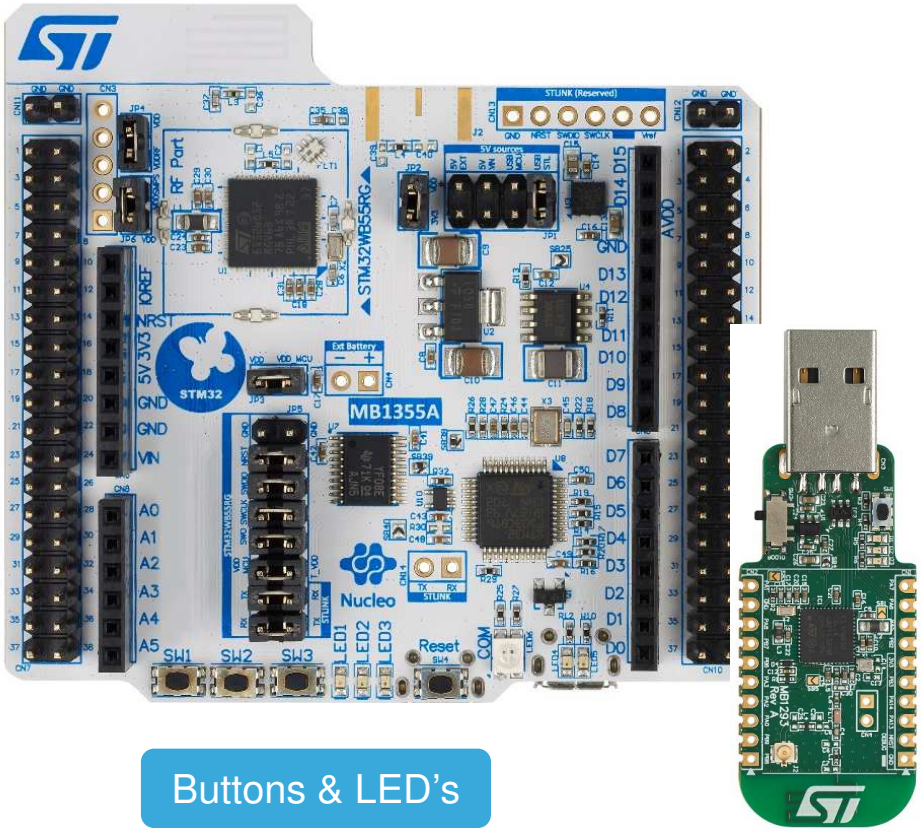
life.augmented

Nucleo

2.4GHz PCB antenna

STM32WB55RGV6
(VQFPN68)

Arduino & Morpho Headers



Buttons & LED's

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

life.augmented

Dongle

STM32WB55CGU6
(VQFPN48)

Button & LED’s

GPIO for simple apps

SWD interface
but no ST-Link

2.4GHz PCB antenna or uFL

life.augmented

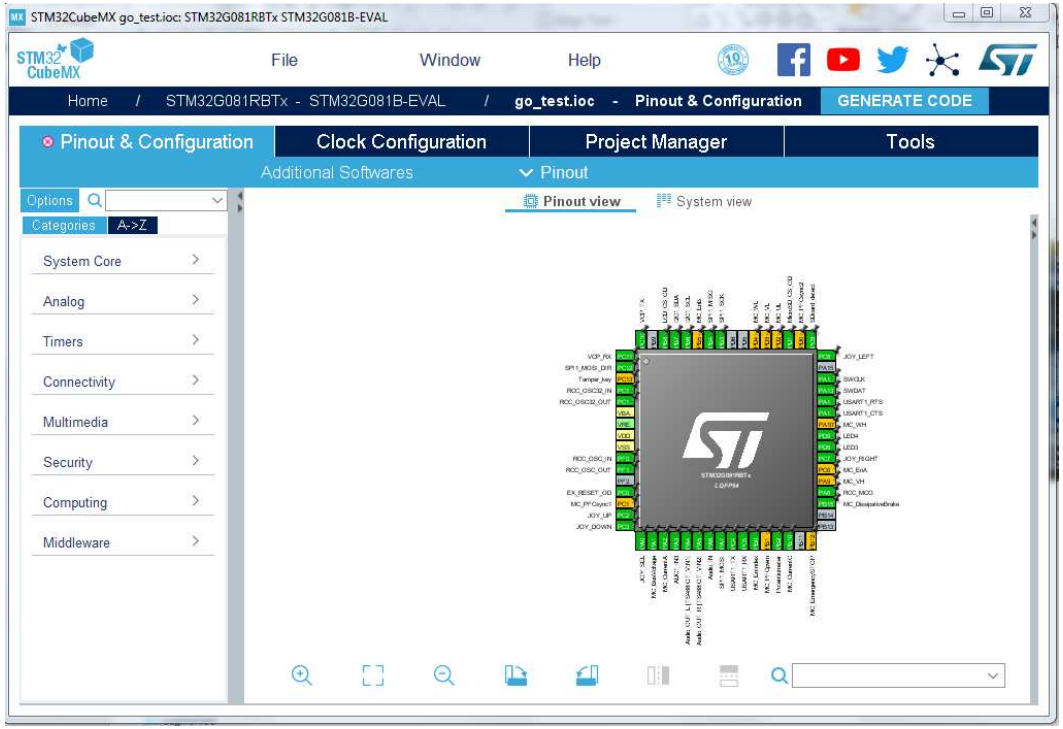
Cube Tools

- STM32CubeMX
- STM32CubeProgrammer
- STM32CubeMonitorRF
- CubeWB HAL Firmware

life.augmented

Cube Tools

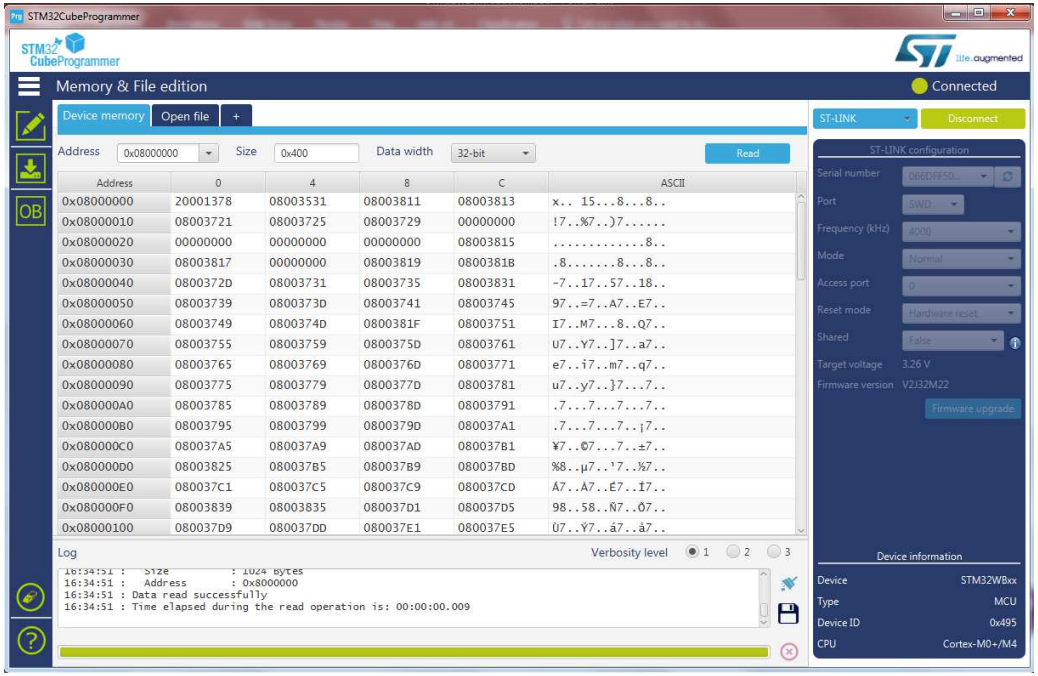
- STM32CubeMX
- STM32CubeProgrammer
- STM32CubeMonitorRF
- CubeWB HAL Firmware



life.augmented

Cube Tools

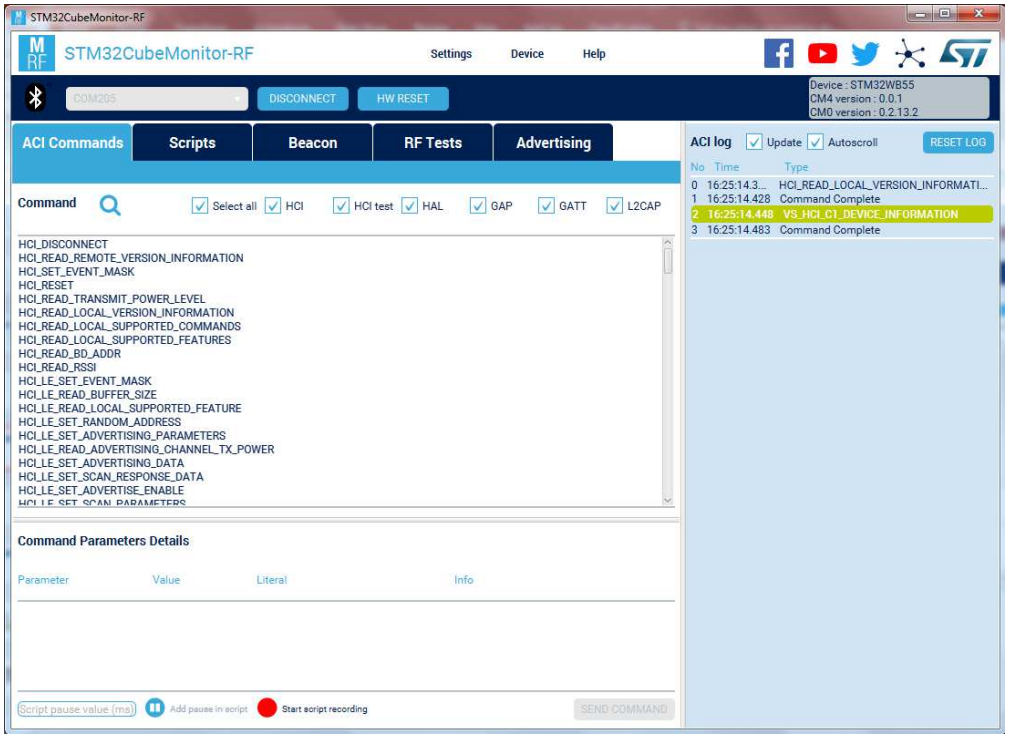
- STM32CubeMX
- STM32CubeProgrammer
- STM32CubeMonitorRF
- CubeWB HAL Firmware



life.augmented

Cube Tools

- STM32CubeMX
- STM32CubeProgrammer
- STM32CubeMonitorRF
- CubeWB HAL Firmware



life.augmented

Bonus Cube Tool!

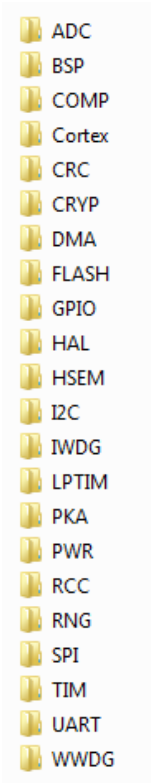
- STM32CubeMX
- STM32CubeProgrammer
- STM32CubeMonitor-Power
- CubeWB HAL Firmware

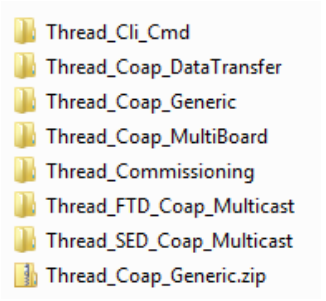
X-NUCLEO-LPM01A

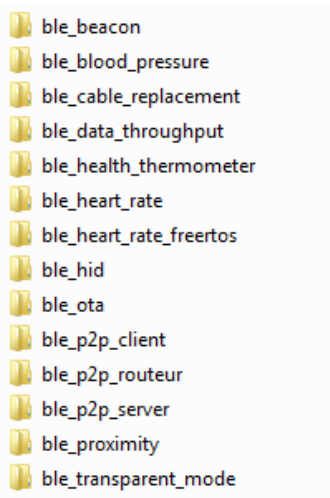
life.augmented

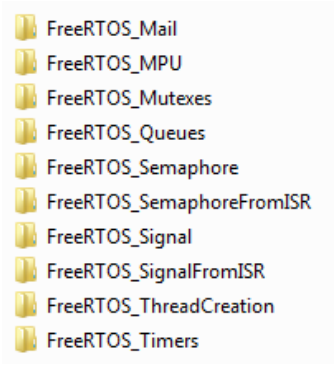
Cube Tools

- STM32CubeMX
- STM32CubeProgrammer
- STM32CubeMonitorRF
- CubeWB HAL Firmware





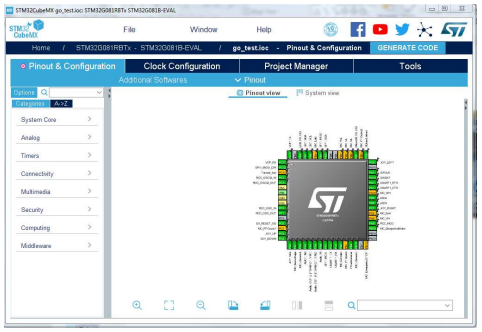




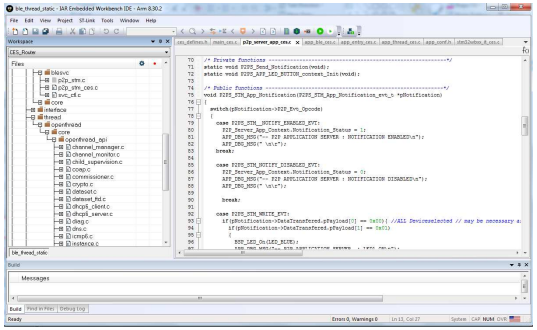
life.augmented

Iterative Design Process

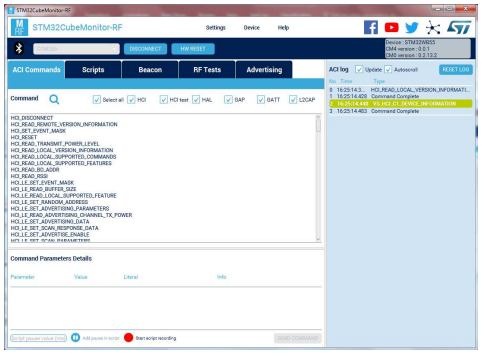
Configure



Code & Debug



Test



Measure

life.augmented

BOM cost

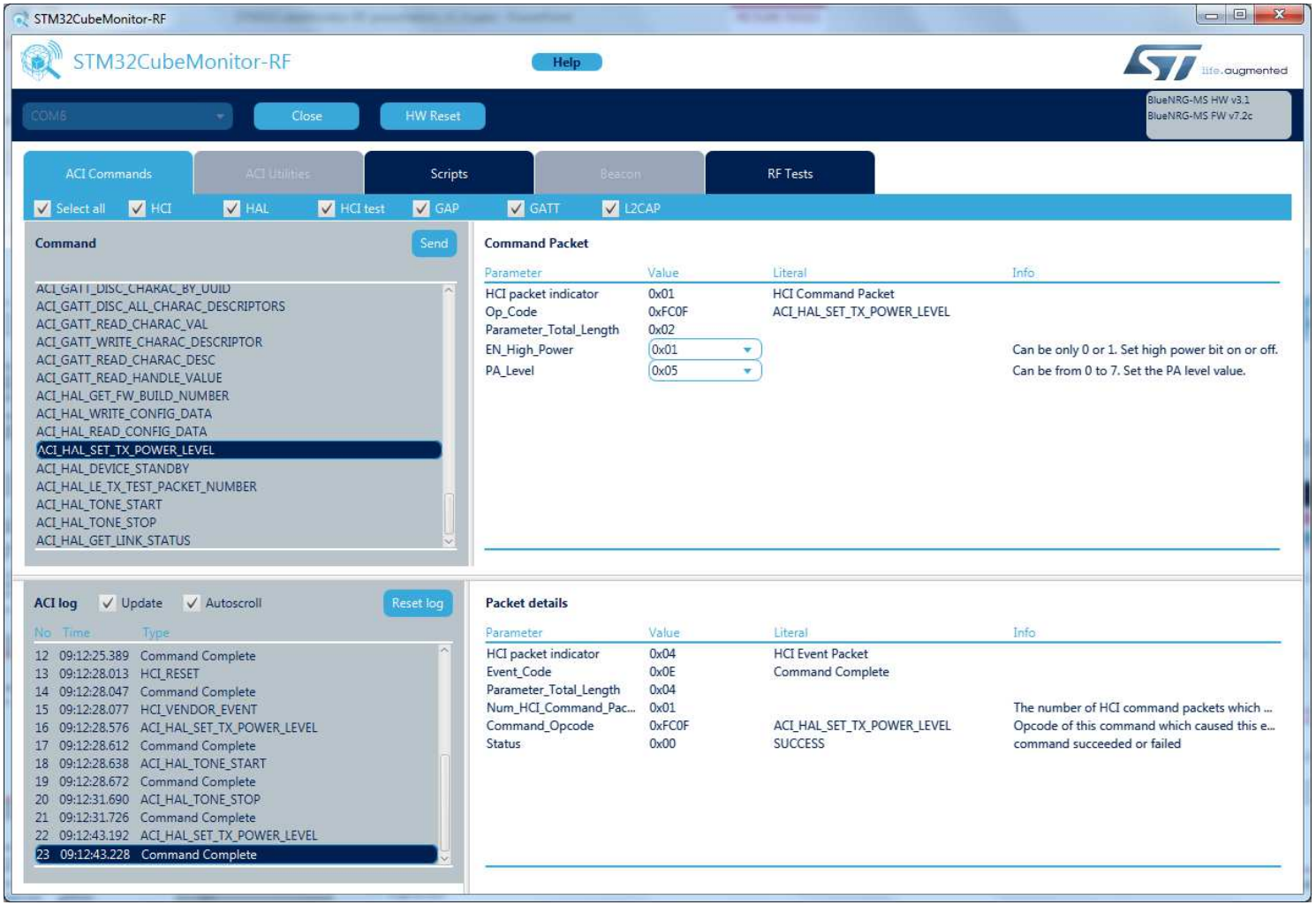
Silicon cost

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

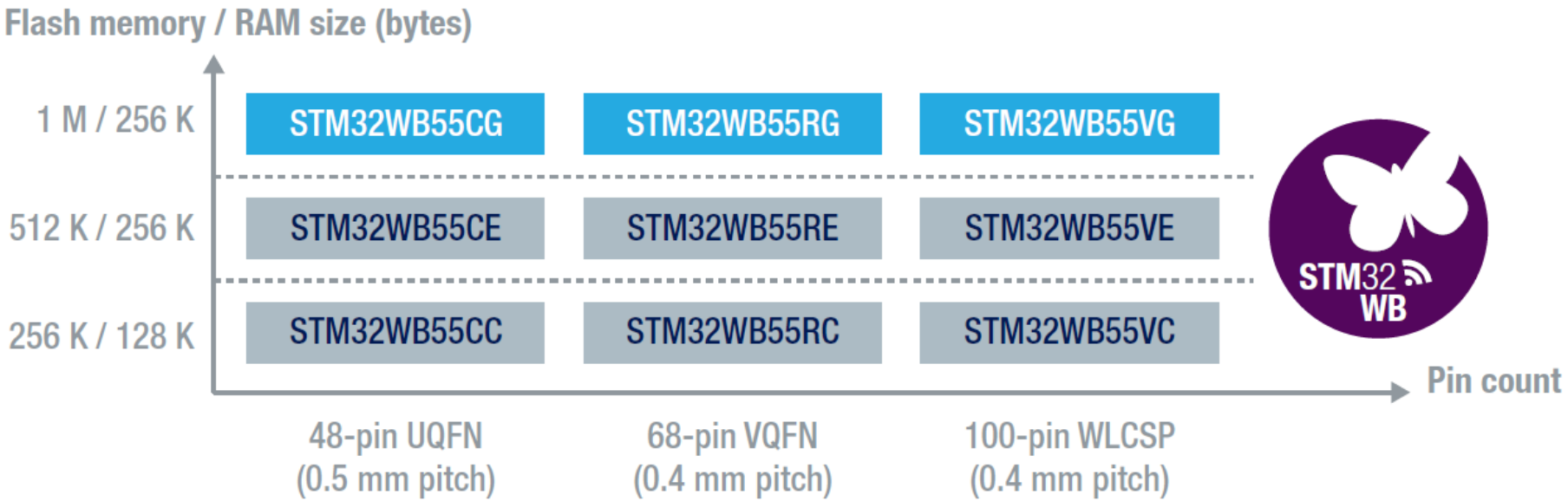
Ecosystem cost

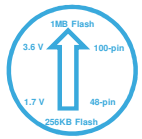
- BLE 5 stack
- OpenThread stack
- Open 802.14.5 MAC stack
- Zigbee 3.0 (coming soon!)
- STM32CubeMX
- STM32CubeMonitorRF
- Atollic C-compiler IDE

STM32CubeMonitorRF



STM32 offering





Releasing Your Creativity

/STM32 @ST_World ST community

life.augmented

www.st.com/stm32wb