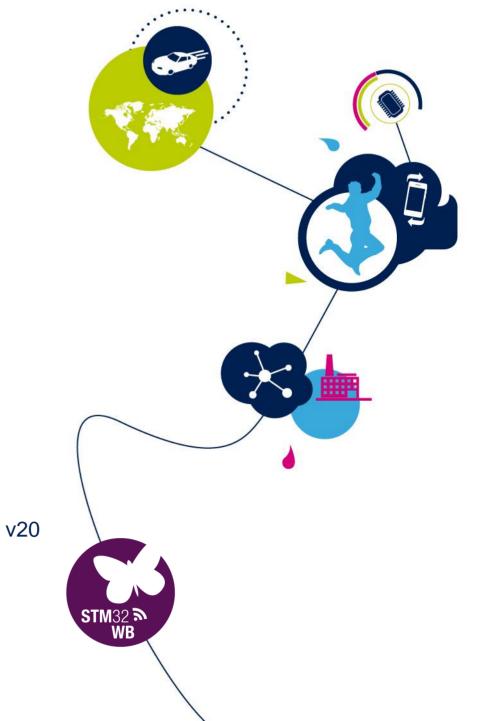
# STM32WB Workshop

Americas Marketing and Applications Team





#### Factoid of the Day

## Harald Blatand Gormsson, Danish King

Reign: 958-986



Haraldur Viegnomine Blaatond, Sorm, angli filius, Rex Danie partium Norv et julin Dhijegui Richardo Norman; Duis bis opon tulit torruite, Gallie Rogas Ludovium et to tharium cum olone M. Rominfifodd sancivit, confitutis apud Ecclofiar Starvie; Rep; Arbus: Epstepir, gros inter Poppo fuello, creditur; Lallum quog; Danieum; Danovircha dictum, curante matre Thyra, instaureri et firmius muniri focit; fieblato, Marchione stervicente.





#### Factoid of the Day

#### a.k.a. Harald "Bluetooth" Gormsson

Bluetooth: A wireless technology named after Harald Bluetooth, with the analogy that Bluetooth would unite devices like Harald Bluetooth united the tribes of Denmark into a single kingdom.



Haraldus Vicomomino Blastond, Sorm, angli filius, Rex Danie partium Norv et julini Digi qui Richardo Norman : Dui bes opom tulit torruita; Gallie Reges Ludousum et totharium: cum ottone M. Rominif foedu sancevit, confribute apud Ecclofiar Starvic; Rep: Arbus: Leofiopir, gros inter Poppo fuello, creditur: Lallum quog; Danicum. Danovircha dictum, curante matre Thira, unteurari et firmius muniri focit: fue lato, Marchione storvicente.







## **STM32WB Introduction**

### **BLE Basics**

**Tools & Firmware** 

### Lot's of Hands-On coding!

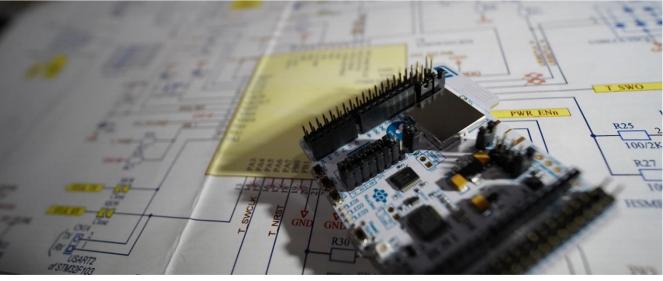
An examination of the desider of any





8:00	Welcome and Tools install (if need	ded) 1:00
9:00	A few words	
	Hands-On: Out-of-the-Box	
	Hands-On: CubeMX	2:15
	BLE Basics	
	Hands-On: HRM	2:45
10:30	Break	and the second
	Architecture	1 151 2 2 1 T .
	Hands-On: CubeMonitorRF	A state of the sta
12:00	Lunch (1h)	

1:00	More WB Detail
	Hands-on: Cable replacement
	Hardware considerations
2:15	Break
	Hands-on: OTA Firmware Updates
2:45	Wrap-Up, Q&A, Survey







#### Prerequisites

6

#### Windows 7/10

- Java JRE v8 (v1.80.0\_191 or newer)
- CubeMX, CubeWB, CubeMonitorRF, CubeProgrammer

IC: STM32WI

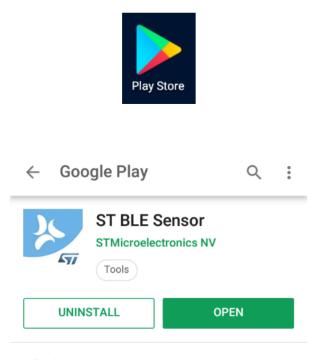
- □ ST BLE Sensor App
- LightBlue Explorer App
- □ IAR EWARM, v8.40.1 + License
- TeraTerm, or equiv.







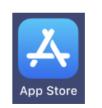
#### ST BLE Sensor app, v4.3



What's new • Last updated Oct 12, 2018

- App renamed to ST BLE Sensor

- Added support to the STM32WB firmware update
- Added STM32WB P2P Server demo





Not Enough Ratings

What's New

Version 4.2.2

Version History

22h ago

Age

Added support to FP-INDPREDMNT1 function pack
Improveed FFT export data form more

#### Preview







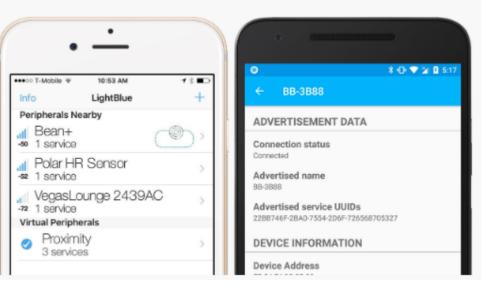
#### LightBlue Explorer

# PunchThrough

#### LightBlue Explorer

The industry-leading BLE test app for iOS and Android. Used by over a half million people, LightBlue Explorer lets you scan, connect to and browse any nearby Bluetooth Smart device. Includes full support for logging data and simulating peripherals.





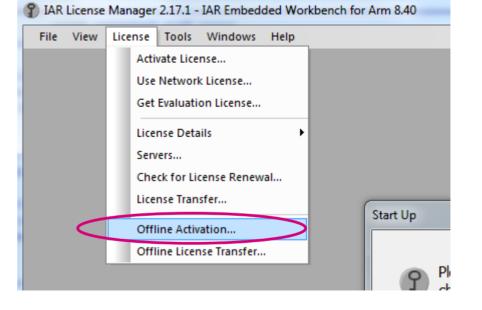




#### IAR EWARM 8.40.1 - License Installation

- Activate the time-limited evaluation license with Activation Response file included in the provided zip file
- From IAR Embedded Workbench, go to Help->License Manager
- From the License manager, go to License->Offline Activation

ile Edit View Project ST-Link Tools Window	Help	
	Content Index Search Product Updates Release Notes IDE Project Management and Building Guide C/C++ Development Guide Assembler User Guide MISRA-C:1998 Reference Guide (Non-C-STAT) MISRA-C:2004 Reference Guide (Non-C-STAT) C-SPY Debugging Guide C-STAT Static Analysis Guide IAR Debug probes User Guide JTAGjet-Trace User Guide Migration IAR on the Web	
uid C	Information Center	-
mo	About	





life.auamen<sup>.</sup>

#### IAR EWARM 8.40.1 - License Installation

# Click "Use an activation response file from IAR Systems" option

License Wizard	×
	<b>PIAR</b> YSTEMS
This wizard will help you to activate a license when the License Ma cannot access the internet.	inager
Generate an activation information file to send to IAR Syster	ns.
License number: XXX-XX-XXX-XXX	
The license number is usually in the format XXX-XXX-XXX	(-XXXX.
Use an activation response file from IAR Systems:	
•	
< <u>B</u> ack <u>N</u> ext >	Cancel

#### Open the ActivationResponse\_7900-043-869-0401.txt file

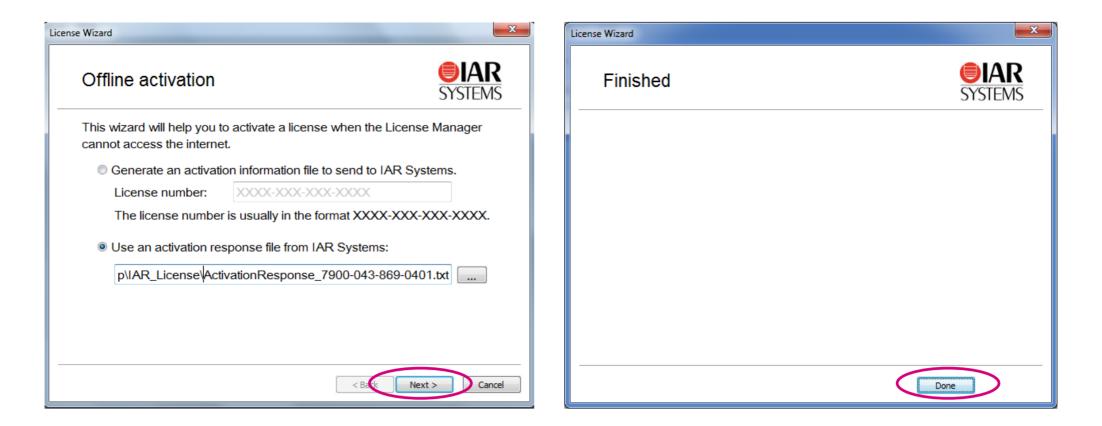
P Open	-	0
	_License 🗸 🗸	Search IAR
Organize 🔻 New folder		
Desktop Name	Date modified	Туре
Recent Places ActivationResponse_7900-043-869-0401.txt	6/7.2019 8:18 AM	Text Document
📃 Desktop 浸 Libraries		





#### IAR EWARM 8.40.1 - License Installation

#### Click "Next"

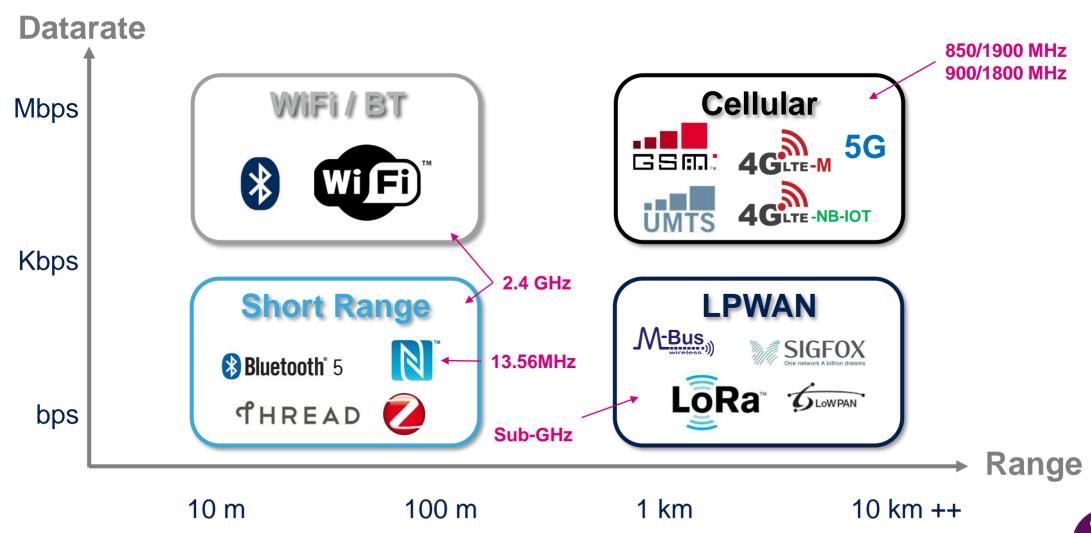








#### **Communication Technologies**







#### Low-data-rate 2.4GHz connectivity



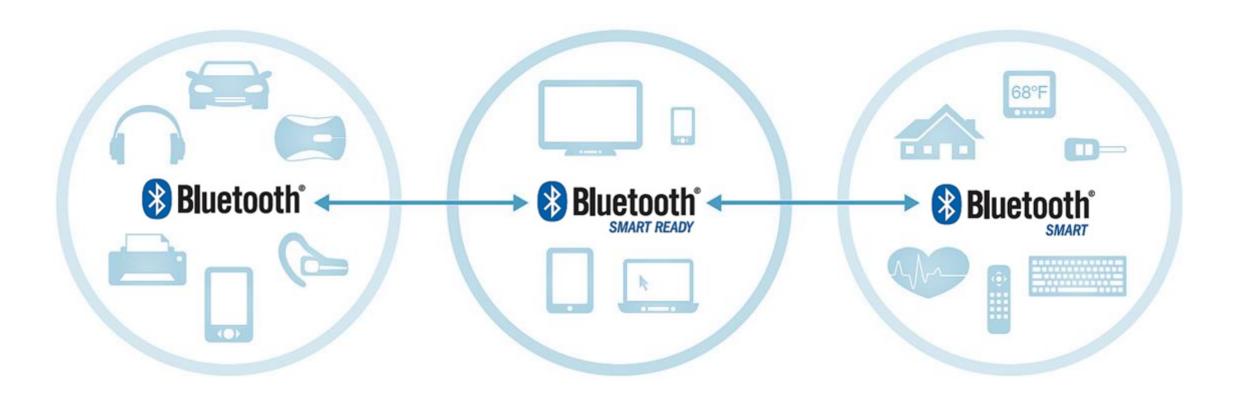
Point-to-point communication with smartphones and other wireless devices

BLE Mesh / 802.15.4 Home automation with Mesh network





#### Classic? Smart Ready? Smart?

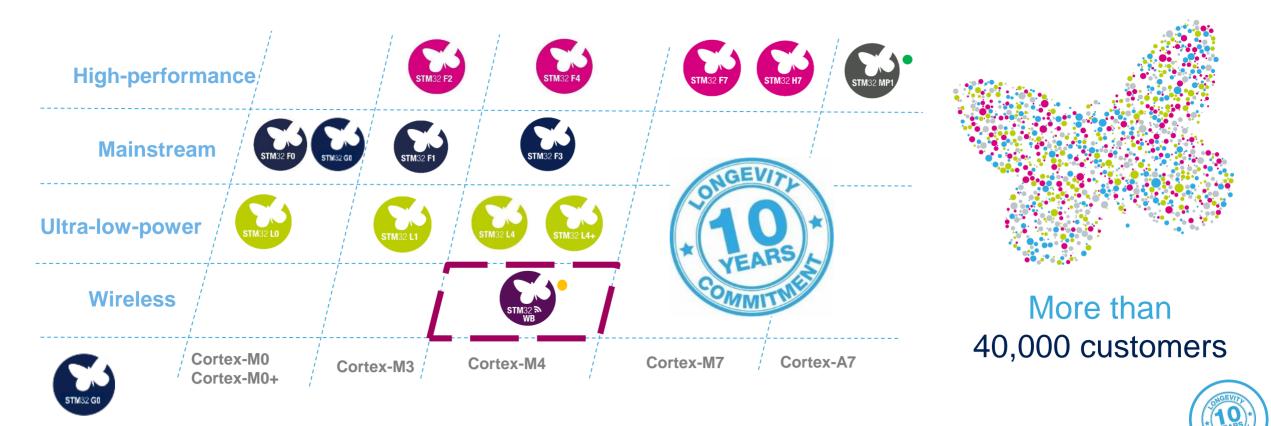






"SMART READY" and "SMART" are abandoned markings

#### STM32 Portfolio



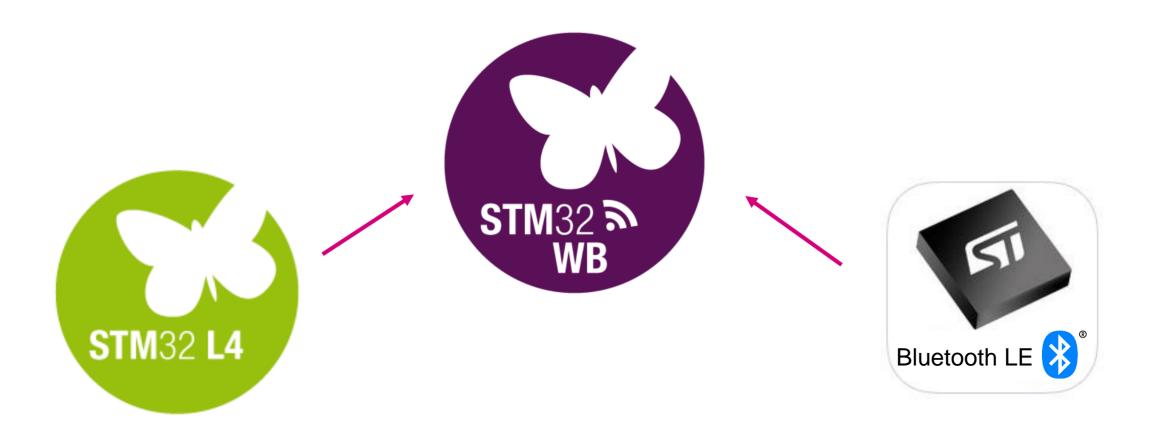
Legend: Cortex-M0+ Radio Co-processor



• Legend: Single or Dual-Core A7 with Cortex M4



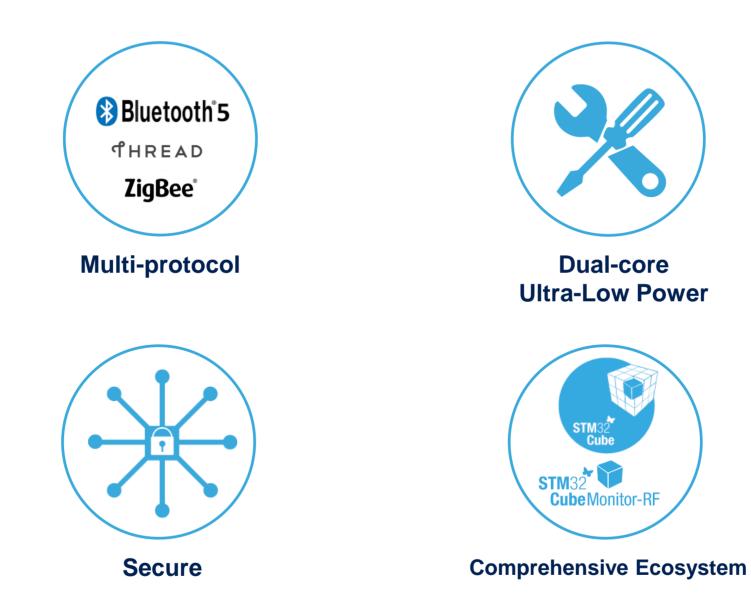
#### Ultra-low-power and RF







#### STM32WB Key Takeaways



life.augmented

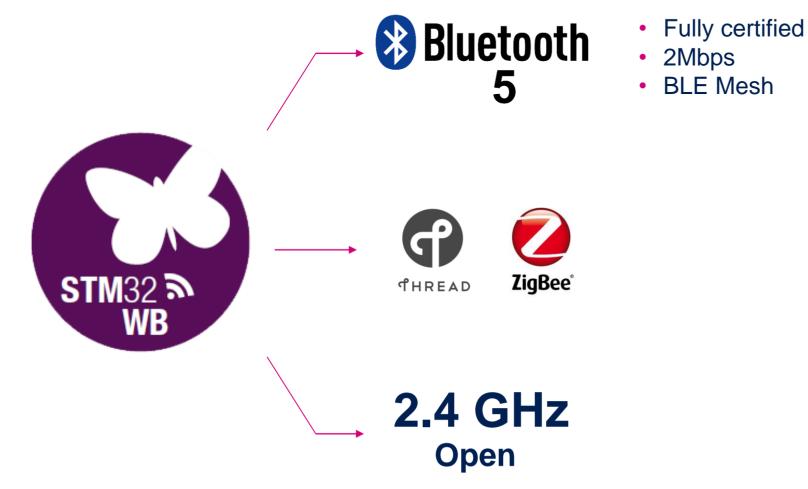


**Multiprotocol** 





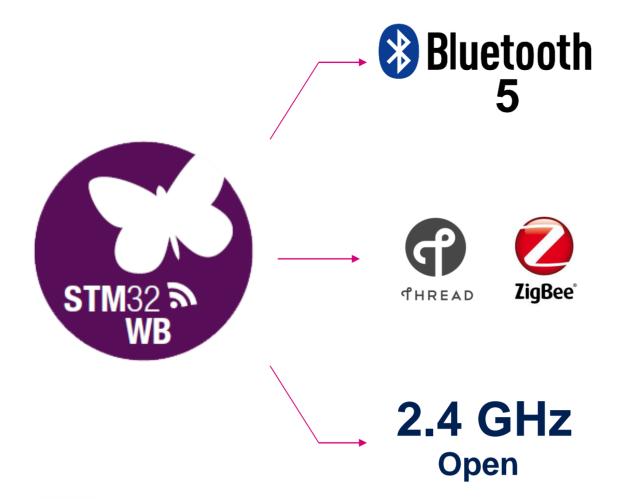








**Multiprotocol** 



• Zigbee 3.0

•

OpenThread

Concurrent BLE + OpenThread





**Multiprotocol** 

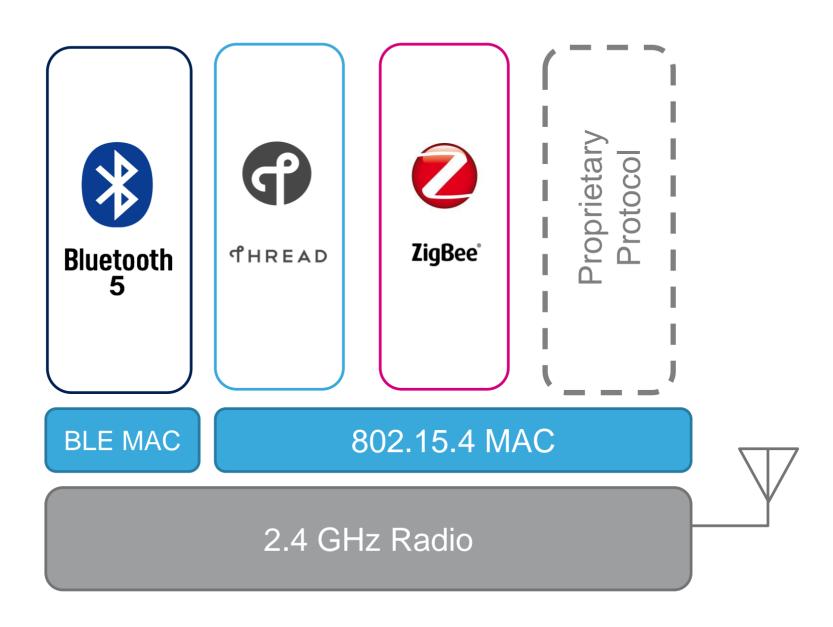








#### Stack + MAC + PHY





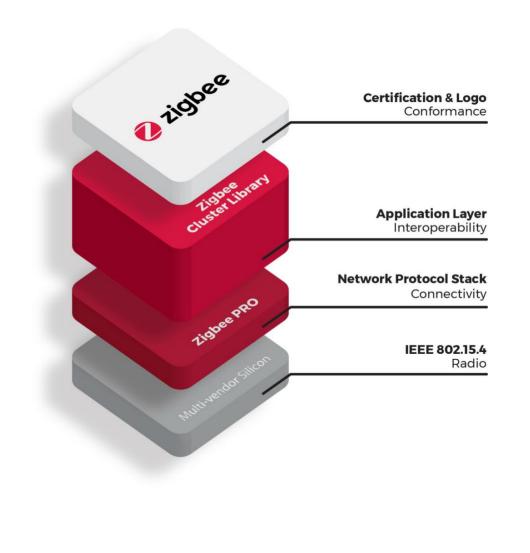


#### Zigbee 3.0 Stack

- Fully certified
- Legacy cluster support
- Revision R21 to R23
- Coming in late 2019

Coming soon in the

ecosystem !







#### A word about Thread

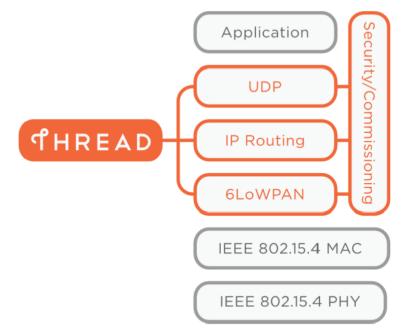
# **THREAD** What it delivers

# 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





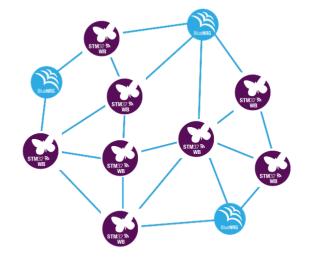
#### **Bluetooth Mesh vs Thread**

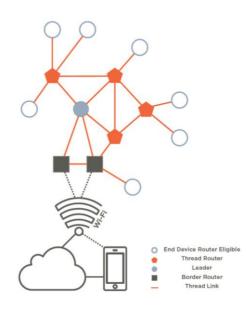
#### **Bluetooth Mesh**

- Based on Bluetooth 4.0 and later
- Broadcast type, flood the network with messages, no routing
- Shorter range, 3kbps application data rate, 1Mbps on-air bit-rate
- High power consumption

#### Thread

- IPv6-based using 802.15.4 MAC
- Routing table approach with network self healing
- Medium range, 40Kbps application data rate, 250Kbps on-air bit-rate
- Low power consumption









26

### STM32CubeMX



## STM32CubeProgrammer



## STM32CubeMonitorRF



### STM32CubeWB





## STM32CubeMX

### STM32CubeProgrammer

### STM32CubeMonitorRF





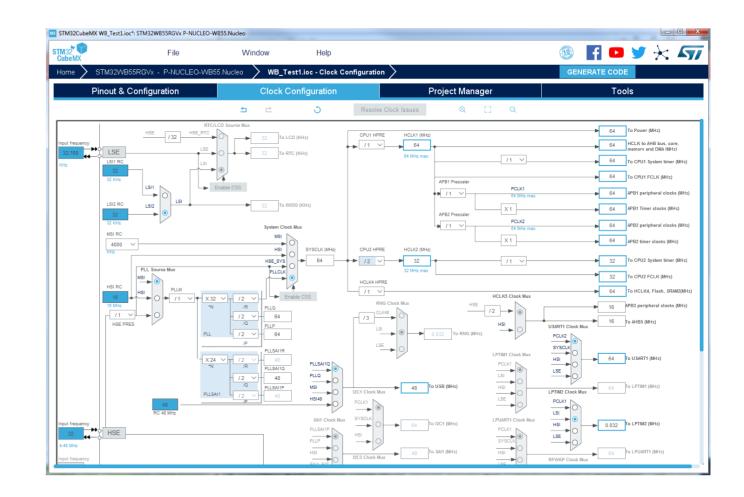


## STM32CubeMX

### STM32CubeProgrammer

### STM32CubeMonitorRF

### CubeWB HAL Firmware





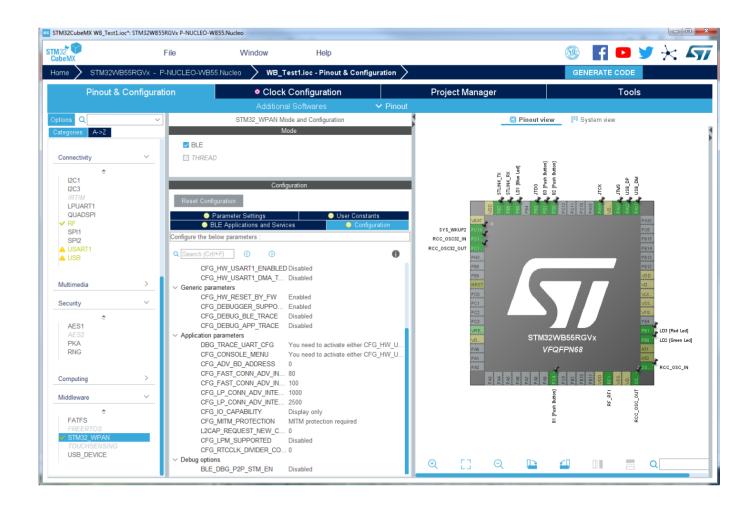


## STM32CubeMX

### STM32CubeProgrammer

### STM32CubeMonitorRF

### **CubeWB HAL Firmware**







### STM32CubeMX

### STM32CubeProgrammer

### STM32CubeMonitorRF

### **CubeWB HAL Firmware**

beMX		File	W	/indow		Help									6	19	- 1				$\mathbf{k}$	5
ne	STM32VVB55RGVx	- P-NUCLEO-WB55	.Nucleo	> w	B_Test1	ioc - Tool:	\$									GEN	ERA	ТЕ СО	DE			
	Pinout & Configu	uration		Olo	ock Co	nfiguratio	n			Pro	oject Mar	ager						Т	ools			
						×	Powe	۶r														
	Change	Reset		Step							Sequence						][ <sup>Trai</sup>	nsitions	Check	er		
				( e	Ū	D	三介	≣ĵ	5	$\square$	e		Ŵ	Ľ	6 <u>1</u> 7	0	<b>_</b>	On	og	Help		
	In Series 2 🌲	In Parallel 1 🌲		Sequ	ence Table																_	
	Capacity	1250.0 mAh			Step	Mode	2.2	Vdd	Range/S		Memory		Bus Free		ck Config		ripher		Step Cu	urrent	Dura	
	Self Discharge	0.3 %/month		2		RUN STOP0	3.3 3.3		NoRange		LASH/ART/ LASH/ART/		z		LL Reg				mA 05 μA		100 ms 50 ms	
	Nominal Voltage	3.0 V		3		LOWPOWE			NoRange		RAM1 Flas				Regulato.			1.	13 mA		20 ms	
0	Max Cont Current	400.0 mA		4		STANDBY RUN	3.3 3.3		NoRange Range1-H		LASH/ART LASH/ART/	0 Hz 32 MH	7		RTC Re Regulat				50 nA .15 mA		200 ms 150 ms	
				Ŭ			0.0		rungern	g		. 02 1111	-		roguiut			0.	10 110 1		100 1110	
	Configuration Parameters BLE Mode Tx Payload (Byte)	At V <sub>DD</sub> 3.3V Connected Slave	<ul> <li>✓</li> <li>6 ♣</li> </ul>	Displa Plot:	All Steps	~				G	onsumptio	n Profil	a hy St	en								
	Connection Interval (ms)	1	000								onsumptio	Prom	e by St	ep								;
	Power Level	0 dBm	~	5	.0	+																
	Average Consumption	SMPS / No SPMS		4	.5	1:RUI	N															
					.0 -														5:RUN			
	STOP2	15.15 µA / 18.86 µA		2	.5														Ļ			
	STOP2 STOP1	15.15 µА / 18.86 µА 25.17 µА / 28.87 µА		23												<u> </u>		_				
			4	/m) u	.0																	
	STOP1	25.17 μA / 28.87 μA	٩	ption (m/	.0																	
	STOP1 STOP0 Peak Consumption Information Notes	25.17 μΑ / 28.87 μΑ 129.97 μΑ / 133.67 μ 9.45 mA / 14.28 mA	Ą	sumption (m/	.0 -																	
	STOP1 STOP0 Peak Consumption Information Notes * Vdd with SMPS	25.17 μA / 28.87 μA 129.97 μA / 133.67 μ 9.45 mA / 14.28 mA 3.3V, 2.4V, 1.8V	A	Consumption (m/	.0				3:LP_	RUN												
	STOP1 STOP0 Peak Consumption Information Notes * Vdd with SMPS * Vdd without SMPS	<b>25.17 μA / 28.87 μA</b> <b>129.97 μA / 133.67 μ</b> 9.45 mA / 14.28 mA 3.3V, 2.4V, 1.8V 3.3V, 2.4V, 1.8V							3:LP_ ↓	RUN												
	STOP1 STOP0 Peak Consumption Information Notes * Vdd with SMPS * Vdd without SMPS * Power Range	25.17 μA / 28.87 μA 129.97 μA / 133.67 μ 9.45 mA / 14.28 mA 3.3V, 2.4V, 1.8V 3.3V, 2.4V, 1.8V Range1 with/without :		1	.0			2:5'	3:LP_ ↓ TOP0	RUN		g.C	ANDRY									
	STOP1 STOP0 Peak Consumption Information Notes * Vdd with SMPS * Vdd without SMPS * Power Range * PHY link Rate	25.17 μA / 28.87 μA 129.97 μA / 133.67 μ 9.45 mA / 14.28 mA 3.3V, 2.4V, 1.8V 3.3V, 2.4V, 1.8V Range1 with/without 3 1 MBit/s		1				2:5'	Ļ	RUN		4:S	ANDBY									
	STOP1 STOP0 Peak Consumption Information Notes * Vdd with SMPS * Vdd without SMPS * Power Range	25.17 μA / 28.87 μA 129.97 μA / 133.67 μ 9.45 mA / 14.28 mA 3.3V, 2.4V, 1.8V 3.3V, 2.4V, 1.8V Range1 with/without :		1	.0	5 50	75 10	Ļ	торо		225 10	ţ		225	250	275	400	125	450	475	500	25
	STOP1 STOP0 Peak Consumption Information Notes * Vdd with SMPS * Vdd without SMPS * Power Range * PHY link Rate	25.17 μA / 28.87 μA 129.97 μA / 133.67 μ 9.45 mA / 14.28 mA 3.3V, 2.4V, 1.8V 3.3V, 2.4V, 1.8V Range1 with/without 3 1 MBit/s		1	.0	5 50	75 10	2:5'	Ļ		1 225 25	ţ	300	325	350	375	400	425	450	475	500 5	525
	STOP1 STOP0 Peak Consumption Information Notes * Vdd with SMPS * Vdd without SMPS * Power Range * PHY link Rate	25.17 μA / 28.87 μA 129.97 μA / 133.67 μ 9.45 mA / 14.28 mA 3.3V, 2.4V, 1.8V 3.3V, 2.4V, 1.8V Range1 with/without 3 1 MBit/s		1	.0	5 50	75 10	Ļ	торо	5 200	1 225 25	50 275 Time (r	300 1 <b>s)</b>	_	350	375	400	425	450	475	500 5	525





### STM32CubeMX

### STM32CubeProgrammer

### STM32CubeMonitorRF

Memory & Fil	e edition						🔵 Connecte
Device memory	Open file +					ST-LINK	- Disconne
Address 0x080	000000 - Size	0x400	Data width	32-bit 💌	Read	ST-L	LINK configuration
Address	0	4	8	с	ASCII	Serial number	066DFF50
0x08000000	20001378	08003531	08003811	08003813	x 1588	Port	SWD -
0x08000010	08003721	08003725	08003729	00000000	!7%7)7	Frequency (kHz	
0x08000020	00000000	00000000	00000000	08003815	8	Frequency (KH2)	4000
0x08000030	08003817	00000000	08003819	0800381B	.888	Mode	Normal
0x08000040	0800372D	08003731	08003735	08003831	-7175718	Access port	0
0x08000050	08003739	0800373D	08003741	08003745	97=7A7E7	Reset mode	
0x08000060	08003749	0800374D	0800381F	08003751	I7M78Q7		Hardware reset
0x08000070	08003755	08003759	0800375D	08003761	U7Y7]7a7	Shared	False
0x08000080	08003765	08003769	0800376D	08003771	e7i7m7q7	Target voltage	
0x08000090	08003775	08003779	0800377D	08003781	u7y7}77	Firmware versio	
0x080000A0	08003785	08003789	0800378D	08003791	.7777		
0х080000в0	08003795	08003799	0800379D	080037A1	.77717		
0x080000C0	080037A5	080037A9	080037AD	080037B1	¥7077±7		
0x080000D0	08003825	080037B5	080037в9	080037BD	%8μ7 <sup>1</sup> 7½7		
0x080000E0	080037c1	080037C5	080037C9	080037CD	Á7Å7É7Í7		
0x080000F0	08003839	08003835	080037D1	080037D5	9858Ñ7Õ7		
0x08000100	080037D9	080037DD	080037E1	080037E5	Ù7Ý7á7å7	~	
Log					Verbosity level 💿 1 💿 2	3	vice information
10:34:51 : 5	1ze : 10	24 вутеs 8000000			^	Device	STM3

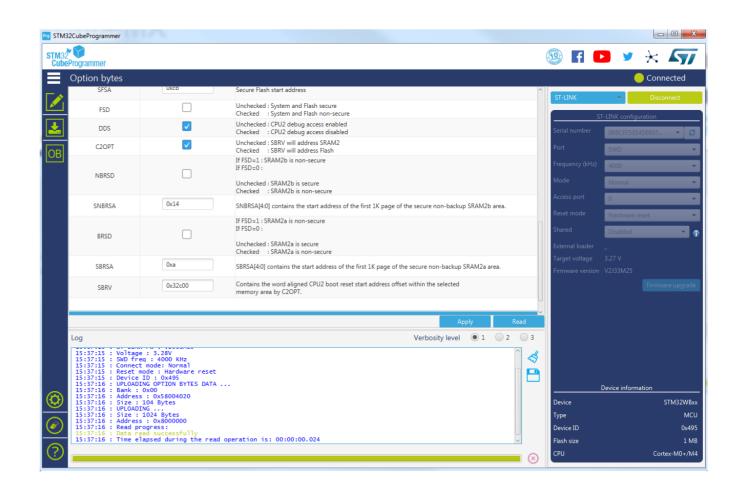




### STM32CubeMX

## STM32CubeProgrammer

### STM32CubeMonitorRF



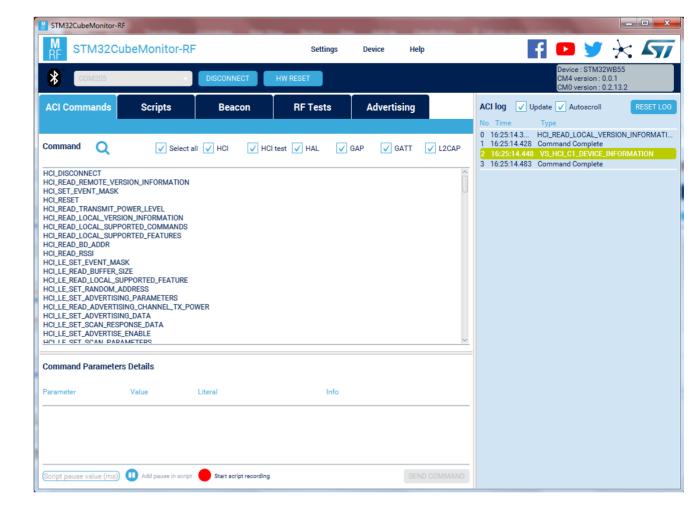




### STM32CubeMX

### STM32CubeProgrammer

### STM32CubeMonitorRF







FreeRTOS Mail

FreeRTOS MPU

FreeRTOS Mutexes

FreeRTOS Queues

FreeRTOS\_Signal

FreeRTOS Timers

CDC Standalone

DFU Standalone

HID Standalone

Mac 802 15 4 FFD

Mac 802 15 4 RFD

MSC Standalone

FreeRTOS Semaphore

FreeRTOS SemaphoreFromISR

FreeRTOS\_SignalFromISR

FreeRTOS ThreadCreation

### STM32CubeMX

### STM32CubeProgrammer

### STM32CubeMonitorRF

## **CubeWB HAL Firmware**





ADC

BSP

COMP

Cortex

CRC

CRVP

DMA

FLASH

GPIO

HAL

12C

IWDG

LPTIM

ΡΚΑ

PWR

RCC

RNG

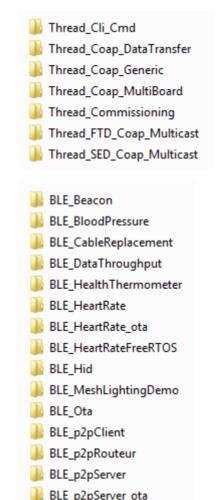
SPI

TIM

UART

WWDG

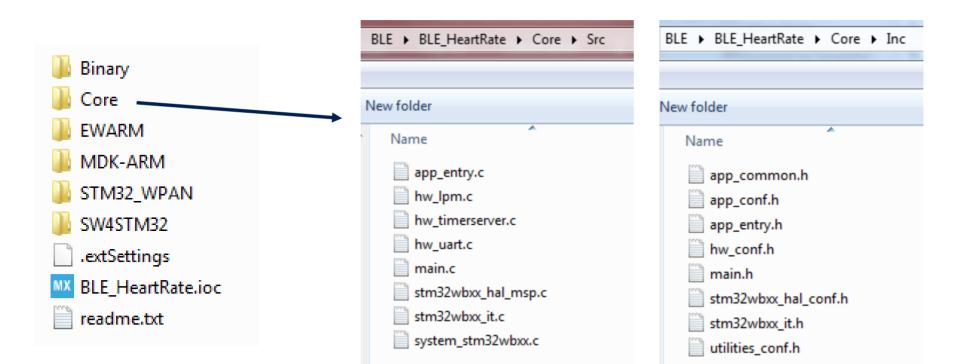
HSEM



- BLE\_p2pServer\_ota
- BLE\_Proximity
- BLE\_TransparentMode

#### CubeWB firmware

#### Core folder contains application-related source code

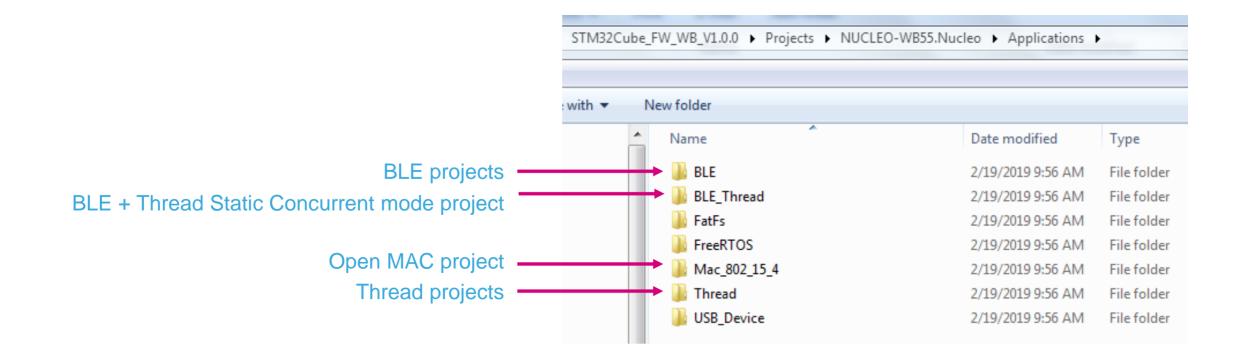






#### CubeWB firmware

#### Different stacks required for different application types









#### CubeWB firmware

"STEP 4" of flash procedure

Date 02/06/2019 02/06/2019 02/06/2019 02/06/2019 02/06/2019 02/06/2019 02/06/2019

#### Encrypted radio stack binaries here

pository   STM32Cube_FW_WB_V1.0.0   Project	ts ► STM32WB_Copr	o_Wireless_Binaries	<b>- - </b> ∮ <del>•</del>
Share with 🔻 New folder			
Name	Date modified	Type	Size
📀 Release_Notes.html	2/19/2019 9:56 AM	Chrome HTML Do	7 KB
stm32wb5x_BLE_HCILayer_fw.bin	2/19/2019 9:56 AM	FTE Binary Export	90 KB
stm32wb5x_BLE_Stack_fw.bin	2/19/2019 9:56 AM	FTE Binary Export	154 KB
stm32wb5x_BLE_Thread_fw.bin	2/19/2019 9:56 AM	FTE Binary Export	481 KB
stm32wb5x_Mac_802_15_4_fw.bin	2/19/2019 9:56 AM	FTE Binary Export	50 KB
stm32wb5x_rfmonitor_phy802_15_4_fw.bin	2/19/2019 9:56 AM	FTE Binary Export	30 KB
stm32wb5x_Thread_FTD_fw.bin	2/19/2019 9:56 AM	FTE Binary Export	330 KB
stm32wb5x_Thread_MTD_fw.bin	2/19/2019 9:56 AM	FTE Binary Export	243 KB

#### HTML file details update procedure

Release Notes for	Update History				
STM32WB Copro Wireless Binaries	V1.0.0 / 06-February-2019				
Copyright © 2019 STMicroelectronics	Main Changes				
577	First release First official release. Binary Install Address and version : Provides Install address for the targeted binary to be use				
life.augmented	Wireless Processor Binary	Install address	Version		
	stm32wb5x_BLE_Stack_fw.bin	0x080CB000	v1.0.0		
License	stm32wb5x_BLE_HCILayer_fw.bin	0x080CD000	v1.0.0		
Electibe	stm32wb5x_Thread_FTD_fw.bin	0x0809F000	v1.0.0		
This software component is licensed by ST under Ultimate Liberty license	stm32wb5x_Thread_MTD_fw.bin	0x080B5000	v1.0.0		
SLA0044, the "License";	stm32wb5x_BLE_Thread_fw.bin	0x08079000	v1.0.0		
You may not use this file except in compliance with the License.	stm32wb5x_Mac_802_15_4_fw.bin	0x080E5000	v1.0.0		
You may obtain a copy of the License at: SLA0044	stm32wb5x_rfmonitor_phy802_15_4_fw.bin	0x080EA000	v1.0.0		
Purpose					
This release covers the delivery of STM32WB Coprocessor binaries.					
Here is the list of the supported binaries:					
<ul> <li>stm32wb5x_BLE_Stack_fw.bin</li> </ul>					
<ul> <li>Full BLE Stack 5.0 certified : Link Layer, HCI, L2CAP, ATT, SM, GAP and GATT database</li> <li>BT SIG Certification listing : Declaration ID D042164</li> </ul>					
<ul> <li>stm32wb5x_BLE_HCILayer_fw.bin</li> </ul>					
HCI Layer only mode 5.0 certified : Link Layer, HCI     BT SIG Certification listing : Declaration ID D042213					
<ul> <li>stm32wb5x_Thread_FTD_fw.bin</li> </ul>					
<ul> <li>Full Thread Device certified v1.1</li> <li>To be used for Leader / Router / End Device Thread role (full features excepting Border Router)</li> </ul>					

For complete documentation on STM32WBxx, visit: [www.st.com/stm32wb]

Nucleo & Dongle boards come preloaded with the BLE stack





#### Bonus Cube Tool!

# STM32CubeMonitor-Power

# \$70

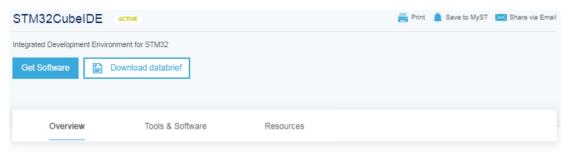








# CubeIDE & Atollic TrueSTUDIO



STM32CubeIDE is an all-in-one multi-OS development tool, which is part of the STM32Cube software ecosystem.



STM32CubeIDE is an advanced C/C++ development platform with IP configuration, code generation, code compilation, and debug features for STM32 microcontrollers. It is based on the ECLIPSE™/CDT framework and GCC toolchain for the development, and GDB for the debugging. It allows the integration of the hundreds of existing plugins that complete the features of the ECLIPSE™ IDE.

STM32CubeIDE integrates all STM32CubeMX functionalities to offer all-in-one tool experience and

save installation and development time. After the selection of an empty STM32 MCU or preconfigured microcontroller from the selection of a board, the project is created and initialization code generated. At any time during the development, the user can return to the initialization and configuration of the IPs or middleware and regenerate the initialization code with no impact on the user code.

STM32CubeIDE includes build and stack analyzers that provide the user with useful information about project status and memory requirements.

STM32CubeIDE also includes standard and advanced debugging features including views of CPU core registers, memories, and peripheral registers, as well as live variable watch, Serial Wire Viewer interface, or fault analyzer.



# Free feature-rich IDE For STM32 developers only

# TrueSTUDIO<sup>°</sup> for STM32





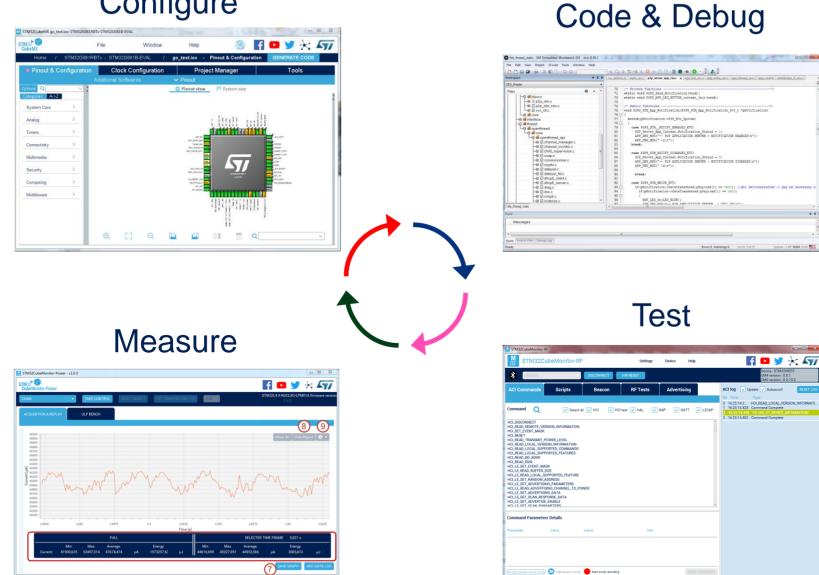




#### **Iterative Design Process**

## Configure

life.augmented





Nucleo

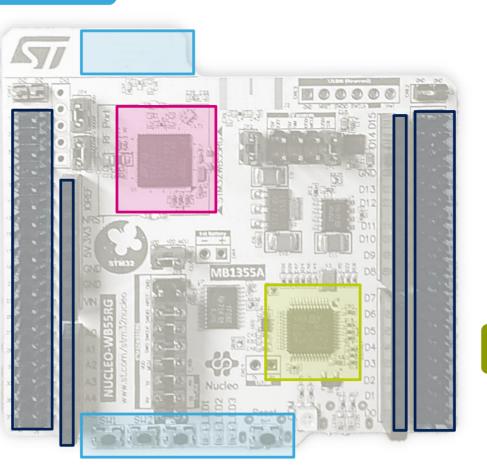
ST-Link/V2-1

41

#### 2.4GHz PCB antenna

STM32WB55RGV6 (VQFPN68)

> Arduino & Morpho Headers



Buttons & LED's





8 Nucleo 1th CR2032 ES MB1355C-0 C 1821 00010 ST-LINK User USB FS Device We will use this one!





Nucleo



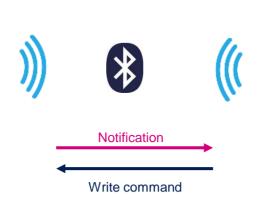




# GATT Server

# **GATT Client**



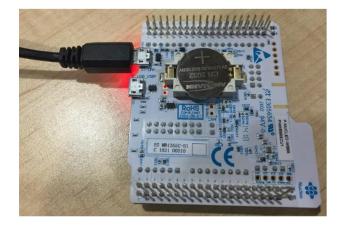








- Power Nucleo board
- Launch ST BLE Sensor app
- What happens?







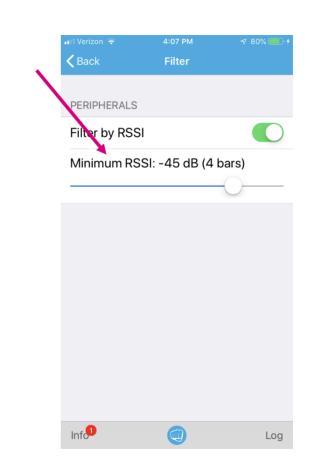


• Launch LightBlue Explorer app

life.augmented

• We can filter by RSSI to find our device (on iOS)

# 🖬 Þ	د الله که	
LightBlue® Explorer	्रहा Sort LightBlue   Explo	rer
DunchThrough	Peripherals Nearby	
Puncinniough	P2PSRV1	
Enjoying LightBlue® Explorer? Learn about our insights into BLE.	-40 No services	
Email Address	P2PSRV1	
SUBSCRIBE DISMISS	-56 No services	
49dBm <b>P2PSRV1</b> 80:E1:26:00:68:E6	P2PSRV1	
StdBm 80.E1.26:00:67:76	-47 No services	
B2PSRV1 -53dbm 80.E1.26.00.99.6F	Virtual Peripherals	
Unnamed 69d8m 44:EC:58:E8:43:F1	🙂 Create Virtual Per	inł
Unnamed -71dBm 52:AF.8C:7C:58:92		'P'
Unnamed -76dBm 7C:28:C5:11:15:CA		
BodBm Unnamed 4EA1:86:D5:7A:E4		
Unnamed		
-94dBm 5F:F6:38:FD:60:83	Note that either the "Device	
Unnamed 948bm 63:02:38:0E:D3:80	Name" or the "Local Name"	
Unnamed		
-95dBm 8C.85.90.6B.0F.C6	may show up on the iOS	
Unnamed 94dBm 88.E9.FE.6D.D3.96	LightBlue App.	
Unnamed 95dBm 15.C6:E0.92:06:A1		
Unnamed 94dBm 32:FA:51:CF:7C:20		
Unnamed Padem DCA904858595	Inf <mark>.</mark> 9	



8%

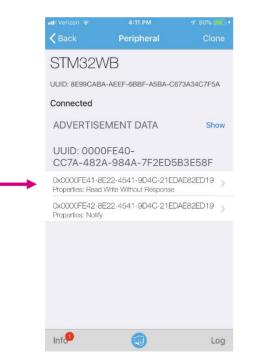
Filter

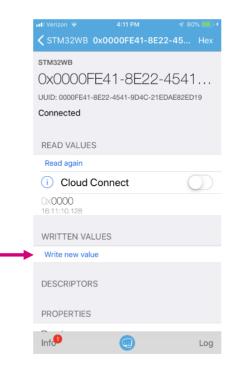
Log



- Click on the "0x0000FE41-" characteristic
- Write new value 101 hex
- Did the LED come on?
- 100 hex to turn it off

life.augmented







D	E	F
А	В	С
7	8	9
4	5	6
1	2	3
≪	0	Done



- Click on the "0x0000FE41-" characteristic
- Write new value 101 hex
- Did the LED come on?
- 100 hex to turn it off

Android	•
Anu.	

14 🖬 🗣 🕴 📾 83% 🔮 3.59 PM	🖾 ⊭ 😪 88% 🔒 4.00 PM.
← P2PSRV1 :	← P2PSRV1
ADVERTISEMENT DATA	PROPERTIES
Connected Connected	Device Address 80£126.00.67:76
Advertised name P2PSRV1	Service UUID 0000fe40-cc7#-482#-984#-7f2ed5b3e58f
DEVICE INFORMATION	Characteristic UUID 0000fe41-8e22-4541-9d4c-21edae82ed19
Device Address 80.E1/26/00.67/76	Able to be read from
GATT SERVICES & CHARACTERISTICS	Writable     Able to be written to
Generic Attribute → Service Changed	× Supports notifications/indications Able to be subscribed to for notifications/indications on changes to the characteristic
Generic Access Device Name Appearance →	READ/INDICATED VALUES
Appearance Perioheral Preferred Connection Parameters	READ AGAIN
0000fe40-cc7a-482a-994a-7f2ad5b3e58f 0000fe1-822-4541-944-21 edse82ad19 → 0000fe42-822-4541-944-21 edse82ad19	No value read recently Tap on one of the buttons above — If available — to begin
	WRITTEN VALUES
	101 WRITE
Ener connector raismetera	 01 01 Wed Apr 17 16:00:20 CDT 2019
	DESCRIPTORS
Select a characteristic to explore	1 2 3 4 5 6 7 8 9 0 Del
0000fe41-8e22-4541-9d4c-21edae82ed19	Q <sup>+</sup> W <sup>×</sup> E <sup>+</sup> R <sup>=</sup> T <sup>′</sup> Y <sup>-</sup> U <sup>×</sup> I <sup>×</sup> O <sup>1</sup> P <sup>1</sup> (3)
0000fe42-8e22-4541-9d4c-21edae82ed19	
	ASDFGHJKL 🖑
	T     T
	Ctrl !@1 ੴ English (US)

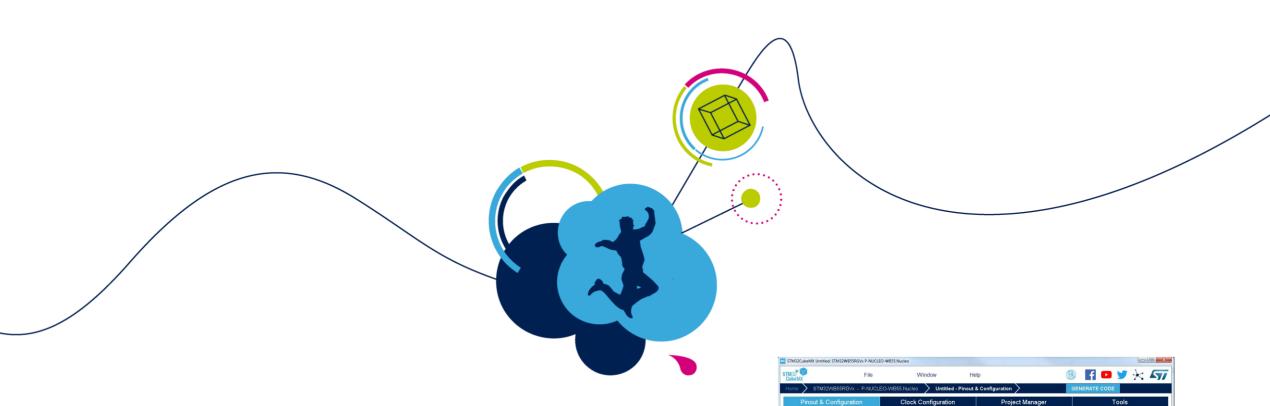


# Your Magic number!









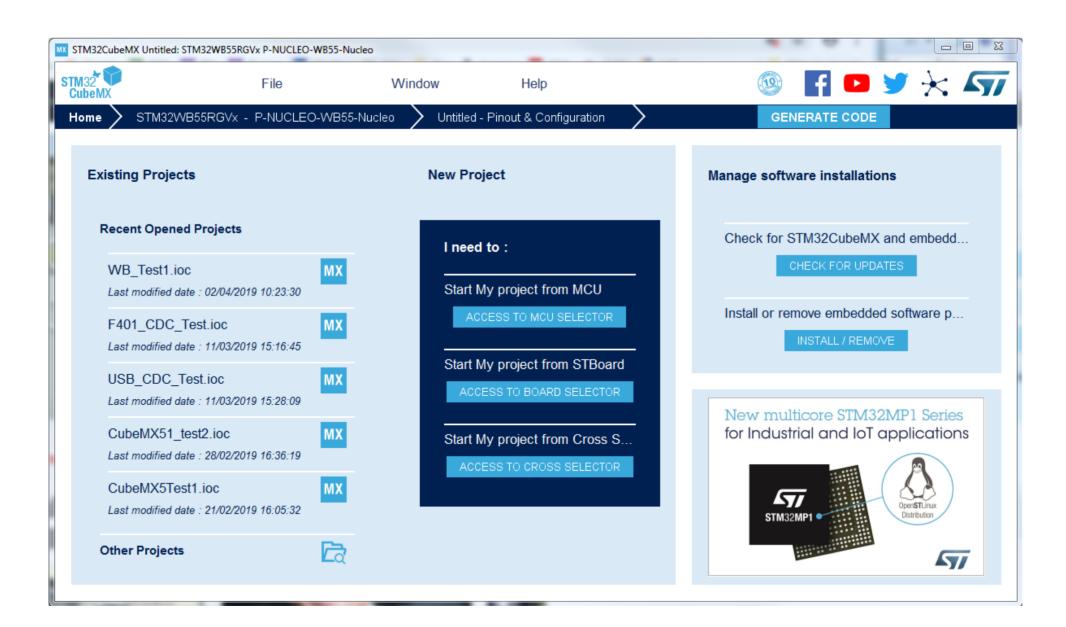
# Hands-On CubeMX

M32 0 ubeMX ome > STM32	WB55RGVx - P-NUCL		ut & Configuration	GENERATE CODE	¥ 🛪 🗖
	onfiguration	Clock Configuration	Project Manager		Tools
Fillout & C	onnguration	Additional Softwares	✓ Pinout		loois
ptions Q	~ \$	· Identification de Contrations	Pinout view     Pinout view		
System Core	×				
Analog	Σ		a sant () a sant ()		
Timers	>	515,940,85			
Connectivity	>	900,0902,047 900,0902,047			
Multimedia	>				
Security	>				
Computing	>			20 (Net Let) 20 (See Let)	
Middleware	5		ENTER STOLE	N0,090,H	
			or (Presidence)		
		Q [] Q		Q	~





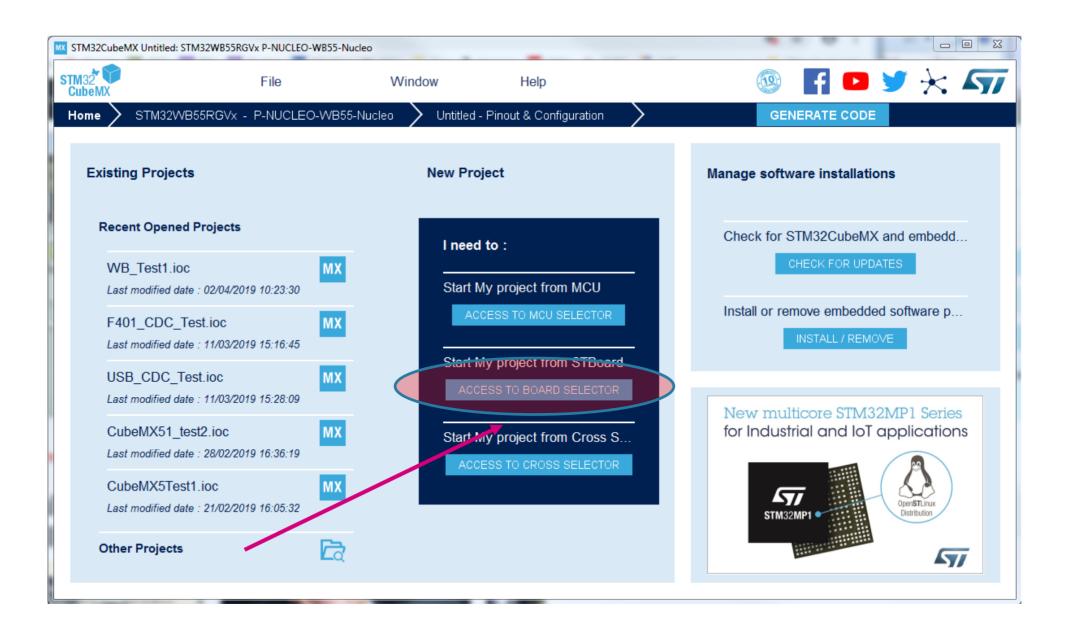
# Launch CubeMX





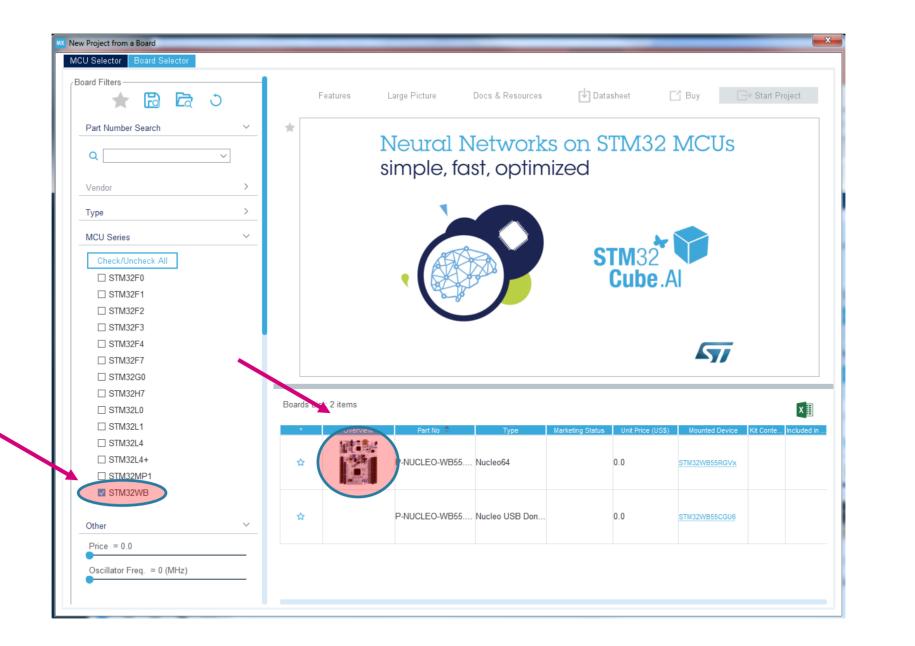


# Launch CubeMX & Start project from Board Selector



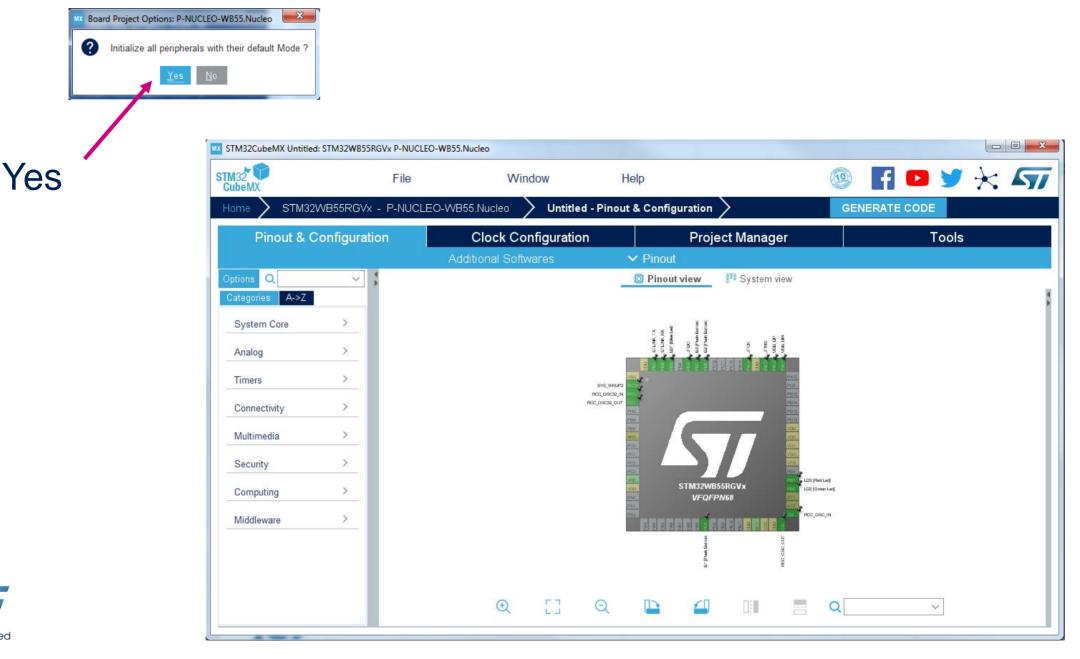


# Filter by STM32WB and double-click on the Nucleo board!











- Name your project
- Recommended Project location: C:\STM32WB\_Workshop\
- Use EWARM V8 toolchain

TM32CubeMX Untitled*: STM32						
132 ubeMX	File	Window	Help	(19)		y 🗙 🏹
ome 🔰 STM32WB55R	GVx 🔪 Untitled	I - Project Manager >		G	ENERATE CODE	
Pinout & Configur	ation	Clock Configuration	Projec	t Manager		Tools
Proj	ect Settings					
	iect Name					
Project	Test1					
Proi	iect Location					
	STM32WB_Workshop		Br	owse		
	lication Structure					
Bas	sic	✓ Do not	generate the main()			
Tool	Ichain Folder Location					
Code Generator	STM32WB_Workshop	\WB_Test1\				
	lehein / IDE					
EW	IARM V8	✓ General	te Under Root			
Link	er Settings					
	imum Heap Size	0x200				
Mini	imum Stack Size	0x400				
dvanced Settings						
Mcu	and Firmware Packa	ae				
ICUs Selection Output						
Series		ines OTMONIA DI	Mcu	Package		quired Peripherals
STM32WB	STM32WBx5	STM32WB5	5CCUx	UFQFPN48	None	



ERATE	CODE 属				
TM32 TO CubeMX	File	Window Help		🚳 F D y 🔆	577
Home > STM32W Pinout & Co	/B55RGVx - P-NUCLEO	WB55.Nucleo Vuntitled - Project N Clock Configuration	Nanager > Project Manager	GENERATE CODE Tools	
Project	Project Settings Project Name [WB_Test1] Project Location [C:\Users\alec bath\Docur Application Structure	nents\ST\Projects\STM32WB\CubeMX-WB\	Browse		
Code Generator	Basic Toolchain Folder Location	Do not generate the main nents\ST\Projects\STM32WB\CubeMX-WB\WB			
Advanced Settings		0x200 0x400			
	Mcu and Firmware Packa Mcu Reference STM32WB55RGVx Firmware Package Name STM32Cube FW_WB V1	and Version			
	Use Default Firmware C:/Users/alec bath/STM3	Location 2Cube/Repository/STM32Cube_FW_WB_V1.0.0	Browse		





# Open Project

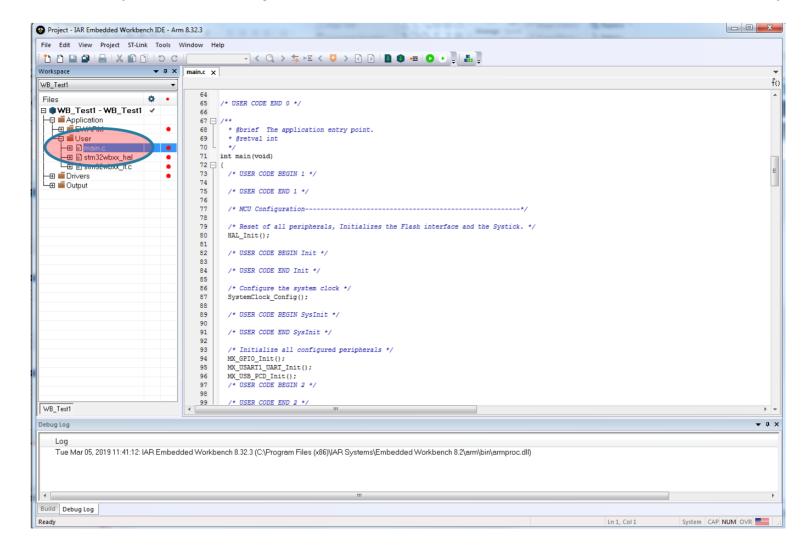
	C:\Users\alec bath\Documents\ST\Projects\STM32WB\CubeMX-WB	
	Application Structure Basic   Do not generate the main()	
	Tool Code Generation	x
herator	C:\\ Too EW Open Fold # Open Project Close	Projects/STM32WB/CubeMX-WB/WB_Test1
	Linker Settings	
	Minimum Heap Size 0x200	
Settings	Minimum Stack Size 0x400	
	Mcu and Firmware Package	
	Mcu Reference	
	STM32WB55RGVx	





# • Expand the User file tree and Open main.c

• Enable line numbers in IAR (Tools > Options > Editor > Show line numbers)





# Add some code to while(1) loop:

You can copy/paste the code bits from LED\_Blinky\_Lab.txt file from your Labs folder

101 102	/* Infinite loop */ /* USER CODE BEGIN WHILE */
103	while (1)
104	] [
105	
106	<pre>HAL_GPIO_TogglePin(GPIOB, GPIO_PIN_5);</pre>
107	HAL_Delay(100);
108	HAL_GPIO_TogglePin(GPIOB, GPIO_PIN_0);
109	HAL_Delay(100);
110	HAL_GPIO_TogglePin(GPIOB, GPIO_PIN_1);
111	HAL_Delay(100);
112	
113	/* USER CODE END WHILE */
114	





Build the project

Make the active project (build files as needed)

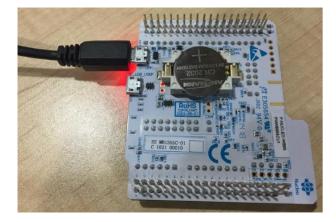
# Check for errors

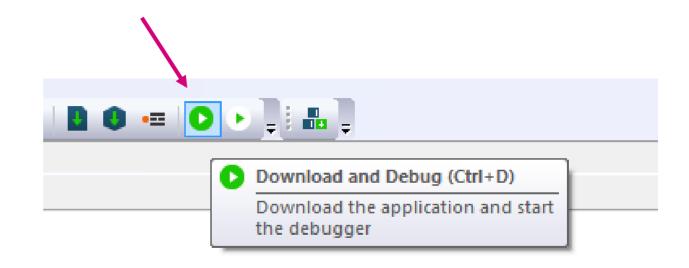
	Build	
		Messages
l		Building configuration: WB_Test1 - WB_Test1 Updating build tree
I	11	main.c
I	11	Linking
1	11	WB_Test1.out
ł		Converting
		Total number of errors: 0 Total number of warnings: 0





# Download & Debug (attach your board) ③

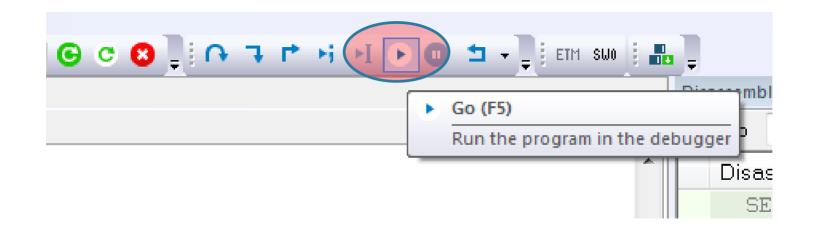








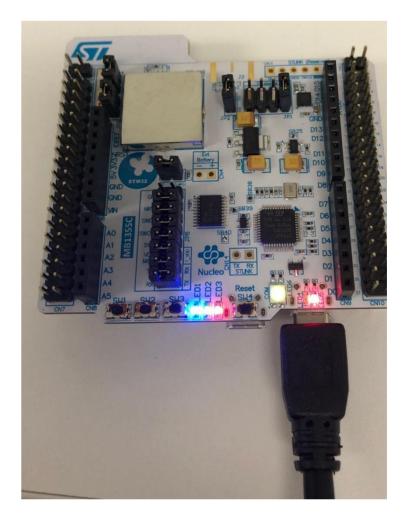
# GO!







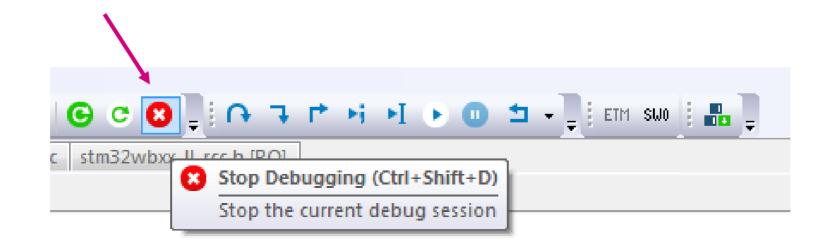
# Enjoy the dancing LED's! ③





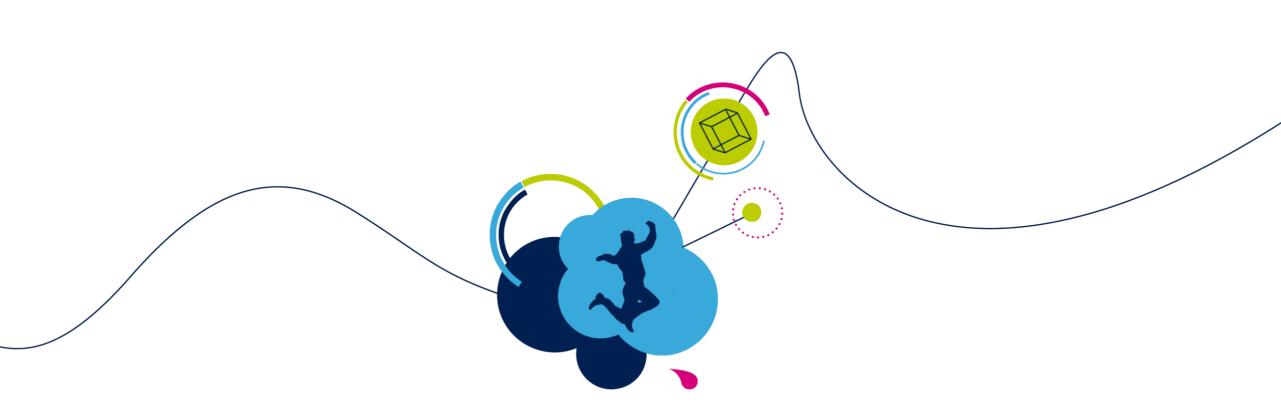


Stop Debugging at the end of each lab and close IAR Embedded Workbench







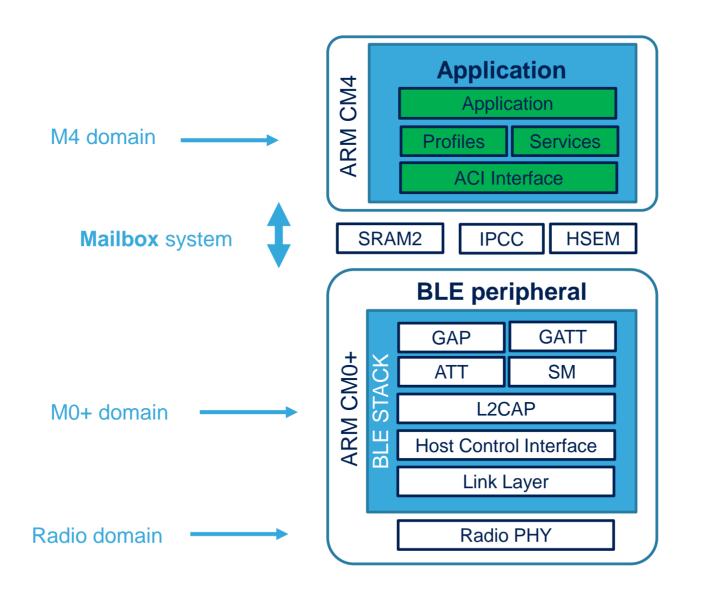


# **BLE Fundamentals**





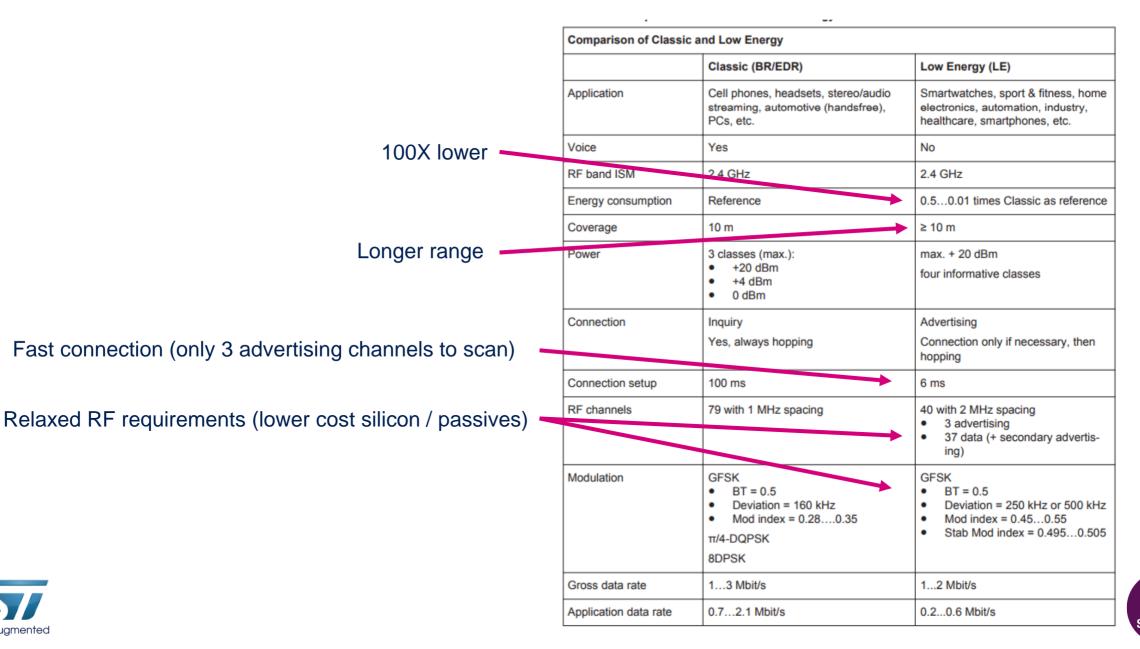
### **BLE Protocol Stack layers**







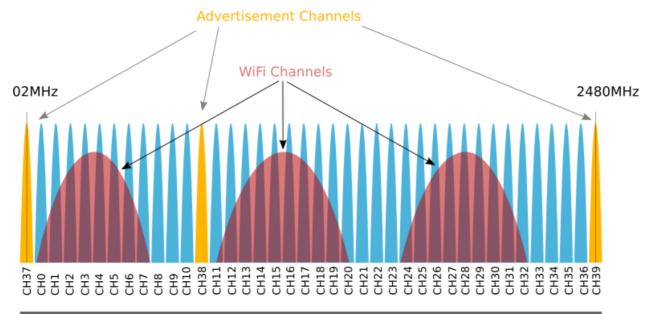
# Bluetooth Classic (BR/EDR) vs Low Energy (LE)





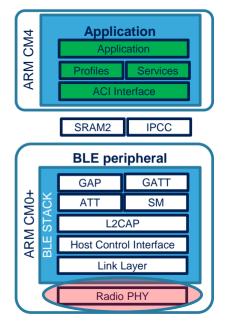
#### Strategically placed advertising channels

#### Remaining 37 channels are data channels



2.4GHz Band

	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	-



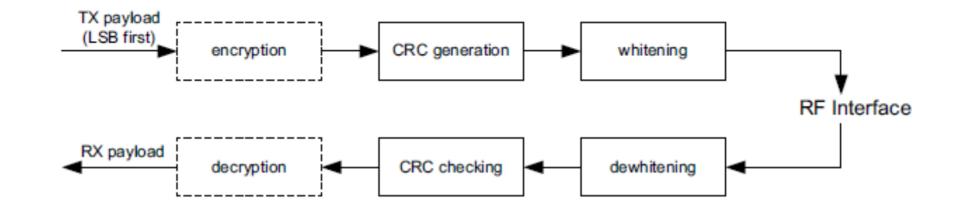


PHY



PHY

69



ARM CM4 **Application** Application Services Profiles ACI Interface SRAM2 IPCC **BLE** peripheral GAP GATT ARM CM0+ ATT SM L2CAP Host Control Interface Link Layer Radio PHY





# Link Layer / HCI / L2CAP

# • Link Layer (LL)

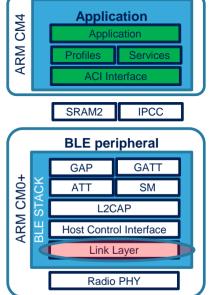
- Radio control
- Defines packet structure
- One or more state machines
- Link-layer-level encryption (via Security Manager)
- Host Control Interface (HCI)
  - Bridge between Radio Domain and M0+ Domain

- L2CAP (Logical Link Control and Adaptation Protocol)
  - Multiplex packets from higher-level protocols (ATT / SMP)
  - Handles segmentation and reassembly of packets
  - Quality of Service (QoS)

life.auamentec





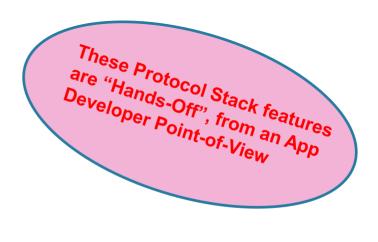


# Link Layer / HCI / L2CAP

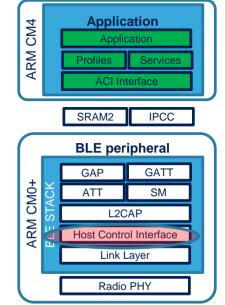
# • Link Layer (LL)

- Radio control
- Defines packet structure
- One or more state machines
- Link-layer-level encryption (via Security Manager)
- Host Control Interface (HCI)
  - Bridge between Radio Domain and M0+ Domain

- L2CAP (Logical Link Control and Adaptation Protocol)
  - Multiplex packets from higher-level protocols (ATT / SMP)
  - Handles segmentation and reassembly of packets
  - Quality of Service (QoS)









# Link Layer / HCI / L2CAP

# • Link Layer (LL)

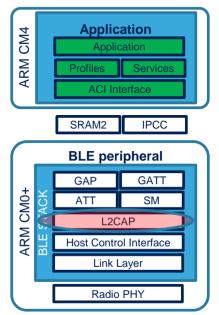
- Radio control
- Defines packet structure
- One or more state machines
- Link-layer-level encryption (via Security Manager)
- Host Control Interface (HCI)
  - Bridge between Radio Domain and M0+ Domain

# • L2CAP (Logical Link Control and Adaptation Protocol)

- Multiplex packets from higher-level protocols (ATT / SMP)
- Handles segmentation and reassembly of packets
- Quality of Service (QoS)

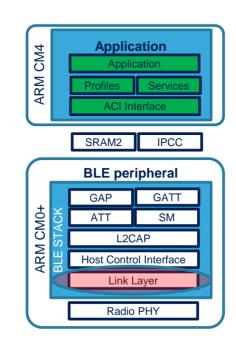








- Standby state: Sleep, Stop, Standby
- Advertising is the key to initiating all BLE communications!
- An Initiator and Advertiser negotiate a Connection
- In a Connection
  - The Link-Layer *Master* is also the GAP Central
  - The Link-Layer *Slave* is also the GAP Peripheral



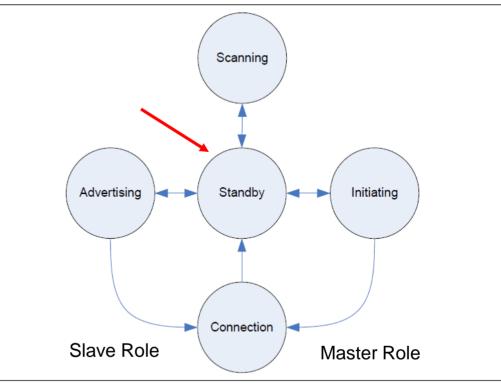
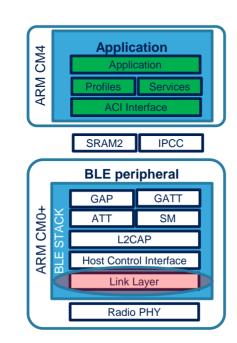


Figure 1.1: State diagram of the Link Layer state machine



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



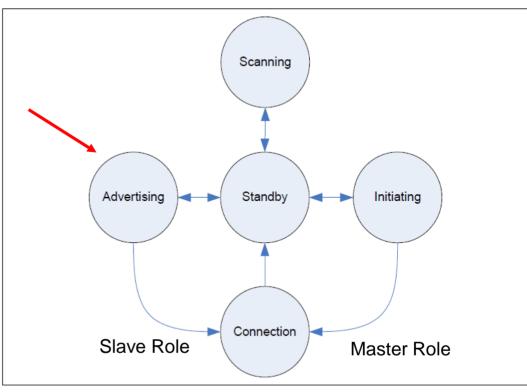


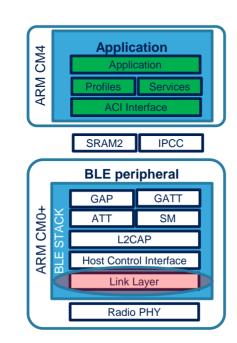
Figure 1.1: State diagram of the Link Layer state machine



- Standby state: Sleep, Stop, Standby
- Advertising is the key to initiating all BLE communications!
- An Initiator and Advertiser negotiate a Connection
- In a Connection

life.auamented

- The Link-Layer *Master* is also the GAP Central
- The Link-Layer Slave is also the GAP Peripheral



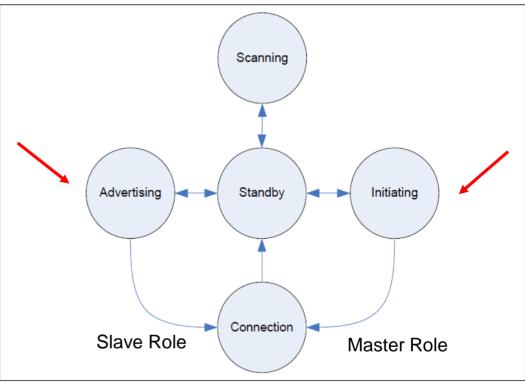


Figure 1.1: State diagram of the Link Layer state machine



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

**ARM CM4** 

**ARM CM0+** 

The Link-Layer *Slave* is also the GAP Peripheral

**Application** 

**ACI Interface** 

**BLE** peripheral

L2CAP

Host Control Interface Link Layer

Radio PHY

SRAM2

GAP

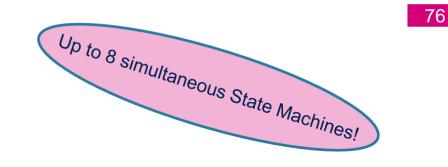
ATT

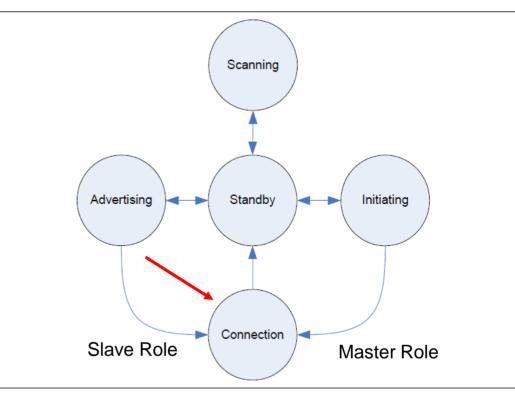
Services

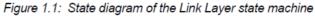
IPCC

GATT

SM





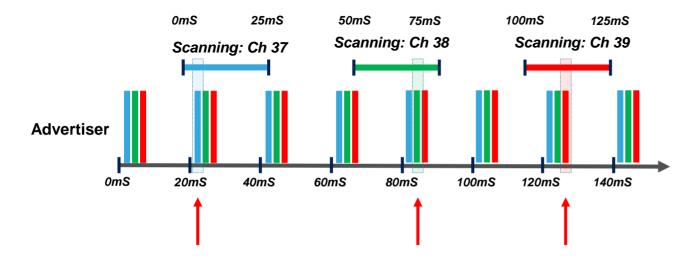






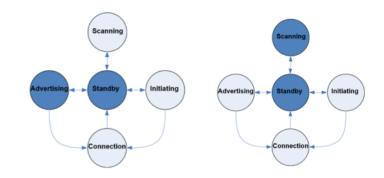
## **Discovery: Advertising & Scanning**

77



**Discovery Events** 

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

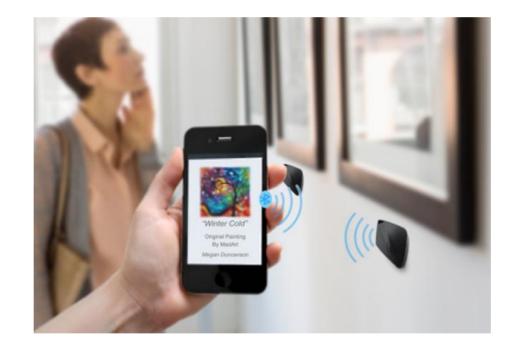




## GAP (Generic Access Profile)

# **Roles and Modes**

- Advertising Mode
- Connected Mode



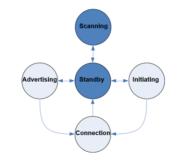
#### Broadcaster

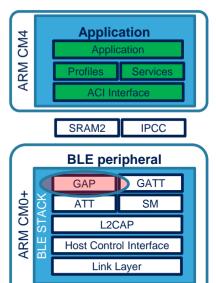
Sends advertising events Can include characteristics and service data Doesn't need receiver Can be discoverable if it does have receiver



#### Observer

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





Radio PHY





## GAP (Generic Access Profile)

# **Roles and Modes**

- Advertising Mode
- Connected Mode



Peripheral

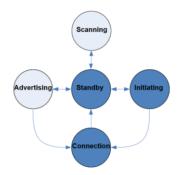
Has transmitter and receiver Always slave Connectable advertising

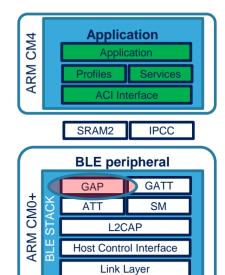




#### Central

Has transmitter and receiver Always master Never advertises





Radio PHY

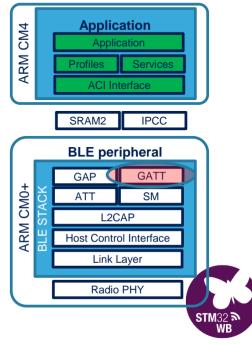




## GATT (Generic Attribute Profile)

## GAP Central is also a "GATT Client" GAP Peripheral" is also a "GATT Server"

🕸 💌		😭 📶 93% 🚺 CLEAR DATA	
SELECT DEVICE	сна	RT	мар
210 200	Over	100% Max	
190 180 170		um Effort	VA –
160 150 140	•	Ance Training	
140 130 120	Fitnes	s / Fat burn	h
110 100 90	Warm Up	/ Cool Down	
80 70			
60 50 40	Restin	g / Inactive	
30 20			
10 0 10:35:12	10:40:51	10:46:31	10:52:11
PAUSI	E	ST	OP

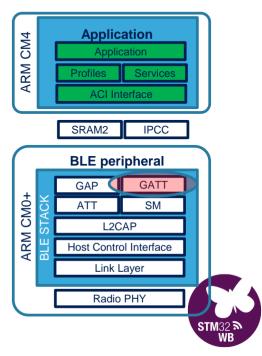




## GATT (Generic Attribute Profile)

GAP Central is also a "GATT Client" GAP Peripheral" is also a "GATT Server"







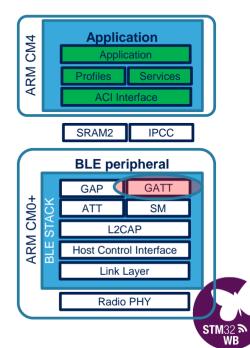
## GATT (Generic Attribute Profile)

## 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

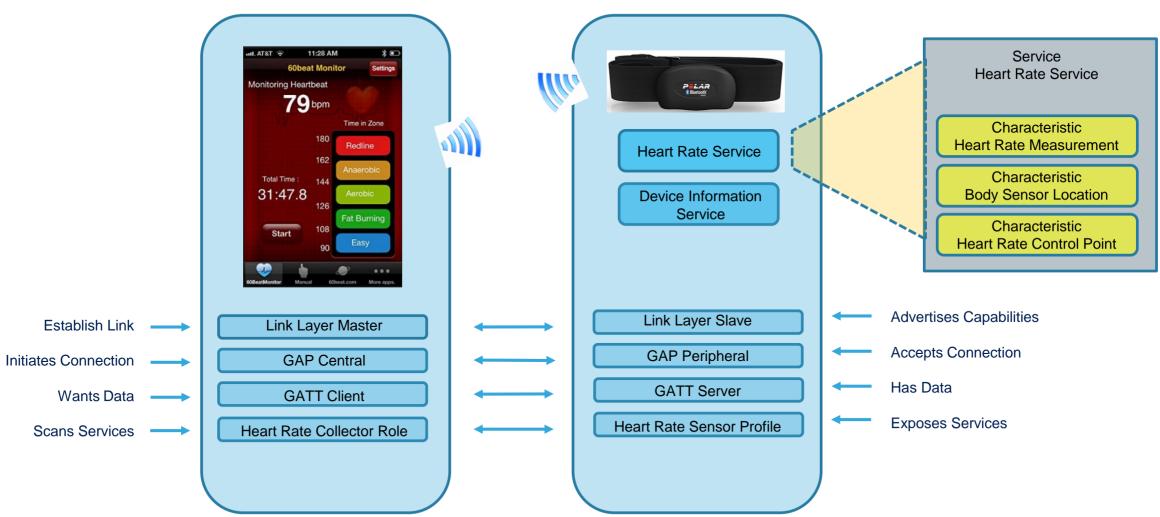


What is my hea	artrate?	
	147 bpm	
What is your M	fr ID?	P=LAR * Bluetopti
	Polar	





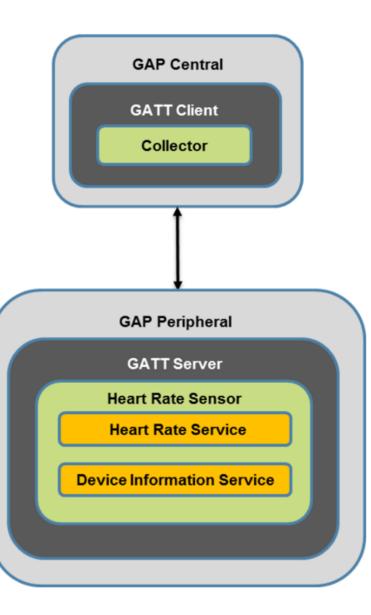
## GATT: Profiles, Services, Characteristics & Descriptors







## SIG-defined profiles

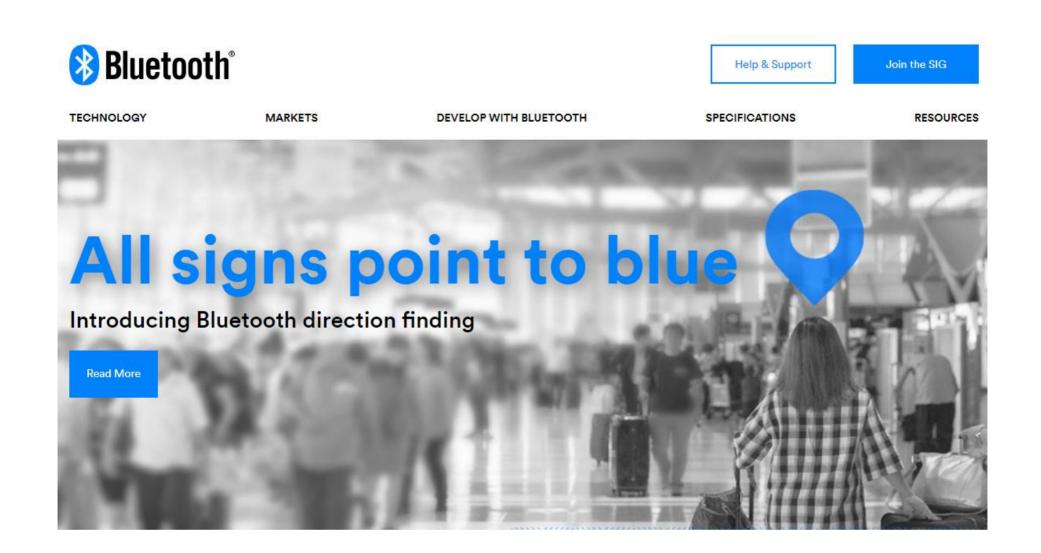






## **Bluetooth SIG**

85



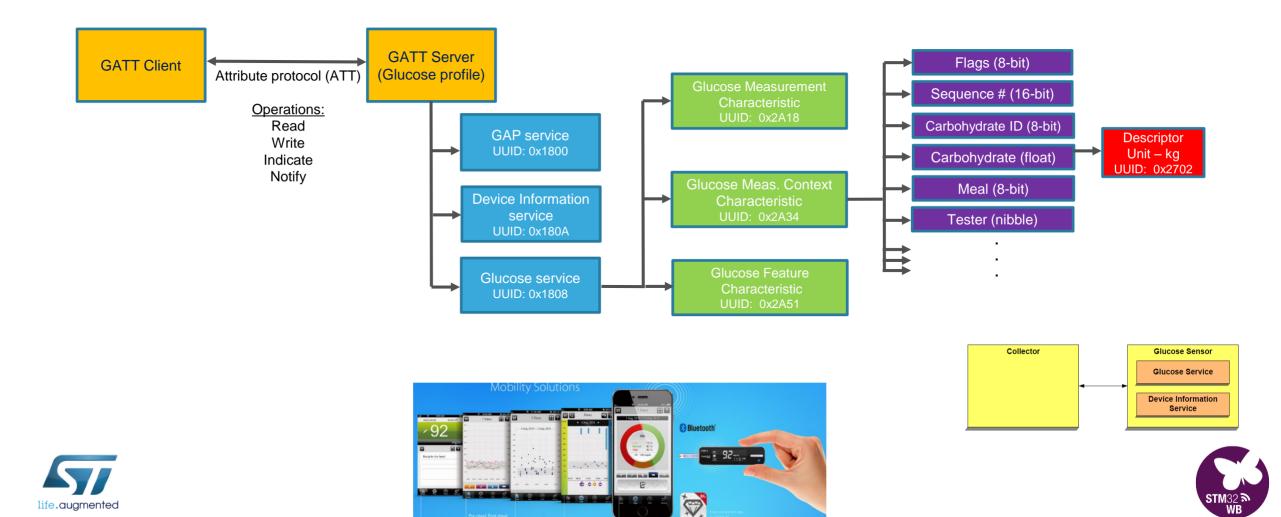




www.bluetooth.com

## **GATT Glucose Profile**

## GLP Profile defines two roles: Collector & Glucose Sensor

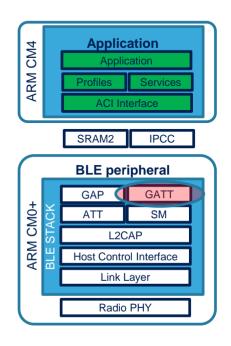


## GATT Database details – Handles, UUID's & Values

Once the GATT Server's database information is known to the GATT Client, it can reference data via Handles

- "What is the temperature reported by the Thermometer Service?" ATT read command of Handle 0x0102
- "What are the units of temperature used?" ATT read command of Handle 0x0104

Handle	UUID	Description	Value
0x0100	0x2800	Thermometer service definition	UUID 0x1816
0x0101	0x2803	Characteristic: temperature	UUID 0x2A2B Value handle: 0x0102
0x0102	0x2A2B	Temperature value	20 degrees
0x0104	0x2A1F	Descriptor: unit	Celsius
0x0105	0x2902	Client characteristic configuration descriptor	0x0000
0x0110	0x2803	Characteristic: date/time	UUID 0x2A08 Value handle: 0x0111
0x0111	0x2A08	Date/Time	1/1/1980 12:00





# Attribute protocol details (ATT)

• Access GATT database information on the Server

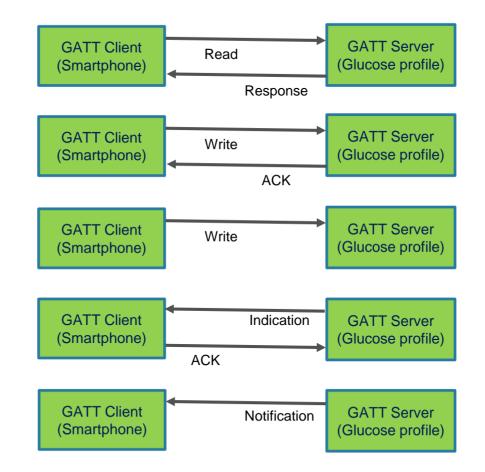
### • Operations

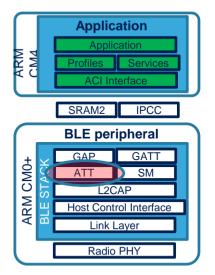
- Read
- Write / Write without response
- Indicate / Notify

### • Four elements

- 16-bit Handle
- **Type** of attribute (UUID)
- Value
- Attribute **Permissions** (Read-only, etc)

Handle	UUID	Description	Value
0x0100	0x2800	Thermometer service definition	UUID 0x1816
0x0101	0x2803	Characteristic: temperature	UUID 0x2A2B Value handle: 0x0102
0x0102	0x2A2B	Temperature value	20 degrees
0x0104	0x2A1F	Descriptor: unit	Celsius
0x0105	0x2902	Client characteristic configuration descriptor	0x0000
0x0110	0x2803	Characteristic: date/time	UUID 0x2A08 Value handle: 0x0111
0x0111	0x2A08	Date/Time	1/1/1980 12:00









- Battery Monitoring Service (BAS)
- Alert Notification Service (ANS)
- Elapsed motor use in minutes
- Unlock the drill via smartphone password
  - Add standard Services & Characteristics (16-bit UUID's from Bluetooth SIG)
  - Create custom services (128-bit UUID's)







### • Universally Unique Identifiers (UUID's) are simply 128-bit (16-byte) numbers:

#### 10c17863-9471-4427-8d66-82579bf9161a

- Format is typically arranged as 4-2-2-2-6 and hexadecimal is assumed
- To send packets more efficiently, the Bluetooth SIG has adopted a standard 112-bit UUID base:
  - 0000XXXX-0000-1000-8000-00805F9B34FB
- With a 16-bit SIG-identified service, characteristic, etc, you can use this short-form
  - For example, the Glucose Service in our CGM profile is:
  - 00001808-0000-1000-8000-00805F9B34FB
- Custom services / characteristics / descriptors need a fully defined 128-bit UUID
  - Our Custom Drill needs an Unlock service.
  - We can generate a random UUID for it at https://www.uuidgenerator.net/
- There is also a 32-bit UUID specifier option



.

•

.



- Universally Unique Identifiers (UUID's) are simply 128-bit (16-byte) numbers:
  - 10c17863-9471-4427-8d66-82579bf9161a
  - Format is typically arranged as 4-2-2-6 and hexadecimal is assumed
  - To send packets more efficiently, the Bluetooth SIG has adopted a standard 112-bit UUID base:

#### 0000XXXX-0000-1000-8000-00805F9B34FB

- With a 16-bit SIG-identified service, characteristic, etc, you can use this short-form
  - For example, the Glucose Service in our CGM profile is:
  - 00001808-0000-1000-8000-00805F9B34FB
- Custom services / characteristics / descriptors need a fully defined 128-bit UUID
  - Our Custom Drill needs an Unlock service.
  - We can generate a random UUID for it at https://www.uuidgenerator.net/
- There is also a 32-bit UUID specifier option



.

.



- Universally Unique Identifiers (UUID's) are simply 128-bit (16-byte) numbers:
  - 10c17863-9471-4427-8d66-82579bf9161a
  - Format is typically arranged as 4-2-2-6 and hexadecimal is assumed
  - To send packets more efficiently, the Bluetooth SIG has adopted a standard 112-bit UUID base:
    - 0000XXXX-0000-1000-8000-00805F9B34FB
  - With a 16-bit SIG-identified service, characteristic, etc, you can use this short-form
    - For example, the Glucose Service in our CGM profile is:

#### 00001808-0000-1000-8000-00805F9B34FB

Glucose service UUID: 0x1808

- Custom services / characteristics / descriptors need a fully defined 128-bit UUID
  - Our Custom Drill needs an Unlock service.
  - We can generate a random UUID for it at https://www.uuidgenerator.net/
- There is also a 32-bit UUID specifier option



.

.....



- Universally Unique Identifiers (UUID's) are simply 128-bit (16-byte) numbers:
  - 10c17863-9471-4427-8d66-82579bf9161a
  - Format is typically arranged as 4-2-2-6 and hexadecimal is assumed
  - To send packets more efficiently, the Bluetooth SIG has adopted a standard 112-bit UUID base:
    - 0000XXXX-0000-1000-8000-00805F9B34FB
  - With a 16-bit SIG-identified service, characteristic, etc, you can use this short-form
    - For example, the Glucose Service in our CGM profile is:
    - 00001808-0000-1000-8000-00805F9B34FB
  - Custom services / characteristics / descriptors need a fully defined 128-bit UUID
    - Our Custom Drill needs an Unlock service.
    - We can generate a random UUID for it at <u>https://www.uuidgenerator.net/</u>
- **Online UUID Generator**

Your Version 4 UUID: ab03db97-0ef5-4ff3-8d5c-72df085ce891

Refresh page to generate another.



There is also a 32-bit UUID specifier option



.

•

.

## **Custom Drill Profile**

### • Standard Services & Characteristics (16-bit UUID's)

- Battery service (BAS) UUID: 0x180F
  - Battery Level Characteristic: 0x2A19
- Alert Notification Service UUID: 0x1811
  - Alert Notification Control Point Characteristic: 0x2A44
  - Unread Alert Status Characteristic : 0x2A45
  - New Alert Characteristic : 0x2A46
  - Supported New Alert Category Characteristic: 0x2A47
  - Supported Unread Alert Category Characteristic : 0x2A48
- Create custom services (128-bit UUID's)

.

- **10c17863-9471-4427-8d66-82579bf9161a** (Motor run time service)
  - 5567fa77-721f-4e1a-9875-7ae95ead642d xxx Characteristic
  - 3d78d6f3-7d34-4f89-a14d-ed3cac297438 xxx Characteristic
- 0226b0db-d9a6-49c8-bce1-fccd3a40e6e2 (Unlock service)
  - 997e28a5-f05e-4027-89c7-e84ce4ce67ec xxx Characteristic
  - b3b7d2a1-4eeb-4a39-85ef-7ddd7b1e4abf xxx Characteristic

#### Name: Battery Service

Type: org.bluetooth.service.battery\_service Assigned Number: 0×180F

#### Name: Battery Level

Type: org.bluetooth.characteristic.battery\_level Assigned Number: 0×2A19

### **Name: Alert Notification Service**

Type: org.bluetooth.service.alert\_notification Download / View

Assigned Number: 0×1811

#### **Name: Alert Notification Control Point**

Type: org.bluetooth.characteristic.alert\_notification\_control\_point 。

Assigned Number: 0×2A44

#### Name: Supported New Alert Category

Type: org.bluetooth.characteristic.supported\_new\_alert\_category a

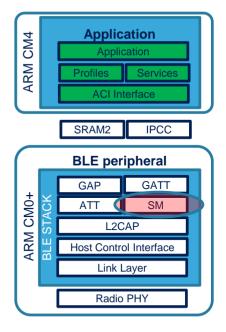
Assigned Number: 0×2A47





## **Security Topics**

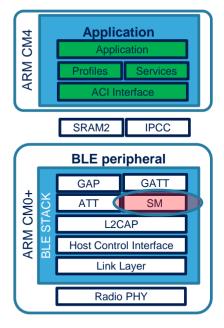
- **Connection**: GAP Central connected to a GAP Peripheral (Connection interval = 7.5ms to 4 secs)
- **Pairing**: Connected devices exchange encryption keys to **encrypt** the link. There are now **paired**.
- **Bonding**: Paired devices can be bonded Keys are stored for the next connection.
- Whitelisting: Restrict connections from any other than known devices.







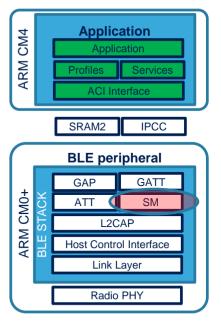
- **Security Topics**
- **Connection**: GAP Central connected to a GAP Peripheral (Connection interval = 7.5ms to 4 secs)
- **Pairing**: Connected devices exchange encryption keys to **encrypt** the link. There are now **paired**.
- **Bonding**: Paired devices can be bonded Keys are stored for the next connection.
- Whitelisting: Restrict connections from any other than known devices.







- **Security Topics**
- **Connection:** GAP Central connected to a GAP Peripheral (Connection interval = 7.5ms to 4 secs)
- **Pairing**: Connected devices exchange encryption keys to **encrypt** the link. There are now **paired**.
- **Bonding**: Paired devices can be bonded Keys are stored for the next connection.
- Whitelisting: Restrict connections from any other than known devices.

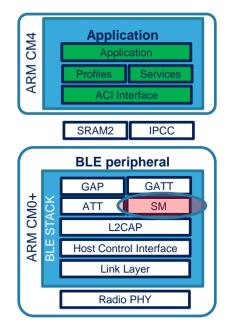






- **Security Topics**
- **Connection**: GAP Central connected to a GAP Peripheral (Connection interval = 7.5ms to 4 secs)
- **Pairing**: Connected devices exchange encryption keys to **encrypt** the link. There are now **paired**.
- **Bonding**: Paired devices can be bonded Keys are stored for the next connection.
- Whitelisting: Restrict connections from any other than known devices.

- Security modes are deployed after a BLE connection is established
- BLE Link Layer uses AES-128 CCM mode for authenticated encryption





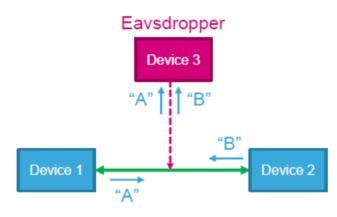


# **Typical attacks**

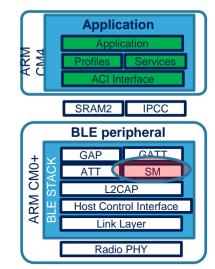
- Passive eavesdropping:
  - A third device listens in to the data being exchanged between the two paired devices
  - Overcome by AES-CCM encryption

### • MITM

- A malicious device impersonates the other two legitimate devices
- Identity tracking
  - Malicious entity associates BLE device address to physically track the user
  - BLE overcomes this is by periodically changing the device address.







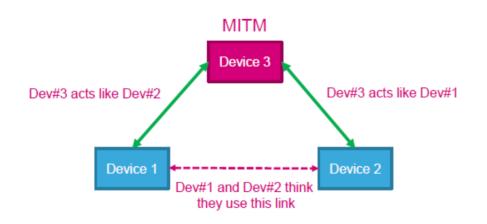


# **Typical attacks**

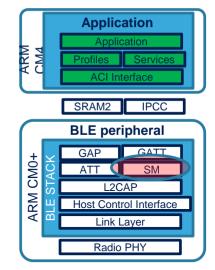
- Passive eavesdropping:
  - A third device listens in to the data being exchanged between the two paired devices
  - Overcome by AES-CCM encryption

### • MITM

- A malicious device impersonates the other two legitimate devices
- Identity tracking
  - Malicious entity associates BLE device address to physically track the user
  - BLE overcomes this is by periodically changing the device address.









# **Typical attacks**

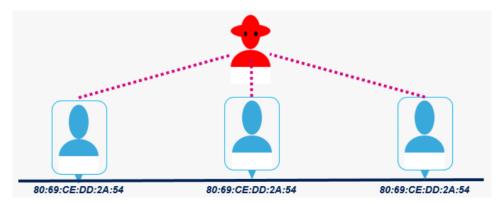
- Passive eavesdropping:
  - A third device listens in to the data being exchanged between the two paired devices
  - Overcome by AES-CCM encryption

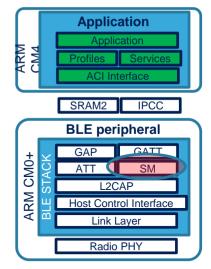
### • MITM

• A malicious device impersonates the other two legitimate devices

### Identity tracking

- Malicious entity associates BLE device address to physically track the user
- BLE overcomes this is by periodically changing the device address.









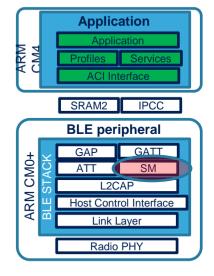
# **Pairing Methods**

### • Just Works<sup>™</sup>:

- Still vulnerable to MITM attack
- Out of Band (OOB) Pairing:
  - Keys exchanged over a different wireless technology such as NFC

### • Passkey:

- 6-digit number entered on each device
- Assumes keypad capability
- Numeric Comparison:
  - Similar to Just Works<sup>TM</sup>, but adds a 6-digit confirmation value
  - Additional protection from MITM attacks







# **Pairing Methods**

### • Just Works<sup>™</sup>:

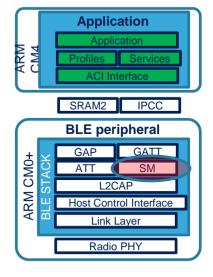
• Still vulnerable to MITM attack

## • Out of Band (OOB) Pairing:

• Keys exchanged over a different wireless technology such as NFC

### • Passkey:

- 6-digit number entered on each device
- Assumes keypad capability
- Numeric Comparison:
  - Similar to Just Works<sup>TM</sup>, but adds a 6-digit confirmation value
  - Additional protection from MITM attacks





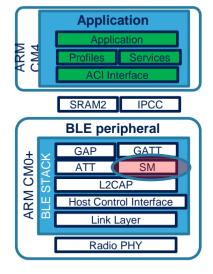


# **Pairing Methods**

- Just Works<sup>TM</sup>:
  - Still vulnerable to MITM attack
- Out of Band (OOB) Pairing:
  - Keys exchanged over a different wireless technology such as NFC

### • Passkey:

- 6-digit number entered on each device
- Assumes keypad capability
- Numeric Comparison:
  - Similar to Just Works<sup>TM</sup>, but adds a 6-digit confirmation value
  - Additional protection from MITM attacks

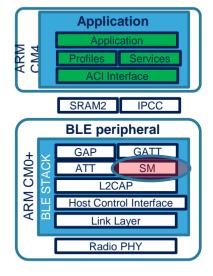






# **Pairing Methods**

- Just Works<sup>TM</sup>:
  - Still vulnerable to MITM attack
- Out of Band (OOB) Pairing:
  - Keys exchanged over a different wireless technology such as NFC
- Passkey:
  - 6-digit number entered on each device
  - Assumes keypad capability
- Numeric Comparison:
  - Similar to Just Works<sup>TM</sup>, but adds a 6-digit confirmation value
  - Additional protection from MITM attacks







## Link Layer Filtering

## A "White List" can **optionally** be used to filter device addresses

- Advertising State An advertiser shall process connection requests only from devices in the White List
- Scanning State A scanner shall process advertising packets only from White-Listed devices
- Initiating State An initiator shall process connectable advertising packets only from White-Listed devices





## **BLE Sniffer**



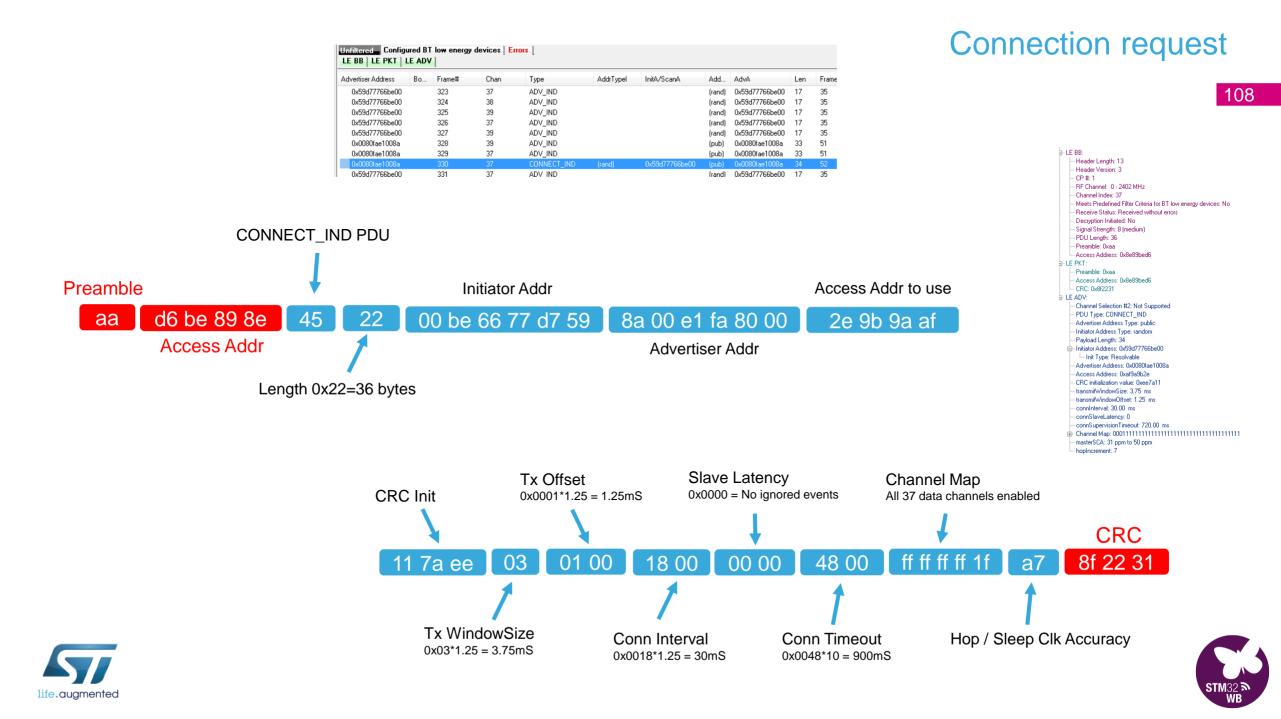
Frame Display - Nordic Dev Kit.cfa										
le Edit View Format Filter Bookmarks Options Win	The distance of the second sec		TAT In a	Eiter Include eac	b frame where the oro	tocal "ATT" exists »AND where the pro	torol "I E DD" winte			
					in numero one pro					
Frame 383: Len+25 LE BB:		1 # 0 0	00	Find:		Summary: ATT		+ Basepand	I with Auto-travi	erse
- CP # 1		nfigured BT low e			1.4					
- Channel Index 21 - 2448 MHz	Baseband	ninguied bit low e	nergy devi	ces	-					
- Meets Predefined Filter Criteria for BT low energy devices. No				IL LIGELD CHD				_		
- Decrypted by Analyzer: No	LE 88 LE PK	I LE ADV LE	DATA	LL   L2CAP   SMP	ATT Data					
- Event Status: Everything was ok,	Bookmark	Frame#	Role	Opcode	Handle	UUD	Database	Error code	Fram.	
- PDU Length: 12	a source and the					Characteristic		End code		
LE FKT		321	Master	Read Request	6		d386/tbb(S)		22	
- Preamble: 0x55		324	Slave	Read Response	5	Peripheral Preferred Connection Pa			25	
- Access Address: Oxd3058bb		325	Master	Read Request	2	Peripheral Preferred Connection Pa	d386ffbb(S)		22	
- CRC: 0x925a20		328	Slave	Read Response	1	Peripheral Preferred Connection Pa	d386ffbb(S)		28	
LE DATA:		331	Master	Read Request	8	Primary Service	d396ffbb(S)		22	
L2CAP.		334	Slave	Read Response	8	Generic Attribute Profile	d386#bb(S)		22	
- PDU Length: 6		337	Master	Read Request	9	Primary Service	d386/lbb(S)		22	
- Channel ID: 0x0004 (Attribute Protocol)		340	Slave	Read Response	9	Glucose	d386itbb(S)		22	
ATT:		343	Master	Read Request	10	Characteristic	d38684PP(2)		22	
- Floke Stave		346	Slave	Read Response	11	Glucose Measurement	d386/lbb(S)		25	
- Signature Present: No.		347	Master	Read Request	11	Glucose Measurement	d386ftbb(S)		22	
- PDU Type is Command: No		350	Slave	Read Response	11	Glucose Measurement	d3868bb(S)		22	
- Dpcode Read Response		355	Master	Read Request	12	Characteristic Presentation Format	d386/lbb(S)		22	
- "Database: d3860bb(\$1		358	Slave	Read Response	12	Characteristic Presentation Format	d386ftbb(S)		27	
- "Stored Handle: 15		367	Master	Read Request	13	Characteristic	d396ffbb(S)		22	
- "Store Characteristic		369	Master	Read Response	14	Battery Level	d386ilbb(M)		25	
EP Properties		372	Master	Read Request	14	Battery Level	d386ffbb(S)		22	
Entended Properties Permitted: No		375	Slave	Read Response	14	Battery Level	d3968bb(S)		21	
- Authenticated Signed Writer Permitted: No		380	Master	Read Request	15	Characteristic	d386ffbb(S)		22	
-Indicate Permitted No		363	Slave	Fisad Response	16	Battery Power State	d395ilbb(5)		25	
- Polify Permitted: No		388	Master	Read Request	16	Battery Power State	d396ftbb(S)		22	
- Write Permitted: No		391	Slave	Read Response	16	Battery Power State	d306ffbb(S)		23	
- Write Without Response Permittest: No		6.607	Master	Read Request	14	Battery Level	(e28/935/5)		22	
- Fead Permitted: Yes		6.610	Slave	Read Response	14	Battery Level	fe28/935(S)		21	
- Eloadcast Permitted: No		7.895	Master	Write Command	14	Battery Level	fe28/935(S)		23	
- Value Handle: 16		22.242	Master	Read Request	14	Battery Level	13e91693(S)		22	
- UUID Battery Power State		22 245	Slave	Read Response	14	Battery Level	13e91693(S)		21	
- no we can be a second the c		22.735	Master	Read Request	14	Battery Level	13e91693(S)		22	
										_
	1.4									
al Frames: 38 292 Frames Filtered In: 51 Frame #s Selected: 38	33; (1 total)									
					-					

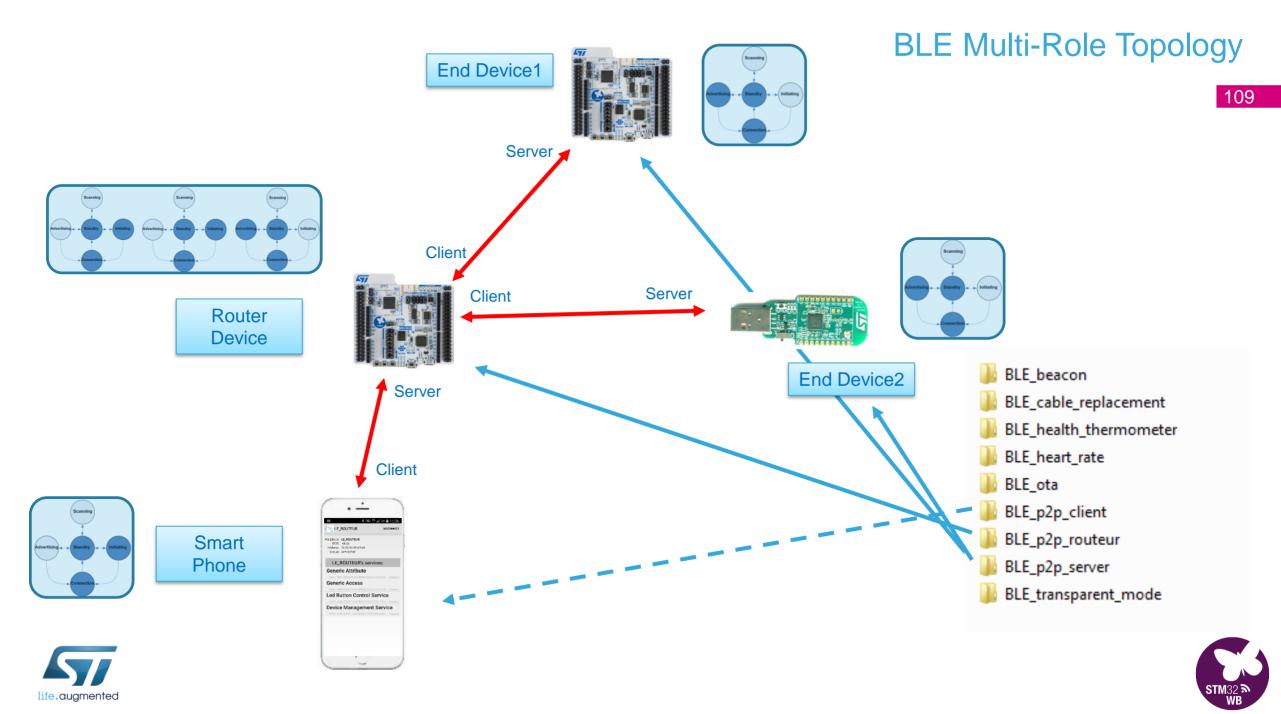
Decode Pane shows comprehensive layered decoders of each frame/message with clear, concise descriptions. Summary Pane displays a one line overview of each data frame/message. Click on any line to reveal detail in mutiple panes below.

Filter Tabs isolate frames by profile or protocol for guick and convenient





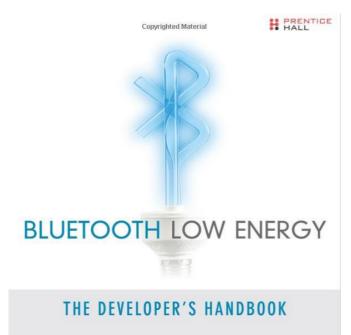




### Dig Deeper

#### 110

#### BLE4.0 only but highly detailed

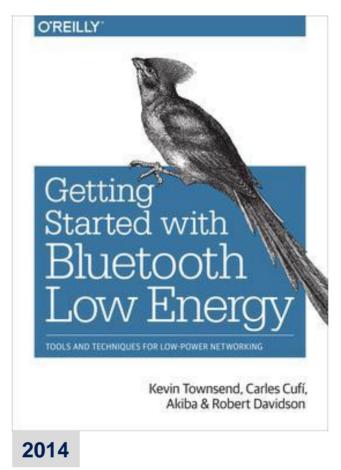


**ROBIN HEYDON** 

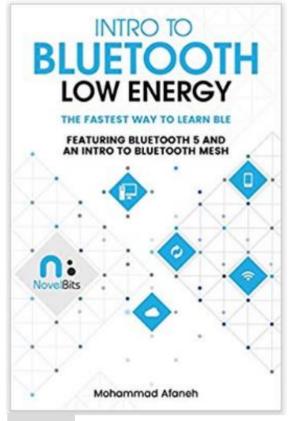
2012



#### Up to 4.1, 5.0 not covered



Includes 5.0 & Mesh





### Dig Deeper

# Bluetooth<sup>®</sup> https://www.bluetooth.com/

# **Core Specifications**

The *Bluetooth®* Core Specification defines the technology building blocks that developers use to create the interoperable devices that make up the thriving Bluetooth ecosystem. The Bluetooth specification is overseen by the Bluetooth Special Interest Group (SIG) and is regularly updated and enhanced by Bluetooth SIG Working Groups to meet evolving technology and market needs.

Specification		Version	Status	Adoption Date
CS	Core Specification	5.0	Active	06 Dec 2016
CSS	Core Specification Supplement	7	Active	06 Dec 2016
CSA	Core Specification Addendum	6	Active	12 Jul 2017









#### Working Groups

Core Specifications

Mesh Networking Specifications

Traditional Profile Specifications

Protocol Specifications

#### GATT Specifications

GATT Overview

life.auamented

More about GATT

GATT Characteristics	Profile Specification		Version	Status	Adoption Date	Informative document showing changes
GATT Declarations GATT Descriptors	ANP	Alert Notification Profile	1.0	Active	13 Sep 2011	N/A
GATT Services Mesh GATT Services XML	ANS	Alert Notification Service	1.0	Active	13 Sep 2011	N/A
Available Schemas	AIOP	Automation IO Profile	1.0	Active	14 Jul 2015	N/A
Errata Service Releases	AIOS	Automation IO Service	1.0	Active	14 Jul 2015	N/A
Qualification Test Requirements	BAS	Battery Service	1.0	Active	27 Dec 2011	N/A
Assigned Numbers	PCS	Rody Composition Sorvice	10	Activo	21 Oct 2014	8178



## **GATT Specifications**

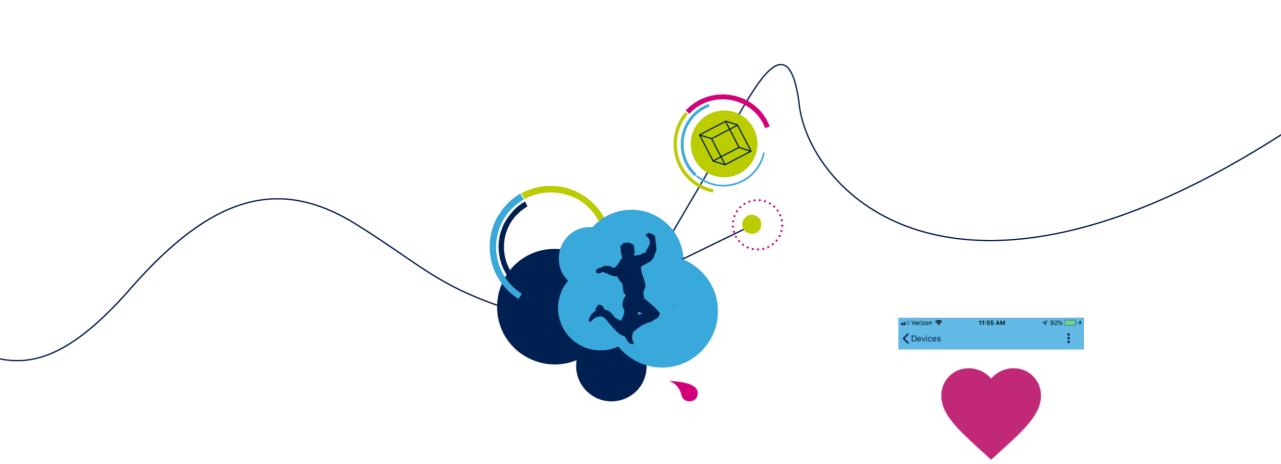
Generic Attributes (GATT) services are collections of characteristics and relationships to other services that encapsulate the behavior of part of a device.

A GATT profile describes a use case, roles, and general behaviors based on the GATT functionality, enabling extensive innovation while maintaining full interoperability with other Bluetooth® devices.

The documents in the "Informative document showing changes" column are provided as a courtesy to help readers identify changes between two versions of a Bluetooth specification. When implementing specifications, use the adopted versions in the "Adopted Version" column.







## Hands-On Heart-Rate Monitor



72 bpm

Energy: 20 kJ RR Interval: 1.00 s







### Hands-On: HRM example

### All CubeWB Projects referenced today can be found in the CubeMX Repository folder:

ry 🔻 Share with 👻 New folder			
^ Name	Date modified	Туре	Size
_htmresc	2/19/2019 9:56 AM	File folder	
Documentation	2/19/2019 9:56 AM	File folder	
Drivers	2/19/2019 9:56 AM	File folder	
Middlewares	2/19/2019 9:56 AM	File folder	
Projects	2/19/2019 9:56 AM	File folder	
Utilities	2/19/2019 9:56 AM	File folder	
how_to_program_wireless_stacks.txt	2/19/2019 9:56 AM	Text Document	1
package.xml	2/19/2019 9:56 AM	XML Document	1
Readme.md	2/19/2019 9:56 AM	MD File	2
Release_Notes.html	2/19/2019 9:56 AM	Chrome HTML Do	18

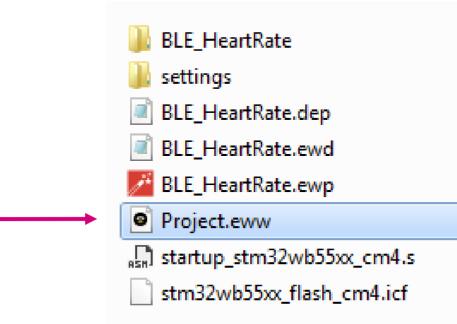




### Hands-On: HRM example

### Open the BLE\_HeartRate workspace

▶ STM32Cube\_FW\_WB\_V1.0.0 ▶ Projects ▶ NUCLEO-WB55.Nucleo ▶ Applications ▶ BLE ▶ BLE\_HeartRate ▶ EWARM ▶

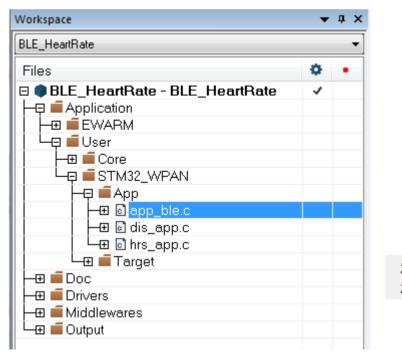






### Open app\_ble.c





Change the advertised local name, using your Magic Number!

(You can change it as you wish, however keep the # of ASCII chars to 5)

229 static const char local\_name[] = { AD\_TYPE\_COMPLETE\_LOCAL\_NAME , 'H', 'R', 'S', 'T', 'M'};
230 
uint8\_t manuf\_data[14] = {

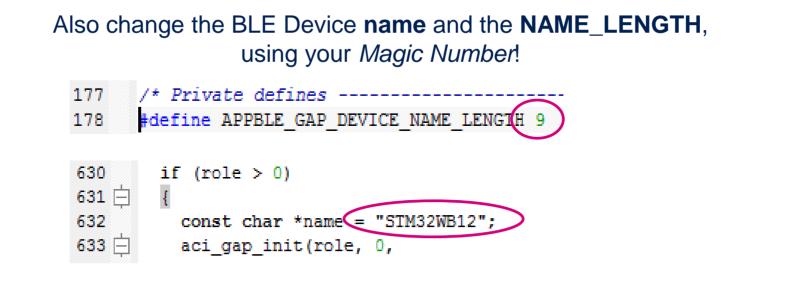
229 static const char local\_name[] = { AD\_TYPE\_COMPLETE\_LOCAL\_NAME ,'S','T','M','1','2'};



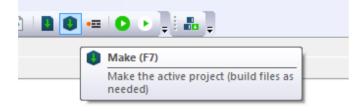


### Hands-On: HRM example

Workspace	•	џ×
BLE_HeartRate		•
Files	•	•
🗆 🌒 BLE_HeartRate - BLE_HeartRate	1	
- 🛱 🛋 Application		
│		
└		
│		
│ └─── 🖬 STM32_WPAN		
│		
│  │  └─⊞		
│ └─⊞ 🛋 Target		
⊣⊞ 🖬 Doc		
⊨ 🖬 🖬 Drivers		
🛏 🖬 Middlewares		
└─⊞ 💼 Output		



#### Build, Program and Launch debugger





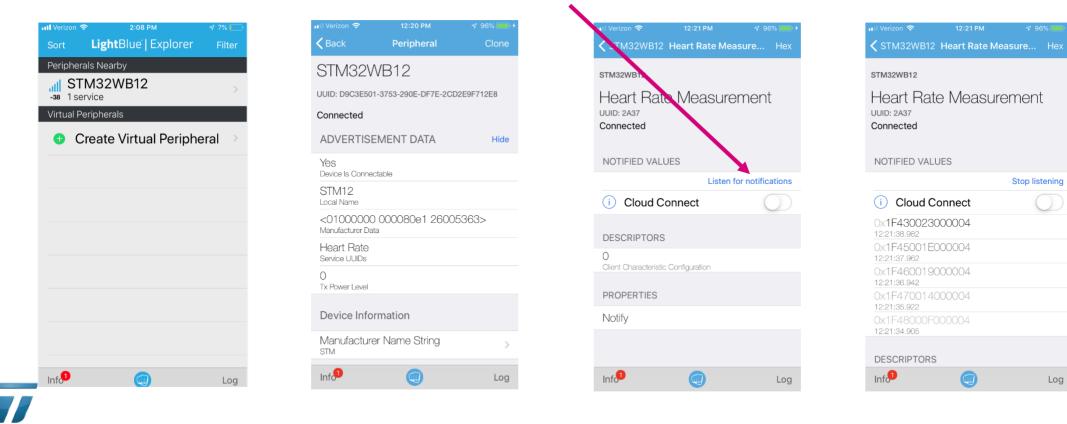




- Open your LightBlue Explorer App on iOS
- Find your device and tap on it
- Show Advertisement Data

life.augmented

Click on the Heart Rate Measurement and Enable Notifications



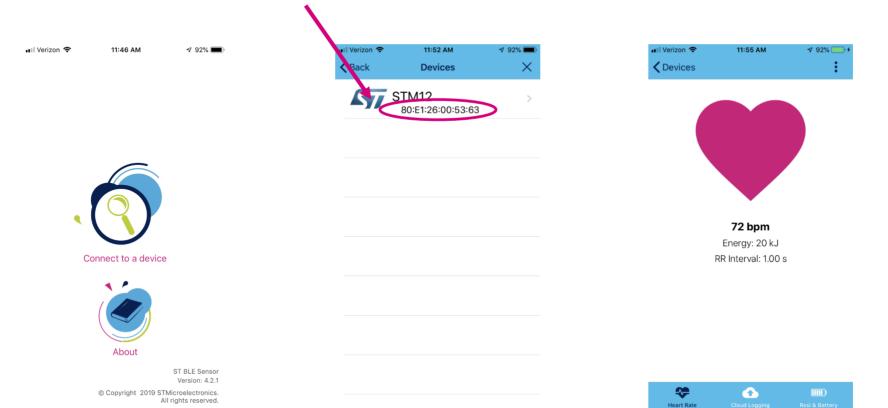
- Open your LightBlue Explorer App on Android
- Find your device and tap on it

Learn Email

- Tap on the Heart Rate section and select Heart Rate Measurement
- Tap on "SUBSCRIBE" to Enable Notifications

¥ #2 🖬	* 15.928 <b>≣</b> 2.01 PM	II :	≰ 🖘 92% 🛢 2:01 PM	■ • ゆ	🗣 🕸 🖘 92% 🗎 2:01 PM	■ 9 ゆ	오 💰 🖘 92% 🛢 2:02 PM
LightBlue® Explorer	Q = 1	← STM12	1	← STM12		← STM12	
PAPER A		ADVERTISEMENT DATA		PROPERTIES		PROPERTIES	
PunchThrough		Connected Connected		Device Address 80:E1:26:00:67:76		Device Address 80:£1:26:00:67:76	
Enjoying LightBlue® Explorer?		Advertised name STM12		Service UUID 0000180d-0000-1000-8000-00805f9b34fb		Service UUID 0000180d-0000-1000-8000-00805f9b34fb	
Learn about our insights into BLE. Email Address		Advertised service UUIDs 0000180D-0000-1000-8000-00805F9B34FB		Characteristic Name Heart Rate Measurement		Characteristic Name Hearl Rate Measurement	
SUBSCRIBE DISMISS		DEVICE INFORMATION		Characteristic UUID 00002a37-0000-1000-8000-00805f9b34fb		Characteristic UUID 00002a37-0000-1000-8000-00805f9b34fb	
STM12 #4dbm 80.51/26.00/67.76		Device Address 80:E1:26:00:67:76		× Readable Able to be read from		× Readable Able to be read from	
Unnamed 888m 12.FEE8F6.74.68		Manufacturer Name String STM		× Writable Able to be written to		X Writable Able to be written to	
Charge 2		GATT SERVICES & CHARACTERISTICS		<ul> <li>Supports notifications/indications</li> <li>Able to be subscribed to for notifications/indications on changes to the characterie</li> </ul>	tic	<ul> <li>Supports notifications/indications</li> <li>Able to be subscribed to for notifications/indications on changes to the chan</li> </ul>	acteristic
48dBm C7.5E:71.F6.4A.0E		Generic Attribute Service Changed	$\rightarrow$	READ/INDICATED VALUES		READ/INDICATED VALUES	
-sodem 75:80:EC:5C:15:2A		Generic Access Device Name Appearance Peripheral Preferred Connection Parameters	$\rightarrow$	READ AGAI SUBSCRIBE		READ AGAIN UNSUBSCRIBE	
44dBm 26/94/38/88FC:47		Device Information Manufacturer Name String	$\rightarrow$	No value read recently Tap on one of the buttons above - if available - to begin		1F 46 00 19 00 00 04 Wed Apr 17 14:02:04 CDT 2019	
-9080m 23:06:90:1E:DC:33		Heart Rate Heart Rate Measurement		DESCRIPTORS		1F 47 00 14 00 00 04 Wed Apr 17 14:02:03 CDT 2019	
-101dbm 13.9C.24:33.31:55		Body Sensor Location Heart Rate Control Point	$\rightarrow$	Client Characteristic Configuration 00002902-0000-1000-8000-00808/9b34/b		1F 48 00 0F 00 00 04 Wed Apr 17 14:02:02 CDT 2019	
-39dBm 5A:5C:C2:8A:0D:97						DESCRIPTORS	
Unnamed -105dBm 48:58:2C:75:D0:87						Client Characteristic Configuration 00002902-0000-1000-8000-00805/9b34fb	
		Select a characte	eristic to explore				
		Heart Rate Measurer					
		Body Sensor Locatio	on				
		Heart Rate Control P	Point				

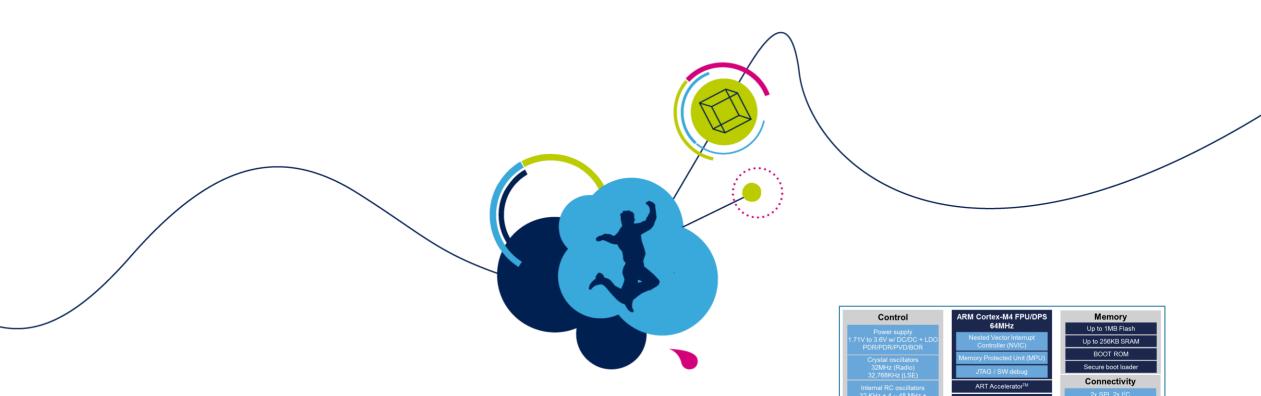
- Disconnect from the LightBlue Explorer App
- Launch the ST BLE Sensor App
- Tap on your device name
- Write down your Nucleo Bluetooth Device Address.
  - > Can you find it in the Mfr-Specific advertised data via LightBlue app?











# **WB** Architecture

Control	AKW COTEX-W4 FF0/DF3	Memory		
Power supply	64MHz	Up to 1MB Flash		
1.71V to 3.6V w/ DC/DC + LDO PDR/PDR/PVD/BOR	Nested Vector Interrupt Controller (NVIC)	Up to 256KB SRAM		
Crystal oscillators	Memory Protected Unit (MPU)	BOOT ROM		
32MHz (Radio) 32,768KHz (LSE)	JTAG / SW debug	Secure boot loader		
Internal RC oscillators	ART Accelerator™	Connectivity		
32 KHz + 4 – 48 MHz + 16 MHz (HSI) + 48MHz	AHB Bus Matrix	2x SPI, 2x I <sup>2</sup> C		
+/- 1% acc, over V and T(°C)	2x DMA 7channels	1x USART LIN, smartcard, IrDA,		
RTC / AWU/ CSS	Multi-Protocol Radio	Modem control		
PLL / FLL	Bluetooth 5™	1x ULP UART		
SysTick timer	IEEE 802.15.4	USB 2.0 FS – Crystal less		
2 watchdogs (WWDG / IWDG)	AES	Quad-SPI (XIP)		
Up to 72 I/Os	ARM Cortex-M0+ MPU	SAI (Full duplex)		
Cyclic Redundancy Check	32MHz	Control		
Voltage scaling (2 modes)	Nested Vector Interrupt	4x 16-bit 32-bit timers		
voltage scaling (2 modes)	Controller (NVIC)	2x ULP 16-bit timers		
Analog	SW debug	Sensing		
2x ULP comparators		16-keys Capacitive touch		
1x 12-bit ADC SAR 4,25Msps	Security	Display		
Temperature sensor	AES 256-bit / PKA TRNG / PCROP	8x40 LCD driver		





### **Balun** – Combine TX and RX signals

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

Harmonic Filter – Reduce out-of-band harmonics

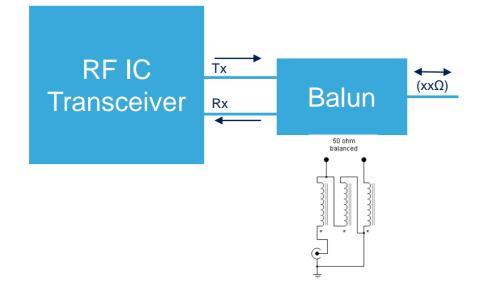




### **Balun** – Combine TX and RX signals

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

Harmonic Filter – Reduce out-of-band harmonics





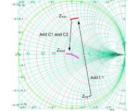


### **Balun** – Combine TX and RX signals

### **Matching Network** $-50 \Omega$ impedance transformation

Harmonic Filter – Reduce out-of-band harmonics





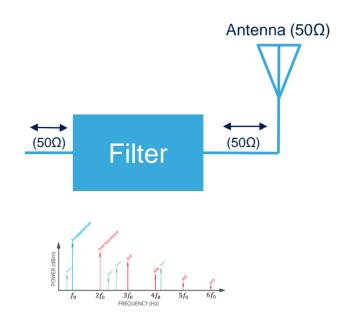




**Balun** – Combine TX and RX signals

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

Harmonic Filter – Reduce out-of-band harmonics



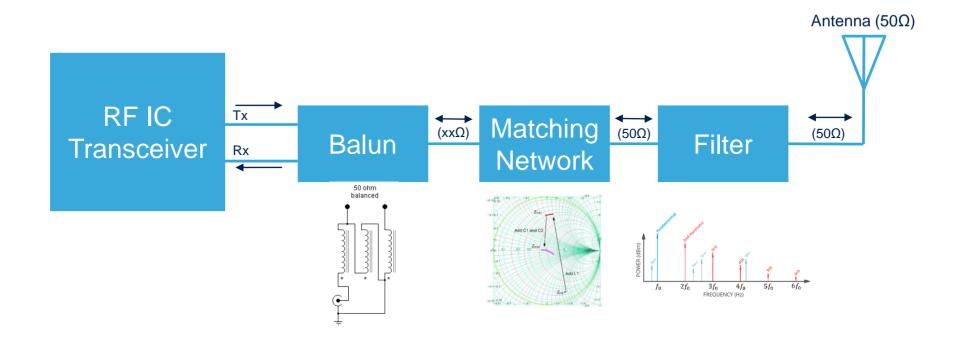




### **Balun** – Combine TX and RX signals

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

Harmonic Filter - Reduce out-of-band harmonics



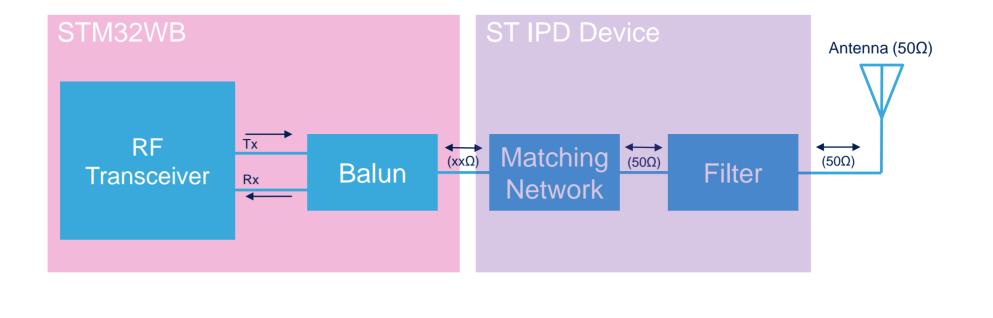


### Basic RF System

### **Balun** – Combine TX and RX signals

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

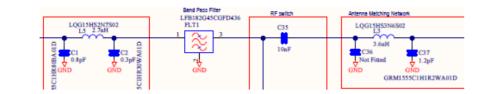
Harmonic Filter - Reduce out-of-band harmonics

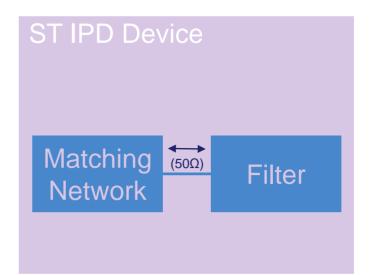




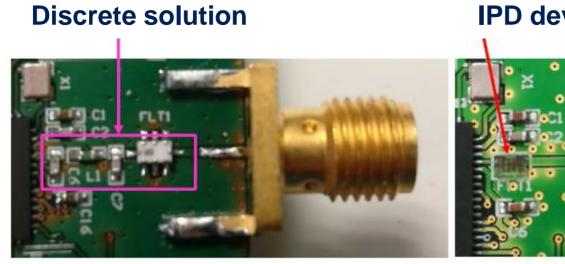


### Matching Network + Harmonic Filter





. . .



### **IPD device from ST**





### **IPD** Filter

### Mass Production NOW



#### MLPF-WB55-01E3

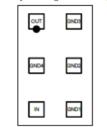
Datasheet

2.4 GHz low pass filter matched to STM32WB55Cx/Rx

### Versions coming for upcoming WLCSP / BGA packages



#### 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<sup>®</sup>2 compliant

#### Applications

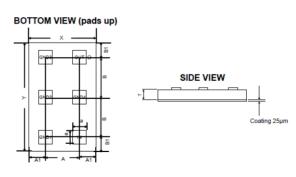
- Bluetooth 5
- OpenThread
- Zigbee®
- IEEE 802.15.4
- Optimized for STM32WB55Cx and STM32WB55Rx





### **IPD** Filter

130



### 1mm x 1.6mm CSP

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

Parameter	Description	Min.	Тур.	Max.	Unit
Х	X dimension of the die	975	1000	1025	μm
Y	Y dimension of the die	1575	1600	1625	μm
А	X pitch		500		μm
В	Y pitch		587		μm

# PCB recommendations included in datasheet

#### Figure 13. PCB land pattern recommendations

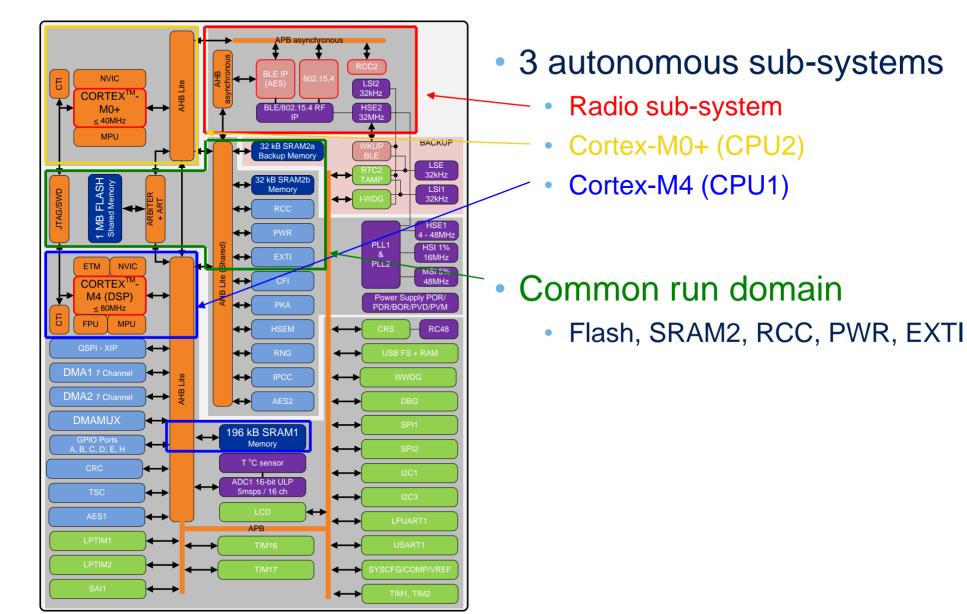
Top\_Layer Top\_Solder \_Mask





### Architecture

131



life.augmented

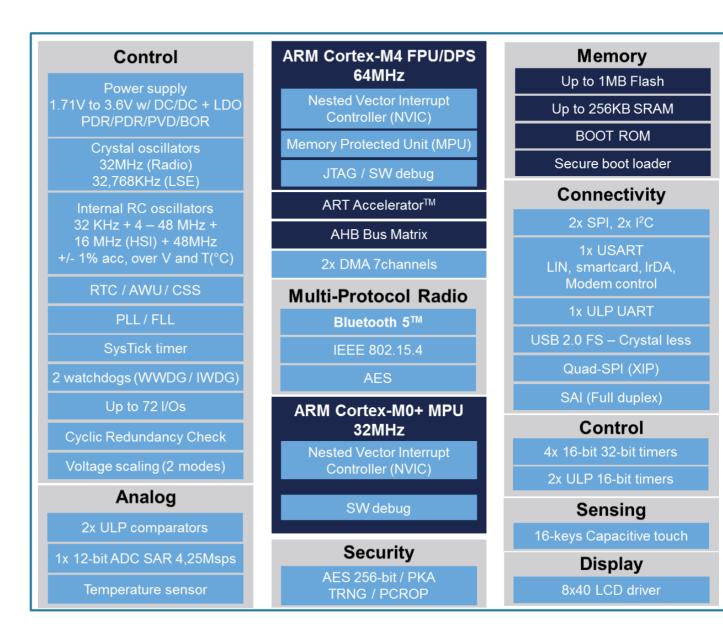


### **Block Diagram**

#### • Radio with integrated balun

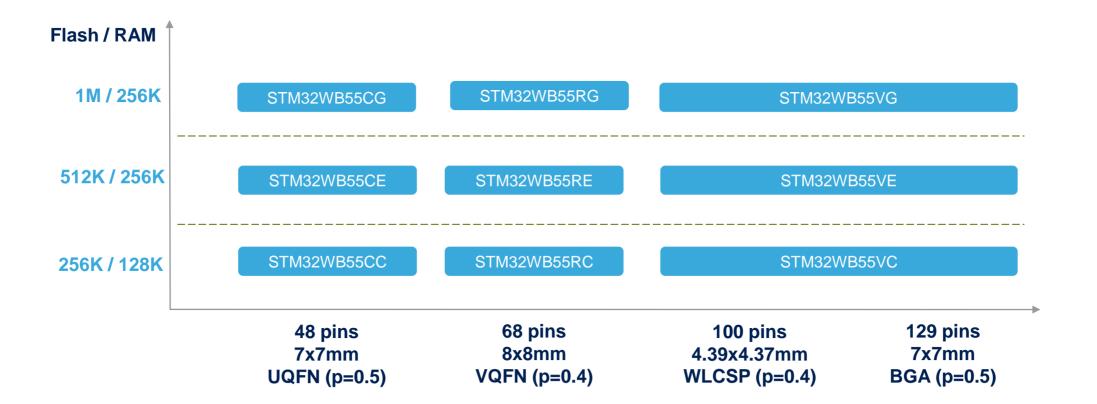
- Output power: +6.0 dBm
- BLE RX sensitivity: -96 dBm
- 802.15.4 RX sensitivity: -100 dBm
- RX: 4.5mA
- TX: 5.2mA (0dBm)
- -40°C to +105°C
- Packages
  - QFN48 / 68
  - WLCSP100
  - BGA129







### STM32WB55 Series Portfolio

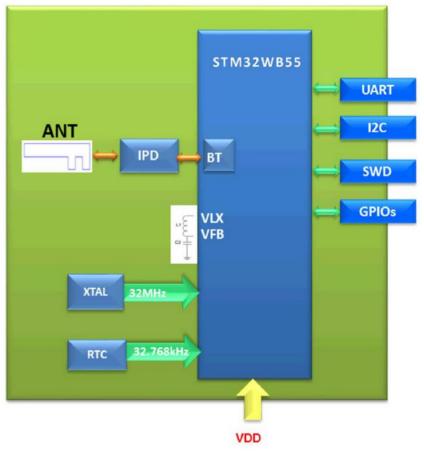






### STM32WB55 Module

- Pre-Certified
- Chip Antenna
- 10x10mm
- Large GPIO count
- Pin pitch = 2 layer PCB-ready
- Production in early 2020.







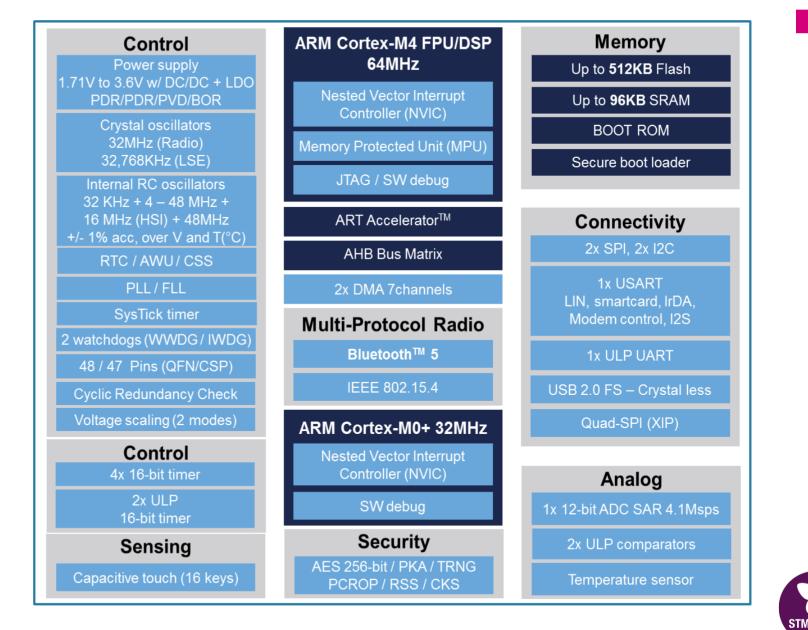
### STM32WB35 – Block Diagram

256KB or 512KB Flash 96KB SRAM

- QFN48
- WLCSP47

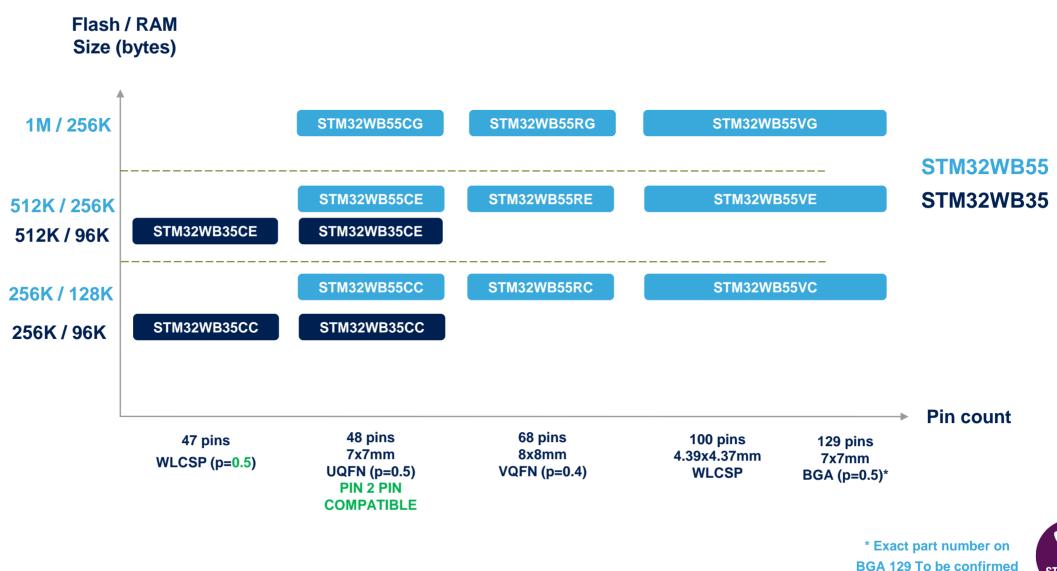
Late 2019





### Positioning

136





STM32

### STM32WB & BlueNRG Series

**DUAL-CORE** 

111



NETWORK PROCESSOR

SINGLE-CORE

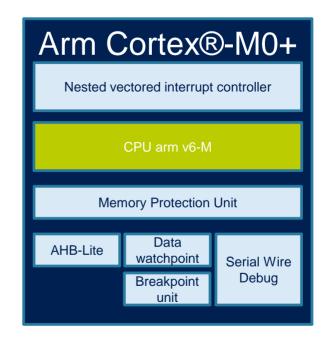
### **APPLICATIONS PROCESSOR**





### Cortex-M0+ processor overview

- ARMv6-M architecture
- Von Neumann architecture
- 2-stage pipeline
- Single-issue architecture
- Single-cycle MULTIPLY







## **ARM**<sup>°</sup>

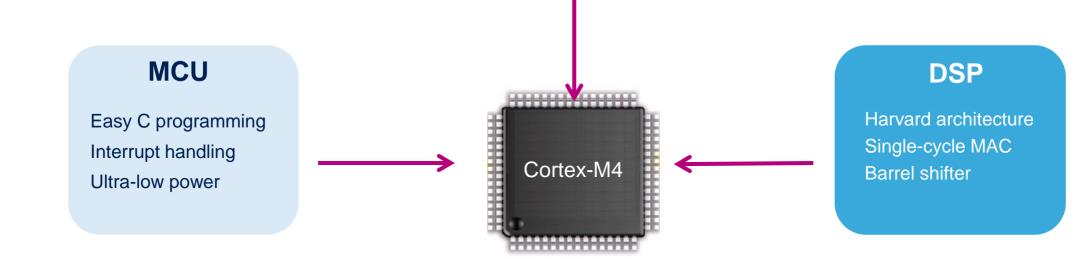
### ARM<sup>®</sup> Cortex<sup>®</sup> M4 Core

139



### FPU

Single precision Better code efficiency Eliminate scaling and saturation Support meta-language tools (MATLAB, etc)





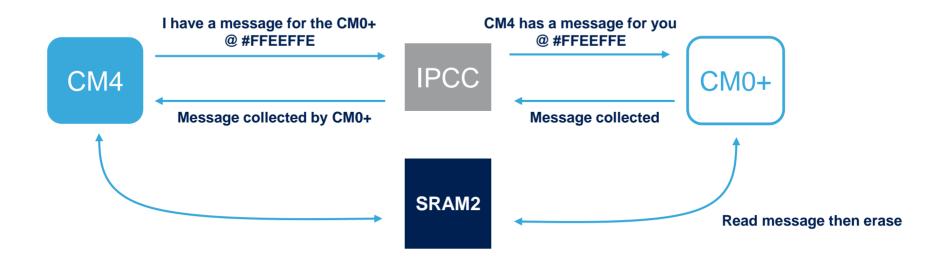
http://www.arm.com/products/processors/cortex-m/cortex-m4-processor.php



### Dual core – How does that work?

### **IPCC: Inter Processor Communication Controller**

HSEM: Hardware Semaphore – prevent shared resource access conflicts

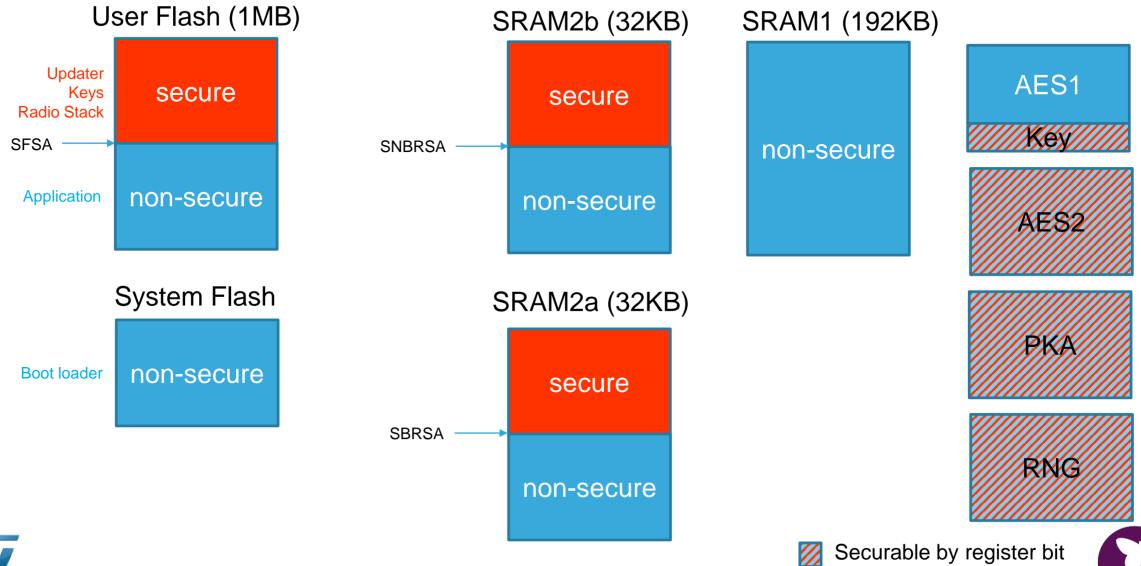


IPCC works in both directions



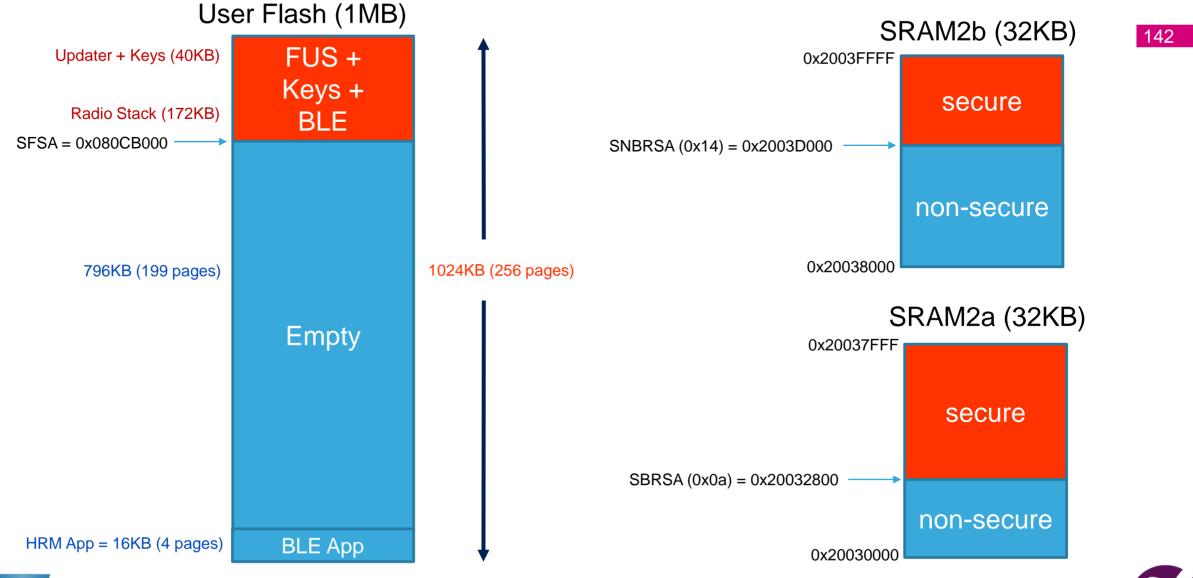


### **Memory Partitioning**





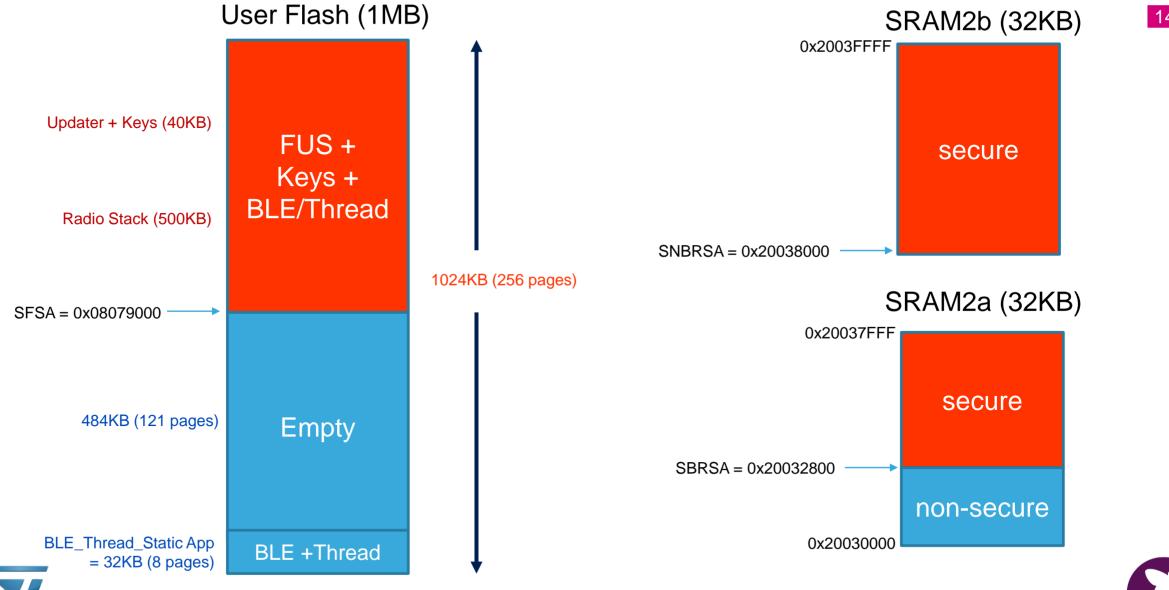
### Memory Partitioning: BLE Stack







### Memory Partitioning: BLE+Thread (Concurrent) Stack



life.augmented

### Release\_Notes.html

#### Release Notes for STM32WB Copro Wireless Binaries

Copyright © 2019 STMicroelectronics



#### License

This software component is licensed by ST under Ultimate Liberty license SLA0044, the "License";

You may not use this file except in compliance with the License.

You may obtain a copy of the License at: SLA0044

#### Purpose

This release covers the delivery of STM32WB Coprocessor binaries.

Here is the list of the supported binaries:

- stm32wb5x\_BLE\_Stack\_fw.bin
  - Full BLE Stack 5.0 certified : Link Layer, HCI, L2CAP, ATT, SM, GAP and GATT database
  - BT SIG Certification listing : Declaration ID D042164
- stm32wb5x\_BLE\_HCILayer\_fw.bin
  - HCI Layer only mode 5.0 certified : Link Layer, HCI
  - BT SIG Certification listing : Declaration ID D042213
- stm32wb5x\_Thread\_FTD\_fw.bin
  - Full Thread Device certified v1.1
  - To be used for Leader / Router / End Device Thread role (full features excepting Border Router)

For complete documentation on STM32WBxx, visit: [www.st.com/stm32wb]



#### Update History

V1.0.0 / 06-February-2019

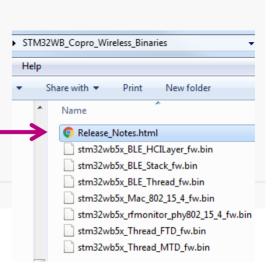
#### Main Changes

#### First release

#### First official release.

Binary Install Address and version : Provides Install address for the targeted binary to be used in "STEP 4" of flash procedure.

Wireless Processor Binary	Install address	Version	Date
stm32wb5x_BLE_Stack_fw.bin	0x080CB000	v1.0.0	02/06/2019
stm32wb5x_BLE_HCILayer_fw.bin	0x080CD000	v1.0.0	02/06/2019
stm32wb5x_Thread_FTD_fw.bin	0x0809F000	v1.0.0	02/06/2019
stm32wb5x_Thread_MTD_fw.bin	0x080B5000	v1.0.0	02/06/2019
stm32wb5x_BLE_Thread_fw.bin	0x08079000	v1.0.0	02/06/2019
stm32wb5x_Mac_802_15_4_fw.bin	0x080E5000	v1.0.0	02/06/2019
stm32wb5x_rfmonitor_phy802_15_4_fw.bin	0x080EA000	v1.0.0	02/06/2019



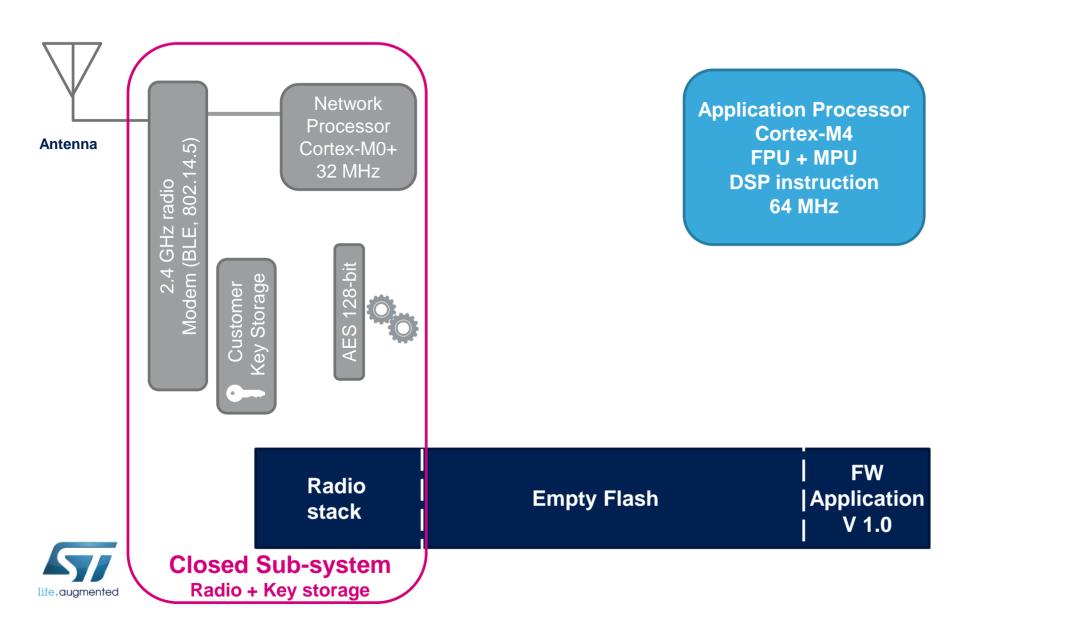


## IoT Protection Ready

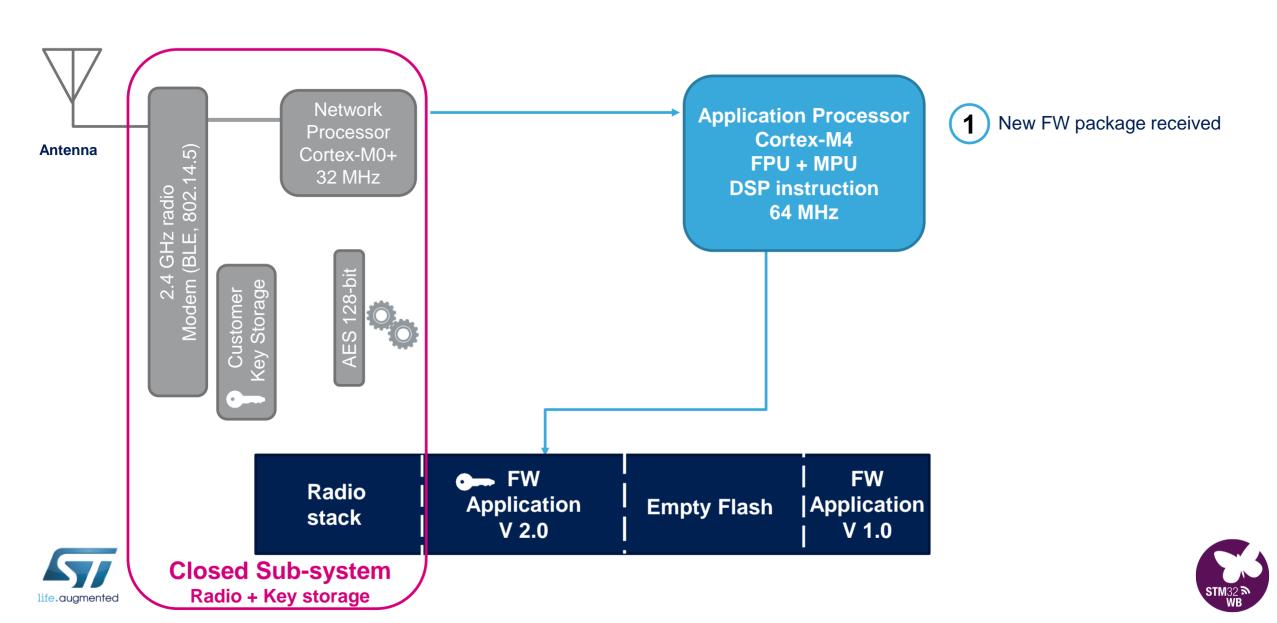
Attacks	Attacks description	STM32WB Countermeasures
Non Invasive	<ul> <li>Environment <ul> <li>Temp / Voltage / Clocks</li> </ul> </li> <li>Fault injection <ul> <li>Exploit debugger</li> <li>Side channel</li> <li>Power Analysis</li> </ul> </li> </ul>	<ul> <li>Temp sensor</li> <li>Power supply monitor</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>
Software	<ul> <li>Break the encryption</li> <li>Extract keys</li> <li>Exploit debugger / test modes</li> <li>Malware</li> <li>Replay</li> </ul>	<ul> <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>

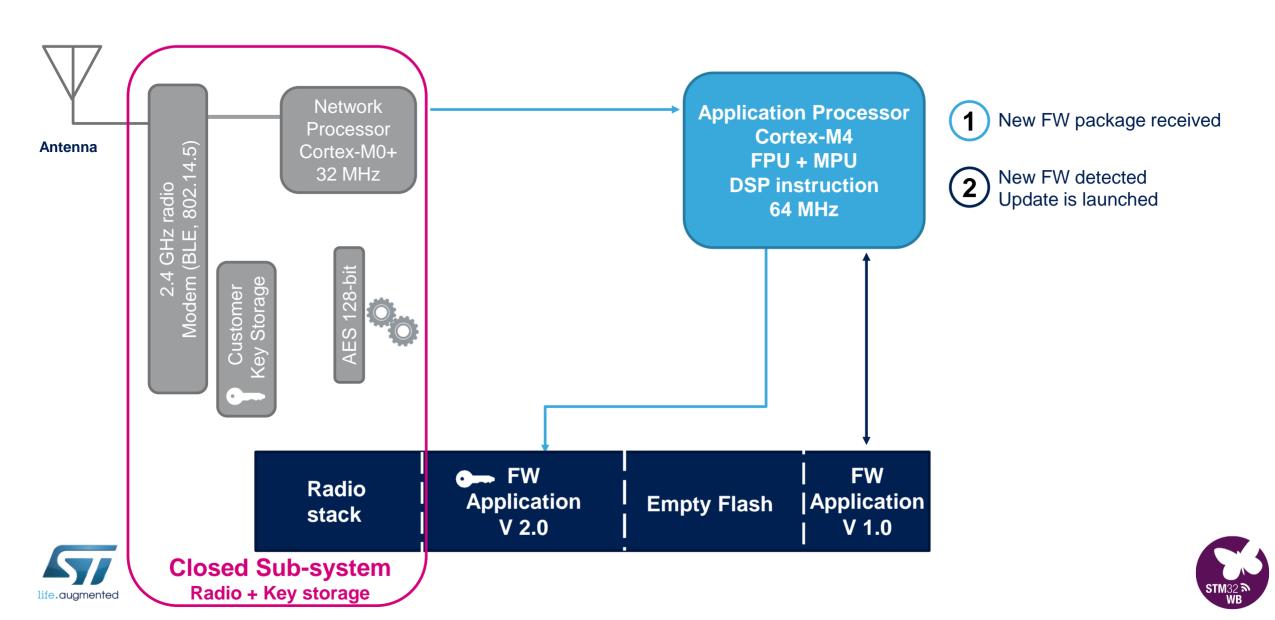


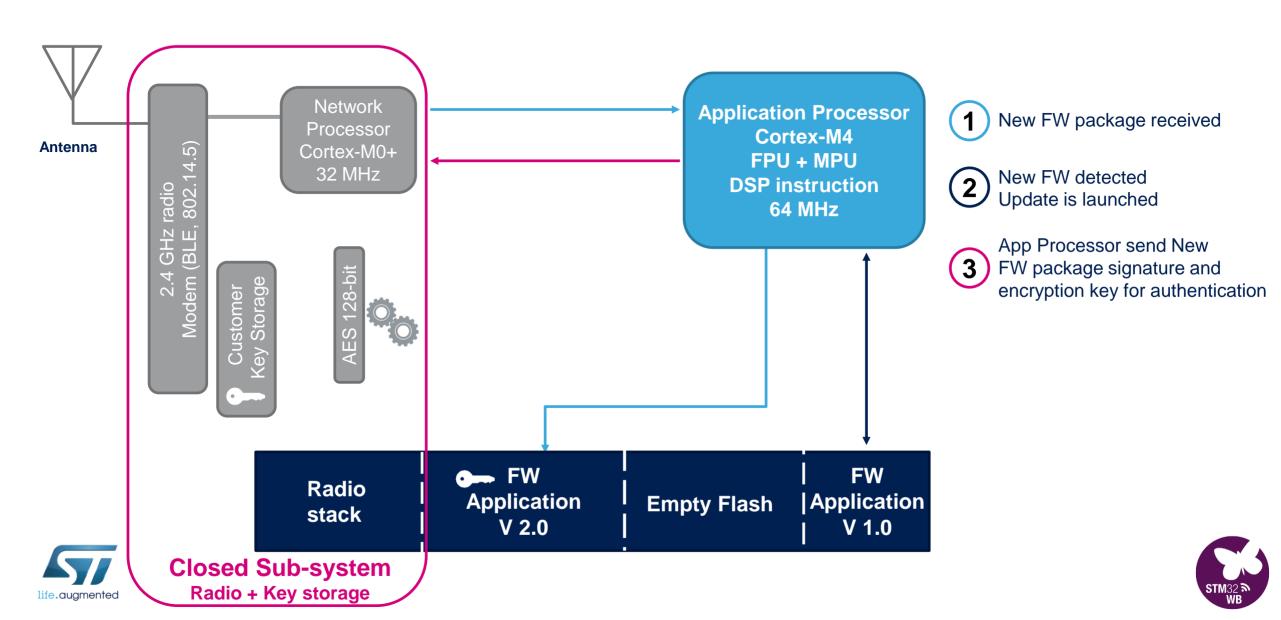


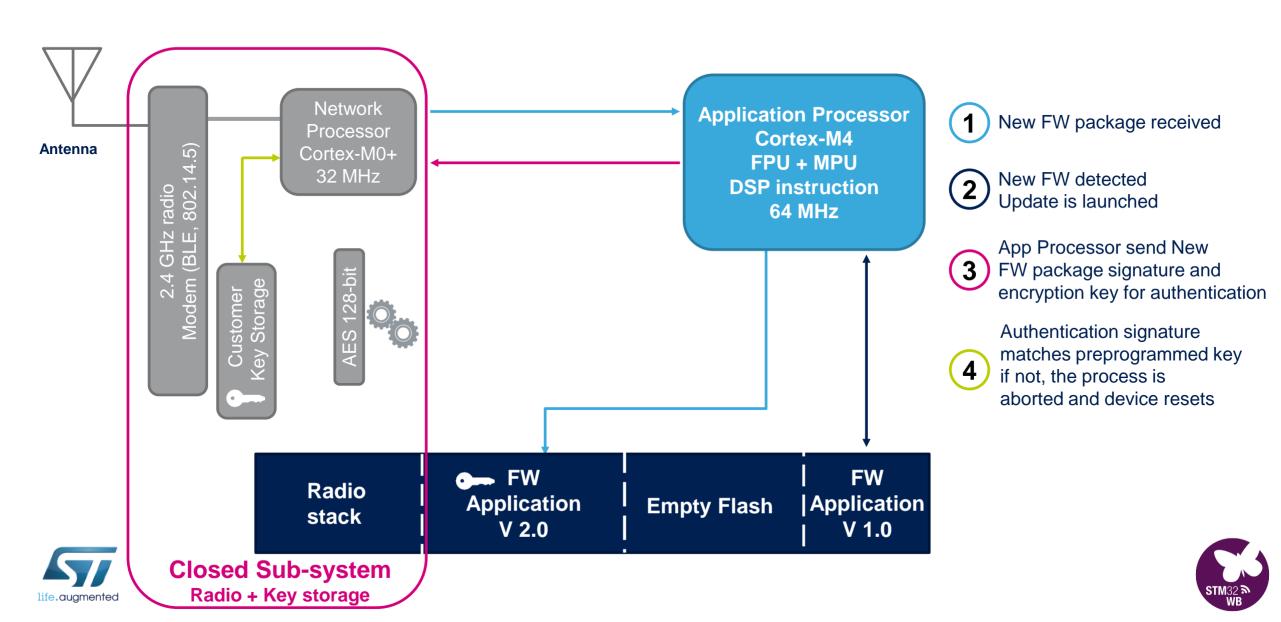


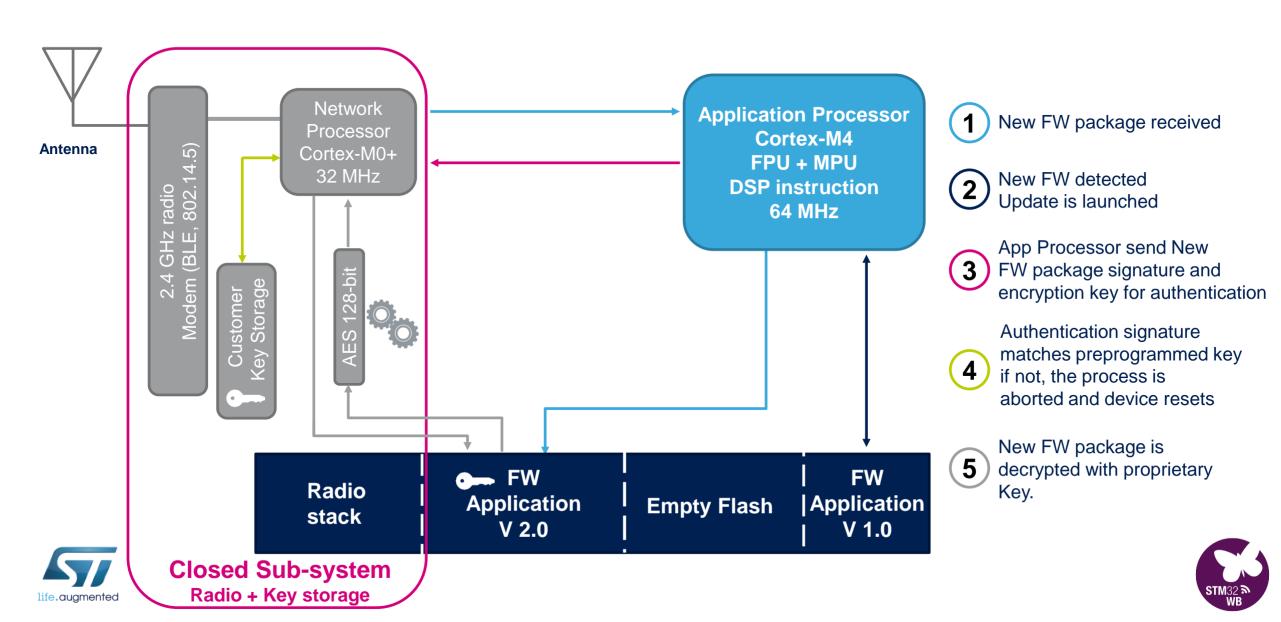


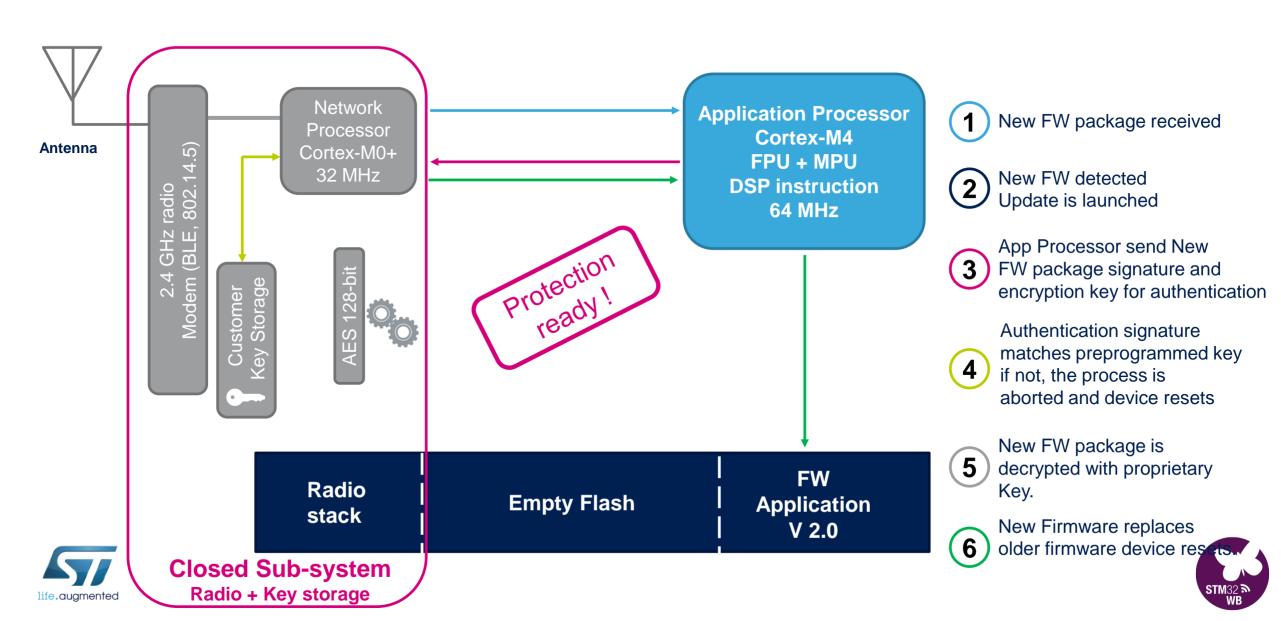






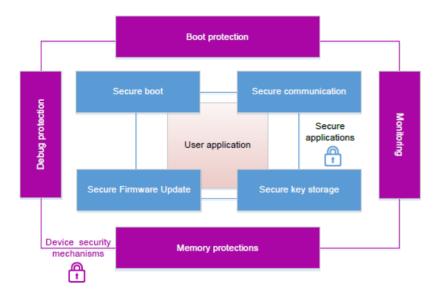


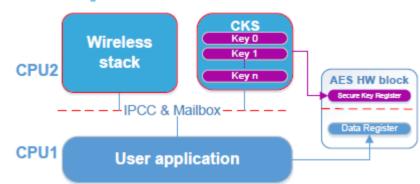




#### AN5156 – Security

#### AN5156 is a deep-dive into many security topics, some common and some WB-specific





#### Figure 13. Dual-core architecture with CKS service

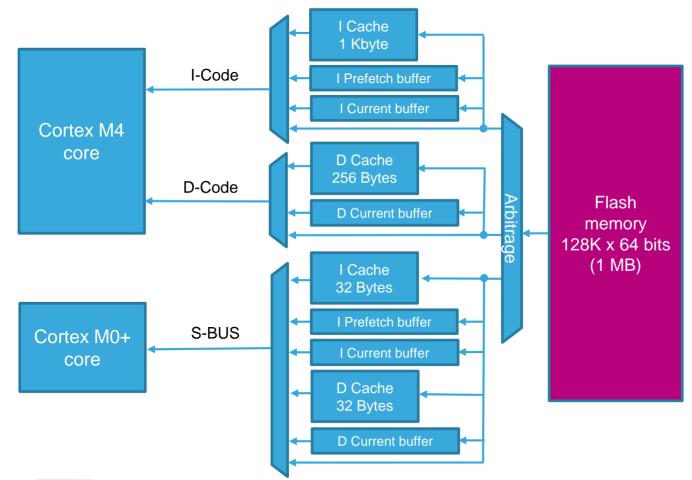
#### Attacks Hardware non-invasive Software Hardware invasive types Remote or local Local board and device level Local device level Scope Software bugs Debug port Probing Power Glitches Protocol weaknesses Laser Technics FIB Trojan horse Fault injection Eavesdropping... Side-channels analysis... Reverse engineering ... Quite low cost. Need only moderately From very low to high Very expensive. Need dedicated/ Cost depending on the security sophisticated equipment and knowledge to heavy equipment and very specific expertise failure targeted implement skills Access to confidential assets Reverse engineering of the device (code and data). (silicon intellectual property) Access to secret data or device internal Objectives Usurpation behavior (algorithm) Access to hidden hardware and software secrets (Flash access ) Denial of service

#### Table 4. Attacks types and costs





#### **ART** Accelerator<sup>™</sup>



#### Cortex-M4

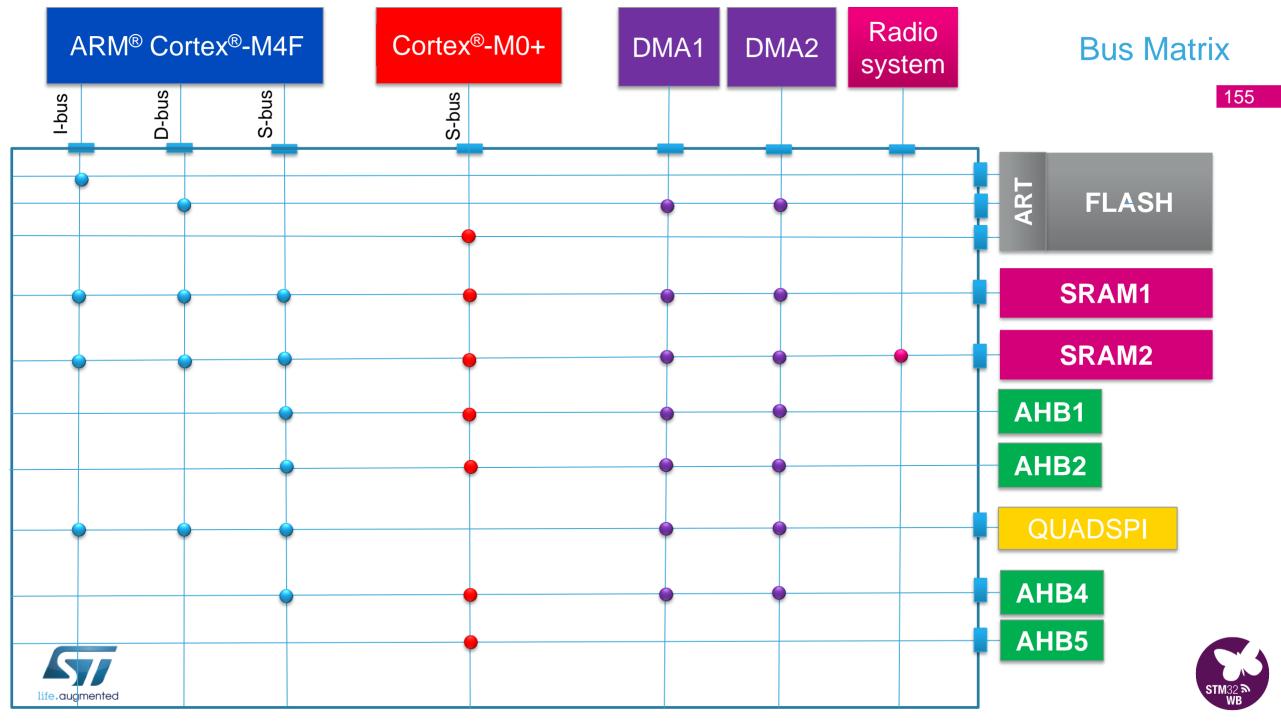
- **Instruction cache** = 32 lines of 4x64 bits
- **Data cache** = 8 lines of 4x64 bits
- Pre-fetch buffer

#### Cortex-M0+

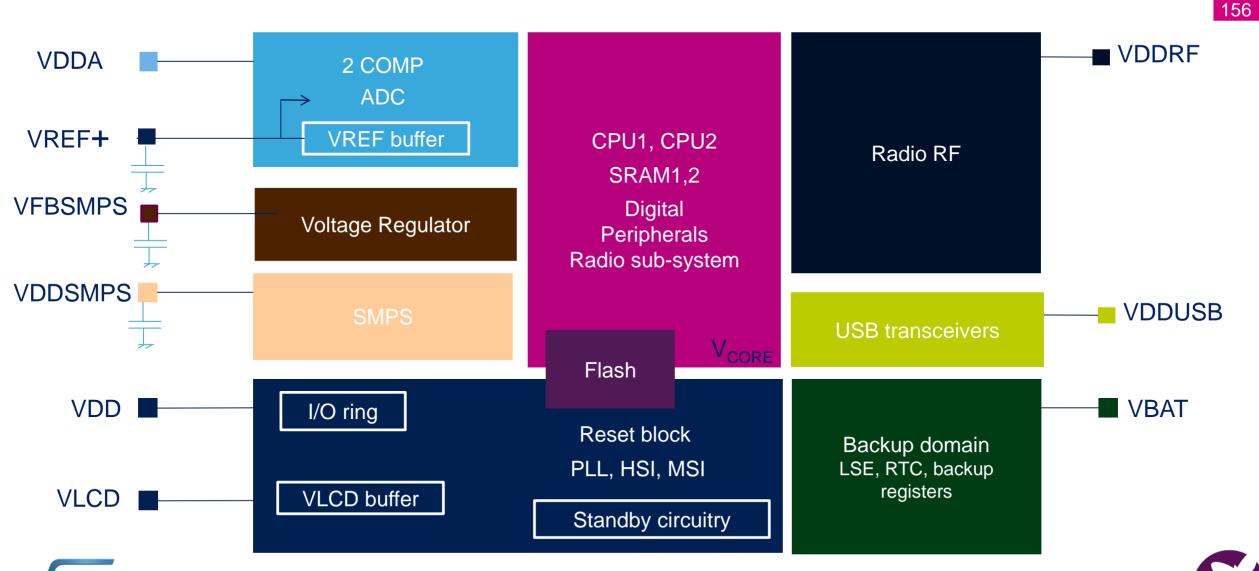
- **Instruction cache** = 4 lines of 1x64 bits
- **Data cache** = 4 lines of 1x64 bits
- Pre-fetch buffer







#### **Power schemes**

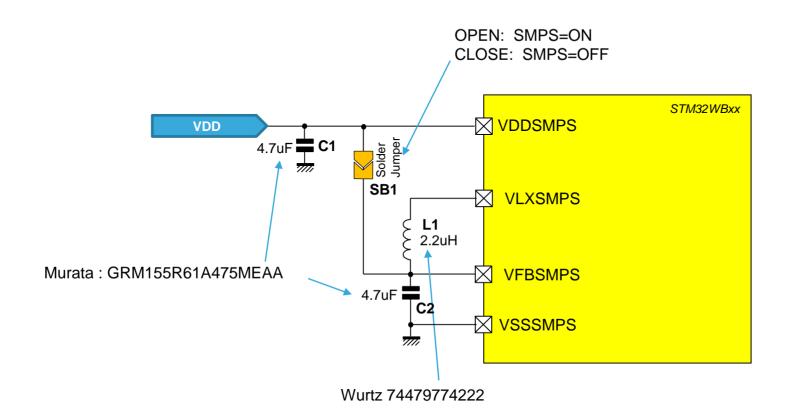






#### **SMPS Schematic**

157\_



8MHz SMPS configuration

For 4MHZ SMPS configuration change  $L1 = 4.7 \mu H$ 





#### **FlexPowerControl**

158



Typ @ VDD =1.8 V @ 25 °C

\* with RTC \*\* from SRAM1



High performance
 CoreMark score = 215
 Outstanding power efficiency

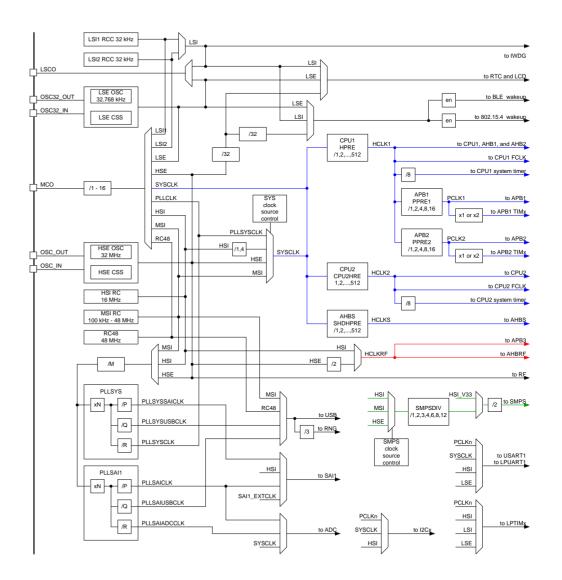
 $\rightarrow$  ULPBbench score = 175



## Clock tree

HSE (32MHz) required for radio operation

LSE (32.768KHz) required for most BLE applications

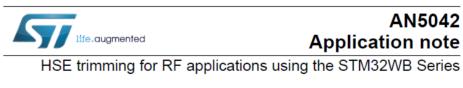


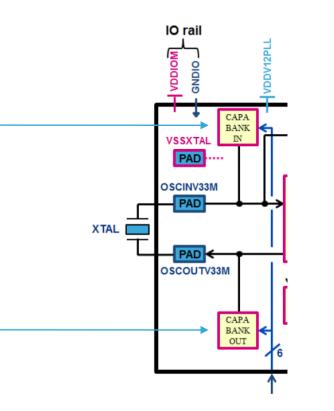




## **HSE Trimming**

- BLE requires very accurate 32 MHz clock
- Frequency can vary
  - Manufacturing process variations
  - Crystal used
  - PCB design
- Integrated load capacitor bank
  - 64 values for fine tuning
  - MCO clock output pin used for measurement at factory test
  - Stored in OTP
- No need for external capacitance
- AN5042 provides details



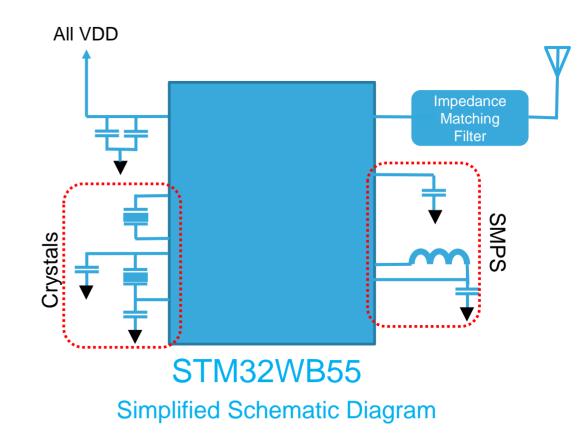






## Silicon Cost Savings

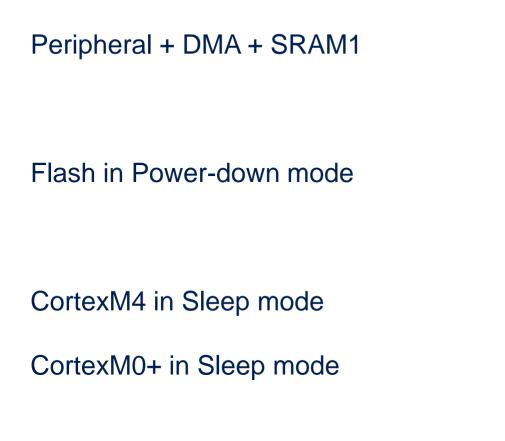
- Embedded RF balun
- Single IPD from ST
- Simple SMPS circuit
- Integrated HSE crystal tuning caps
- Minimal passives needed
- Simple 2 layer PCB design

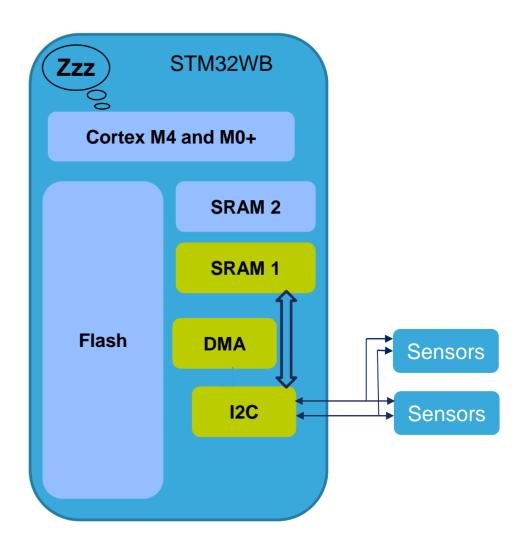






## Batch Acquisition Mode (BAM)











# Hands-On CubeMonitorRF





## STM32CubeMonitor-RF



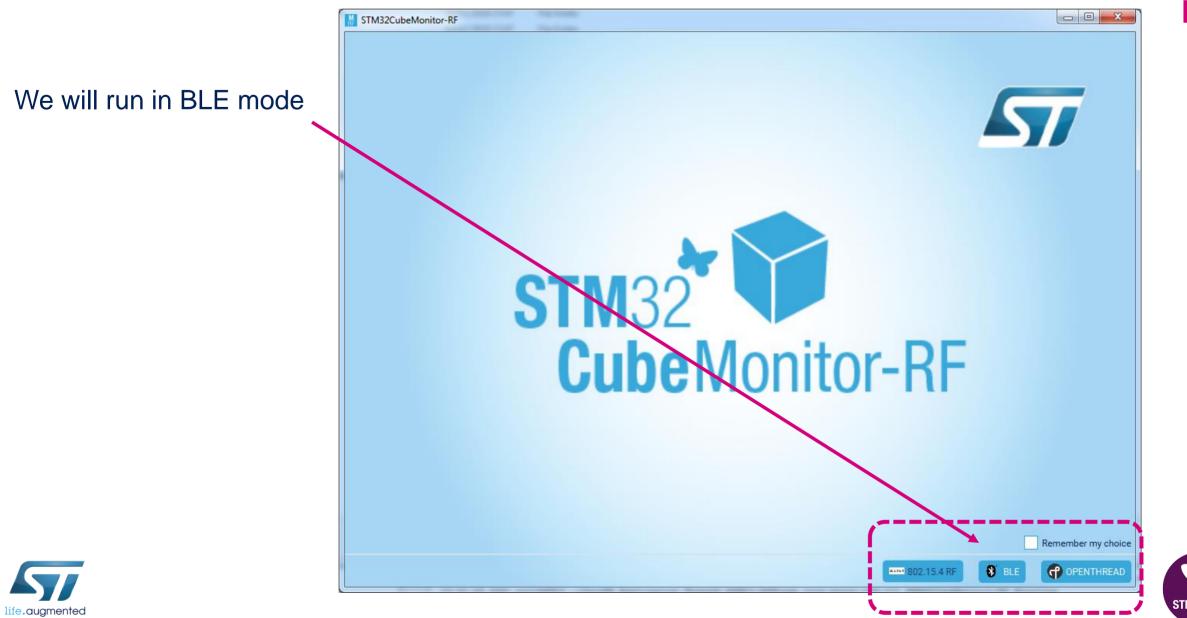
- OpenThread commands
- BLE & 802.15.4 RF tests
- COM-port based







## Mode selection



## Hands-On Time! CubeMonitorRF

#### Open the Transparent Mode workspace

STM32Cube\_FW\_WB\_V1.0.0 Projects NUCLEO-WB55.Nucleo Applications BLE BLE\_TransparentMode WARM

BLE\_TransparentMode
 settings
 BLE\_TransparentMode.dep
 BLE\_TransparentMode.ewd
 BLE\_TransparentMode.ewp
 BLE\_TransparentMode.ewp
 startup\_stm32wb55xx\_cm4.s
 stm32wb55xx\_flash\_cm4.icf





### Hands-On Time! CubeMonitorRF

167

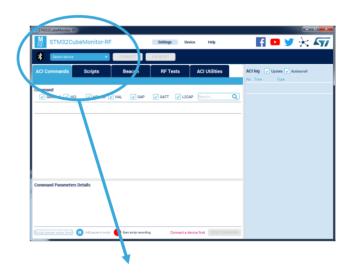
#### Build, Debug & Run on your Nucleo board

Project - IAR Embedded Workbench IDE - Arm 8.32.3		- 🗆 🗙
File Edit View Project ST-Link Tools Window Help		· · · · · · · · · · · · · · · · · · ·
	- < Q, > \$ ≠ ≠ < ♀ > 2 ▷   ■ ● ≠   ○ → ] : ₩ ]	
Workspace		
	stm32wbxx_hal_conf.h main.c x stm32wbxx_hal.c [RO] stm32wbxx_hal.h [RO] stm32wbxx_hal_rcc.c [RO] stm32wbxx_nucleo.c [RO] stm32wbxx_hal_flash	h.c[RO] ₹ f()
BLE_TransparentMode		10
Files 🌣 • 🔺	106 * @retval int 107 / */	<b>^</b>
🗉 🌒 BLE_TransparentMode - BLE_Tr 🗸	108 int main (void)	
	109 🖵 {	
EWARM •	110 /* USER CODE BEGIN 1 */	
	112 /* USER CODE END 1 */ 113	
C app_entry.c	114 /* MCU Configuration*/	
I I I I I I I I I I I I I I I I I I I	115	
→ ⊕ @ hw_uart.c	116 /* Reset of all peripherals, Initializes the Flash interface and the Systick. */	
	117 HAL_Init();	
Output	118	
📃 🔚 app_common.h	<pre>119 /* USER CODE BEGIN Init */ 120 Reset Device();</pre>	
📕 📙 🕞 app_conf.h	120 Rest Device (); 121 Config HSE();	
📕 📙 🛏 🖬 app_entry.h	122 /* USER CODE END Init */	
📄 📄 🖂 cmsis_iar.h	123	
Core_cm4.h	124 /* Configure the system clock */	
Core_cmFunc.h	125 SystemClock_Config();	
In core_cmlnstr.h     In core_cmSimd.h	126 127 /* USER CODE BEGIN SysInit */	
b dbg trace.h	127 /* USER CODE BEGIN SysInit */ 128 PeriphClock Config();	
DLib_Config_Full.h	129 Init Exti(); /**< Configure the system Pover Mode */	
DLib Defaults.h	130 /* USER CODE END SysInit */	
BLE TransparentMode		
Find in Files		<b>→</b> 中 ×
Path	Line String Mat	tched
	11	
Build Debug Log Find in Files		
Ready	Ln 576, Col 19 System CAP, NU	M OVR





## Connect to CubeMonitorRF





#### Select device on relevant COM port

**Connect** to start communication



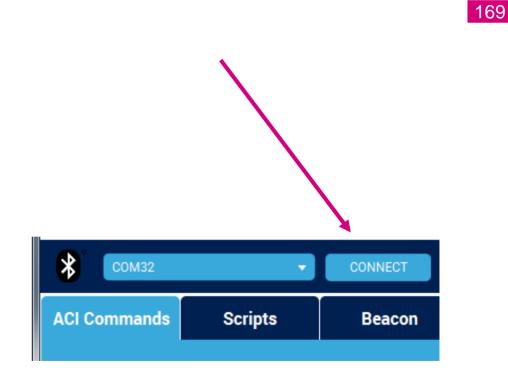




Program via USB debug port

Select device on relevant COM port

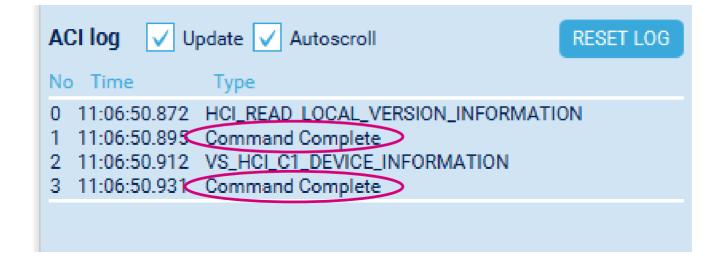
**Connect** to start communication







#### **Command Complete** signals successful communications







#### Click on the Command Complete line to get more information on the command sent

0 1 2	11:06:50.872 HCI_READ_LOC 11:06:50.895 Command Com 11:06:50.912 VS_HCI_C1_DE\	plete /ICE_INFORM	
3	11:06:50.931 Command Com	iplete	
	Parameter	Value	Literal
	HCI packet indicator	0x21	HCI M4 Event Packet
	Event_Code	0x0E	Command Complete
	Parameter_Total_Length	0x42	
	Num_HCI_Command_Packets		
	Command_Opcode		VS_HCI_C1_DEVICE_INFORMATION
	Status	0x00	SUCCESS
	Device Revision	0x2000	
	Device Code Id	0x0495	
	Device Package	0x13	
	Device Type	0x25	
	Device Company	0x000080E1	
	UID64	0x0000D7A5	
	Device UID96	0x203430	
	Safe Boot Information	0x00000000	
		0x000000	
	CM0 and Wireless FW version		
	CM0 and Wireless FW mem		
	CM0 and Wireless FW, Thre		
	CM0 and Wireless FW, BLE i		
	CM4 FW Information	0x00000100	
			🔂 More





172

11:06:50.895 Command Co 11:06:50.912 VS_HCI_C1_E		MATION
11:06:50.931 Command C		
Parameter	Value	Literal
HCI packet indicator	0x21	HCI M4 Event Packet
Event_Code	0x0E	Command Complete
Parameter_Total_Length	0x42	
Num_HCI_Command_Packs	ets 0x01	
Command_Opcode	0xFD62	VS_HCI_C1_DEVICE_INFORMATION
Status	0x00	SUCCESS
Device Revision	0x2000	
Device Code Id	0x0495	
Device Package	0x13	
Device Type	0x25	
Device Company	0x000080E	-
UID64	0x0000D7A	5
Device UID96	0x203430	
Safe Boot Information	0x0000000	-
Rss Information	0x000000	
CM0 and Wireless FW version		
CM0 and Wireless FW mem		-
CM0 and Wireless FW, Thre		
CM0 and Wireless FW, BLE		
CM4 FW Information	0x0000010	0

#### Click on + More for additional detail

#### Command Details

Parameter	Value	Literal	Info
HCI packet indicator	0x21	HCI M4 Event Packet	
Event_Code	0x0E	Command Complete	
Parameter_Total_Length	0x42		
Num_HCI_Command_Packets	0x01		The number of HCI command packets which are allowed to
Command_Opcode	0xFD62	VS_HCI_C1_DEVICE_INFORMATION	Opcode of this command which caused this event.
Status	0x00	SUCCESS	Error code. See Core v4.1, Vol. 2, part D.
Device Revision	0x2000		Device revision information (From MCU)
Device Code Id	0x0495		Device Code identifier (From MCU)
Device Package	0x13		Device Package (from package data register)
Device Type	0x25		Device Type Id (from FLASH UID64)
Device Company	0x000080E1		Device Type Id (from FLASH UID64)
UID64	0x0000D7A5		UID64 (From flash)
Device UID96	0x203430523036500600390048		UID96 from Unique Device ID register
Safe Boot Information	0x0000000		Safe Boot Information (from SRAM2)
Rss Information	0x000000000000000000000000000000000000		Rss Information (from SRAM2)
CM0 and Wireless FW version	0x00020D02		CM0+ Wireless FW Information (from SRAM2)
CM0 and Wireless FW memory size	0x160C002C		CM0+ Wireless FW Information (from SRAM2)
CM0 and Wireless FW, Thread information	0x0000000		CM0+ Wireless FW Information (from SRAM2)
CM0 and Wireless FW, BLE information	0x0000000		CM0+ Wireless FW Information (from SRAM2)
CM4 FW Information	0x00000100		CM4 FW Information (Coded in user flash)





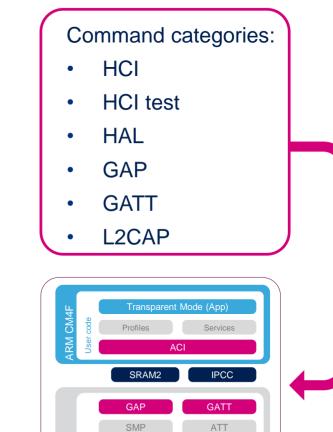
## STM32CubeMonitorRF

173

## Lots of categories to choose and filter from

STM32CubeMonitor-F	RF					X
RF STM32C	ubeMonitor-RF	:	Settings	)evice Help	🛐 🖸 🎽 ·	* 57
Сомз2		DISCONNECT	HW RESET		Device : STM32W CM4 version : 0.0. CM0 version : 0.2.	.1
ACI Commands	Scripts	Beacon	RF Tests	ACI Utilities	ACI log Vupdate Autoscroo No Time Type	RESET LOG
HCLREAD_LIKANSMIT HCLREAD_LOCAL_VER3 HCLREAD_LOCAL_SUP HCLREAD_LOCAL_SUP HCLREAD_BD_ADDR HCLREAD_BD_ADDR HCLREAD_RSSI	RSION_INFORMATION POWER_LEVEL SION_INFORMATION PORTED_COMMANDS PORTED_FEATURES	⊇ HAL ☑ GAP Comma list	gatt v L20	AP Search	0 11:54:3 HCL_READ_LOCAL_VE 1 11:54:32.059 Command Comple 2 11:54:32.063 VS_HCL_C1_DEVIC 3 11:54:32.084 Command Comple 4 11:55:22.099 Command Comple 6 11:55:22.223 ACL_HAL_WRITE_C 7 11:55:22.226 Command Comple 8 11:55:22.240 ACL_HAL_SET_TX_J 9 11:55:22.240 ACL_HAL_SET_TX_J 9 11:55:22.256 ACL_GATT_INIT 1 11:55:22.259 Command Comple 10 11:55:22.259 Command Comple 11 (Lapacket indi 0x04 HCL Ev	te E_INFORMATION te CONFIG_DATA te POWER_LEVEL te
HCLLE_SET_EVENT_MASK				Event_Code 0x0E Comm Parameter_Tota 0x04 Num_HCl_Com 0x01 Command_Opc 0xFD01ACI_GA Status 0x00 SUCCE		
Parameter HCl packet indicator Op_Code Parameter_Total_Length Connection_Handle Type	0x01 H 0x0C2D H	iteral ICI Command Packet ICI_READ_TRANSMIT_P(	Specifies	vhich Connection_Handle d Current Transmit Power	16 11-55-20 500 ACL GAD DELETE	E_AD_TYPE ete E_AD_TYPE ete E_ADV_DATA
Script pause value (ms)	Add pause in acript	Start acript recording	) 	SEND COM	MMAND	

life.augmented



L2CAP

Radio PHY

DTM

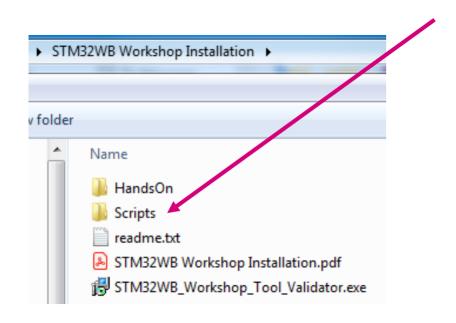
Link Layer

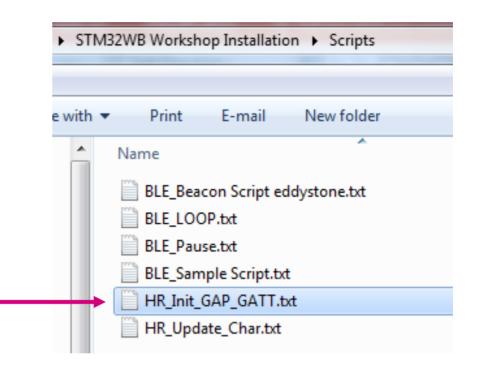
ARM CM0+ BLE stad



#### Open and Edit the HR\_Init\_GAP\_GATT.txt Script file

(In your installation zip file, Scripts folder)









**Scripts** 

**Scripts** 

175

HR\_Init\_GAP\_GATT.txt - Notepad

File Edit Format View Help

# Use hashtags to add comments

Send(HCI\_RESET)

Send(ACI\_HAL\_SET\_TX\_POWER\_LEVEL;0x00;0x18)

#SET Bluetooth Address
Send(ACI\_HAL\_WRITE\_CONFIG\_DATA;0x00;0x06;0x112233445566)

#Sand(ACT WAL SET DADTO ACTIVITY MASK.OVOOOG)

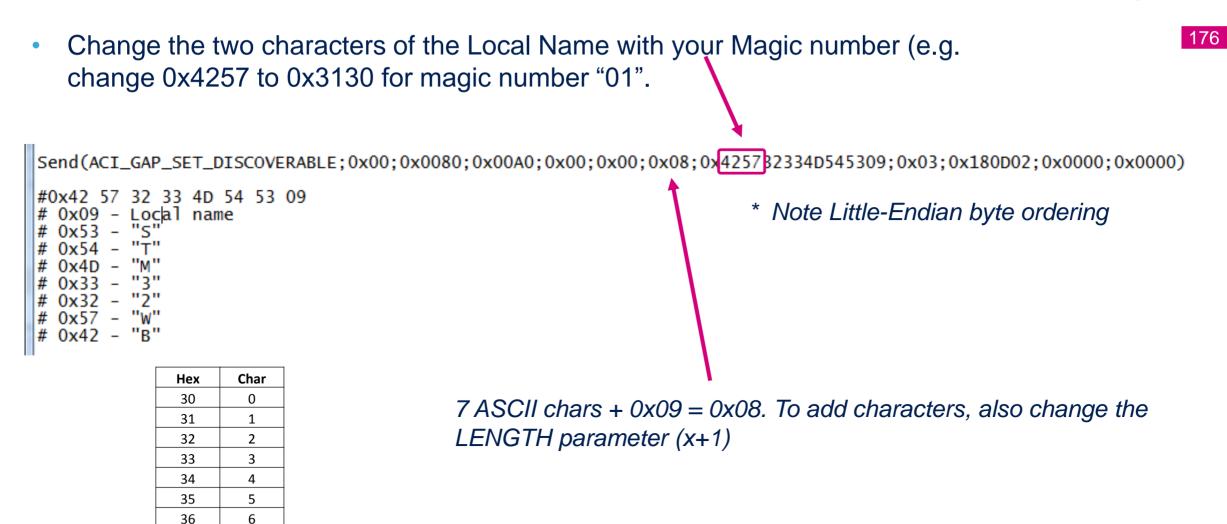
#### Set the Bluetooth Address

Send(ACI\_HAL\_WRITE\_CONFIG\_DATA;0x00;0x06;0x112233445566)





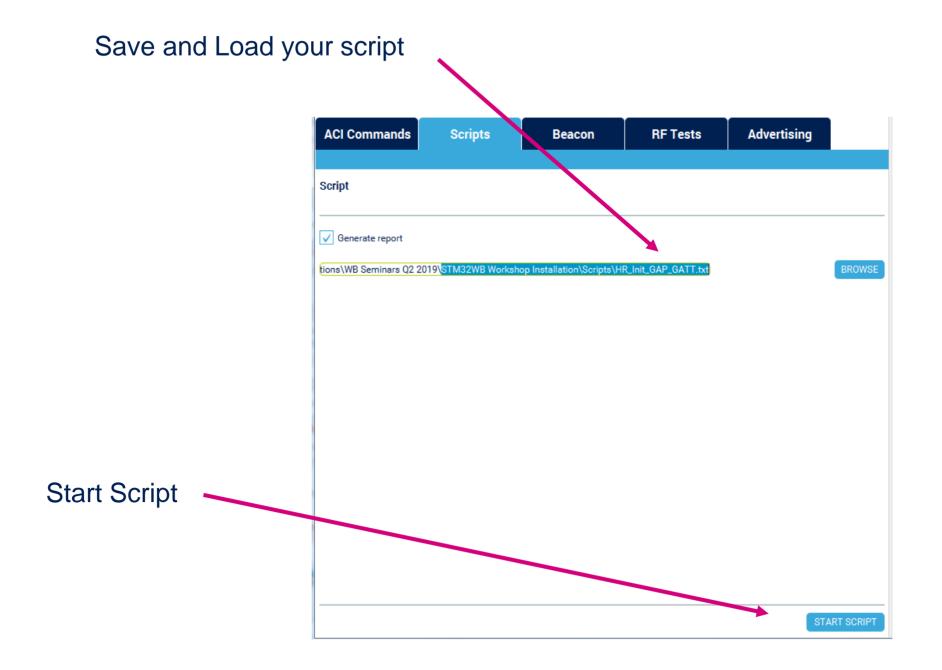






\* ASCII Character Set for Magic numbers

## Scripts



life.augmented



## LightBlue | Explorer App

#### Find your device

••• Verizon LTE	9:06 AM	<b>1</b> 29% 💽 )
	<b>ht</b> Blue   Explorer	Filter
Peripherals N		
<b>STM32</b> -41 1 service	ZVVB	>
Virtual Periph	nerals	
🕀 Creat	e Virtual Peripl	neral >
Info		Log

#### Show ADV data

Λ.	
UUID: 4A337D50-EF51-EEA9-EA84-0B3C97	9A273B
Connected	
ADVERTISEMENT DATA	Show
Heart Rate	

Heart Rate Measurement Properties: Read Notify

Enable I	Notific	ations
III Verizon LTE	9:11 AM ate Measure	≉ 28% ∎⊃ ment Hex
bluenrg Heart Rate   UUID: 2A37 Connected	Veasure	ement
READ/NOTIFIED V	ALUES	•
Read again	Listen	for notifications
i Cloud Con	nect	$\bigcirc$
0x <b>0000</b> 09:10:54.974		
DESCRIPTORS		
O Client Characteristic Co	nfiguration	
PROPERTIES		
Read		
NIntify		
Info		Log





## STM32CubeMonitorRF

#### Now load the *HR\_Update\_Char.txt* script to send Notification Updates

STM32WB Workshop Installation      Scripts					
7 51111	· STWSZWD WORKSTOP Installation · Scripts				
re with 🔻	Print E-mail New folder				
	Name				
	BLE_Beacon Script eddystone.txt				
	BLE_LOOP.txt				
	BLE_Pause.txt				
	BLE_Sample Script.txt				
	HR_Init_GAP_GATT.txt				
	HR_Update_Char.txt				
=					

#### Dummy Heart Rate Values are sent

I Verizon LTE	9:03 AM	1 29% 🔲
<b>〈</b> bluenrg <b>Hear</b> t	Rate Measure	ment Hex
bluenrg		
Heart Rate		ement
READ/NOTIFIED	VALUES	Stop listening
i Cloud Co	nnect	
0x <b>8045</b> 09:03:55.409		
0x8040 09:03:54.389		
0x8046 09:03:53.369		
0x8052 09:03:52.319		
0x8049 09:03:51.299		
DESCRIPTORS		
Info		Log





#### **Scripts**

## Application Note AN5270 describes the ACI/HCI commands available

- via CubeMonitorRF
- via Application API's

#### 2.3.2 ACI\_HAL\_WRITE\_CONFIG\_DATA

#### Description

This command writes a value to a low level configure data structure. It is useful to setup directly some low level parameters for the system in the runtime.

Input parameters

#### Table 108. Input parameters

Parameter	Size	Description	Possible values
Offset	1	<ul> <li>Offset of the element in the configuration data structure which has to be written. The valid offsets are:</li> <li>0x00: Bluetooth public address, value length to be written: 6 bytes</li> <li>0x06: DIV used to derive CSRK, value length to be written: 2 bytes</li> <li>0x08: Encryption root key used to derive LTK and CSRK, value length to be written: 16 bytes</li> <li>0x18: Identity root key used to derive LTK and CSRK, value length to be written: 16 bytes</li> <li>0x2C: Link layer without host (for certification purposes), Value length to be written: 1 byte</li> <li>0x2E: Static random address: 6 bytes</li> <li>0x2F: Disable watchdog (1=disable, 0=enable), value length to be written: 1 byte</li> </ul>	<ul> <li>0x00: CONFIG_DATA_PUBADDR_OFFSET</li> <li>0x06: CONFIG_DATA_DIV_OFFSET</li> <li>0x08: CONFIG_DATA_ER_OFFSET</li> <li>0x18: CONFIG_DATA_IR_OFFSET</li> <li>0x2C: LL_WITHOUT_HOST</li> <li>0x2E: CONFIG_DATA_RANDOM_ADDRESS_WR</li> <li>0x2F: CONFIG_DATA_WATCHDOG_DISABLE</li> </ul>
Length	1	Length of data to be written	-
Value	Length	Data to be written	-





# Lunchtime!

NRST 8

PHJ-BOOTA

GN

10

BAT



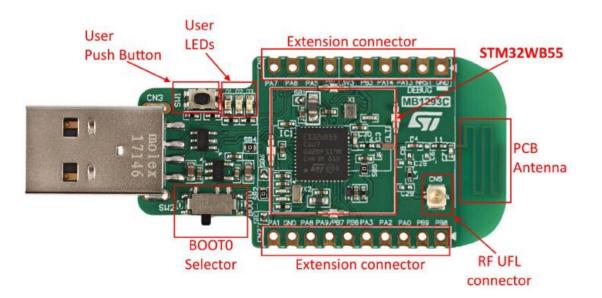


### WB55 Dongle Board

The USB Dongle is quite useful as the CubeMonitorRF sniffer

This project uses the USB CDC class directly (not the STLINK VCOM port) to parse commands

Although there is no STLINK on board, the USB bootloader can be invoked via **BOOT0 switch** & CubeProgrammer, and the binary can be programmed

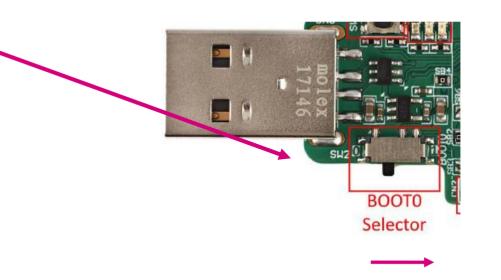






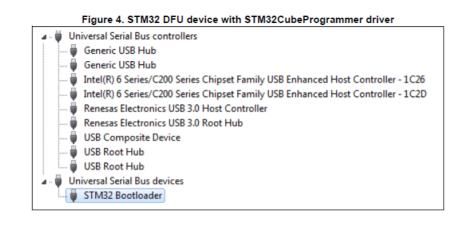
# Dongle config

- Move Dongle Switch to Bootloader mode
- Plug in Dongle



#### Bootloader active to the right

• Ensure the driver has enumerated "STM32 Bootloader"





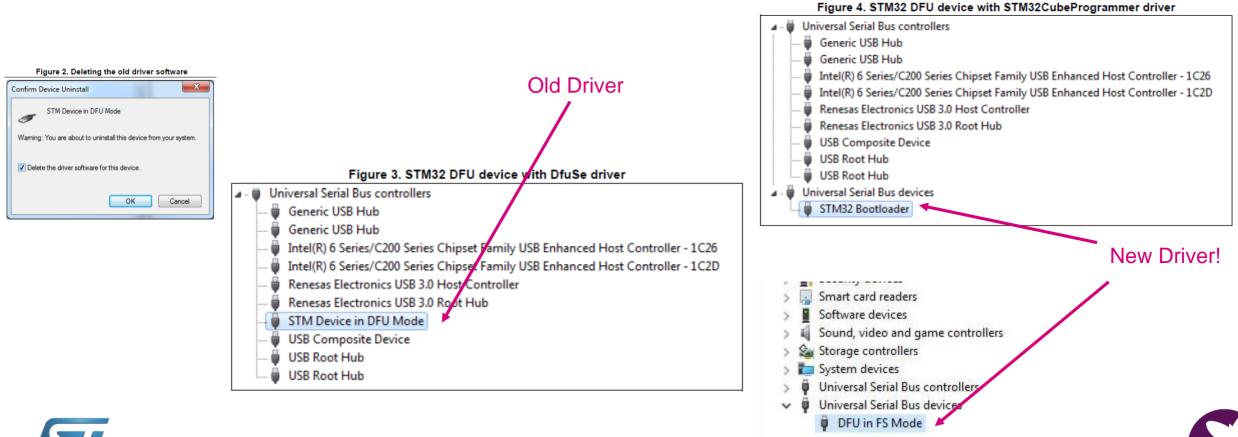


# **CubeProgrammer User Manual**

#### Chapter 1.2.4 details the DFU driver install / update procedure

life.auamente

Old or Native MS drivers must be replaced to properly access the bootloader



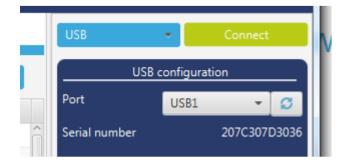
## CubeProgrammer

#### Open STM32 CubeProgrammer



#### Select **USB** mode and **Connect**

Memory & File	edition							Connecte
Device memory	Open file +						ST-LINK	<ul> <li>Disconne</li> </ul>
Address 0x08000	0000 👻 Size	0x400	Data width	32-bit 👻	Re	ad	ST-LIP	NK configuration
Address	0	4	8	с	ASCII		Serial number	066DFF50
	20001378	08003531	08003811	08003813	× 1588	<u>^</u>	Port	SWD -
0×08000000 0×08000010	08003721	08003725	08003729	00000000	!7%7)7			
0x08000020	00000000	00000000	00000000				Frequency (kHz)	4000
0x08000030	08003817	00000000	080039	0800381B	.888		Mode	Normal
0x08000040	0800372D	08003731	08003735	08003831	-7175718	L	Access port	0
0x08000050	08003739	08007-00	08003741	08003745	97=7A7E7		Reset mode	
0×08000060	08003749	0800374D	0800381F	08003751	17M78Q7		Keset mode	Hardware reset
0×08000070	080 5755	08003759	0800375D	08003761	U7Y7]7a7		Shared	False
0x08000080	08003765	08003769	0800376D	08003771	e7i7m7q7		Target voltage	
0x02 00090	08003775	08003779	0800377D	08003781	u7y7}77		Firmware version	
0x080000A0	08003785	08003789	0800378D	08003791	.777			
0х080000в0	08003795	08003799	0800379D	080037A1	.777;7			
0x080000C0	080037A5	080037A9	080037AD	080037B1	¥7©77±7			
0x080000D0	08003825	080037B5	080037B9	080037BD	%8μ7 <sup>1</sup> 7½7			
0x080000E0	080037C1	080037C5	080037C9	080037CD	Á7Å7É7Í7			
0x080000F0	08003839	08003835	080037D1	080037D5	9858Ñ7Ő7			
0x08000100	080037D9	080037DD	080037E1	080037E5	Û7Ý7á7å7	~		
Log					Verbosity level 💿 1 💿 :	2 🔘 3	Devi	ice information
16:34:51 : 51 16:34:51 : Add		4 вутеs 000000				^	Device	STM3



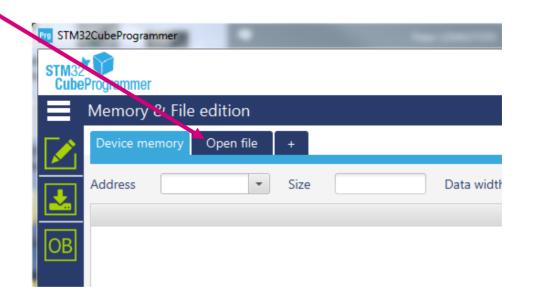




# CubeProgrammer

#### Open the BLE\_TransparentModeVCP\_reference.hex file for Dongle

<ul> <li>NUCLEO-WB55.USBDongle</li> </ul>	Applications   BLE   BLE_TransparentModeVCP	•
Help		
Include in library 👻 🛛 Sl	are with 🔻 New folder	
ube_FW_WB_V1.0.0	Name	Date
sc	Binary	2/19
entation	Core	2/19
	EWARM	2/19
wares	STM32_WPAN	2/19
5	SW4STM32	2/19
.EO-WB55.Nucleo .EO-WB55.USBDongle	readme.txt	2/19
32WB Copro Wireless Binaries		



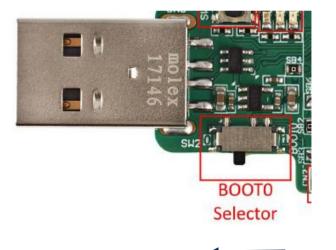


# Dongle config

- Disconnect from CubeProgrammer
- Unplug Dongle
- Move Dongle Switch back to normal boot mode
- Plug Dongle back in for normal boot startup
- Now you should be able to use COMxx in CubeMonitorRF
  - (may differ from COM74)





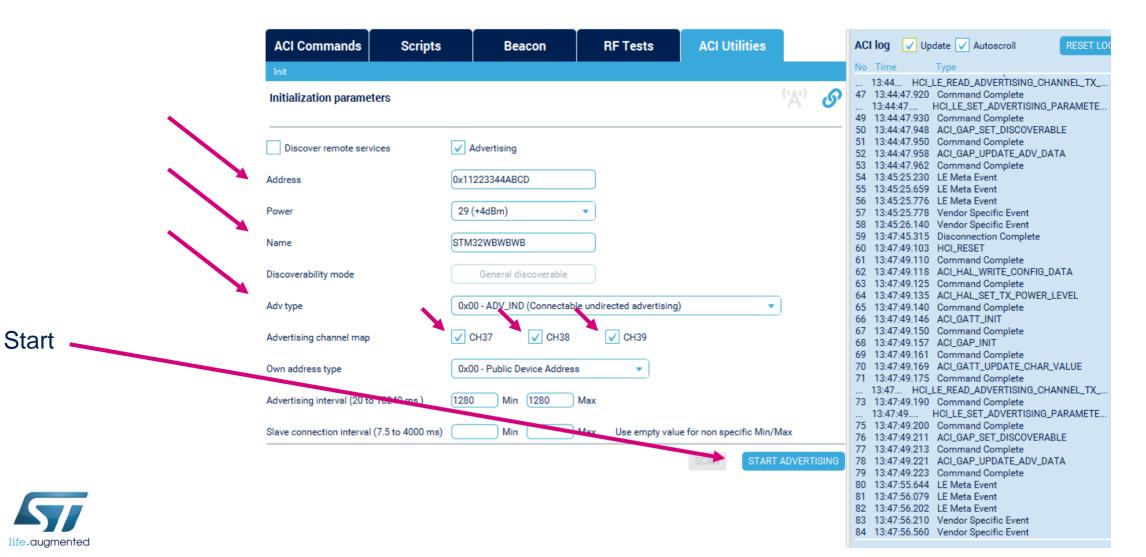


#### Normal Boot to the left



# **CubeMonitorRF**

- Change the Bluetooth Address and Name. (Use your Magic Number!)
- Use Connectable advertising on all channels (37/38/39)

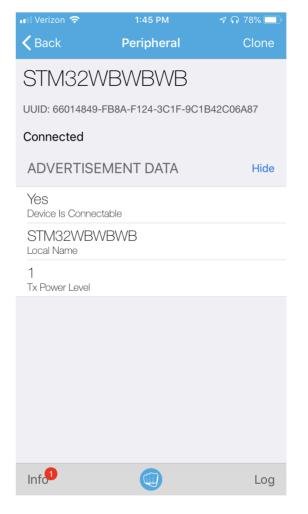




# LightBlue Explorer

#### • Use LightBlue Explorer to connect to and interrogate your GAP peripheral

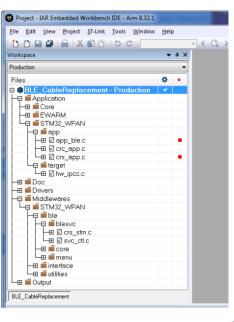
•••• Veri	zon 🗢 1:45 PM -	7 🎧 78% 🔲
Sort	LightBlue   Explorer	Filter
Peri	pherals Nearby	
-76	Unnamed No services	>
ll	LumeCube8802005	>
ull.	STM322B No services	>
.11   -94	Unnamed No services	>
-92	Unnamed No services	>
-53	STM32WBWBWB No services	>
Virtu	ual Peripherals	
Ð	Create Virtual Periph	eral >
Info		Log







# Hands-On Custom GATT & Cable Replacement





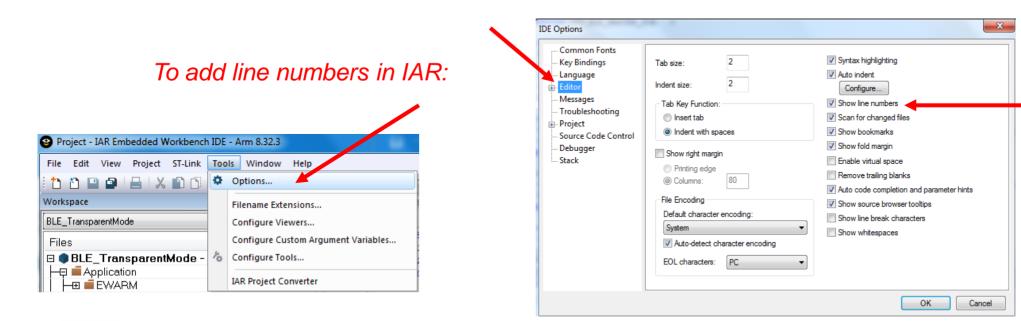
# Hands On Time! Custom GATT

# Open, Compile, Program & Run the Nucleo Board CableReplacement example

### Add a custom GATT Characteristic for LED control

life.augmented

You can copy/paste the code bits from CableReplacement\_Lab.txt file from your install files Labs folder

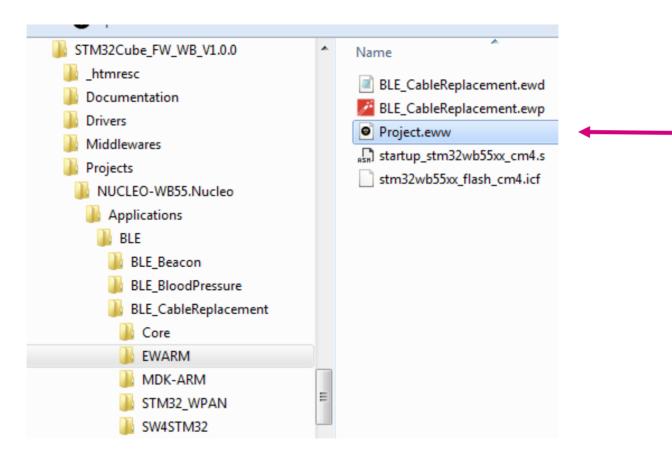




# BLE\_CableReplacement Project

### • Open the workspace

STM32Cube\_FW\_WB\_V1.0.0 ▶ Projects ▶ NUCLEO-WB55.Nucleo ▶ Applications ▶ BLE ▶ BLE\_CableReplacement ▶ EWARM ▶





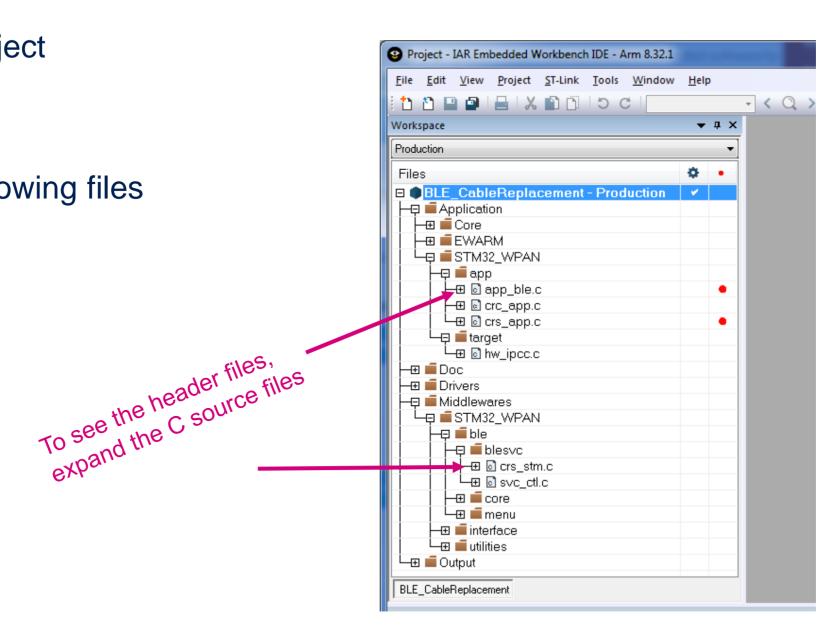


# BLE\_CableReplacement Project

# Build the Project

# • Open the following files

- app\_conf.h
- app\_ble.c
- ble\_conf.h
- crs\_stm.h
- crs\_stm.c
- crs\_app.c







### **BLE Role Configuration**

- STM32WB is the GAP Peripheral / GATT server
- Smartphone is the GAP Central / GATT client.

### **Compile for GATT Server**

Modify the #define (line# 100 of app\_conf.h)

#define GATT\_CLIENT 0 /\* 1 = Device is GATT Client, 0 = Device is GATT Server \*/





#### **BLE Device Names**

# Identify your unique device with your magic number

195

• Modify your local name (line# 204 of app\_ble.c)

static const char local\_name[] = { AD\_TYPE\_COMPLETE\_LOCAL\_NAME, 'C', 'R', 'S', '0', '1' };

• Modify your BLE device name (line# 822 of app\_ble.c)

```
const char *name = "BLEcore";
```

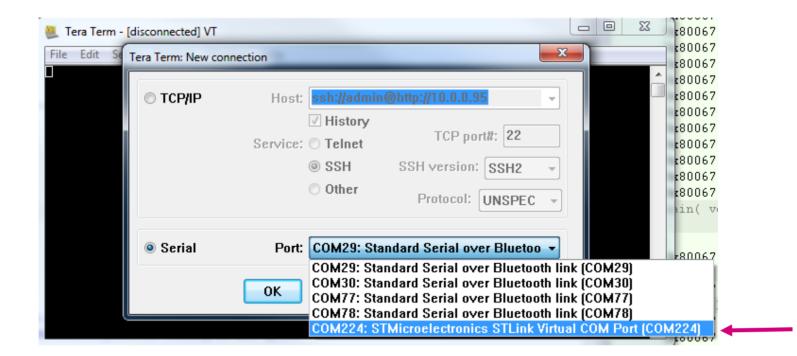
• Ensure that the BLE device name length in ASCII chars matches (line# 165 of app\_ble.c)

#define APPBLE GAP DEVICE NAME LENGTH 7





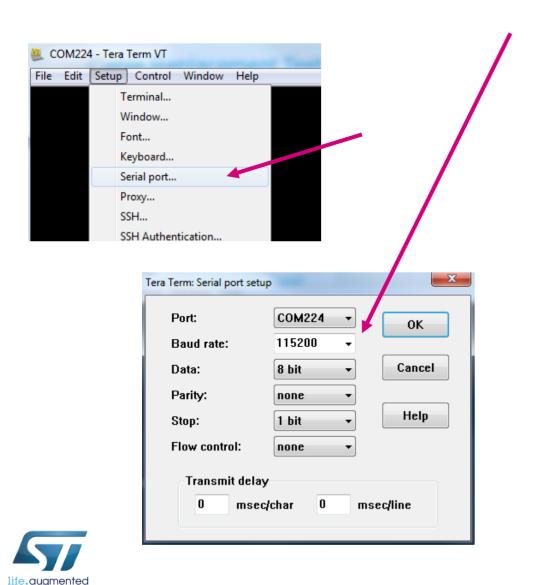
- Build and Run the project
- Connect your TeraTerm to the Nucleo's STLink Virtual COM port



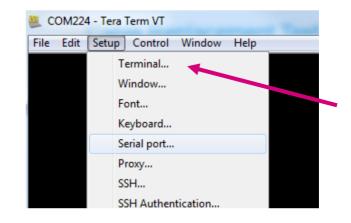




#### Configure your Serial port for 115,200bps / N / 8 / 1



#### **Configure Terminal Setup**



	<b>\</b>
Tera Term: Terminal setup	X
Terminal size 80 × 24 ☑ Term size = win size	New-line Receive: CR+LF → Transmit: CR+LF → Cancel
Auto window resize	Help
Answerback: Coding (receive) UTF-8 🗸	■ Auto switch (VT<->TEK) Coding (transmit) UTF-8 ▼
locale: american	CodePage: 65001



- Connect to your device with LightBlue Explorer
- Send and receive ASCII-based messages using the different characteristics

ull Verizon 奈 ✔Back	<sup>10:41 АМ</sup> Peripheral	✓ 15%  Clone		ul Verizon 奈 <b>〈</b> BLE-CRS-01	10:45 AM	⊲ 15% — 8E22-4 Hex	ull Verizon 奈 <b>♦</b> Back	з:01 РМ Edit Value	<b>1</b> 72% 🔲	-			4 - Ter					Trent .
BLE-CRS	S-01 -7164-0C11-C357-A3C5E	ED2D9C10			E62-8E22		41	Hex		File	E	dit	Setu	p C	ontrol	Window	Help	
Connected				Connected	3E22-4541-9D4C-21	1EDAE82ED19												
ADVERTISE	MENT DATA	Show		READ/NOTIFIED V	ALUES								Rec	eive	-			
CC7A-482/	A-984A-7F2ED5B E22-4541-9D4C-21EDA			Read again i Cloud Co	onnect	Stop listening							nee	6146	-			
Properties: Read	E22-4541-9D4C-21EDA Write Without Response E22-4541-9D4C-21EDA			0x <b>41424344</b> 10:45:40.049			D	E	F									
	Properties: Read Notify		$\mathbf{N}$	0×68656C60 10:45:30.900 0×00000000000	D6F	000000000000000000000000000000000000000	А	В	С									
				10:45:11.999 DESCRIPTORS			7	8	9				ABC	DE				
				0 Client Characterist	ic Configuration		4	5	6				1120					
				PROPERTIES			1	2	3				Tra	nsmi	t:			
Info		Log		Info <sup>1</sup>		Log		0	Done				he l	10				

#### Write values to Nucleo



Enable Notifications to receive messages from Nucleo



Transmit: he llo

#### • Here is the LightBlue Explorer on Android

	考 🕾 54% 📾 11:13 AM	🖬 @ 1 8 % 54% 8 11:13 AM	₩ © 1 *	: ⇔.52% @ 11:21 AM	\$ 10 525 @ 11:22 AM	
← CRS01	E.	← CRS01 :	← CRS01	← CRS01		
ADVERTISEMENT DATA		ADVERTISEMENT DATA	BRADERTIFO	PROPERTIES		
Connection status Connected		Connection status Connected	PROPERTIES Device Address	Device Address 80:E1:26:00:58:E6		
Advertised name CRS01		Advertised name	80/E1/26:00:68:E6	Service UUID 0000fe60-cc7a-482a-94	34a-7f2ed5b3e58f	
Advertised service UUIDs 8FE58305-2E7F-4A98-2A49-7ACC60FE0000		Advertised service UUIDs BFE58305-227F-4A98-2A46-7ACC60FE0000	Service UUID 0000fe60-cc7a-482a-984a-7f2ed5b3e58f	Characteristic UU 0000fe62-8e22-4541-9	D d4c-21 edae82ed19	
DEVICE INFORMATION		DEVICE INFORMATION	Characteristic UUID 0000fe62-8e22-4541-9d4c-21edae82ed19	Readable Able to be read fr	om	
Device Address 80 E1 26:00:58 E6		Device Address BOET 26 COSEF6		× Writable Able to be written	to	
GATT SERVICES & CHARACTERISTICS		GATT SERVICES & CHARACTERISTICS	v Writable	Supports noti Able to be subscr	ifications/indications ibed to for notifications/indications on changes to the characteristic	
Generic Attribute Service Changed	$\rightarrow$	Generic Attribute	Able to be written to	READ/INDICATE		
Generic Access Device Name Appearance	$\rightarrow$	Generic Accer= Dryce Name Appensions Select a characteristic to explore →	<ul> <li>Supports notifications/indications</li> <li>Able to be subscribed to for notifications/indications on changes to the characteristic</li> </ul>		SUBSCRIBE	
Peripheral Preferred Connection Parameters 0000fe60-cc7a-482a-984a-7f2ed5b3e58f		Perpheral Perfect 00000fe60-cc2 00000fe61-8e22-4541-9d4c-21edae82ed19	READ/INDICATED VALUES	31 32 33 34 35 Mon Apr 15 11 22 08 C0	37 2019.	
0000fe61-8e22-4541-9d4c-21edae82ed19 0000fe62-8e/22-4541-9d4c-21edae82ed19	~	0000fe614dc24 0000fe624ec24 0000fe624ec24 0000fe628ec24541-9d4c-21edae82ed19	READ AGAIN UNSUBSCRIBE	68 65 6C 6C 6F Mon Apr 15 11:22:01 00	JT 2019	
			No value read recently Tap on one of the buttons above — if available — to begin	DESCRIPTORS		
			DESCRIPTORS	Client Characteris 00002902-0000-1000-8	tic Configuration 000-00805f9b34fb	
			Client Characteristic Configuration			
			00002902-0000-1000-8000-00805/9b34fb			
					📒 COM224 - Tera Term VT	
					File Edit Setup Control Windo	w Help
			Write values to N	lucion		
				lucieo		
	_				Receive:	
	Enal	ble Notifications to red	ceive messages from N	ucleo		
			J			
					ABODE	
					ABCDE	



199

STM32

# Add a custom characteristic to an existing Service

#### Add the UUID definition (line# 74 of ble\_conf.h)

#define STM\_LED\_UUID128 0x00, 0x00, 0xfe, 0x64, 0x8e, 0x22, 0x45, 0x41, 0x9d, 0x4c, 0x21, 0xed, 0xae, 0x82, 0xed, 0x19

Add event element (line# 37 of crs\_stm.h)

typedef enum {

STM\_LED\_WRITE\_EVT,
CRS NOTIFY ENABLED EVT,

} CRS\_Opcode\_evt\_t;







•••

- From IAR, right click on the file tab and select "File Properties"
- Uncheck the "Read-only" box
- Click OK

1 2 [- 3 4 5 6	/** * @file crs_stm.h * @author MCD Applic * @version V0.0.1.alg		
6 7	* gdate 04-Septemb	The Properties of	
8 9	* Sbrief Reader for	crs stm.c module	
9	***************	*****	****
10	* Sattention		
11			

	crs_stm h
Type of file:	H File (h)
Opens with:	Windows Shell CommonQhange
Location:	C:\STM32Cube_FW_WB_V1.0.0\Middlewares\S
Size:	2.43 KB (2.490 bytes)
Size on disk:	4.00 KB (4.096 bytes)
Created:	Tuesday, February 19, 2019, 3:56:00 PM
Modified:	Tuesday, February 19, 2019, 3:56:00 PM
Accessed:	Today, April 16, 2019, 7 minutes ago
Athbutes:	Bead only Bidden Advanced.









```
• Check for the handle (line# 122 of crs_stm.c)
```

```
case EVT_BLUE_GATT_ATTRIBUTE_MODIFIED:
```

```
attribute_modified = (aci_gatt_attribute_modified_event_rp0*)blue_evt->data;
if(attribute_modified->Attr_Handle == (CRSContext.LedWriteClientToServerCharHdle + 1))
{
```

```
Notification.CRS_Evt_Opcode = STM_LED_WRITE_EVT;
Notification.DataTransfered.Length = attribute_modified->Attr_Data_Length;
Notification.DataTransfered.pPayload = attribute_modified->Attr_Data;
CRSAPP_Notification(&Notification);
```





```
• Add uuid array (line# 193 of crs_stm.c)
uint8_t led_uuid[] = { STM_LED_UUID128 };
```

```
• Change the Max_Attribute_Records parameter (line# 215 of crs_stm.c)
hciCmdResult = aci_gatt_add_service(
```

UUID\_TYPE\_128, (Service\_UUID\_t \*) &uuid, PRIMARY\_SERVICE, 8, &(CRSContext.SvcHdle));





204

Add LED characteristic (line# 281 of crs\_stm.c)





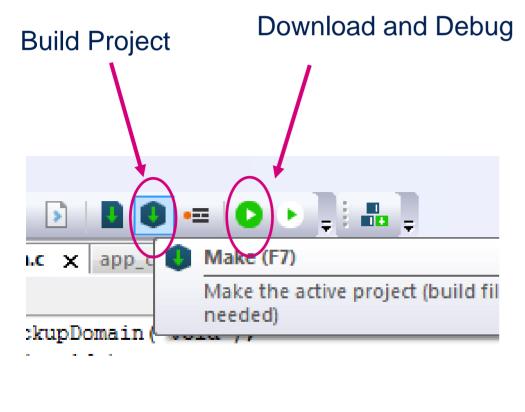
```
    Add event action (line# 194 of crs_app.c)
```

```
case STM_LED_WRITE_EVT:
    if(pNotification->DataTransfered.pPayload[0] == 0x01)
    {
       BSP_LED_On(LED_BLUE);
    }
    if(pNotification->DataTransfered.pPayload[0] == 0x00)
    {
       BSP_LED_Off(LED_BLUE);
    }
    break;
```





## **Compile and Program**





	* • *	57 s 58 s 59 s 60 s 61 s 62	<pre>static void Reset_BackupDomain( void ); static void Init_RIC( void ); static void SystemClock_Config( void ); static void Reset_DEv(c ( void ); static void Reset_DEv( void ); static void Init_Exti( void ); /* Functions Definition*/</pre>	
BLE_CableReplacement - Production  Application  EWARM  STM32_WPAN  G STM32_WPAN  G app  G app  G c s app.c  G stranget  G str	-	57 s 58 s 59 s 60 s 61 s 62 63 d 64	<pre>static void Init_RTC( void ); static void SystemClock_Config( void ); static void Reset_Price( void ); static void Reset_IPCC( void ); static void Init_Exti( void );</pre>	
Application     Application     Gree     Cree     STM32_WPAN     Gene     STM32_WPAN     Gene	*	58 s 59 s 60 s 61 s 62 63 / 64	<pre>static void SystemClock_Config( void ); static void Reset_Device( void ); static void Reset_IFCC( void ); static void Init_Exti( void );</pre>	
Application     Application     Gree     Cree     STM32_WPAN     Gene     STM32_WPAN     Gene		59 s 60 s 61 s 62 63 / 64	<pre>static void Reset_Device( void ); static void Reset_IPCC( void ); static void Init_Exti( void );</pre>	
		60 s 61 s 62 63 / 64	<pre>static void Reset_IPCC( void ); static void Init_Exti( void );</pre>	
EWARM     STM32_WPAN     G    spp     fm    spp_ble.c     H    spc_capp.c     G    scs_app.c		61 s 62 63 / 64	<pre>static void Init_Ext( void );</pre>	
		62 63 64		
		63 64	/* Functions Definition*/	
□   + ⊕ D app_ble.c   + ⊕ D crc_app.c   - ⊕ D crc_app.c - ⊕ ■ target - ⊕ ■ target - ⊕ ■ torw_ipc.cc		64	/* Functions Definition*/	
⊢⊞ © crc_app.c   └⊞ © crs_app.c └ၝ ■ target └⊞ © hw_jpcc.c ─────────				
L L⊞ © crs_app.c L = target L ⊞ © hw_ipc.c -⊞ ■ Doc		65 🗆 /		
L L⊞ © crs_app.c L = target L ⊞ © hw_ipc.c -⊞ ■ Doc				
L-p			* @brief Main program	
└─── © hw_ipcc.c ─── ■ ■ Doc			* @param None	
-🗄 🛑 Doc			* gretval None	
		69 L		
			int main( void )	
		71 📮	{	
-🖓 🛋 Middlewares		72	HAL_Init();	
Lp STM32_WPAN		73		
		74	Reset Device();	
- 🛱 🖬 blesvc		75		
R Core etmo		76 🗖	/**	
La la svc_ctl.c		77	* When the application is expected to run at higher speed, it should be better to set the correct system clock	
		78	* in system stm32yyxx. so that the initialization phase is running at max speed.	
		79 -	*/ system_stmozyyxxtb so that the initialization phase is funning at max speed.	
		80		
—⊞ Interface □⊞ Interface		81	Systemators_contry(), / Contryute the system crock -/	
		82	<pre>Init_Exti();</pre>	
-🖽 🛋 Output		83	THT0_001( / /	
		84		
		84	<pre>Init_RTC();</pre>	
			APPE_Init();	
		87		
		88	while(1)	
		89 🛱		
LE CableReplacement		90	SCH Run (~0) :	•
				P
Id				<b>•</b> 9
Messages				
Building configuration: BLE_CableReplacement	at - Producti	ion		
Updating build tree	it i rodada			
Opadang bala ree				
Configuration is up-to-date.				
Configuration is up-to-date.				
			III	
ild Debug Log				





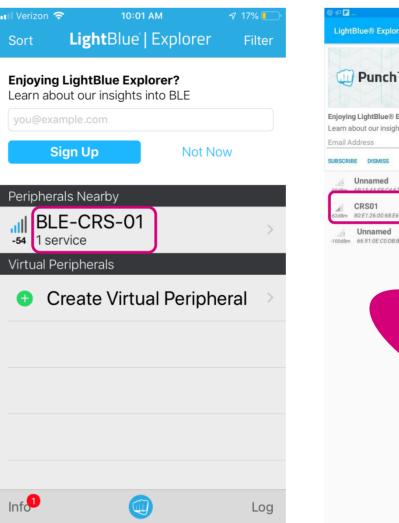
# Start LightBlue App

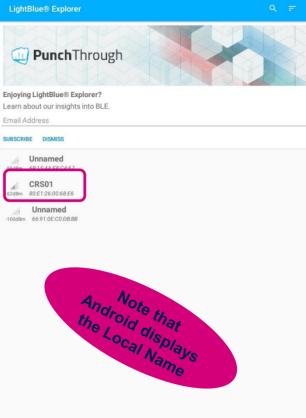
• Launch the LightBlue app



• Find your device

• Select your device







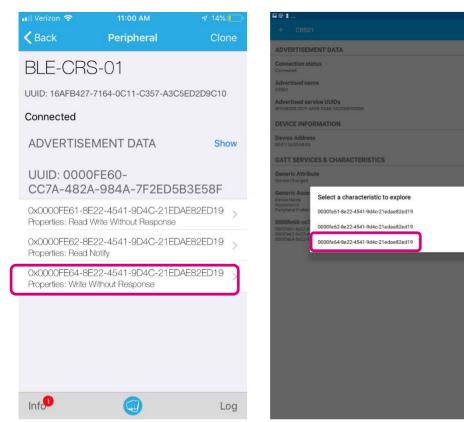


# LightBlue App

# Find your LED characteristic UUID

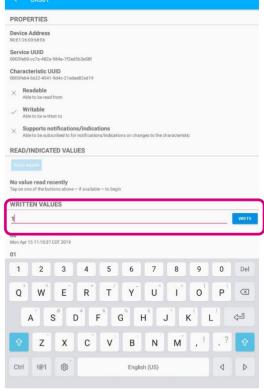
-----

< BLE



#### Write new value

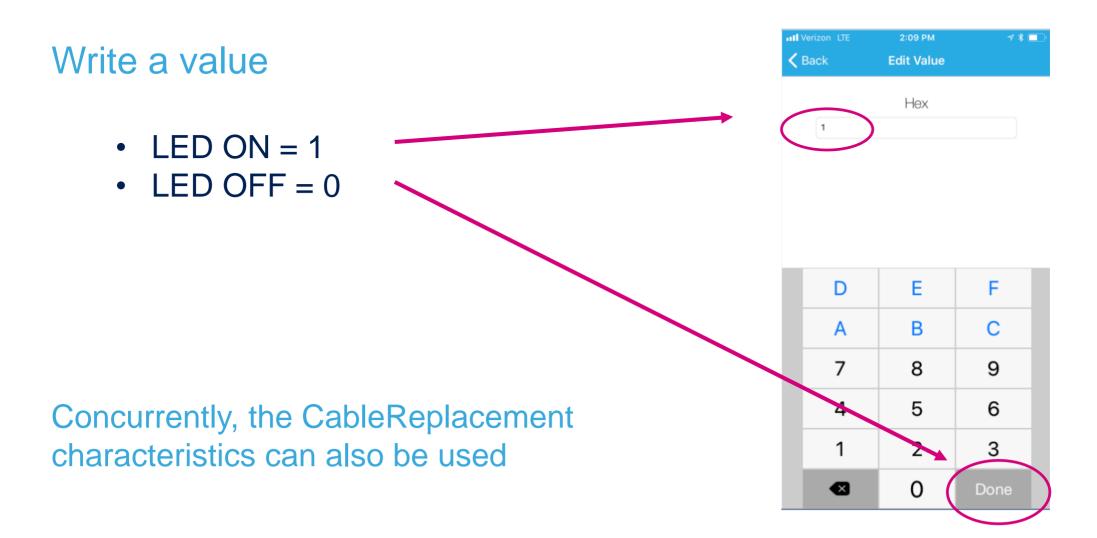
III Verizon 🗢 11:00 AM	7 14% 🔛	•••••	
Kerken	I Hex	← CRS01	
		PROPERTIES	
BLE-CRS-01		Device Address 80:E1:26:00:68:E6	
0x0000FE64-8E22-454	11	Service UUID 0000fe60-cc7a-482a-984a-7f2ed	15b
UUID: 0000FE64-8E22-4541-9D4C-21EDAE82	ED19	Characteristic UUID 0000fe64-8e22-4541-9d4c-21ede	e8
Connected		× Readable Able to be read from	
		✓ Writable Able to be written to	
WRITTEN VALUES		× Supports notification Able to be subscribed to fo	
Write new value		READ/INDICATED VAL	JE
DESCRIPTORS		READ ACAN No value read recently Tap on one of the buttons above: WRITTEN VALUES	- 1
FROFERIES		1	
Write Without Response		Mon Apr 15 11:10:37 CDT 2019	_
		01	
		1 2 3	
		Q <sup>+</sup> W <sup>+</sup> E <sup>+</sup>	
		A S I	D
		ŶZX	
Info <b>9</b>	Log	Ctrl !@1 🐯	





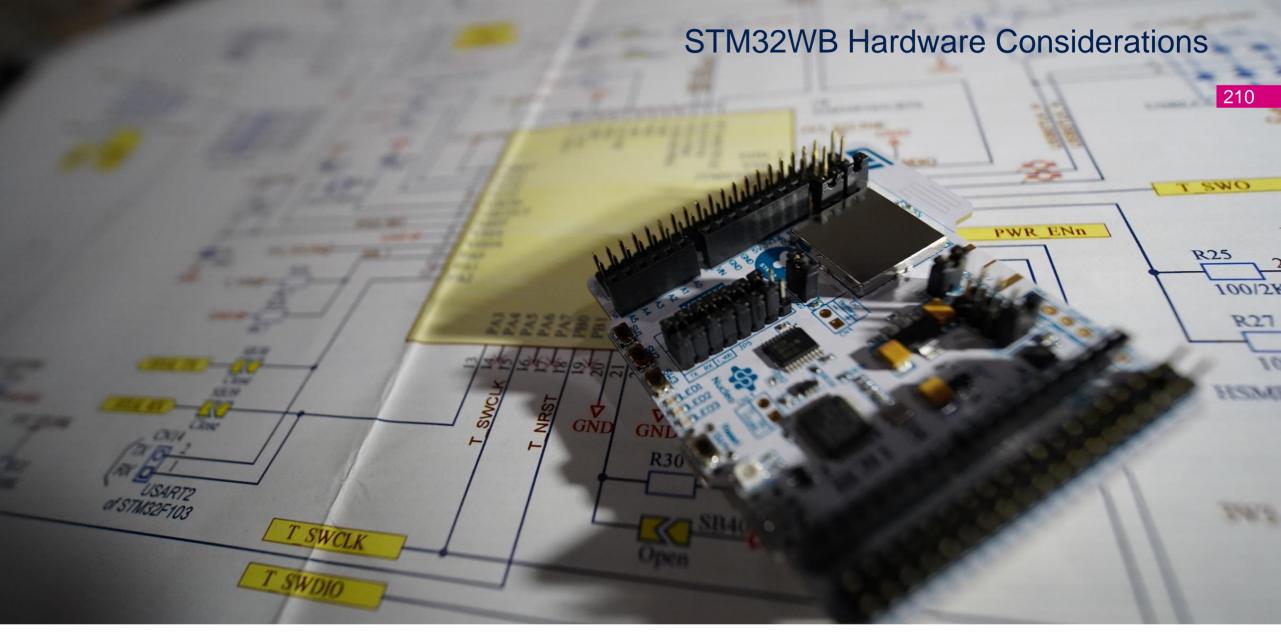


# LightBlue App













# **Delivery State**

#### FUS + BLE Stack



#### FUS + BLE Stack



#### **FUS only**

#### Stack must be loaded

48-pin UQFN 68-pin VQFN (0.5 mm pitch) (0.4 mm pitch)

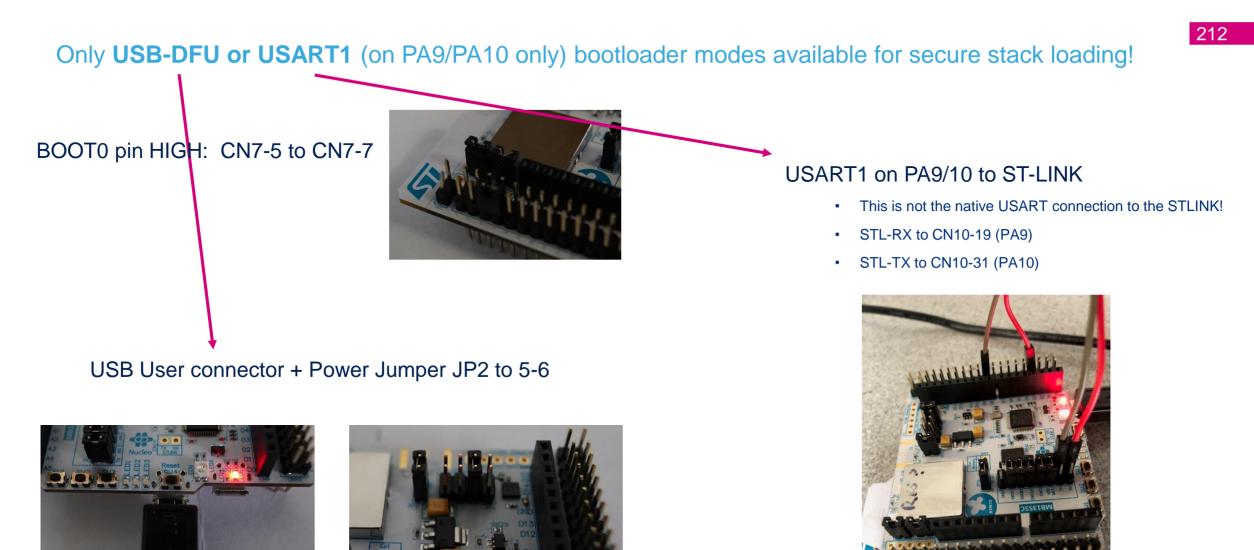








#### Nucleo Hardware Config for Bootloader access



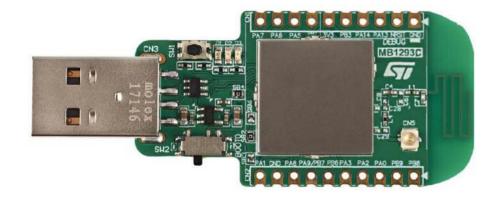


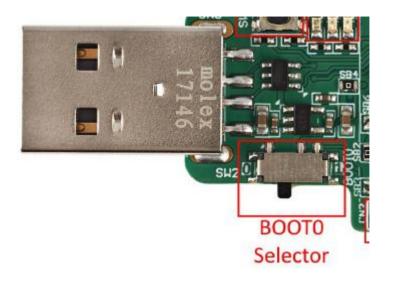


#### **Dongle Hardware Config for Bootloader access**

As we have seen, configuring the Dongle board for USB-DFU is quite easy.

Move the switch and repower the board





Bootloader active to the right





### AN5185: Firmware Update Services

#### AN5185 details the sequence to create your own secure stack loader project, running on the M4

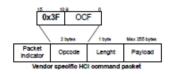
• Command / Response HCI event transactions to the M0+ similar to BLE

#### FUS commands

FUS uses same commands/response structure as wheless stacks and based on HCI model. FUS uses a subset of the HCI commands, namely:

- Vendor specific HCI command packet: used to send command from Cortex®-M4 to Cortex®-M0+.
- HCI command complete event packet: used to send response from Cortex<sup>®</sup>-MD+ to Cortex<sup>®</sup>-M4
- Vendor specific HCI event packet: used to send asynchronous events from Cortex®-MD+ to Cortex®-M4.

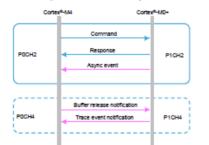
#### Figure 6. FUS HCI subset





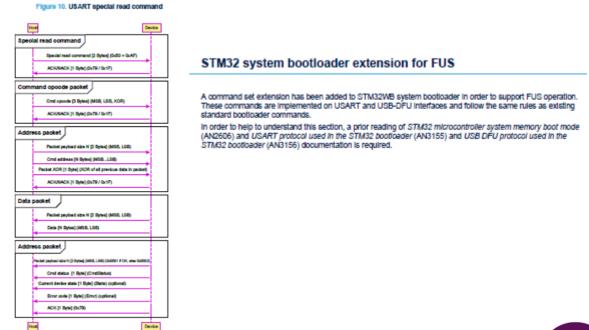


#### Figure 5. IPCC channels used by FUS



# life.augmented

#### Also details on the bootloader sequences used





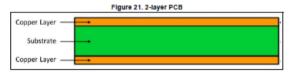
### AN5165: Hardware design

#### AN5165 details RF hardware considerations

- PCB stackup recommendations
- RF Front-end (discrete or IPD-based)
- SMPS passives selection
- Clocks

#### 2-layer PCB

With the 2-layer PCB (see Figure 21), the RF signals and routing are on the top layer while the bottom layer is used for grounding under the RF zones, and for routing in others parts. The ground plane must be continuous under the RF zones, otherwise the return path current can increase and degrade the RF performance.

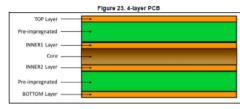


#### 4-layer PCB

With the 4-layer PCB shown in Figure 23, it is recommended to have the following distribution:

TOP layer: RF signal and routing on the top layer.

- INNER1 layer: grounding under the RF zones, routing in the others parts.
- INNER2 layer: power and low frequency routing.
- BOTTOM layer: low frequency routing.

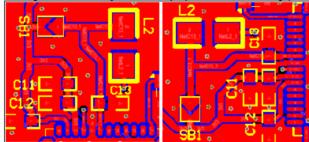




#### 6.1.2 SMPS

In addition to the recommendations given in Section 4.3: SMPS, to avoid important current loop when the STM32WB is in SMPS mode, it is recommended to place C11, C12 and C13 as close as possible to their respective plas on STM32WB. Do not forget to connect the solder pad to ground to have a strong current return path.

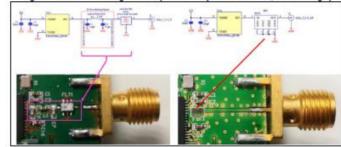
Figure 28. Detail of PCB layout for the SMPS part (UFQFPN48 left, VFQFPN68 right)



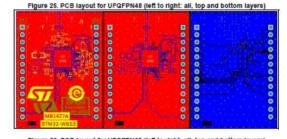
#### UFQFN48/VFQFN68 reference boards with IPD

The goal of the IPD (integrated passive device) is to replace the discrete matching network plus the integrated low-pass filter keeping equivalent TX/RX performance. Figure 41 shows the differences between the two approaches.





#### Layout recommendations for the 2-layer PCB



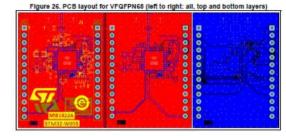
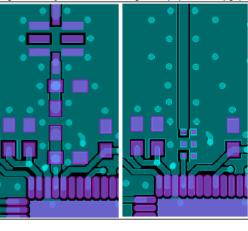


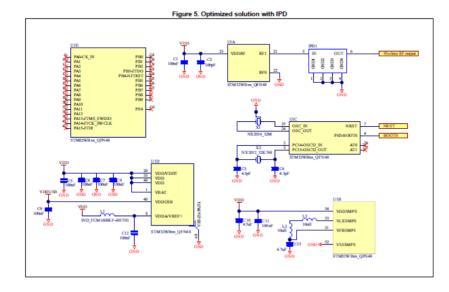
Figure 44. PCB layout with discrete matching network (left) and with IPD (right)





#### AN5290: Minimal BOM

#### AN5290 details the minimal Bill-of-Materials needed for various scenarios



Designator	Description	Comment	Footprint	Manufacturer	Part number
C1, C5, C6, C7, C8, C9, C11, C12	Capacitor, not polarized (X5R)	100 nF decoupling capacitors		Murata	GRM155R61H104KE19D
C2		100 pF decoupling capacitors	0402	Yageo	CC0402KRX7R9BB101
C3, C4	Capacitor, not polarized	4.3 pF LSE crystal capacitor		Murata	GRM1555C1H4R3CA01D
C10, C13	4.7 µF decoupling capac			Mulata	GRM155R61A475MEAAD
L1	Coll	Filtering coll	0603	TAI-TECH	FCM1608KF-601T03
L2	Inductor	10 µH SMPS Inductor	0805	Murata	LQM21FN100M70L
L3	I I GGC COI	10 nH SMPS Inductor	0402	Mulata .	LQG15WZ10NJ02D
X1	Operation	32 MHz - HSE	NX2016	NDK	NX2016SA_32MHz
X2	Crystal	32.768 kHz - LSE	NX2012	NDK	NX2012SA_32-768kHz
IPD1	Integrated passive device	Matching network and low-pass filter	Bumpless CSP	STMicroelectronics	MLPF-WB55-01E3

\_\_\_\_\_ 

Figure 4. Optimized solution with discrete components

Table 4. Dill of malastals	Contractor of a studios -	when the states	
Table 1, Bill of materials	- Opamized solution	with discrete	components

Designator	Description	Comment	Footprint	Manufacturer	Part number
C1, C5, C6, C7, C8, C9, C11, C12	Capacitor, not polarized (X5R)	100 nF decoupling capacitors		Murata	GRM155R61H104KE190
C2	Capacitor, not polarized	100 pF decoupling capacitors		Yageo	CC0402KRX7R9BB101
C3, C4		4.3 pF LSE crystal capacitor	0402		GRM1555C1H4R3CAD1
C10, C13		4.7 µF decoupling capacitor		Murata	GRM155R61A475MEAA
C14		0.8 pF matching network		Murata	GRM1555C1HR80BAD1
C15		0.3 pF matching network			GRM1555C1HR30WA01
L1	Coll	Filtering coll	0603	TAI-TECH	FCM1608KF-601T03
L2	Inductor	10 µH SMPS inductor	0805		LQM21FN100M70L
L3		10 nH SMPS Inductor	0400	Murata	LQG15WZ10NJ02D
L4		2.7 nH matching network	0402		LQG15HS2N7S02D
X1	Constal	32 MHz - HSE	NX2016	NDK ·	NX2016SA_32MHz
X2	Crystal	32.768 kHz - LSE	NX2012		NX2012SA_32-768kHz
FLT1	Low-pass filter	Harmonics rejection	-	Murata	LFL212G45TC1A007



# AN5129: PCB Antenna design

### AN5129 details a "meander-style" PCB antenna design

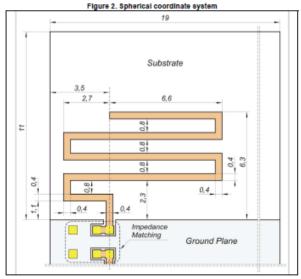
Layout specification

AN5129

217

#### 3 Layout specification

The PCB antennas, including the electrical parameters of PCB materials used, are layout sensitive. It is recommended to use a layout as close as possible to the one shown in *Figure* 2.



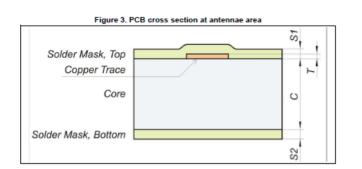
The electrical parameters and performance of the PCB antenna are also determined by the substrate used, in particular the thickness of the core and dielectric constants.

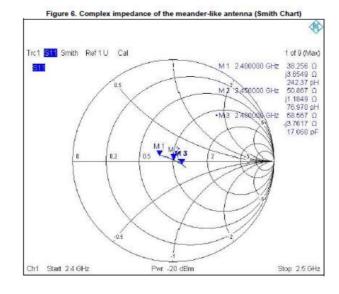


AN5129 Application note



Low cost PCB antenna for 2.4 GHz radio: meander design for STM32WB Series







# AN5246: SMPS

### AN5246 details SMPS use cases, component selection, and various typical operating parametrics



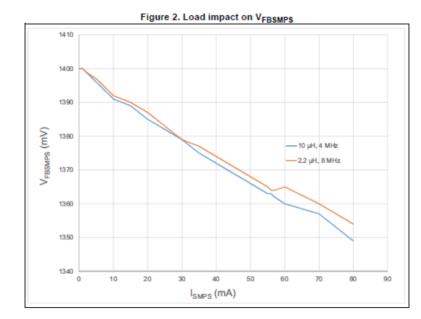
AN5246 Application note

Usage of SMPS on STM32WB Series microcontrollers

#### Introduction

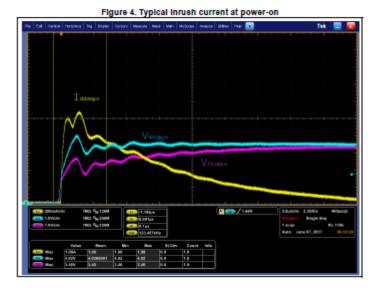
This document describes how the use the SMPS (switched mode power supply) integrated in microcontrollers of the STM32WB Series. It is intended to be used by system architects and by HW and board-level SW developers.

The patented implementation detailed in this document differs from the standard ones because it is able to maintain the RF transceiver full performance while, at the same time, providing the best power figure in burst application like those generally used by Bluetooth<sup>®</sup> Low Energy and IEEE 802.15.4 protocols.



#### Inrush current at power ON

As the SMPS starts in BYPASS mode when powering up, the bulk capacitance needs to be powered when  $V_{DD}$  rises. At start up, when the  $V_{DD}$  voltage enters the 0.7 to 1 V range, the SMPS PMOS starts to conduce and  $V_{\text{FBDSMPS}}$  follows  $V_{\text{DDSMPS}}$ . This leads to a temporary inrush current that can be as high as 1.1 A if the power supply is strong enough.



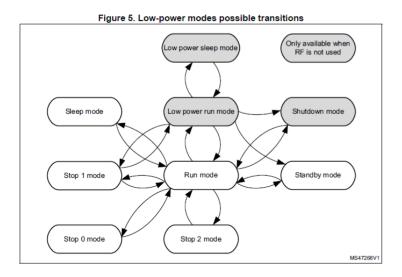




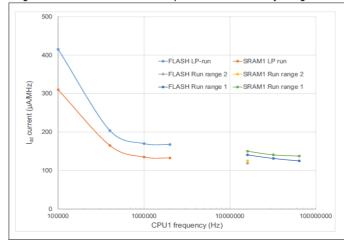
# AN5071: Ultra-Low Power Design

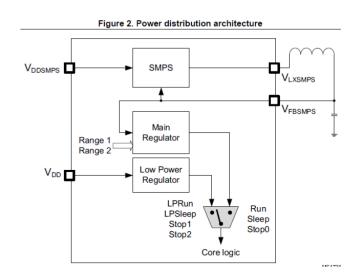
AN5071 details the multitude of low-power options available on the WB

AN5071
Application note
STM32WB ultra-low-power features overview



#### Figure 3. STM32WB55 - Current consumption for different memory configurations





#### Table 2. STM32WB55 performance with SMPS

Configuration	mA/MHz	CoreMark <sup>®</sup> per MHz	CoreMark <sup>®</sup> per mA
FLASH ART On	0.077	3.25	42
SRAM1	0.073	2.40	33





# AN5155: CubeWB Examples

### AN5155 is an exhaustive list of all firmware examples and descriptions

#### 220

	-		
Thread_Cli_Cmd	How to control the Thread $^{\textcircled{O}}$ stack via Cli commands.	х	CubeMx
Thread_Coap_DataTransfer	How to transfer large blocks of data through the CoAP messaging protocol.	х	х
Thread_Coap_Generic	How to build Thread® application based on Coap messages.	х	CubeMx
Thread_Coap_MultiBoard	How to use Coap for sending message to multiple boards.	-	х
Thread_Commissioning	How to use Thread <sup>®</sup> commissioning process.	-	х
Thread_FTD_Coap_Multicast	How to exchange multicast Coap messages.	х	х
Thread_SED_Coap_Multicast	How to exchange a Coap message using the Thread® protocol.	х	х
	Thread_Coap_DataTransfer Thread_Coap_Generic Thread_Coap_MultiBoard Thread_Commissioning Thread_FTD_Coap_Multicast	Thread_Cli_Cmd         How to control the Thread® stack via Cli commands.           Thread_Coap_DataTransfer         How to transfer large blocks of data through the CoAP messaging protocol.           Thread_Coap_Generic         How to build Thread® application based on Coap messages.           Thread_Coap_MultiBoard         How to use Coap for sending message to multiple boards.           Thread_Commissioning         How to use Thread® commissioning process.           Thread_FTD_Coap_Multicast         How to exchange multicast Coap messages.	Thread_Cli_Cmd         How to control the Thread® stack via Cli commands.         X           Thread_Coap_DataTransfer         How to transfer large blocks of data through the CoAP messaging protocol.         X           Thread_Coap_Generic         How to build Thread® application based on Coap messages.         X           Thread_Coap_MultiBoard         How to use Coap for sending message to multiple boards.         -           Thread_Commissioning         How to use Thread® commissioning process.         -           Thread_FTD_Coap_Multicast         How to exchange multicast Coap messages.         X

Module Name	Project Name	Description	P- NUCLEO- WB55.US BDongle	P- NUCLEO- WB55.Nuc leo
	ADC_AnalogWatchdog_Init	How to use an ADC peripheral with an ADC analog watchdog to monitor a channel and detect when the corresponding conversion data is outside the window thresholds.	-	CubeMx
	ADC_ContinuousConversion_TriggerSW	How to use an ADC peripheral to perform continuous ADC conversions on a channel, from a software start.	-	x
	ADC_ContinuousConversion_TriggerSW_Init	How to use an ADC peripheral to perform continuous ADC conversions on a channel, from a software start.	-	CubeMx
	ADC_ContinuousConversion_TriggerSW_LowPow er_Init	How to use an ADC peripheral with ADC low-power features.	-	CubeMx
	ADC_GroupsRegularInjected_Init	How to use an ADC peripheral with both ADC groups (regular and injected) in their intended use cases.	-	CubeMx
	ADC_Oversampling_Init	How to use an ADC peripheral with ADC oversampling.	-	CubeMx
ADC	ADC_SingleConversion_TriggerSW_DMA_Init	How to use an ADC peripheral to perform a single ADC conversion on a channel, at each software start. This example uses the DMA programming model (for polling or interrupt programming models, refer to other examples).	-	CubeMx
	ADC_SingleConversion_TriggerSW_IT_Init	How to use an ADC peripheral to perform a single ADC conversion on a channel, at each software start. This example uses the interrupt programming model (for polling or DMA programming models, please refer to other examples).	-	CubeMx
	ADC_SingleConversion_TriggerSW_Init	How to use an ADC peripheral to perform a single ADC conversion on a channel at each software start. This example uses the polling programming model (for interrupt or DMA programming models, please refer to other examples).	-	CubeMx
	ADC_SingleConversion_TriggerTimer_DMA_Init	How to use an ADC peripheral to perform a single ADC conversion on a channel at each trigger event from a timer. Converted data are indefinitely transferred by DMA into a table (circular mode).	-	CubeMx
	ADC_TemperatureSensor	How to use an ADC peripheral to perform a single ADC conversion on the internal temperature sensor and calculate the temperature in Celsius degrees.	-	x

#### *CubeMx* denotes that there is an "ioc" CubeMX project file also

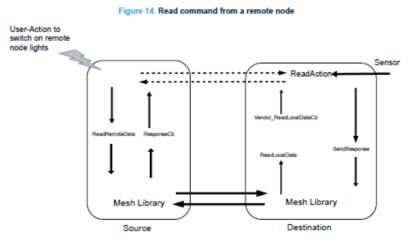




# AN5292: BLE Mesh

### AN5292 shows how to get started using BLE Mesh

#### Figure 7. Internal project folder NUCLEO-WB55.Nucleo Applications BLE Thread FatFs FreeRTOS Mac\_802\_15\_4 Thread USB Device STM32WBx5 setup source and include file BLE MeshLightingDemo IAR project workspace Core EWARM Application source and include files app. STM32\_WPAN target Mailbox source file for communication between M0 and M4



The response data from the node is sent via the BLEMesh\_SendResponse function.

#### Figure 10. VCOM window

COM65:115200bps - Tera Term VT	
Fichier Edition Configuration Contrôle Fenêtre(W) Aide	
BLE-Mesh Lighting Demo v1.09.000 BLE-Mesh Library v01.09.000 MAC Address = [80]:[e1]:[26]:[00]:[2d]:[8f]	•

#### MAC address management

Each node in the mesh network requise a unic MAC address. The following table describes the available options to configure the MAC addresses for a node

#### Table 2. MAC address management

Number	MAC address Management	Comments
1	Using external MAC address	User can program the nodes with desired unique MAC address. This is stored at specific location in the flash. It is the user's responsibility to make sure that the programmed MAC address in the device is compliant with the Bluetooth communication requirements.
2	Using the unique device serial number	It is possible to configure the MAC address of the device using the unique serial number available in each device. This is the default setting.
3	Using static random MAC address	It is possible to configure the MAC address of devices using the static random MAC address







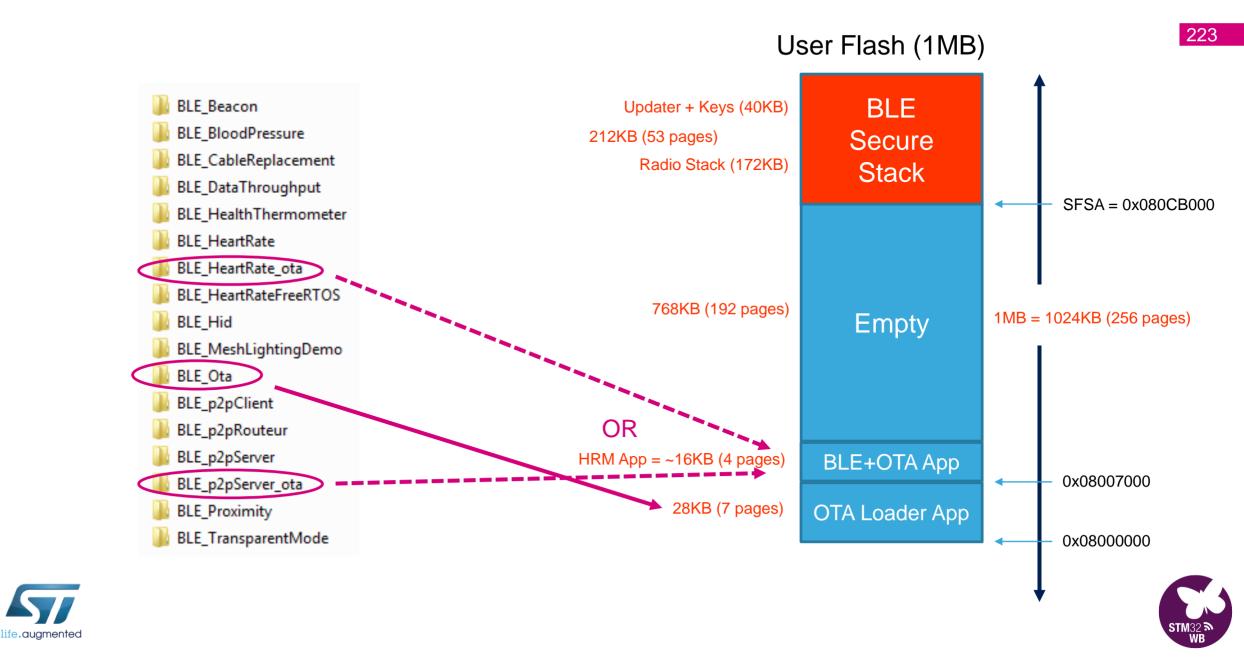
Over-the-Air	Firmware	U

OTA Updater	
SEARCH FOR DEVICES	
Select device       0x80E126005363 - P2PSR12 - 0TA enabled       mage base dataress (nex)	
Image file path	BROWSE
	UPDATE



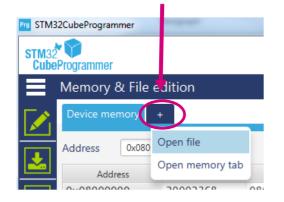


# **Over-The-Air Firmware Updates**

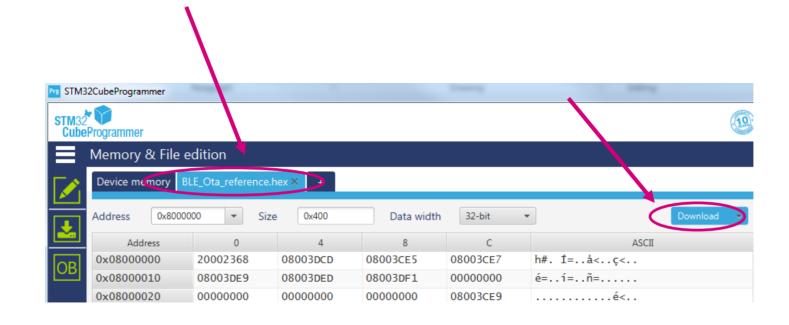


# **OTA Loader App**

## Flash Nucleo board with **BLE\_Ota\_reference.hex** using CubeProgrammer



Re	pository > STM32Cube_FW_WB_V1.0.0	► P	Projects 🕨 NUCLEO-WB55.	Nucleo 🕨 A	Applications	► BLE ►	BLE_Ota	<ul> <li>Binary</li> </ul>
lp								
у 🔻	Share with 🔻 New folder							
*	Name		Date modified	Туре		Size		
	BLE_Ota_reference.hex		2/19/2019 9:56 AM	HEX File		45	KB	







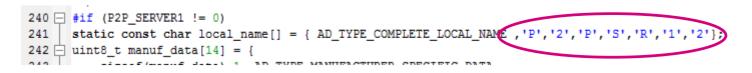


# P2P Server + OTA project

### Load and personalize your BLE\_p2pServer\_ota.eww project

sitory	► STN	M32Cube_FW_WB_V1.0.0 > Projects >	NUCLEO-WB55.Nucleo 🕨 Appli	cations + BLE + BLE	_p2pServer_ota
ools	Help				
pen y		Share with 🔻 New folder			
ers	*	Name	Date modified	Туре	Size
		BLE_p2pServer	4/10/2019 2:52 PM	File folder	
		鷆 settings	4/10/2019 2:52 PM	File folder	
		BLE_p2pServer_ota.ewd	2/19/2019 9:56 AM	EWD File	32 KB
		📂 BLE_p2pServer_ota.ewp	2/19/2019 9:56 AM	Embedded Wizard	47 KB
		Project.eww	2/19/2019 9:56 AM	IAR IDE Workspace	1 KB

### In app\_ble.c



#### 178 #define APPBLE\_GAP\_DEVICE\_NAME\_LENGTH 9

772 const char \*name = "STM32WB12";

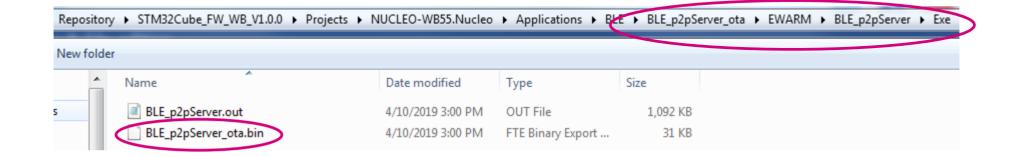




# Server + OTA App

### Flash your newly created **BLE\_p2pServer\_ota.bin** to 0x08007000

Device memory BI	LE_p2pServer_ota_i	reference.bin ×	+			ST-LI
Address 0x0	▼ Size	0x400	Data width	32-bit 👻		Downland 👻
Address	0	4	8	С	ASCII	Read
0x0000000	20002740	0800E325	0800E345	0800E347	@'. %ãEãGã	Save As
0x0000010	0800E349	0800E34B	0800E34D	00000000	IãKãMã	Verify
0x0000020	0000000	0000000	0000000	0800E34F	0ã	Address 0x08007000
0x0000030	0800E351	00000000	0800E353	0800E355	QãSãUã	



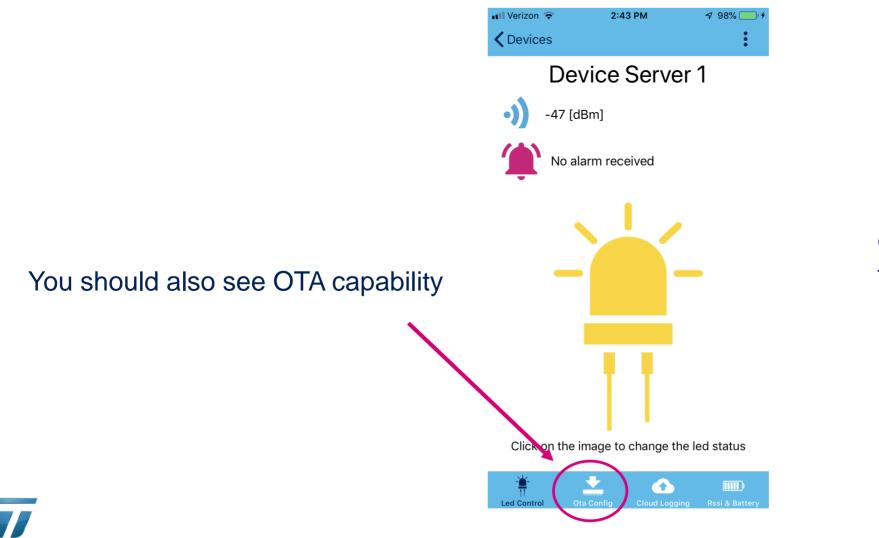




# Server + OTA App

### Verify functionality on the ST BLE Sensor app

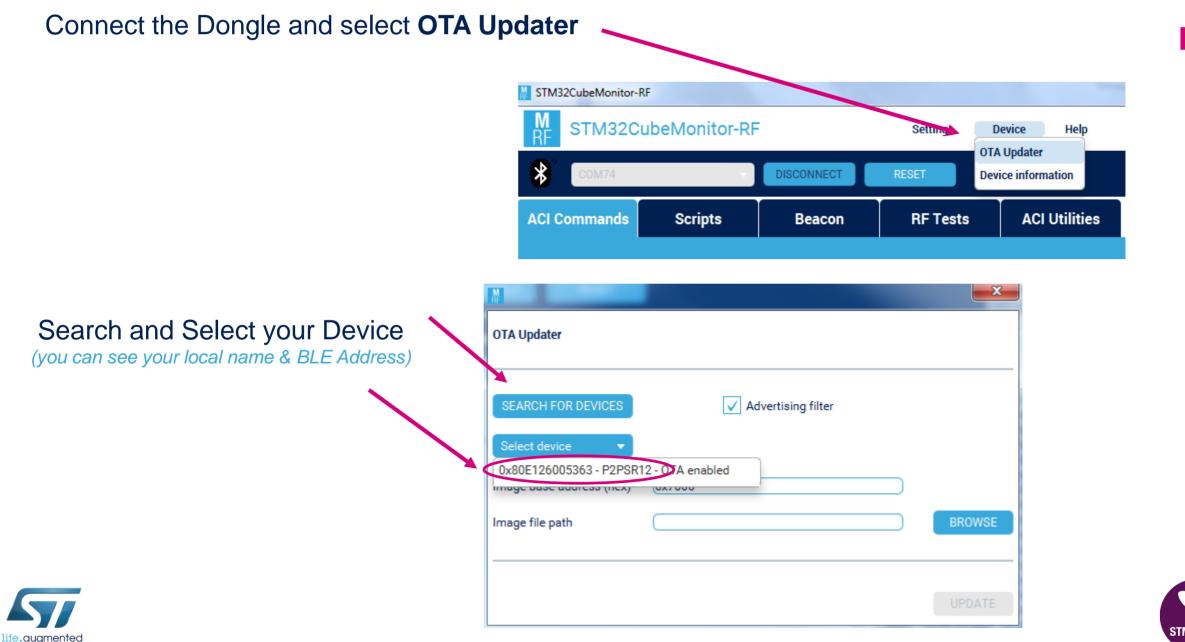
life.auamente



Once seen, disconnect from your device



# **Connect to OTA-enabled device**



# **Update BLE Application**

### Browse for the other OTA binary

• BLE\_HeartRate\_ota\_reference.bin

M		× ×
OTA Updater		
SEARCH FOR DEVICES	Advertising filter	
0x80E1260053 ▼		
Image base address (hex)	0x7000	
Image file path	e_ota\Binary\BLE_HeartRate_ota_reference.bin	BROWSE
		UPDATE

### Update image

	Advertising filter	
Image base address (hex)	0x7000	
Image file path	C:\Users\alec bath\STM32Cube\Repository\S	

#### Repository + STM32Cube\_FW\_WB\_V1.0.0 + Projects + NUCLEO-WB55.Nucleo + Applications + BLE + BLE\_HeartRate\_ota + Binary

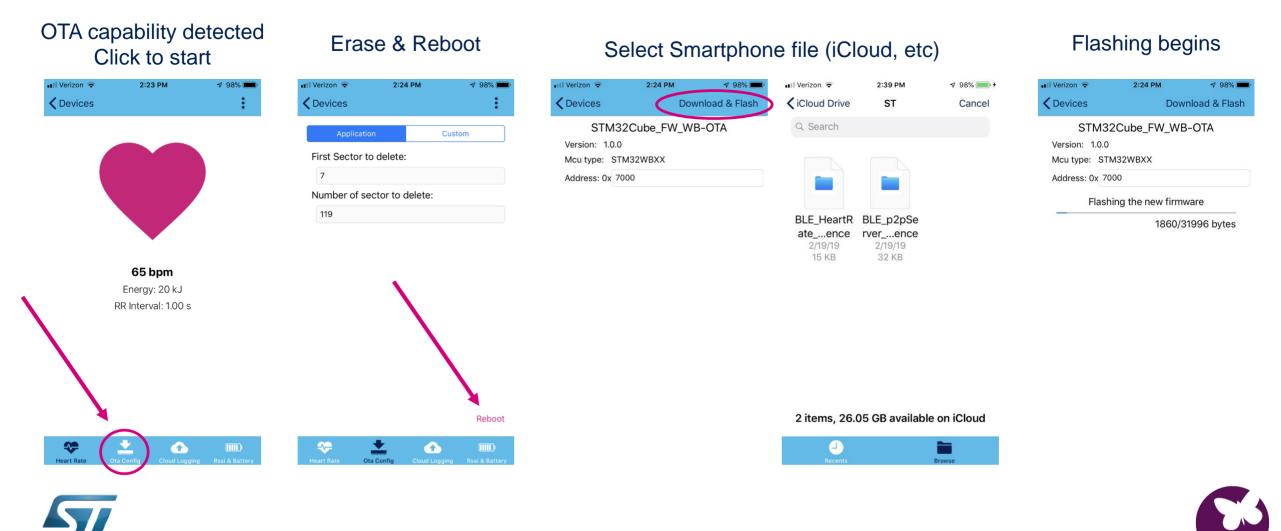
v Tools	v Tools Help									
Include in	Include in library 🔻 Share with 🔻 New folder									
	<u>^</u>	Name	Date modified	Туре	Size					
;		BLE_HeartRate_ota_reference.bin	2/19/2019 9:56 AM	FTE Binary Export	15 KB					





# Update via ST BLE Sensor app

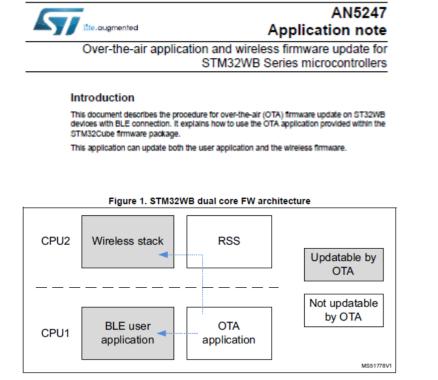
#### 2<u>30</u>

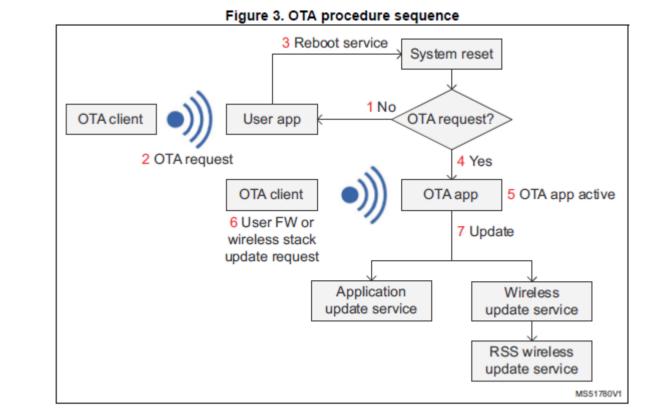


life.augmented

231

### AN5247 details the OTA application in further detail.









# iOS / Android Smartphone app

### BlueST SDK on Github: <a href="https://github.com/STMicroelectronics/BlueSTSDK\_Android">https://github.com/STMicroelectronics/BlueSTSDK\_Android</a>

, Inc. [US]   htt	tps://github.com/	/STMicroelect	ronics/BlueS	TSDK_Android						
<b>(</b> )	Why GitHub? ~	Enterprise	Explore $\sim$	Marketplace	Pricing $\sim$				Sign in	Sigr
STM	licroelectronics	/ BlueSTSE	)K_Android	ł		• Watch	25	\star Star	44	<b>♀</b> Fork
<b>&lt;&gt;</b> Co	de 🕕 Issues (8	) 🏦 Pull re	equests 0	Projects 0	Insights					
				ne to over 36 mill	GitHub today lion developers workin projects, and build soft					Dismi

24 commits	2 branches	🛇 0 releases	1 contributor	办 BSD-3-Clause
Branch: master   New pull r	request		[	Find File Clone or download -
GiovanniVisentini Add the p		Latest commit Øb772cb on Mar 26		
BlueSTExample	Add the possibility to use a	custom advertise format		a month ago
BlueSTSDK	Add the possibility to use a	custom advertise format		a month ago
.gitignore	- Update android libs			2 years ago
LICENSE	Initial commit			4 years ago
README.md	Add the possibility to use a	custom advertise format		a month ago
build.gradle	Add the possibility to use a	custom advertise format		a month ago
settings.gradle	Initial commit			4 years ago

#### **BlueST SDK**

BlueST is a multi-platform library (Android and iOS supported) that permits easy access to the data exported by a Bluetooth Low Energy (BLE) device that implements the BlueST protocol.

#### **BlueST Protocol**

#### Advertise

The library will show only the device that has a vendor-specific field formatted in the following way:

Length	1	1	1	1	4	6
Name	Length	Field Type	Protocol Version	Device Id	Feature Mask	Device MAC (optional)
Value	0x07/0xD	0xFF	0x01	0xXX	0xXXXXXXXX	0xXXXXXXXXXXXXXX

• The Field Length must be 7 or 13 bytes long.

- The Device Id is a number that identifies the type of device. It is used to select different types of feature mask and can manage more than 32 features. Currently used values are:
  - 0x00 for a generic device
  - 0x01 is reserved for the STEVAL-WESU1 board
  - 0x02 is reserved for the STEVAL-STLKT01V1 (SensorTile) board
  - 0x03 is reserved for the STEVAL-BCNKT01V1 (BlueCoin) board
  - a Ov04 is recorded for the STEVAL IDROORV172 (RhoNDC 2) heard





# **Bonus Lab!** SIG RF Certification Tests

### Packet Error Rate (PER) tests with two boards connected

ACI Commands	Scripts	Beacon	RF Tests	ACI Utilities					
Test mode									
Select test mode									
Transmitter test (TX)									
Packet error test (PER	)	_							

ACI Commands	Scripts	Beacon	RF Tests
Test mode > Packet Error	Rate (PER)		
Connect tester			
сом222 🗸	CON	NECT	
		Connect a	second board
			r instance)





# **Bonus Lab!** SIG RF Certification Tests

### Packet whitening is disabled in Direct Test Mode (DTM)

life.auar

ACI Commands	Scripts	Beacon	RF Tests	ACI Utilities		ARM CM4	Application Application Profiles Services		
Test mode > Packet Erro	or Rate (PER) > COM22	2				AR	ACI Interface		
Configure tester (COM	1222)						SRAM2 IPCC		
							BLE peripheral		
PA Level		31 (+6	dBm)	•		ARM CM0+ BLE STACK			
TX Frequency		2402 M	/Hz (Channel 37)	•		ARM			
Length of Data		0x25	,	•		C	Radio PHY DTM		
						ion tosti	20		
Packet Payload		0x00 -	Pseudo-Random bit se	quence 9	rower mansimiss	Power Transmission testing			
РНҮ		0x01 - 0x02 -	Pseudo-Random bit see Pattern of alternating b Pattern of alternating b	its '11110000'	Frequency Deviat	tion test	ing		
Back		0x04 -	Pseudo-Random bit sec Pattern of all '1' bits Pattern of all '0' bits	quence 15	Carrier Frequency	y Accura	acy testing		
Test measurement			Pattern of alternating b Pattern of alternating b		1				

# We Greatly Value Your Feedback

Use your phone to scan the QR code or type the link into your browser.



https://www.surveymonkey.com/r/PLYWMDC







# **Releasing Your Creativity**

