Embedded Linux Conference
Europe

OpenIoTSummit
Europe

Bluetooth Low Energy Controller in Zephyr OS

Vinayak Kariappa Chettimada
Consultant, Nordic Semiconductor ASA
SixOctets Systems, Bengaluru

@vkchettimada

THE LINUX FOUNDATION

Introduction

Vinayak Kariappa Chettimada

- Over 16 years in the industry
- Primary contributing maintainer of Zephyr BLE controller subsystem
  - Original author
- Architect and lead developer Bluetooth Software Stacks
  - nRF8001/2 firmware, SoftDevices for nRF51 Series and latest nRF52 series
- Prior experiences with leading mobile phone and automotive manufacturer
  - Headset, Handsfree, Advanced Audio support in car kits and their IOP with phones
- Windows applications and web technologies
- Linux user and developer since a student

Bluetooth

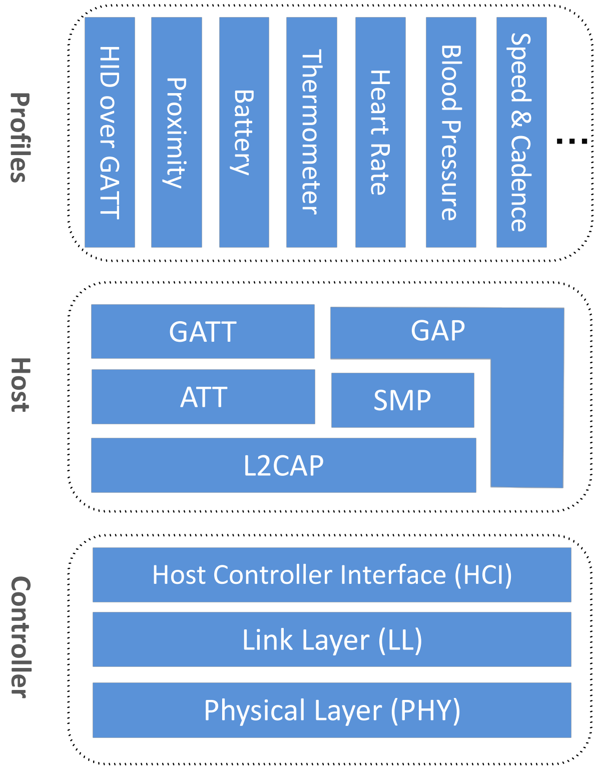
- Short range, low-power
- Frequency hopping spread spectrum (FHSS)
- 2.4 GHz ISM band
- Bluetooth Special Interest Group formed in 1998
- 20 Years
- Billions of products shipped
- 33000+ SIG member companies

Bluetooth Low Energy (BLE)

- Ultra Low Power
- Optimized for short burst data transmission
  - Small packets
  - Short RX and TX windows
- Race to idle
  - Turn radio on as seldom as possible
  - Turn radio off as soon as possible
- Fast connection in 6 ms and teardown
- Simple stateless operation
  - Data in form of parameter-value
- Low memory footprint
- Coin-cell battery 1+ year

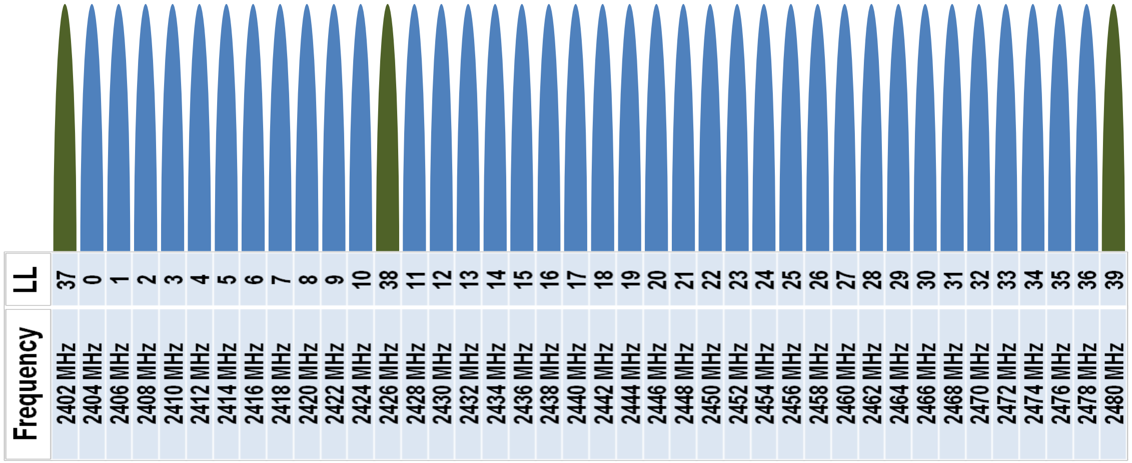
Technology

BLE Stack


Profiles
HID over GATT
Proximity
Battery
Thermometer
Heart Rate
Blood Pressure
Speed & Cadence
…
Host
GATT
GAP
ATT
SMP
L2CAP
Controller
Host Controller Interface (HCI)
Link Layer (LL)
Physical Layer (PHY)

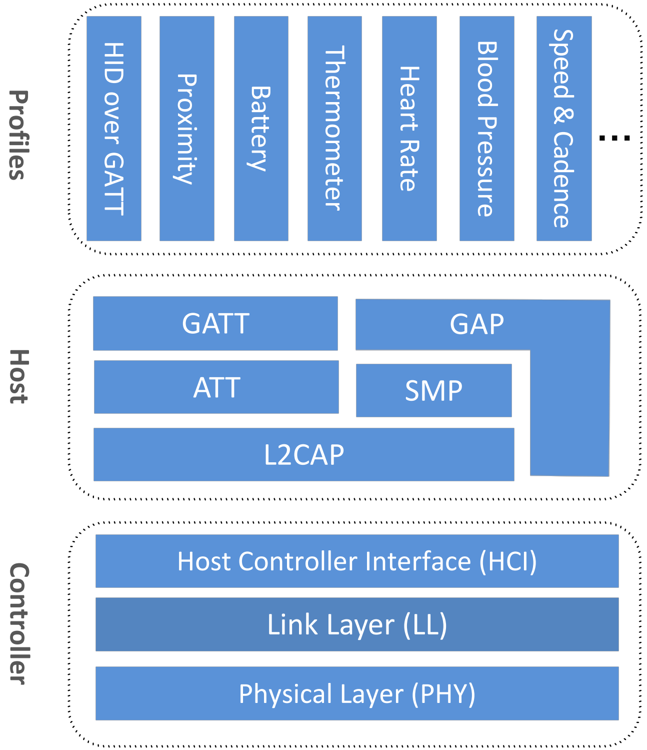
BLE: PHY

- **2.4 GHz** free ISM band
- **1 Mbit/s** and **2 Mbit/s** signalling rate
- **GFSK** modulation
- **+20 dBm** maximum transmit power
- **40** RF channels
- **3** advertising channels reserved for:
  - Broadcast
  - Discover
  - Connect
- **37** data channels



LL	37	0	1	2	3	4	5	6	7	8	9	10	38	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	39
Frequency	2402 MHz	2404 MHz	2406 MHz	2408 MHz	2410 MHz	2412 MHz	2414 MHz	2416 MHz	2418 MHz	2420 MHz	2422 MHz	2424 MHz	2426 MHz	2428 MHz	2430 MHz	2432 MHz	2434 MHz	2436 MHz	2438 MHz	2440 MHz	2442 MHz	2444 MHz	2446 MHz	2448 MHz	2450 MHz	2452 MHz	2454 MHz	2456 MHz	2458 MHz	2460 MHz	2462 MHz	2464 MHz	2466 MHz	2468 MHz	2470 MHz	2472 MHz	2474 MHz	2476 MHz	2478 MHz	2480 MHz

BLE: Link Layer

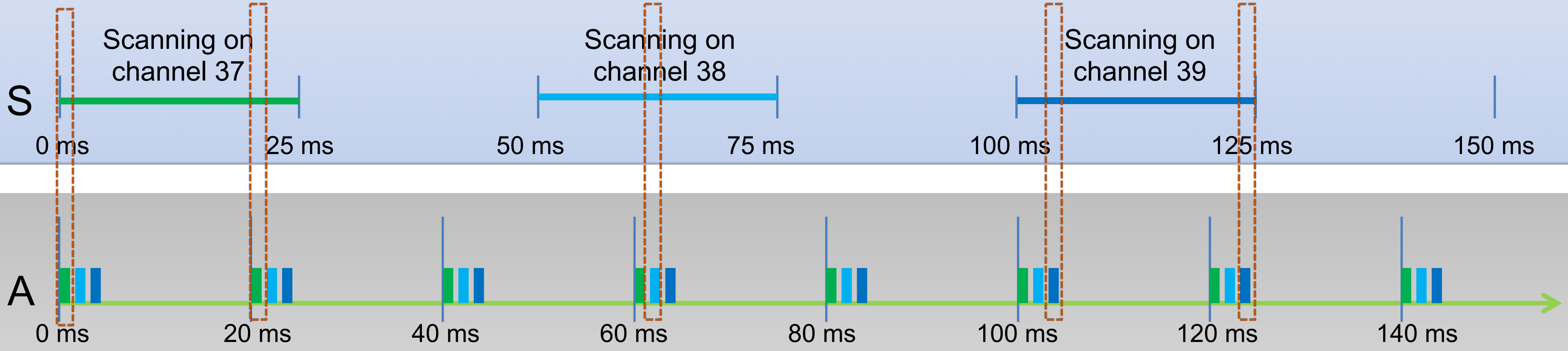


- **Advertising:** connectable and non-connectable
- **Scanning:** active or passive
- **Slave and Master:** connection role
- **31 bytes** legacy advertising payload size
- **255 bytes** extended advertising on data channels with additional chaining
- **27-255 bytes** maximum payload size per PDU
- **AES-128** built-in encryption
- **CCM**
  - Counter with
  - Cipher Block Chaining
  - Message Authentication Code

THE LINUX FOUNDATION

Advertising and Scanning

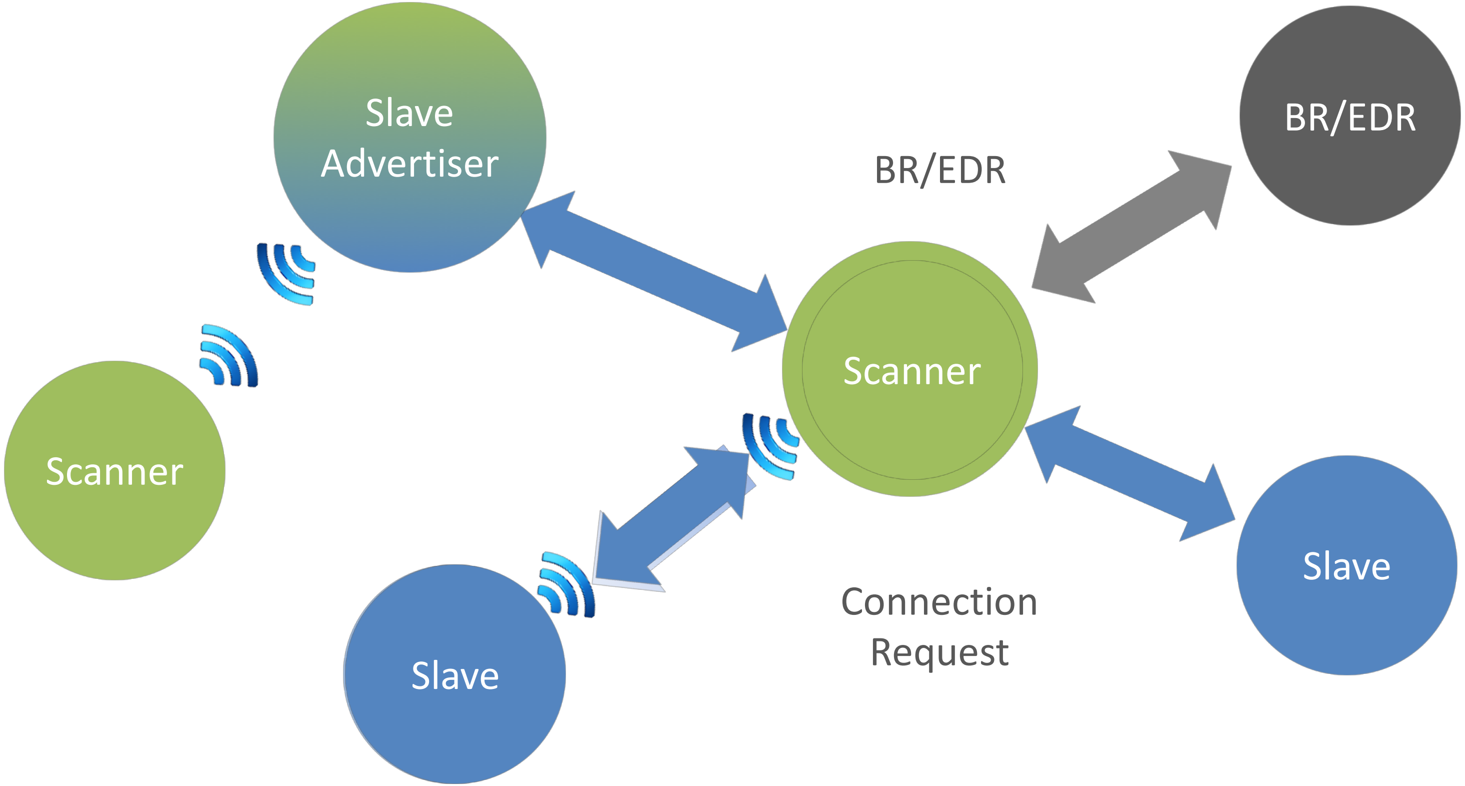
Scanner scan interval = 50 ms
Scanner scan window = 25 ms



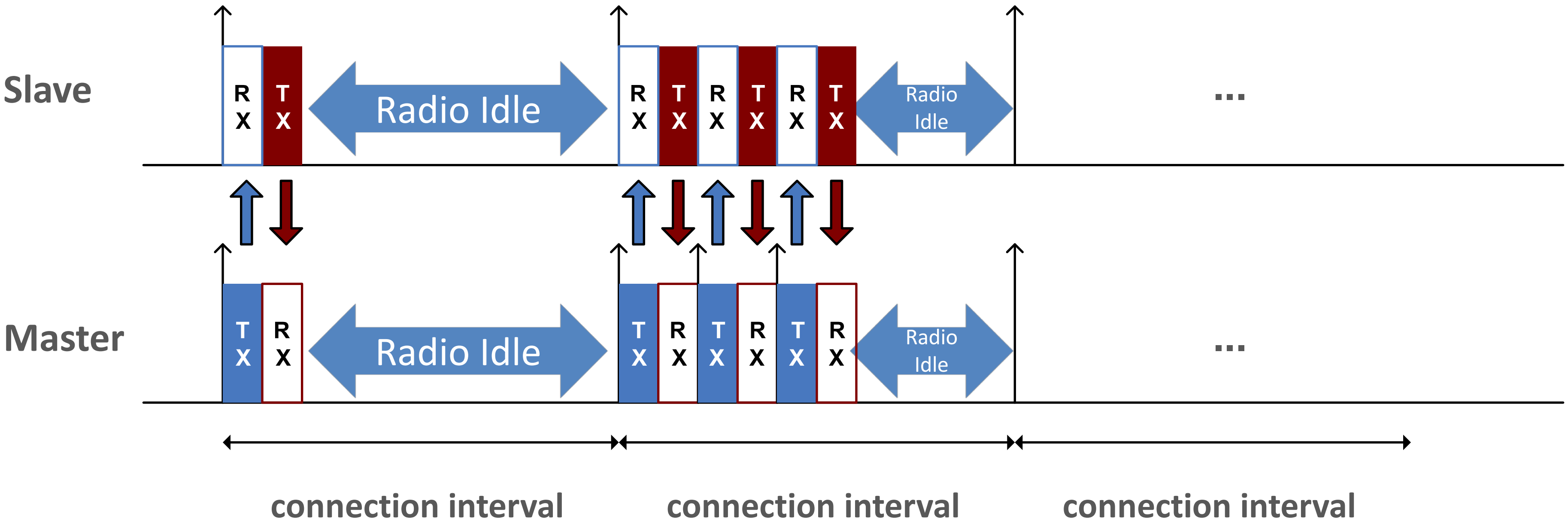
Advertising on **37**, **38** and **39**

Advertiser advertising interval = 20 ms

Topology


Slave Advertiser
BR/EDR
BR/EDR
Scanner
Scanner
Slave
Slave
Connection Request

Connection

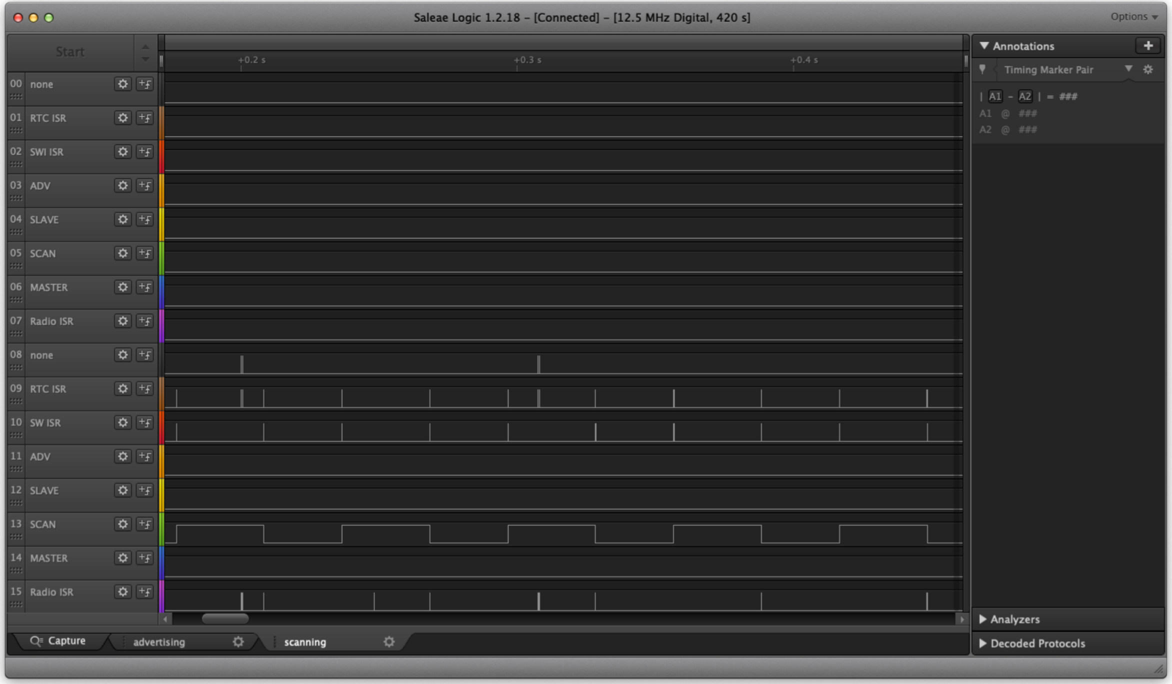


- Selectable Connection Interval: **7.5 ms to 4 s**

Advertising, Scanning, slave and master

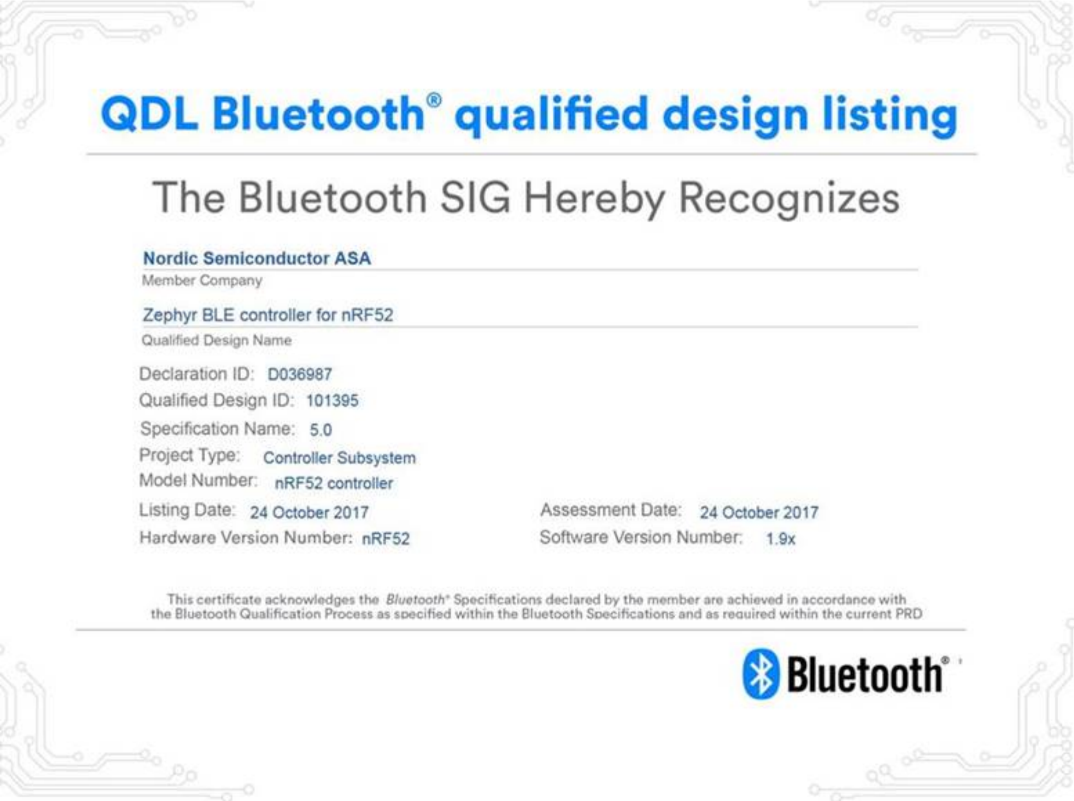
- Demo using Zephyr OS
  - samples/bluetooth/peripheral
  - samples/bluetooth/central_hr

Advertising, Scanning, slave and master



Controller

Conformance



QDL Bluetooth® qualified design listing

The Bluetooth SIG Hereby Recognizes

Nordic Semiconductor ASA
Member Company

Zephyr BLE controller for nRF52
Qualified Design Name

Declaration ID: D036987
Qualified Design ID: 101395
Specification Name: 5.0
Project Type: Controller Subsystem
Model Number: nRF52 controller

Listing Date: 24 October 2017 — Assessment Date: 24 October 2017
Hardware Version Number: nRF52 — Software Version Number: 1.9x

This certificate acknowledges the *Bluetooth®* Specifications declared by the member are achieved in accordance with the Bluetooth Qualification Process as specified within the Bluetooth Specifications and as required within the current PRD

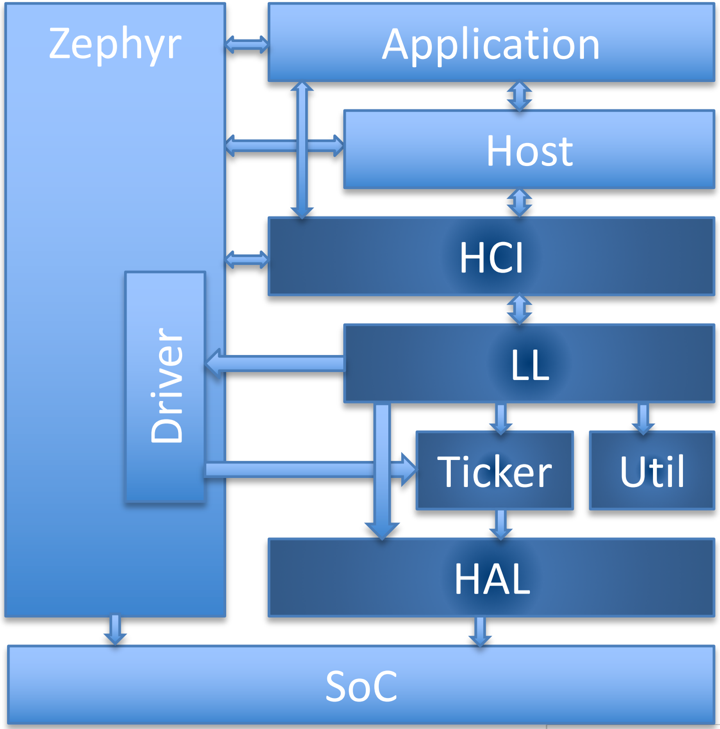
Bluetooth®

Features

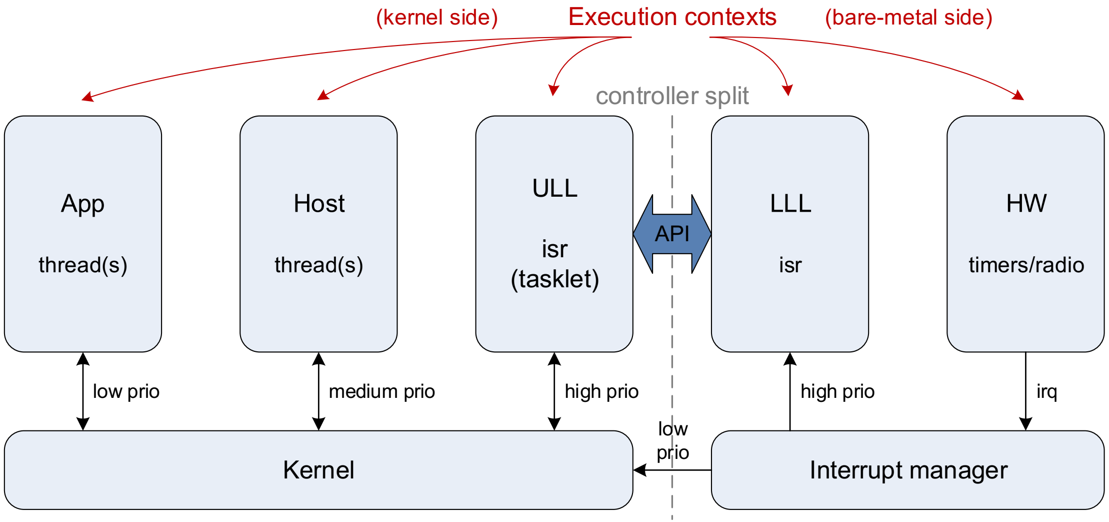
- BLE 5.0 compliant
- Unlimited role and connection count, all roles supported
- Concurrent multi-protocol support ready
- Intelligent scheduling of roles to minimize overlap
- Portable design to any open BLE radio, currently supports Nordic Semiconductor nRF51 and nRF52 Series

Architecture

- Zephyr
  - Threads, fifo, semaphore
- HCI
  - Host Controller Interface, Bluetooth standard
  - Provides Zephyr Bluetooth HCI Driver
- HAL
  - Hardware Abstraction Layer
  - Vendor Specific, Replace with Zephyr Driver
- Ticker
  - Soft real time radio/resource scheduling
- LL_SW
  - Software-based Link Layer
  - States and Roles, control procedures, packet controller
- Util
  - Bare metal memory management
  - Queues of variable count, lockless
  - FIFO, fixed count, lockless, ISR-ISR-Thread
  - Mayfly



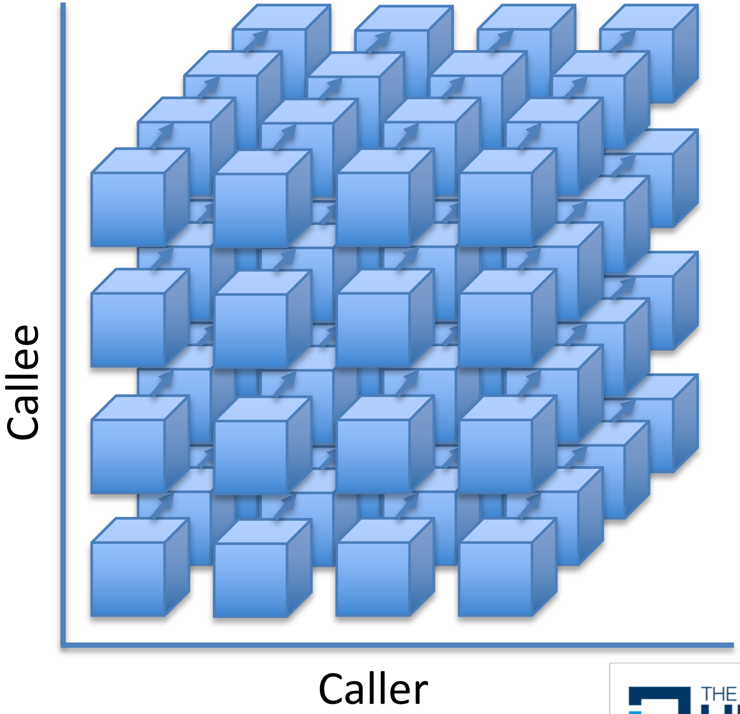
Multi-vendor execution contexts



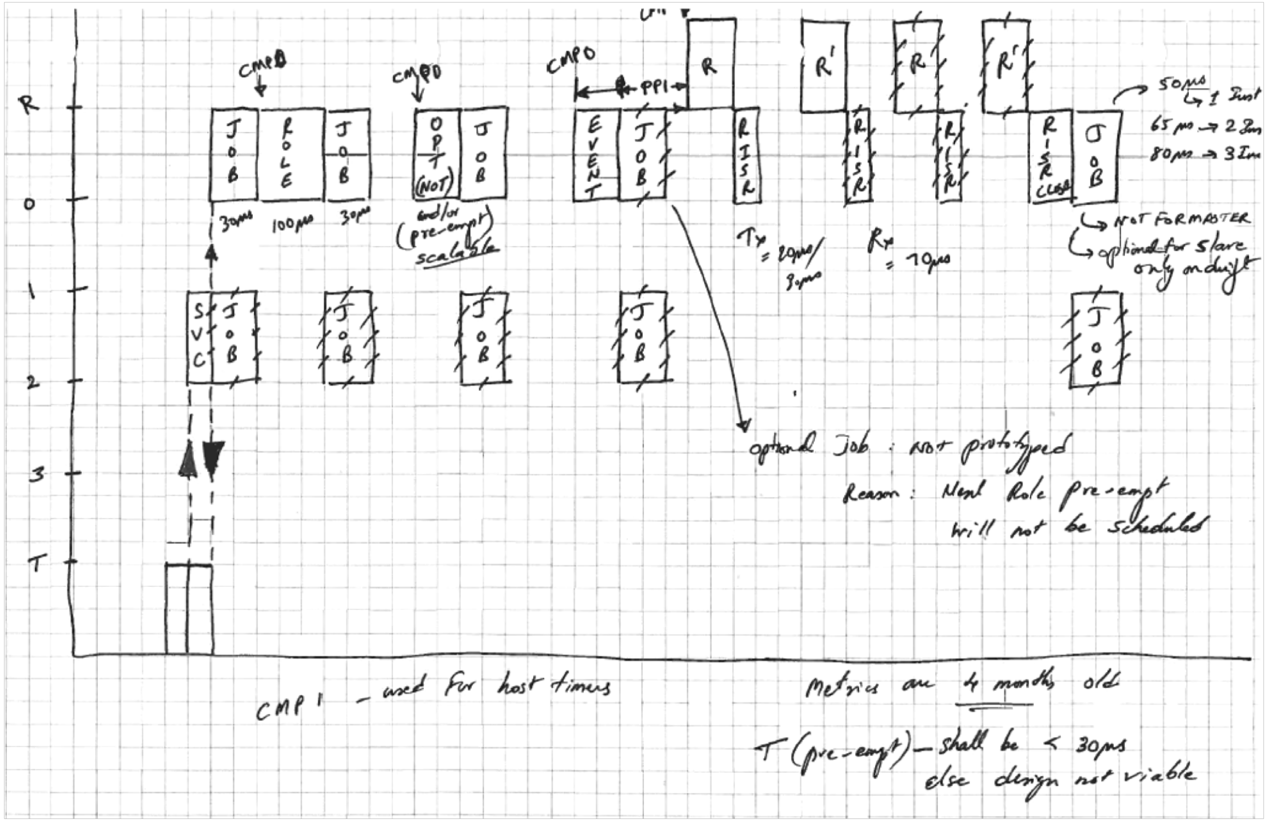
- Vendor Specific Lower Link Layer (LLL)
  - Open or closed source
  - Bare-metal
  - High priority Direct ISR
- Open source Upper Link Layer (ULL)
  - Mayfly ISR infrastructure
  - Ideally use Kernel features

Mayfly

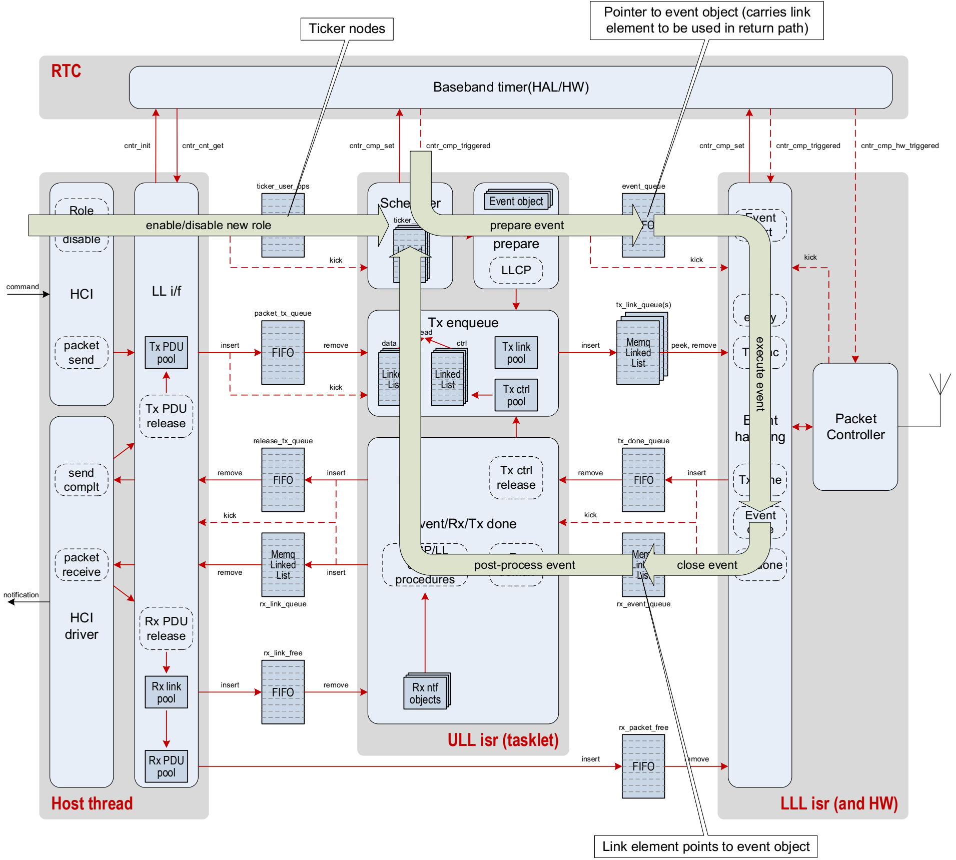
- Multi-instance scalable ISR execution contexts
- Mayfly is to ISR, as Work is to Thread
- Race-to-idle execution
- Priorities map to IRQ priorities
- Cross context scheduling
- Lock-less, bare metal



Scheduling


R
0
1
2
3
T
CMPB
CMPD
CMPO
PPI
JOB
ROLE
JOB
OPT (NOT)
JOB
EVENT
JOB
R
RISR
R'
RISR
R
RISR
R'
RISR CLOSE
JOB
30μs
100μs
30μs
and/or (pre-empt) scalable
Tx = 20μs/ 9μs
Rx = 10μs
50μs ↳ 1 Inst
65μs → 2 Ins
80μs → 3 Ins
↳ NOT FOR MASTER
↳ optional for slave only on drift
SVC
JOB
JOB
JOB
JOB
JOB
optional Job: not prototyped
Reason: Next Role pre-empt will not be scheduled
CMP1 – used for host timers
Metrics are 4 months old
T (pre-empt) – shall be < 30μs else design not viable

Scheduling

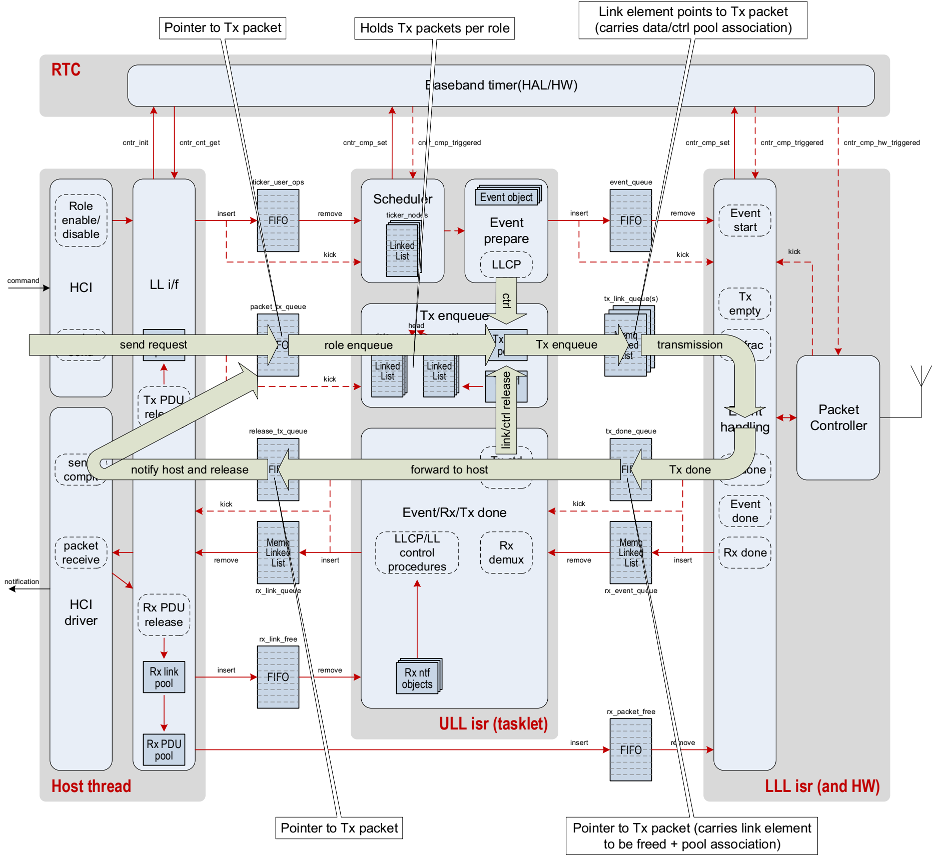


Ticker nodes

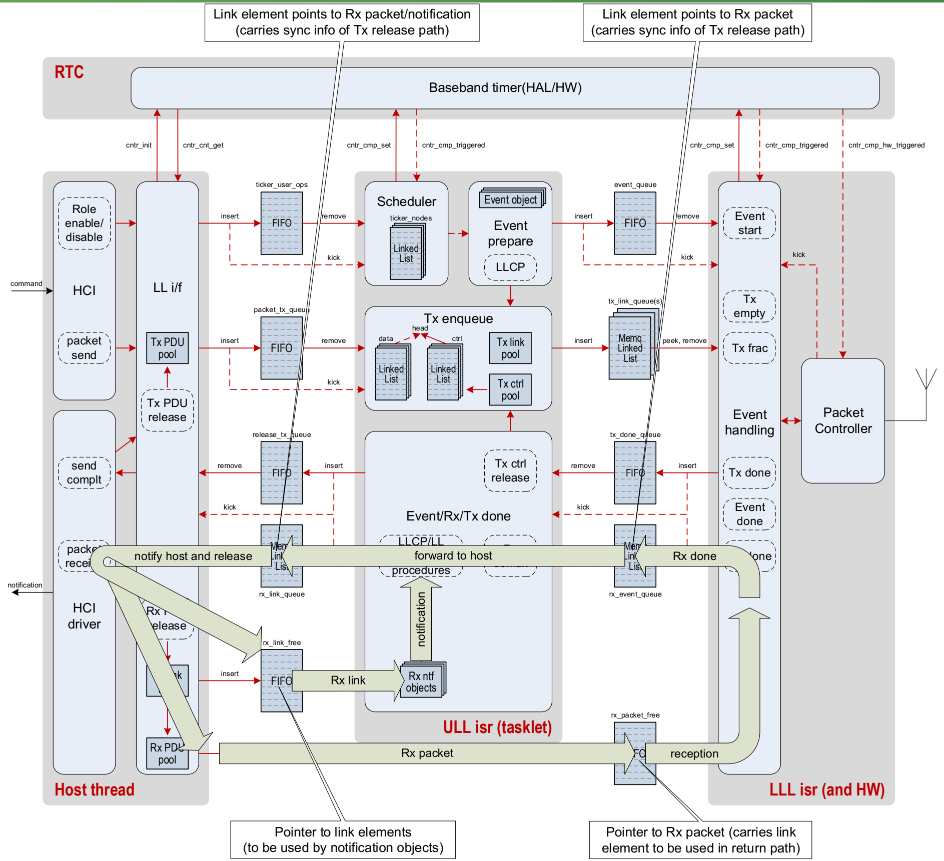
Pointer to event object (carries link element to be used in return path)

Link element points to event object

Data Path: Tx


Pointer to Tx packet
Holds Tx packets per role
Link element points to Tx packet (carries data/ctrl pool association)
RTC
Baseband timer(HAL/HW)
cntr_init
cntr_cnt_get
cntr_cmp_set
cntr_cmp_triggered
cntr_cmp_set
cntr_cmp_triggered
cntr_cmp_hw_triggered
ticker_user_ops
FIFO
insert
remove
kick
Scheduler
ticker_nodes
Linked List
Event object
Event prepare
LLCP
event_queue
FIFO
insert
remove
kick
Event start
kick
Role enable/ disable
HCI
command
LL i/f
packet_tx_queue
FIFO
send request
role enqueue
Tx enqueue
head
Linked List
Linked List
ctrl
Tx enqueue
tx_link_queue(s)
Memq Linked List
transmission
Tx empty
frac
Event handling
Packet Controller
link/ctrl release
kick
Tx PDU release
release_tx_queue
FIFO
notify host and release
send complete
forward to host
tx_done_queue
FIFO
Tx done
done
kick
kick
Event/Rx/Tx done
Event done
packet receive
remove
Memq Linked List
insert
rx_link_queue
remove
Memq Linked List
insert
rx_event_queue
Rx done
LLCP/LL control procedures
Rx demux
notification
HCI driver
Rx PDU release
rx_link_free
insert
FIFO
remove
Rx link pool
Rx ntf objects
Rx PDU pool
ULL isr (tasklet)
rx_packet_free
insert
FIFO
remove
Host thread
LLL isr (and HW)
Pointer to Tx packet
Pointer to Tx packet (carries link element to be freed + pool association)

Data Path: Rx



Link element points to Rx packet/notification (carries sync info of Tx release path)

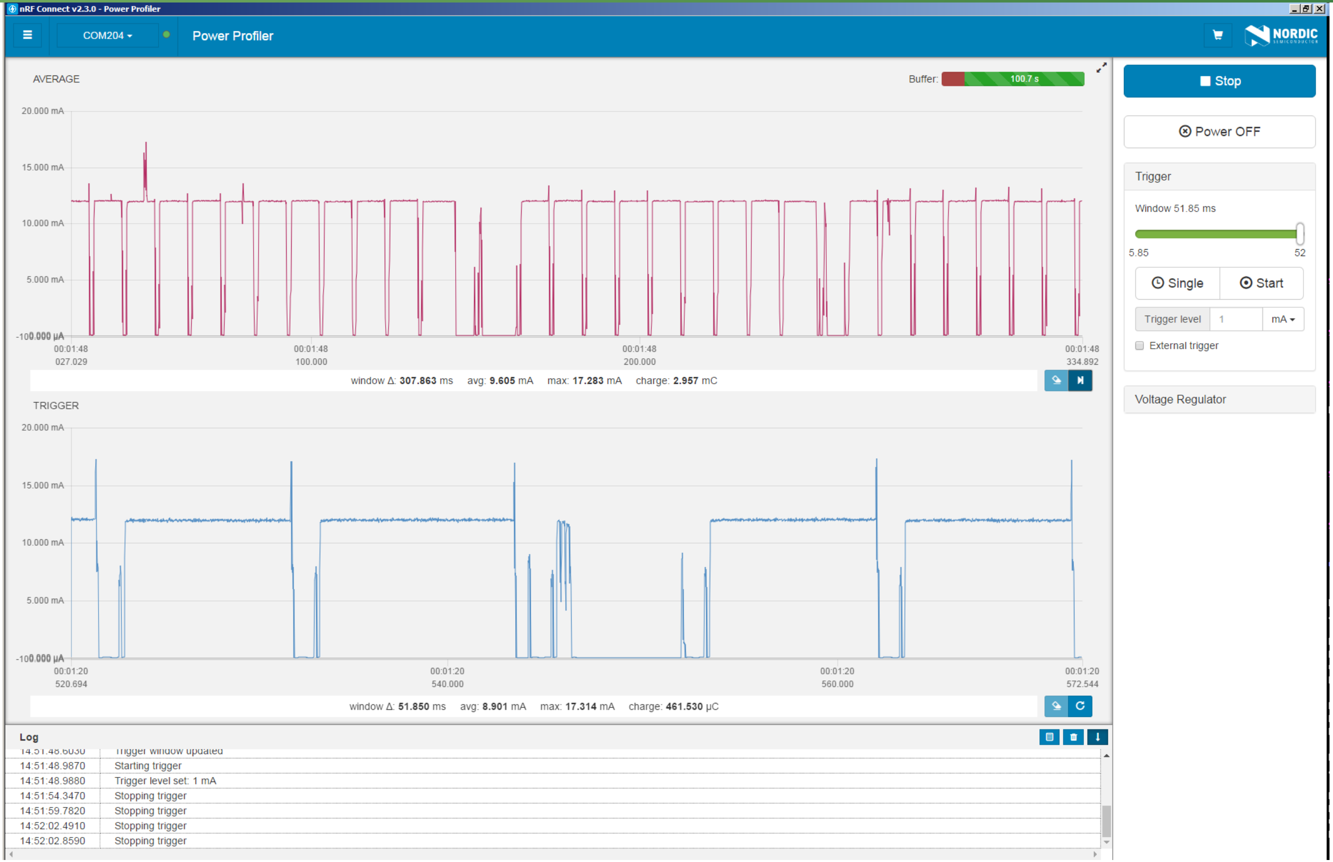
Link element points to Rx packet (carries sync info of Tx release path)

Pointer to link elements (to be used by notification objects)

Pointer to Rx packet (carries link element to be used in return path)

Demonstrations with Q&A

Zephyr Continous Scan with Advertising Event



window Δ: **307.863** ms avg: **9.605** mA max: **17.283** mA charge: **2.957** mC

window Δ: **51.850** ms avg: **8.901** mA max: **17.314** mA charge: **461.530** µC

Window 51.85 ms

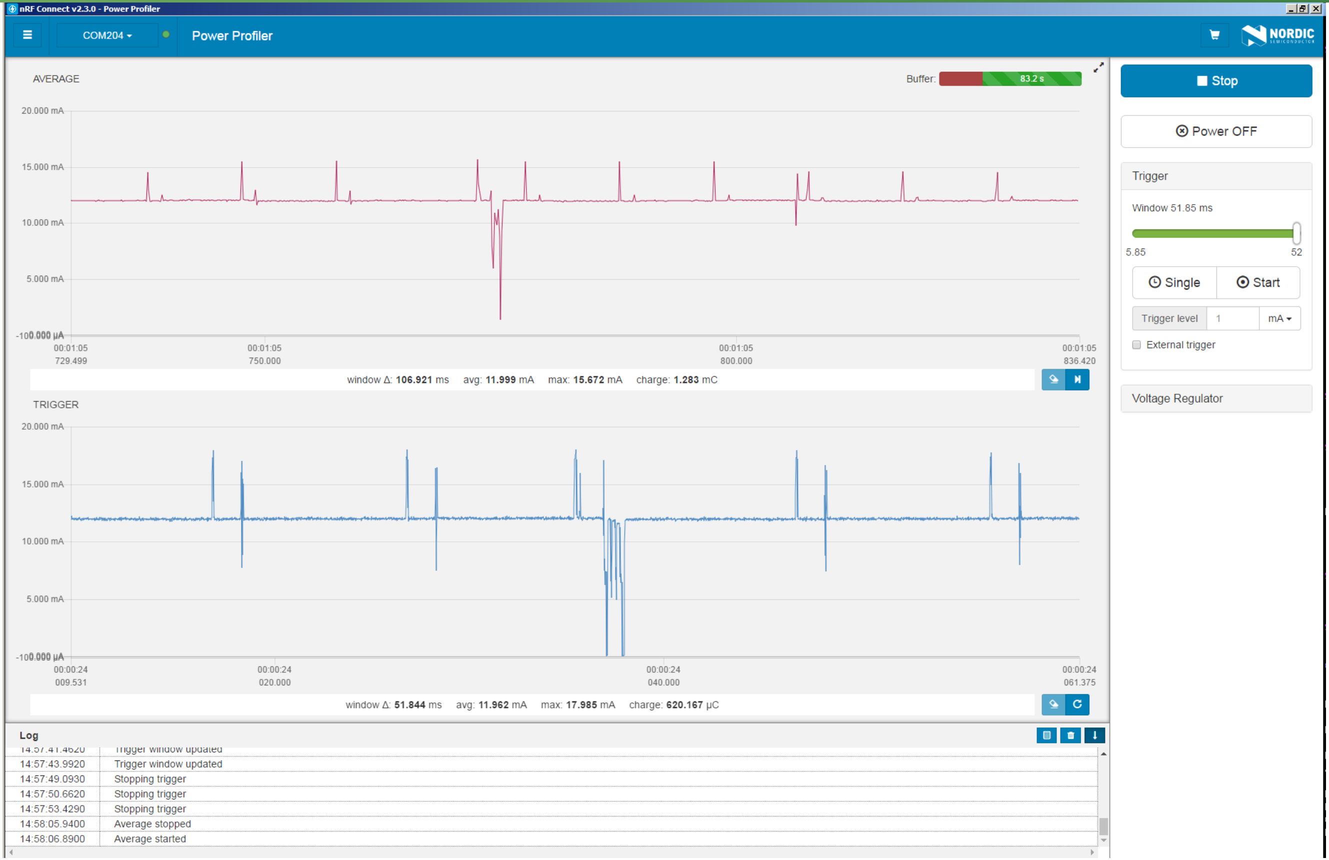
Trigger level 1 mA

☐ External trigger

```
14:51:48.6030    Trigger window updated
14:51:48.9870    Starting trigger
14:51:48.9880    Trigger level set: 1 mA
14:51:54.3470    Stopping trigger
14:51:59.7820    Stopping trigger
14:52:02.4910    Stopping trigger
14:52:02.8590    Stopping trigger
```

THE LINUX FOUNDATION

Zephyr Recycled Continous Scan with Advertising Event



window Δ: **106.921** ms avg: **11.999** mA max: **15.672** mA charge: **1.283** mC

window Δ: **51.844** ms avg: **11.962** mA max: **17.985** mA charge: **620.167** µC

Trigger

Window 51.85 ms

5.85 — 52

Trigger level: 1 mA

□ External trigger

```
14:57:41.4620  Trigger window updated
14:57:43.9920  Trigger window updated
14:57:49.0930  Stopping trigger
14:57:50.6620  Stopping trigger
14:57:53.4290  Stopping trigger
14:58:05.9400  Average stopped
14:58:06.8900  Average started
```

Improvement pipeline and resume

- Continuous events for continuous scanning and directed advertising
  - Are truly continuous with very low Radio Idle when switching Tx/Rx state or channels
  - Radio idle time: Min. 70us to Max. 300us
- Events extend into unreserved time space
- Reserved time space events pre-empt overlapping unreserved time space events
  - Pre-emptor is placed in a **pipeline** to perform the pre-emption just-in-time to the event's Radio start
- Pre-emptee event can decide to **resume** after pre-emptor

Thank You

Embedded Linux Conference

Europe

OpenIoTSummit

Europe

THE LINUX FOUNDATION