Bluetooth Low Energy System-on-Chip

SDDEC26-10: Open-Source Radio Microcontroller

Zane Salti, Aiden Han-Lindemyer, Parker Pederson, Tyler Bibus,
Akash Gojuru, Jackson Doyle, Seth Klaassen, Daniel Pytel

Project Motivation

Bluetooth Low Energy (BLE) is widely used in IoT, mobile, and embedded systems. However:

- Existing BLE chipsets are proprietary and closed-source
  - Internal controller and PHY (physical) designs are not accessible
- This limits research, education, and customization

Goal:

Develop a fully open-source, **fabricatable** BLE SoC (System-on-Chip).

Project Requirements

Functional Requirements:

- Design must be able to interact with other Bluetooth Low Energy devices
  - Must hit BLE 4.0 Specs (Design Doc Sec. 2.1.1)
- Device must be fabricatable using the open source Sky130 Process Design Kit (PDK)
- Final device must be open source
  - Hardware and Software

User Requirements:

- Documentation must be clear
- Device must be delivered with a documented plan for ChipForge testing

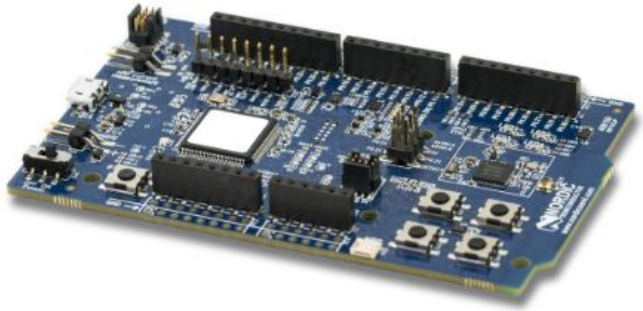
Bluetooth Low Energy Device Solutions Comparison

HackRF One

- Software Defined not Hardware
- Processor and DSP are not open source
- Bluetooth controls are not implemented in hardware

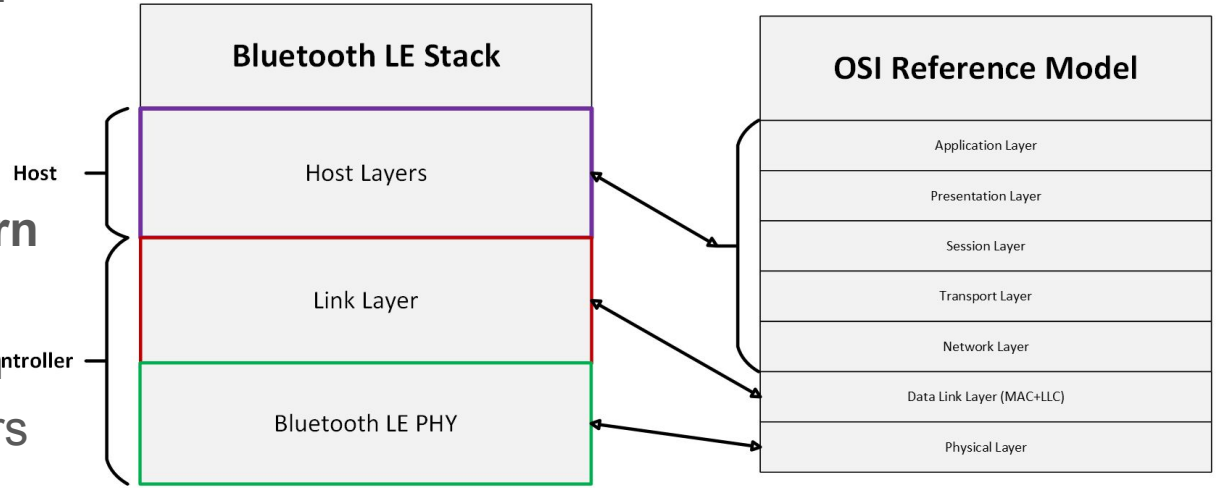
nRF52 DK

- Utilizes Nordic SoC to drive bluetooth in a manner similar to our design
- Nordic SoC is not open source



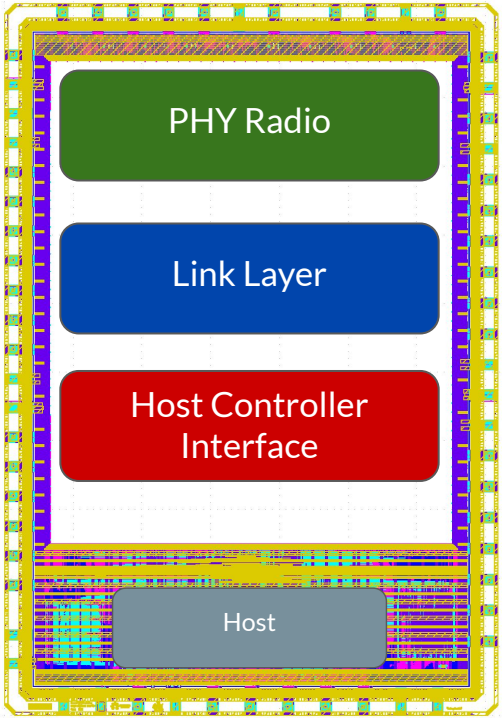
Design Context: Bluetooth Low Energy

- Bluetooth Low Energy
  - Lower data rates than typical Bluetooth.
- Bluetooth can be divided into these layers
- Our **major design concern** is the *controller* portion
  - Software libraries can be used for *host* layers

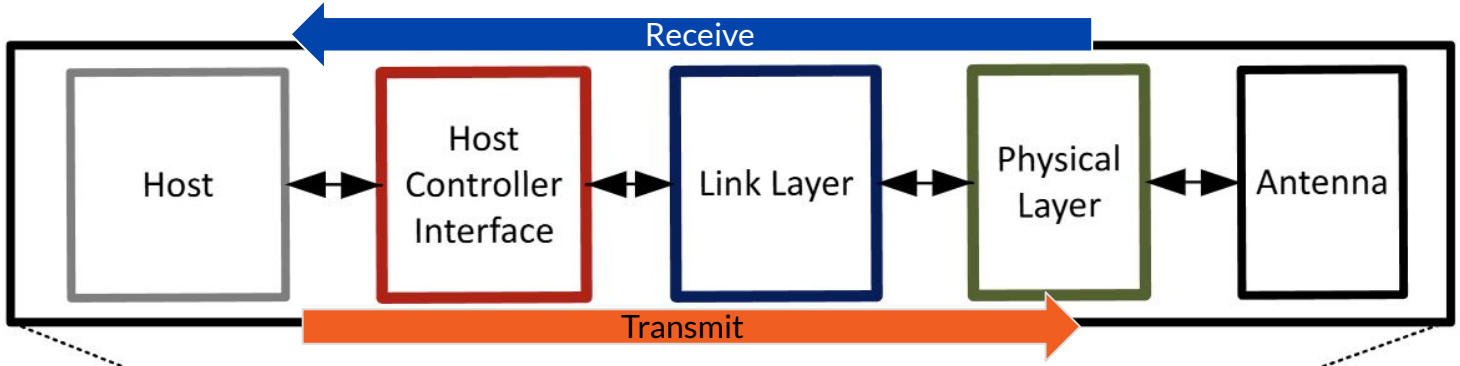


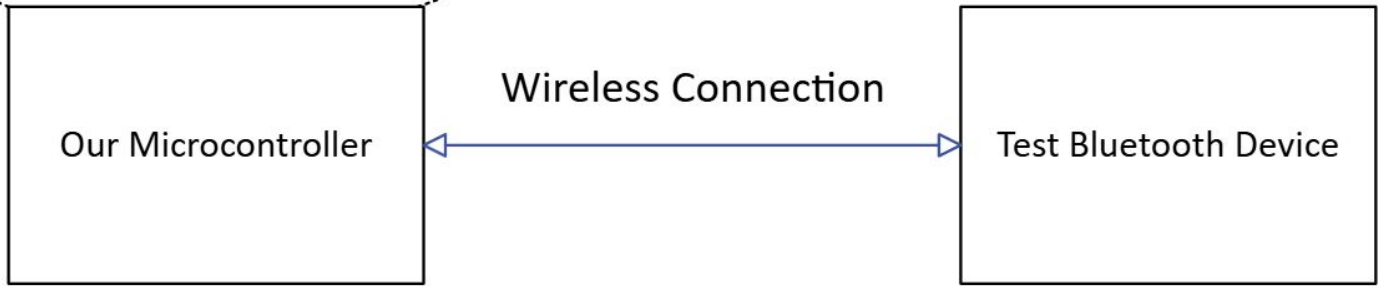
Design Context: SoC

- Skywater 130nm Process
- Working on the Caravel template
  - Management Core (to be used as Host) given to us
- Host and Controller all on one System on Chip
  - Host running on a RISC-V Core
  - Our Link Layer (LL) as custom hardware (digital)
  - Our PHY as custom hardware (analog—mostly)

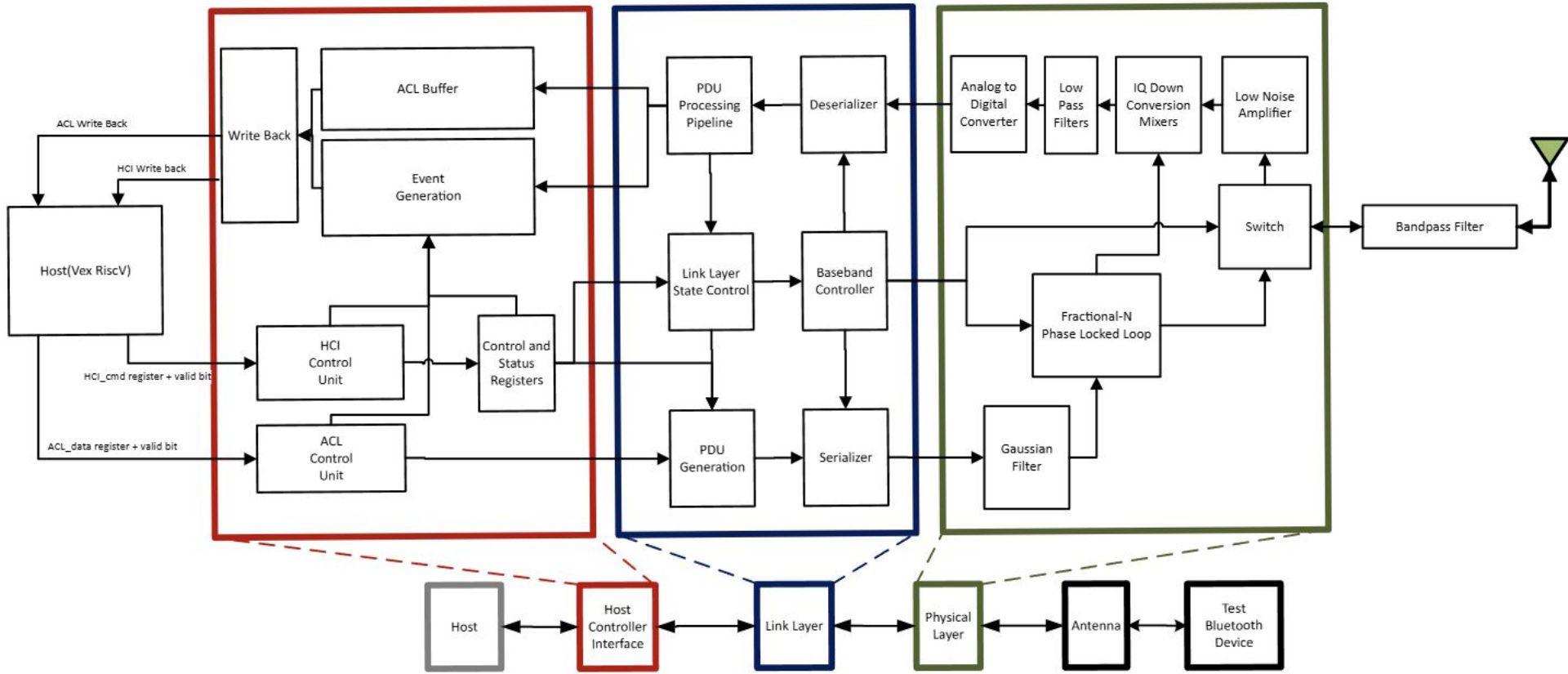


Top Level Overview

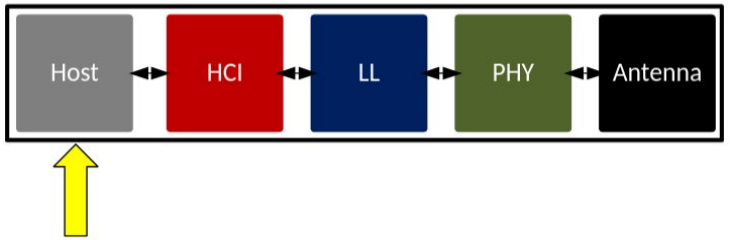




Dataflow


ACL Write Back
HCI Write back
Host(Vex RiscV)
HCI_cmd register + valid bit
ACL_data register + valid bit
Write Back
ACL Buffer
Event Generation
HCI Control Unit
Control and Status Registers
ACL Control Unit
PDU Processing Pipeline
Deserializer
Link Layer State Control
Baseband Controller
PDU Generation
Serializer
Analog to Digital Converter
Low Pass Filters
IQ Down Conversion Mixers
Low Noise Amplifier
Switch
Bandpass Filter
Fractional-N Phase Locked Loop
Gaussian Filter
Host
Host Controller Interface
Link Layer
Physical Layer
Antenna
Test Bluetooth Device

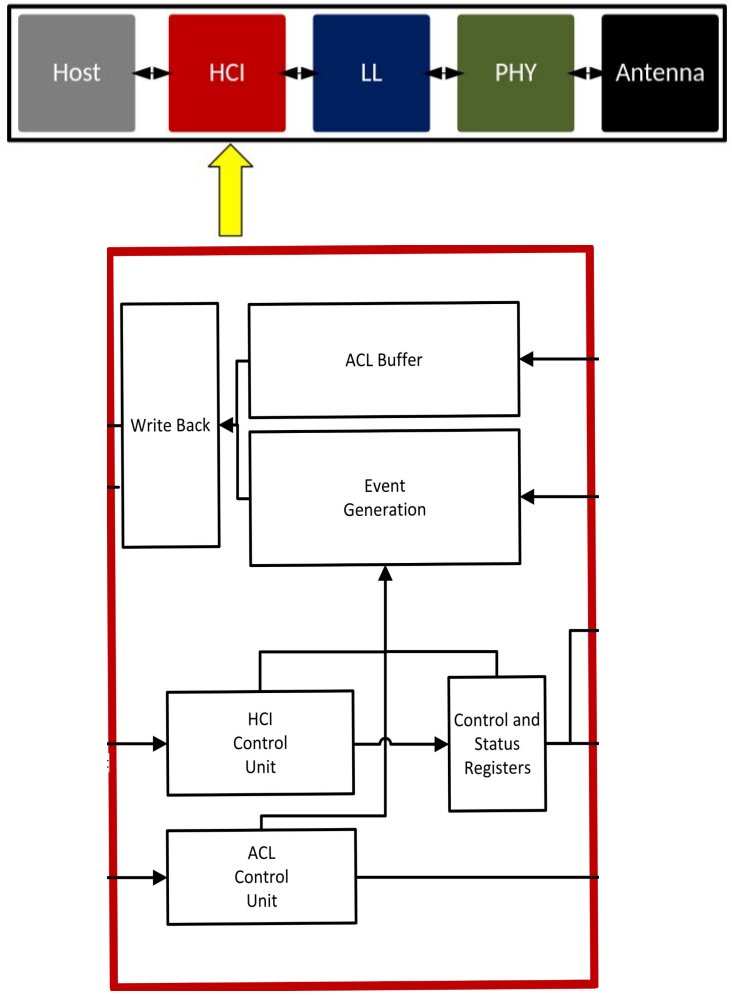
Host



- Open-source Zephyr BLE host will provide all required host protocol layers.
- HCI Drivers will need to be modified by us to work with our controller

Zephyr Host Protocol Layers
https://docs.zephyrproject.org/latest/services/connectivity/bluetooth/bluetooth-le-host.html#id1

Host Controller Interface



HCI Control Unit:

- Register connected to the host via wishbone
- Verify that the commands are correct

Event Generator:

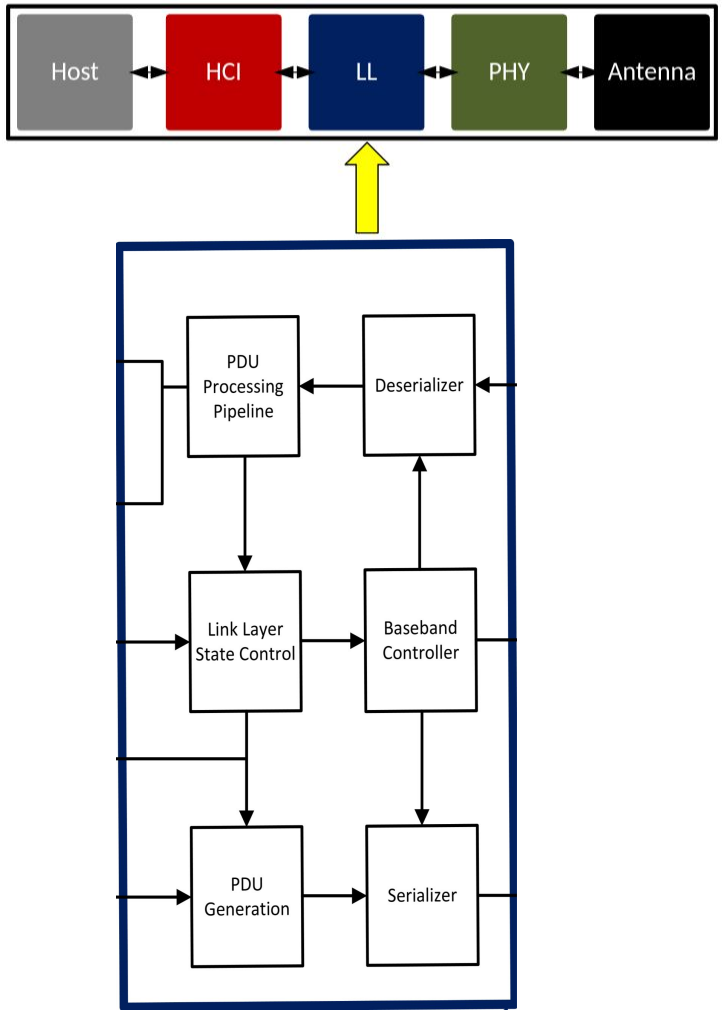
- Take in control signals
- Format return events to be sent to the host

Design Doc Section 4.3.2

Link Layer

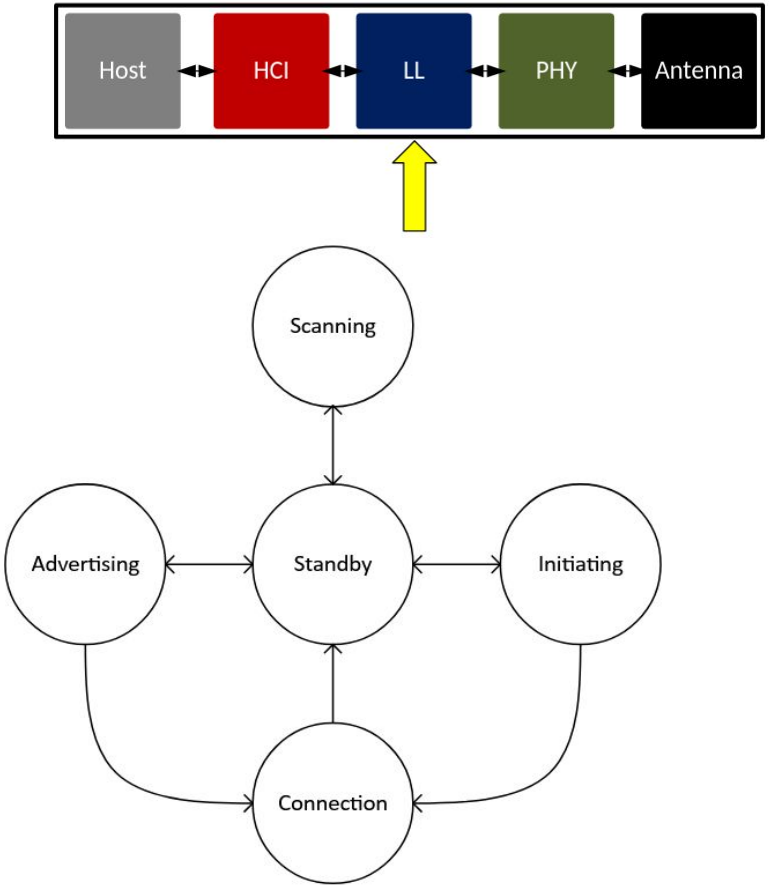
- **PDU Generation:** Builds outgoing packets (advertising or data)
- **Serializer/Deserializer:** Performs CRC, (de)whitening, and (de)serializes into a bitstream
- **PDU processing Pipeline:** Decodes and check incoming packets (CRC)
- **Baseband Controller:** handles timing and channel selection

Design Doc 4.3.3



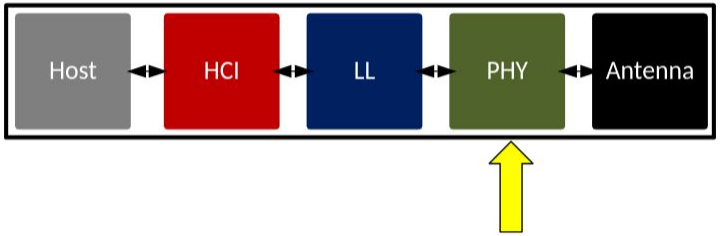
Link Layer States

- **Standby:** Controller is not sending or receiving data.
- **Advertising:** Controller sends advertising packets on BLE channels 37, 38, and 39.
- **Scanning:** Controller scans BLE channels 37, 38, and 39 for advertising devices.
- **Initializing:** Controller found an advertising device, and attempts to establish a connection.
- **Connection:** Controller enters a connected state, exchanging Protocol Data Units (PDUs) while channel hopping in accordance with BLE Protocol.

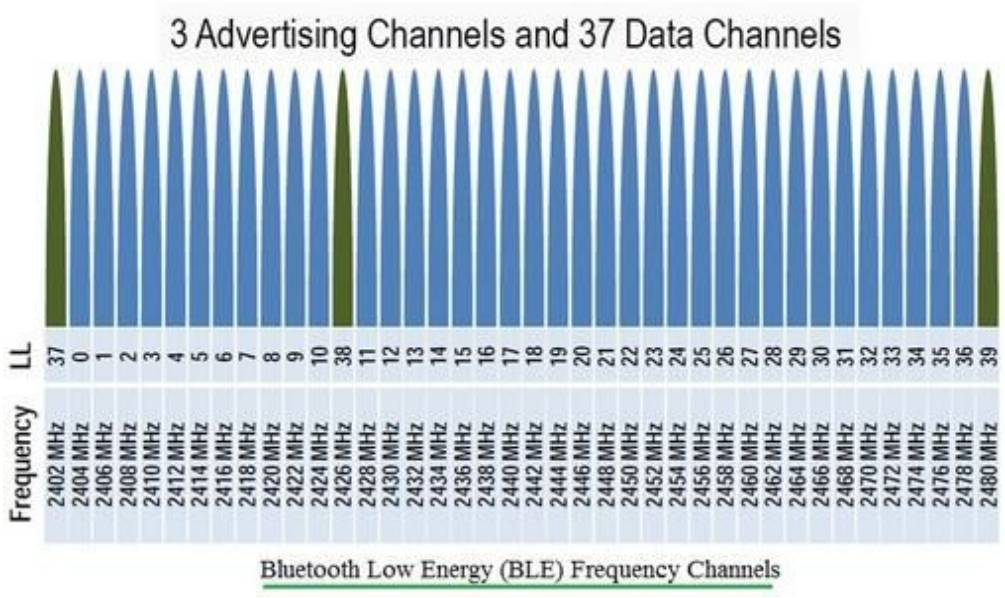


Link Layer State Machine

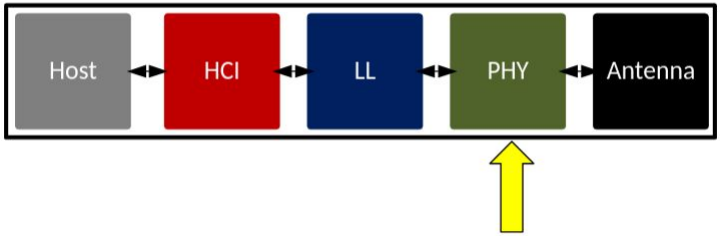
Modulation & Modulation Schemes



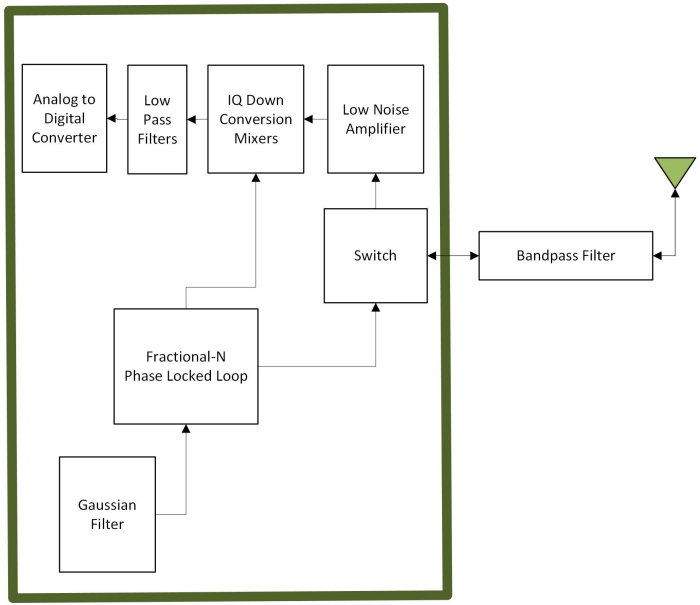
- **LE 1M** is where our project is scoped, which is 1 Million symbols/s
- Frequency Shift Keying is an encoding where symbols are encoded as positive or negative frequency deviations from the center of the channel
- BLE uses Gaussian Frequency Shift Keying (**GFSK**), a type of FSK
  - A gaussian pulse shaping filter is ran on the frequency deviations



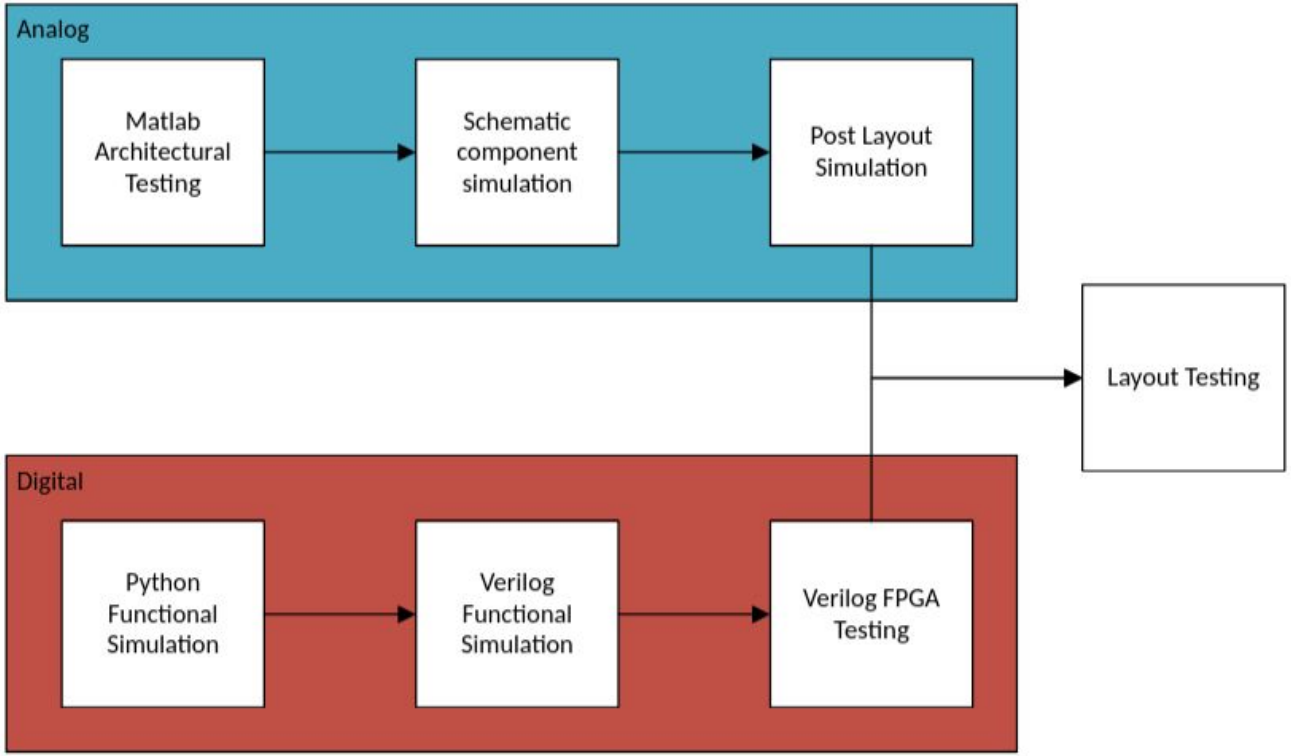
PHY Radio Architecture



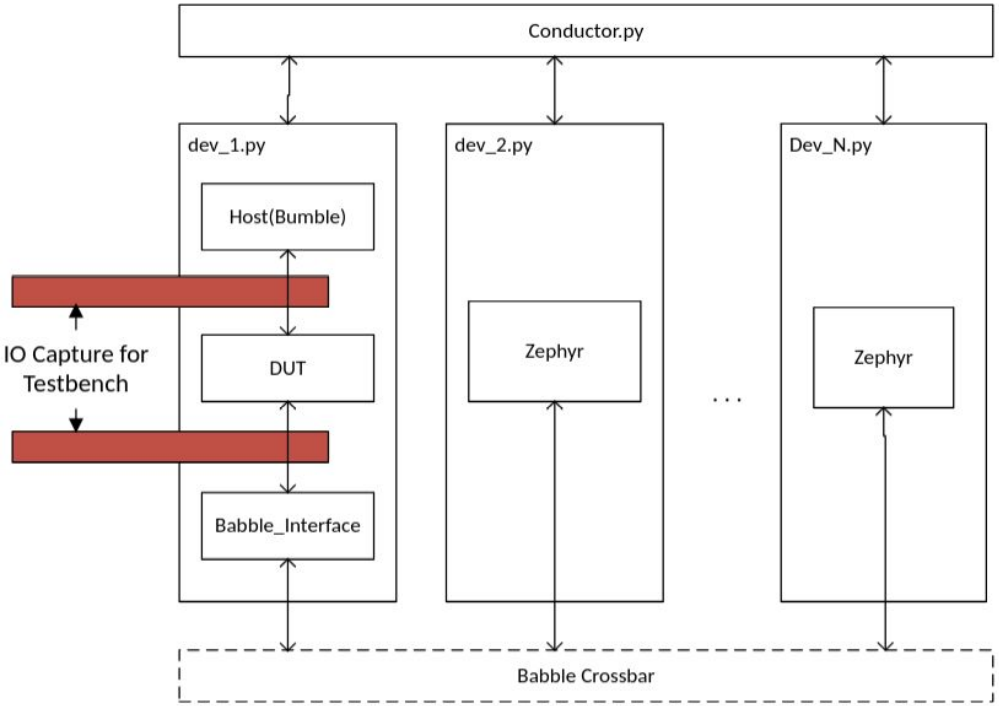
- BLE (and so our architecture) is **Half Duplex**
- Symbols are sent via modulating the **Fractional-N PLL**
- IQ Downconversion Mixers are used to track whether the received signal is positive or negative of the channel center (which the PLL should be set to in receiving)
- **2.4 GHz - 2.483 GHz** bandpass filter off chip to keep signals in BLE range



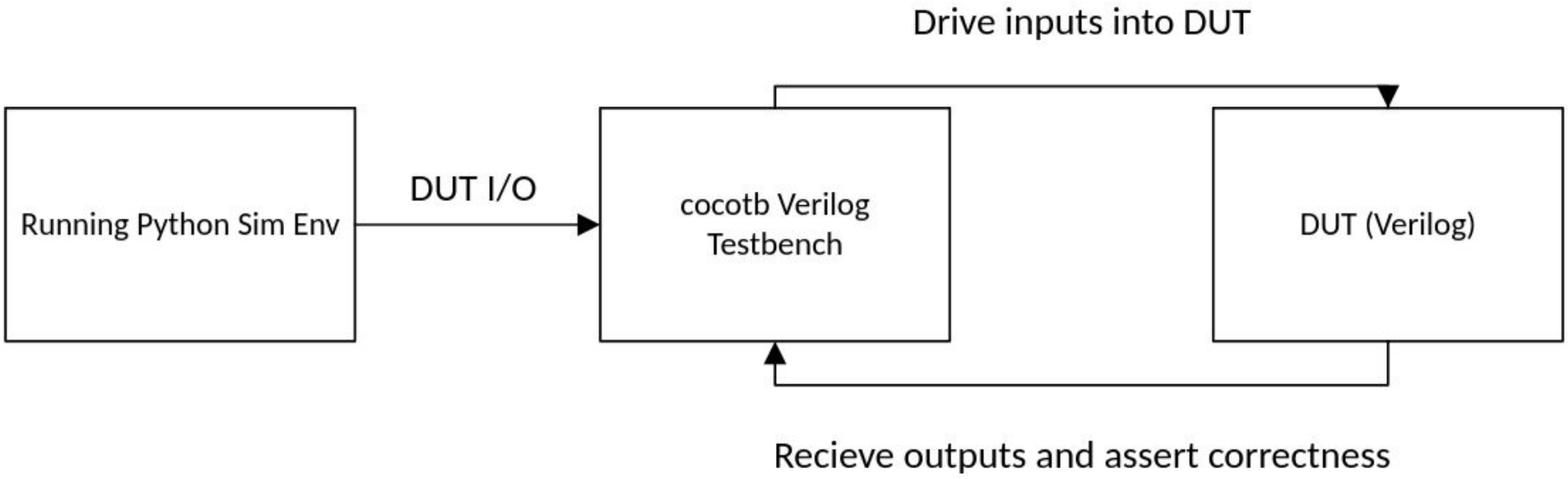
Testing


Analog
Matlab Architectural Testing
Schematic component simulation
Post Layout Simulation
Layout Testing
Digital
Python Functional Simulation
Verilog Functional Simulation
Verilog FPGA Testing

Virtual Simulation Environment

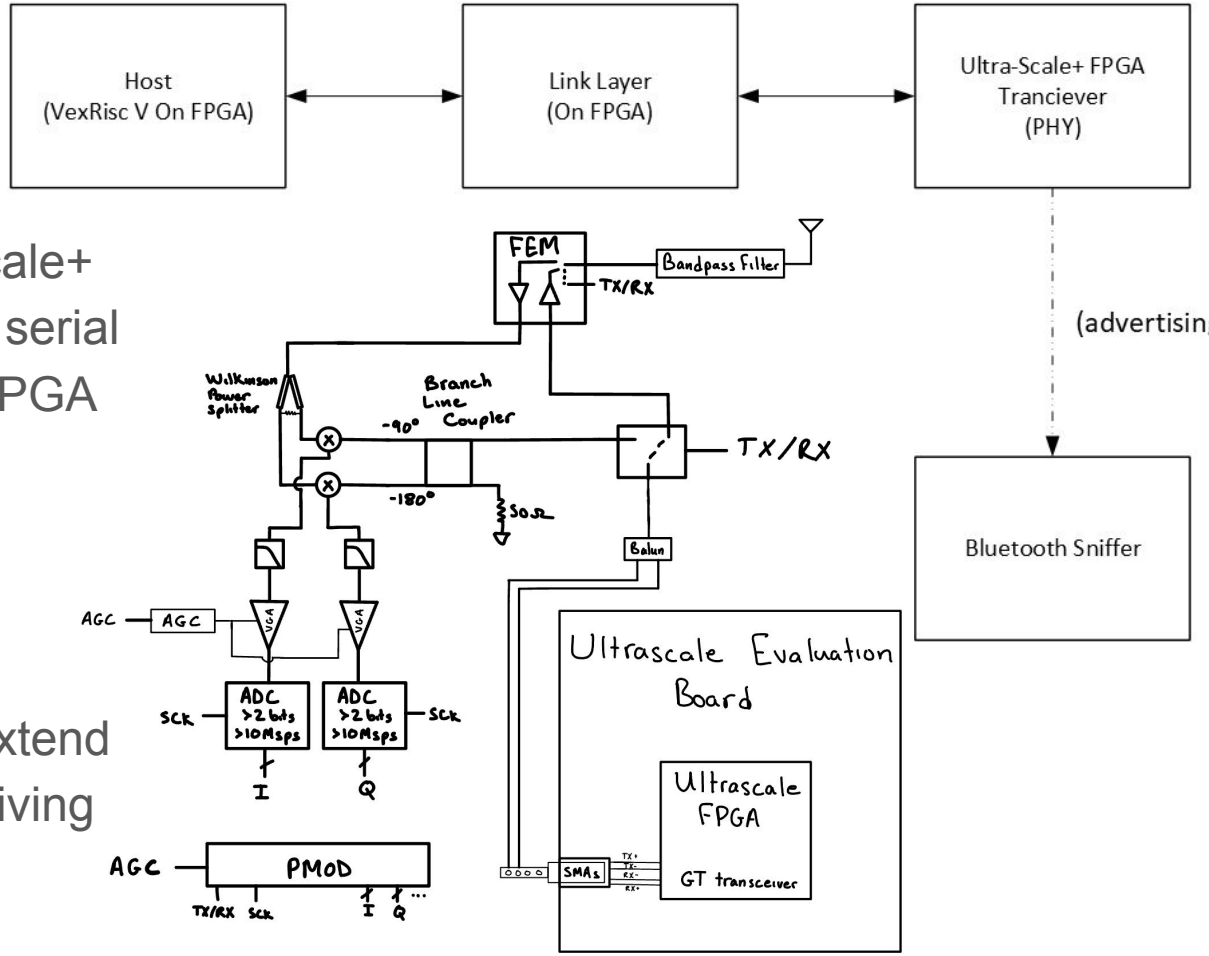


Verilog Functional Simulation



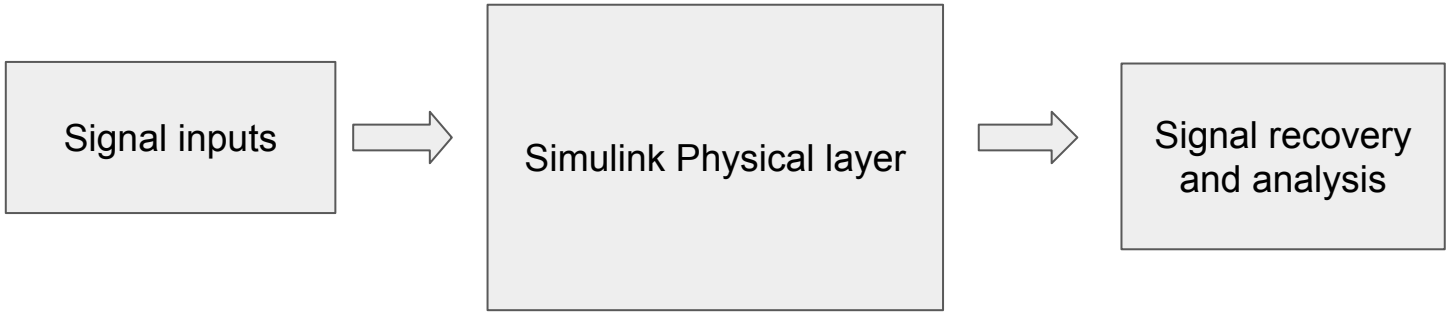
FPGA Testing

- Utilizing the UltraScale+ FPGA's high speed serial transceiver for an FPGA based radio
- Proposed PCB to extend capabilities for receiving



Matlab Architectural Simulation

- Proof of physical layer architectural integrity
- Simulink equipped with robust RF/Mixed signal blocksets
- Allows for noise analysis prior to testing within the analog VLSI toolflow



Schematic Simulation

Schematics are created using Xschem. In Xschem simulations can be run to test functionality.

Cadence is a closed source tool, but can import the SkyWater 130nm PDK.

cadence®

Post Layout Testing

- DRC: Design Rule Checks
  - Validates our layout and checks if it will be possible to fabricate in the given process
- LVS: Layout vs. Schematic
  - Compares the layout to the schematic and gives you a list of differences if there is any
- Post-Layout Parasitic Extraction
  - Processes and returned the parasitic capacitances that are created from your layout

Final Tests and Integration

- Final full layout with combined Digital + Analog
- Post-Layout verification
- ChipFoundry Tapeout

Current results

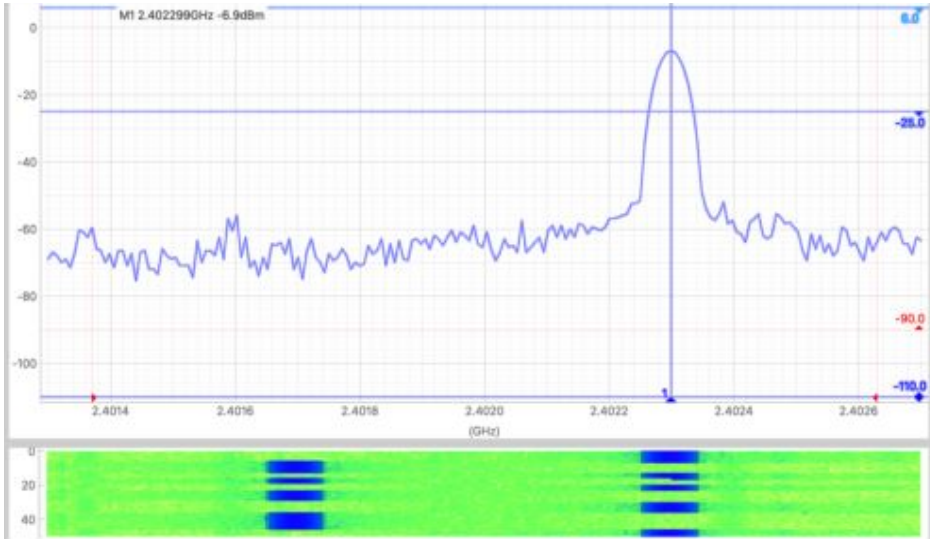
- Digital simulation environment successfully advertise and scan to and from a Zephyr controller using our architecture.

- Serializer (including CRC and whitening) hardware description (SystemVerilog) written and tested using real-world BLE data.

- Analog PLL architecture mostly decided, off chip inductor/VCO determined to likely be a necessity.

FPGA Testing Results

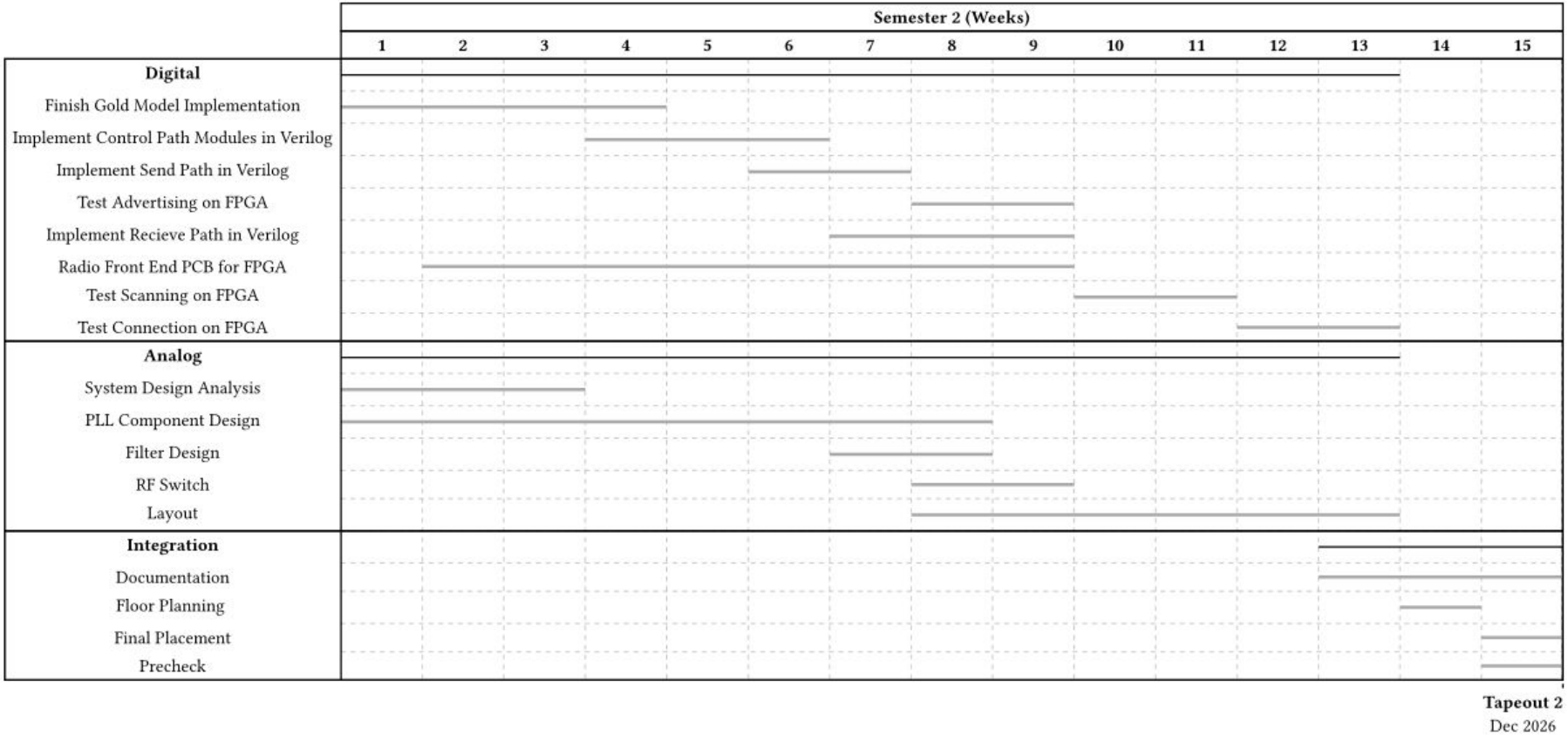
- FSK has currently been achieved
- A gaussian pulse shaping filter has been designed and implemented as a lookup table in hardware (not used yet)



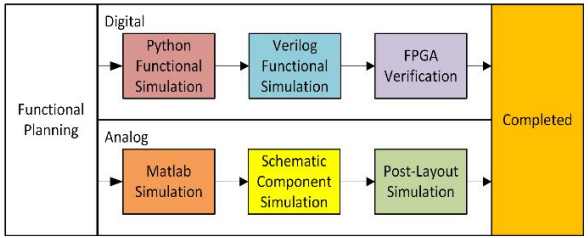
Risks & Mitigation

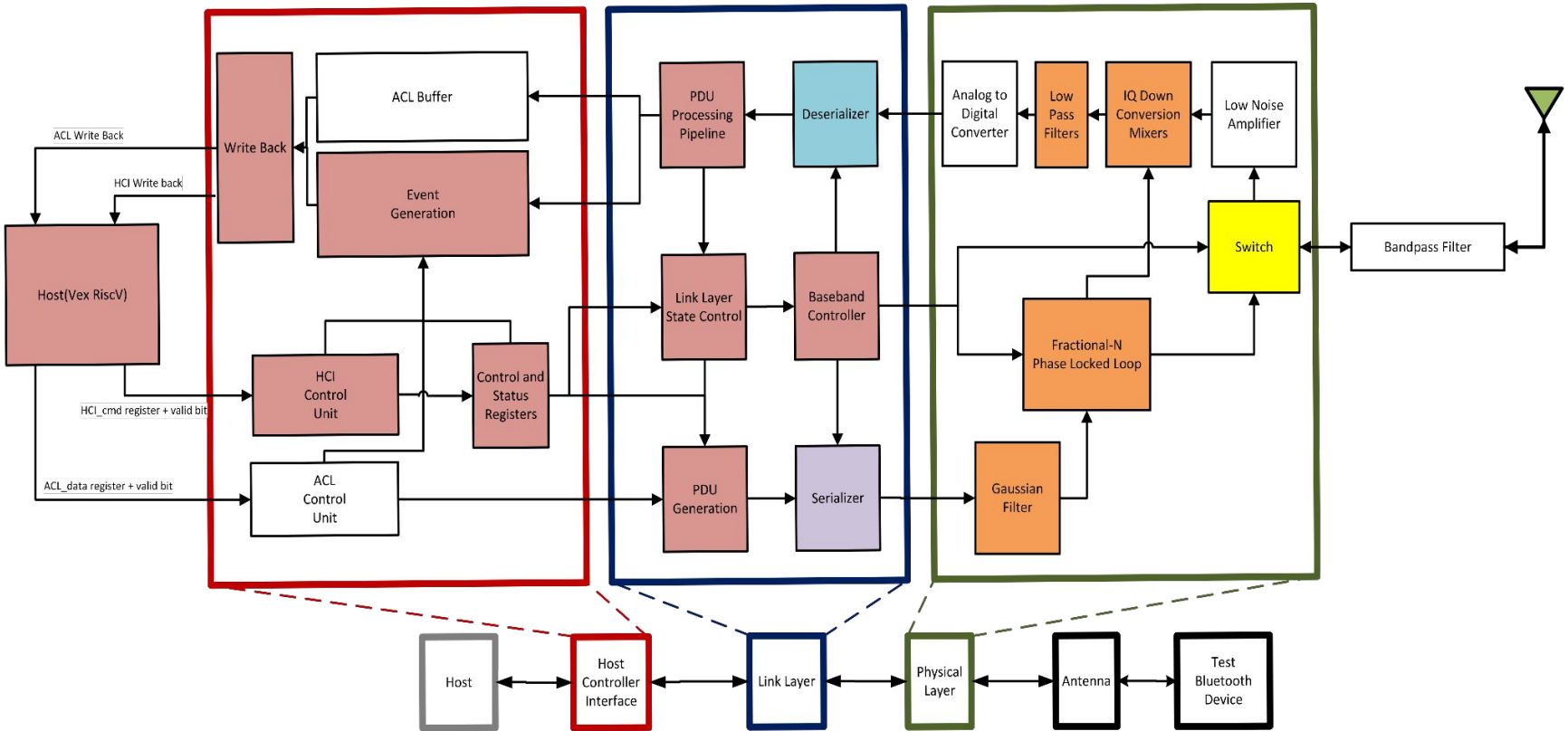
Risk	Severity	Mitigation Plan
On chip inductor proves to have bad characteristics	High	Move inductor off chip and add ports
BLE Protocol Non-compliance	Medium	Make FPGA test interact with real BLE device to show compliance
Parasitic simulation takes too long to run	High	Utilize ETG VM for accelerating simulations
Digital pipeline has a deadlock condition	Low	Gold standard model provides a non-locking pipeline

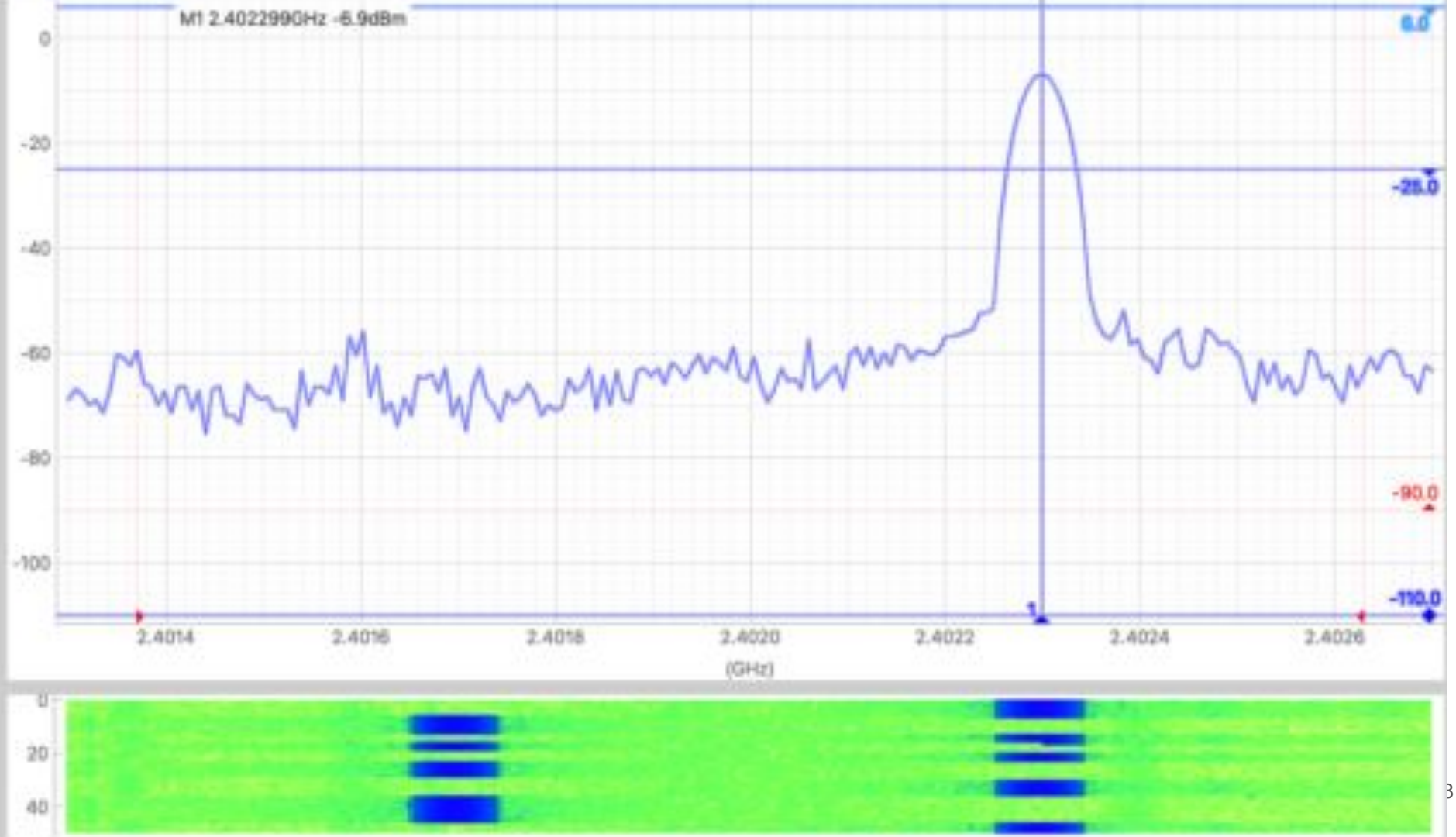
Next Semester Planning

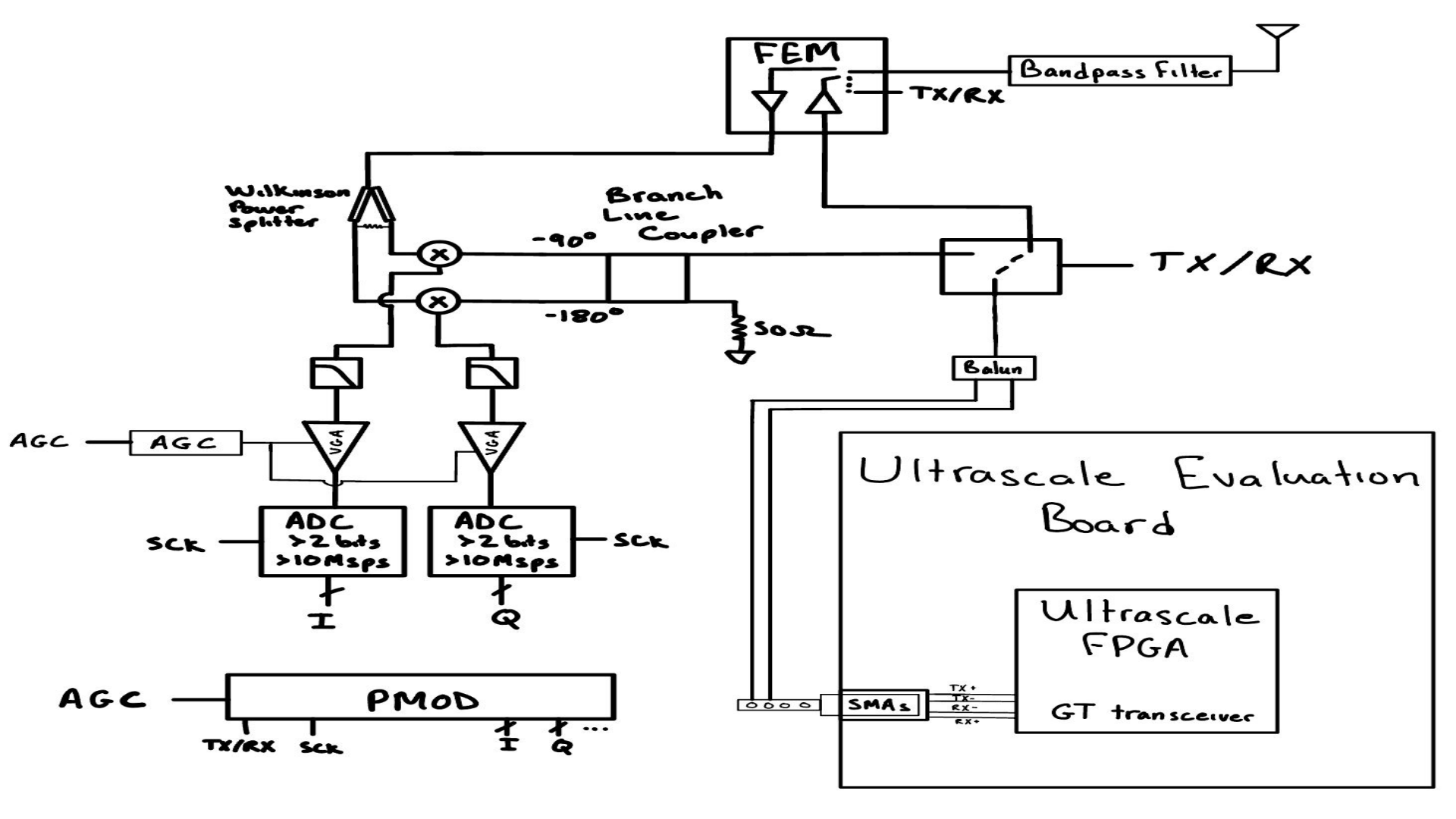


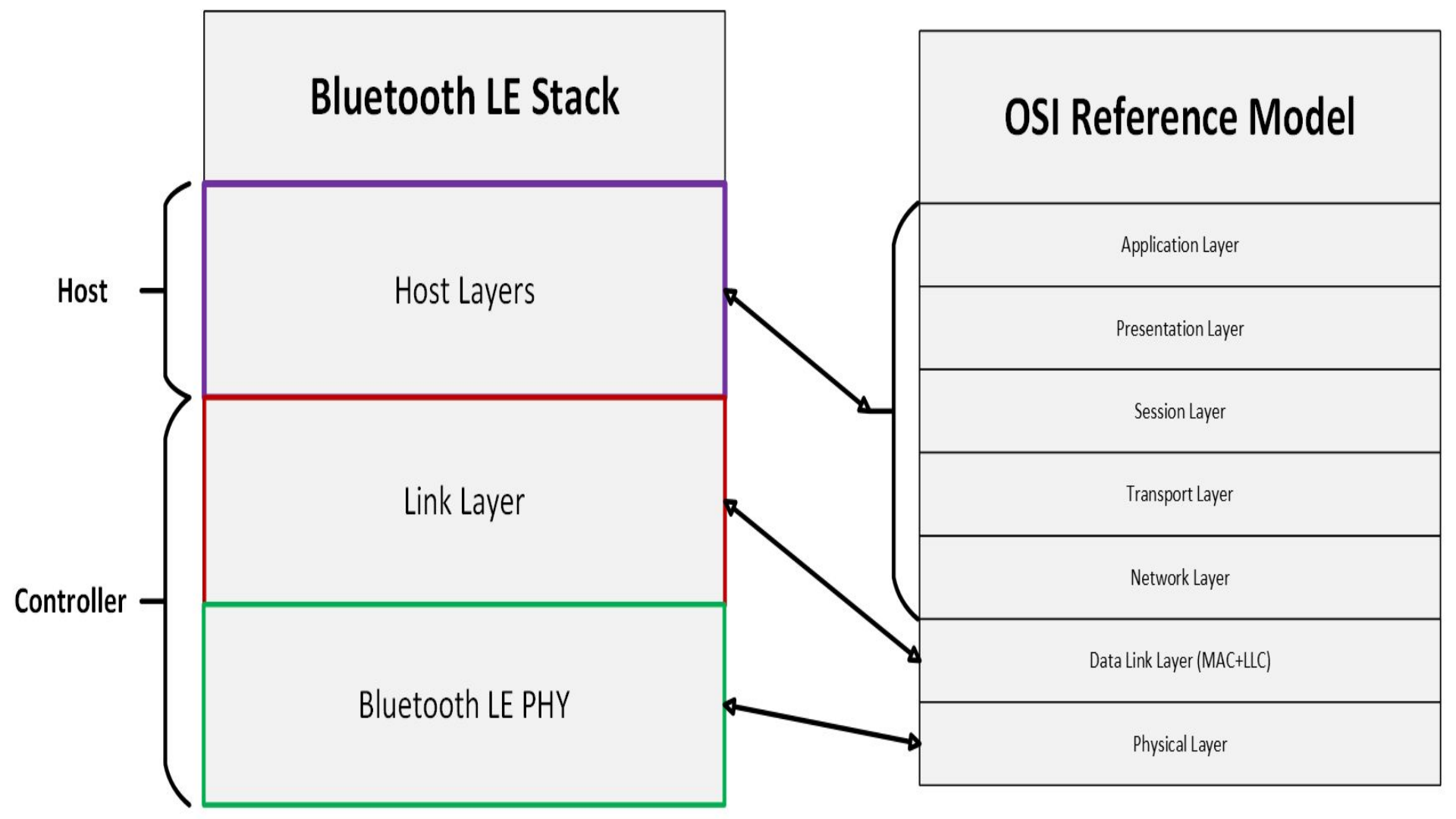
Status


Functional Planning
Digital
Python Functional Simulation
Verilog Functional Simulation
FPGA Verification
Analog
Matlab Simulation
Schematic Component Simulation
Post-Layout Simulation
Completed


ACL Write Back
HCI Write back
Write Back
ACL Buffer
Event Generation
Host(Vex RiscV)
HCI_cmd register + valid bit
HCI Control Unit
Control and Status Registers
ACL_data register + valid bit
ACL Control Unit
PDU Processing Pipeline
Deserializer
Link Layer State Control
Baseband Controller
PDU Generation
Serializer
Analog to Digital Converter
Low Pass Filters
IQ Down Conversion Mixers
Low Noise Amplifier
Switch
Bandpass Filter
Fractional-N Phase Locked Loop
Gaussian Filter
Host
Host Controller Interface
Link Layer
Physical Layer
Antenna
Test Bluetooth Device


M1 2.4022990Hz -6.9dBm
0
-20
-40
-60
-80
-100
6.0
-25.0
-90.0
-110.0
2.4014
2.4016
2.4018
2.4020
2.4022
2.4024
2.4026
(GHz)
0
20
40


FEM
Bandpass Filter
TX/RX
Wilkinson Power Splitter
Branch Line Coupler
-90°
-180°
50Ω
TX/RX
Balun
AGC
AGC
VGA
VGA
ADC >2 bits >10Msps
ADC >2 bits >10Msps
SCK
SCK
I
Q
Ultrascale Evaluation Board
Ultrascale FPGA
GT transceiver
SMAs
TX+
TX-
RX-
RX+
AGC
PMOD
TX/RX
SCK
I
Q
...


Bluetooth LE Stack
Host
Controller
Host Layers
Link Layer
Bluetooth LE PHY
OSI Reference Model
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer (MAC+LLC)
Physical Layer