ECE 445: Senior Design Lab – Spring 2019

Passive Aircraft Radar

Team 5 : Rushik Desai, Benjamin Du & Kyle Rogers

Professor : Professor Michael Oelze

TA : Kyle Michal

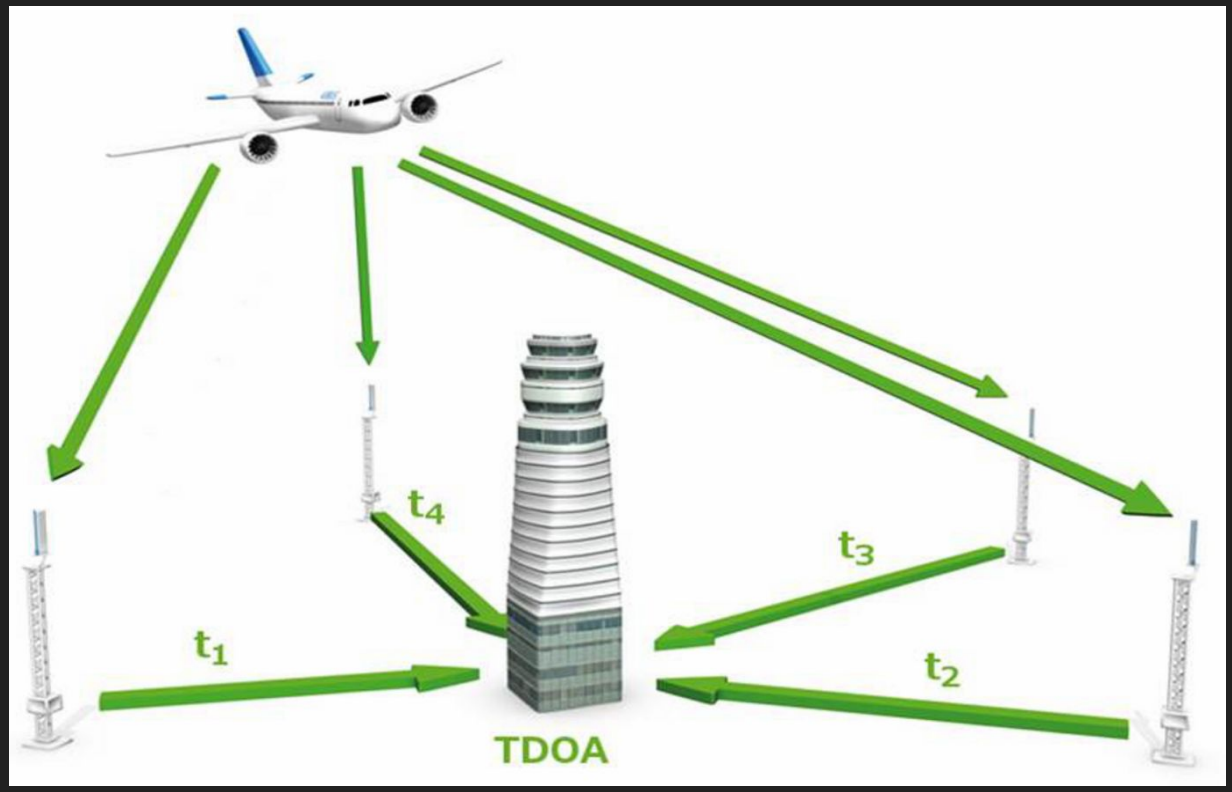
Sponsor : Professor Kirill Levchenko

Problem Statement

- Automatic Dependent Surveillance-Broadcast (ADS-B) is a system in which aircraft broadcast data into the air for tracking purposes
- Data typically consists of GPS position, and can be received by ground stations and other aircraft
- ADS-B is vulnerable to spoofing [1]

Solution

- Create a receiver network
- Each receiver should be capable of creating a timestamp when it receives the transponder signal
- Timestamps can be used in a Time Delay of Arrival (TDOA) calculation in order to calculate an aircraft’s position
- Rely ONLY on the time of signal reception rather than the signal data



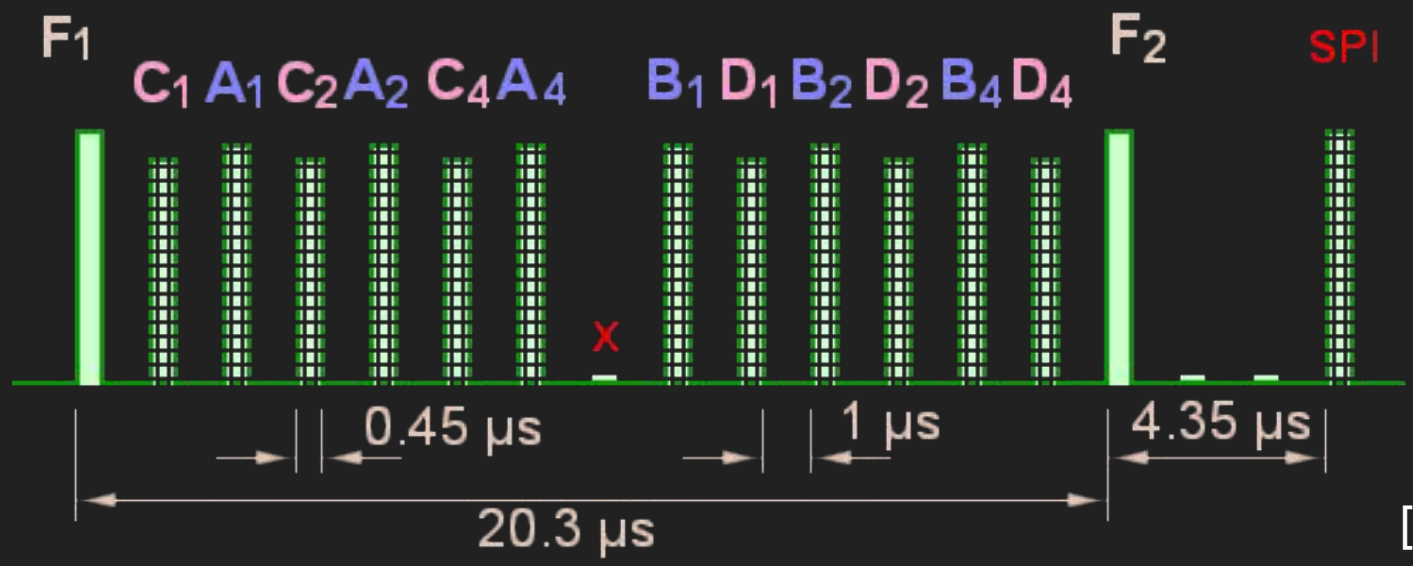
Project Objectives

- Capture and demodulate transponder signal
- Estimate aircraft position using TDOA
- Generate timestamp per capture event
  - Synchronize with common time reference
- Power design using Power over Ethernet (PoE)
  - IEEE 802.3af PoE standard [2]
- Create a low-cost design (under $100)

Design

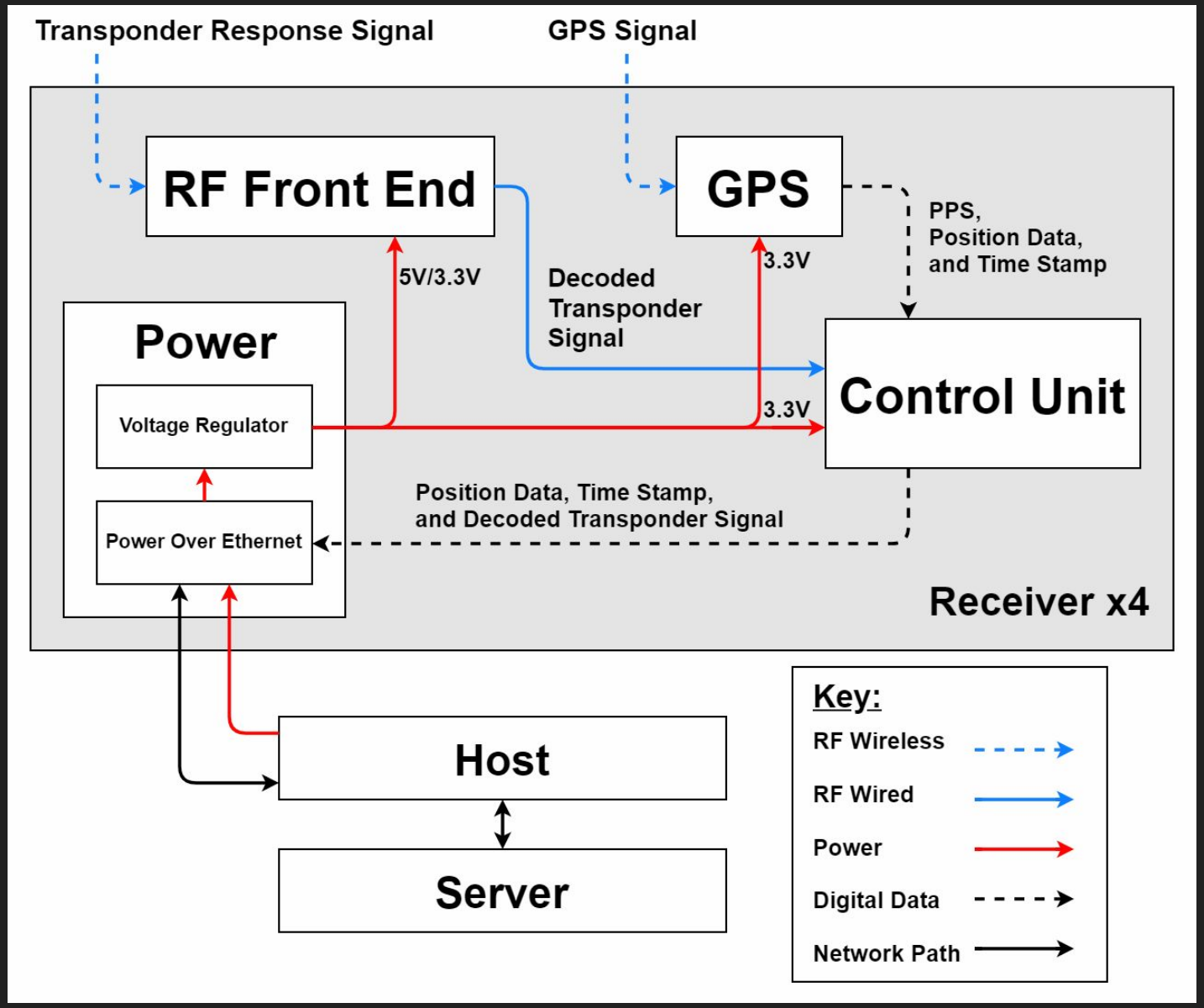
Aircraft Transponder Signal

- Modulation scheme: on/off keying
- Carrier frequency: 1090 MHz
- Period: 1.45 μs
- Pulse width: 0.45 μs

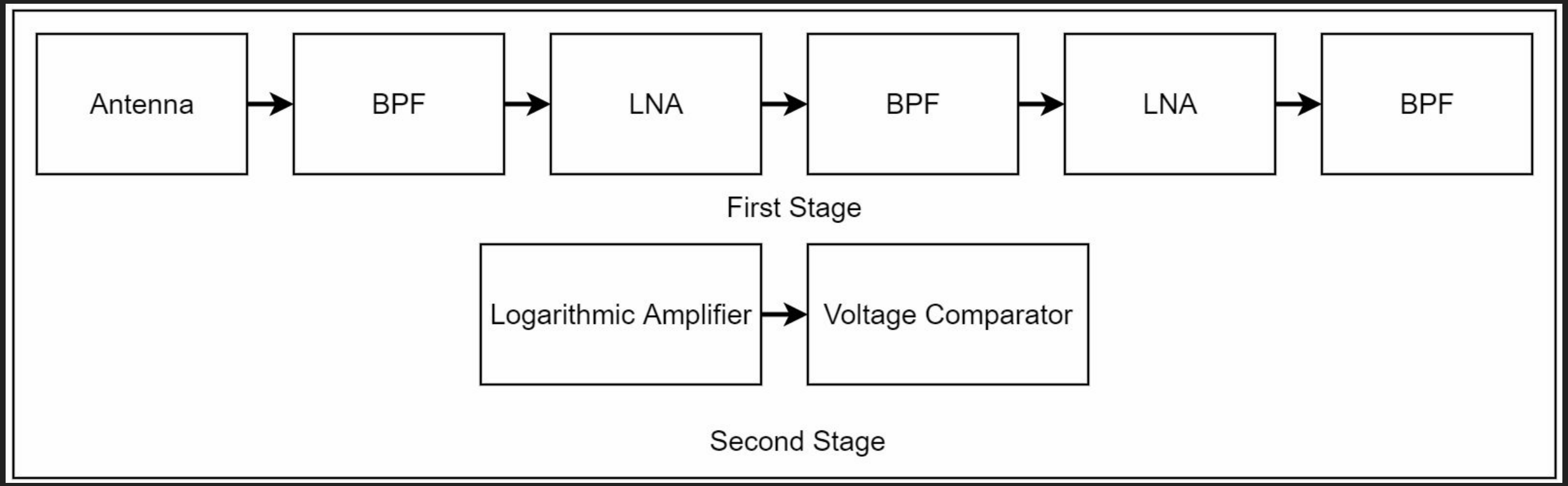


[3]

High-Level Diagram



RF Front End Block Diagram



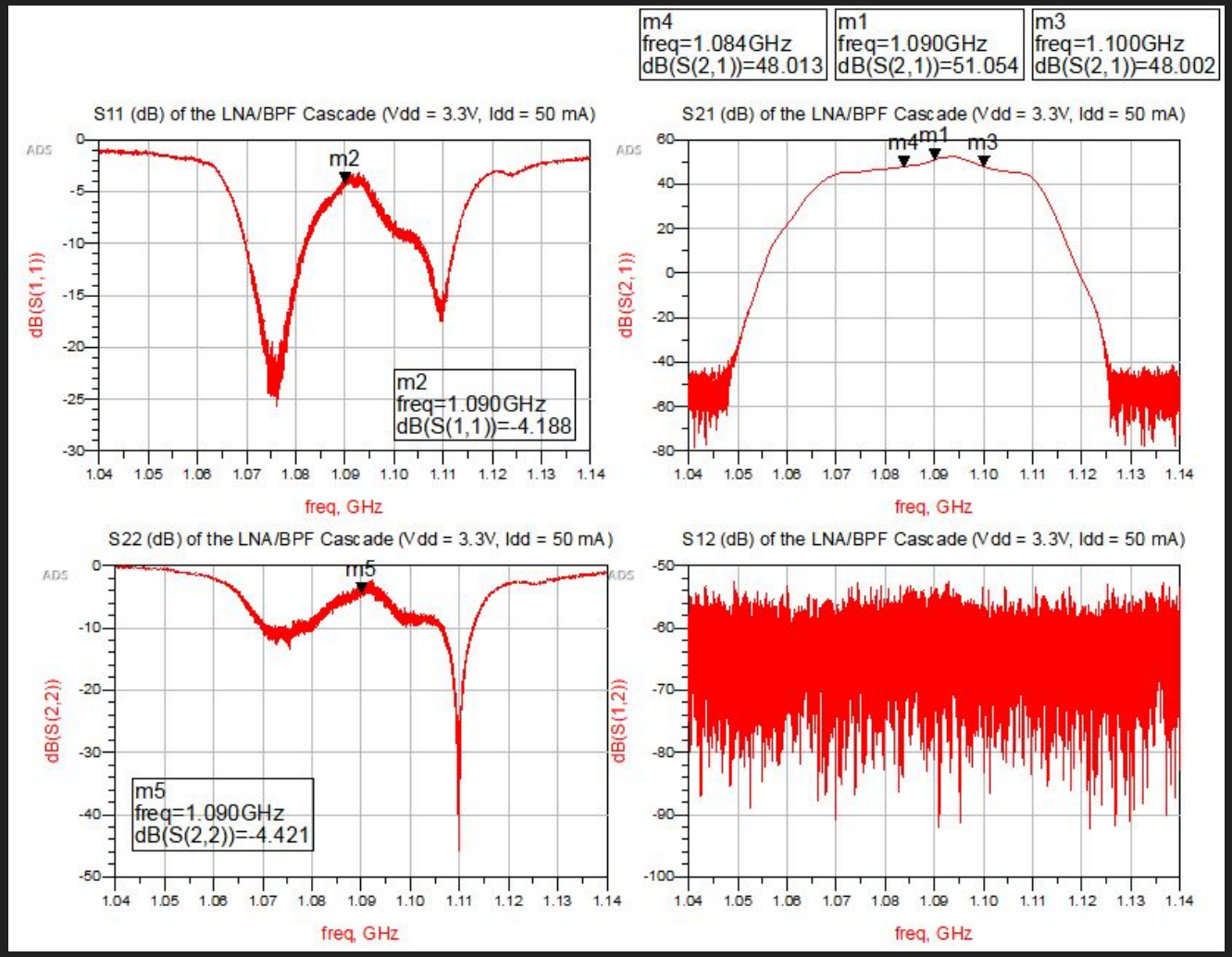
Received Power Calculation

- $G_T = G_R = 1$
- $R = 12$ km
- $P_T = 250$ W [4]
- $\lambda = 0.275$ m at 1090 MHz

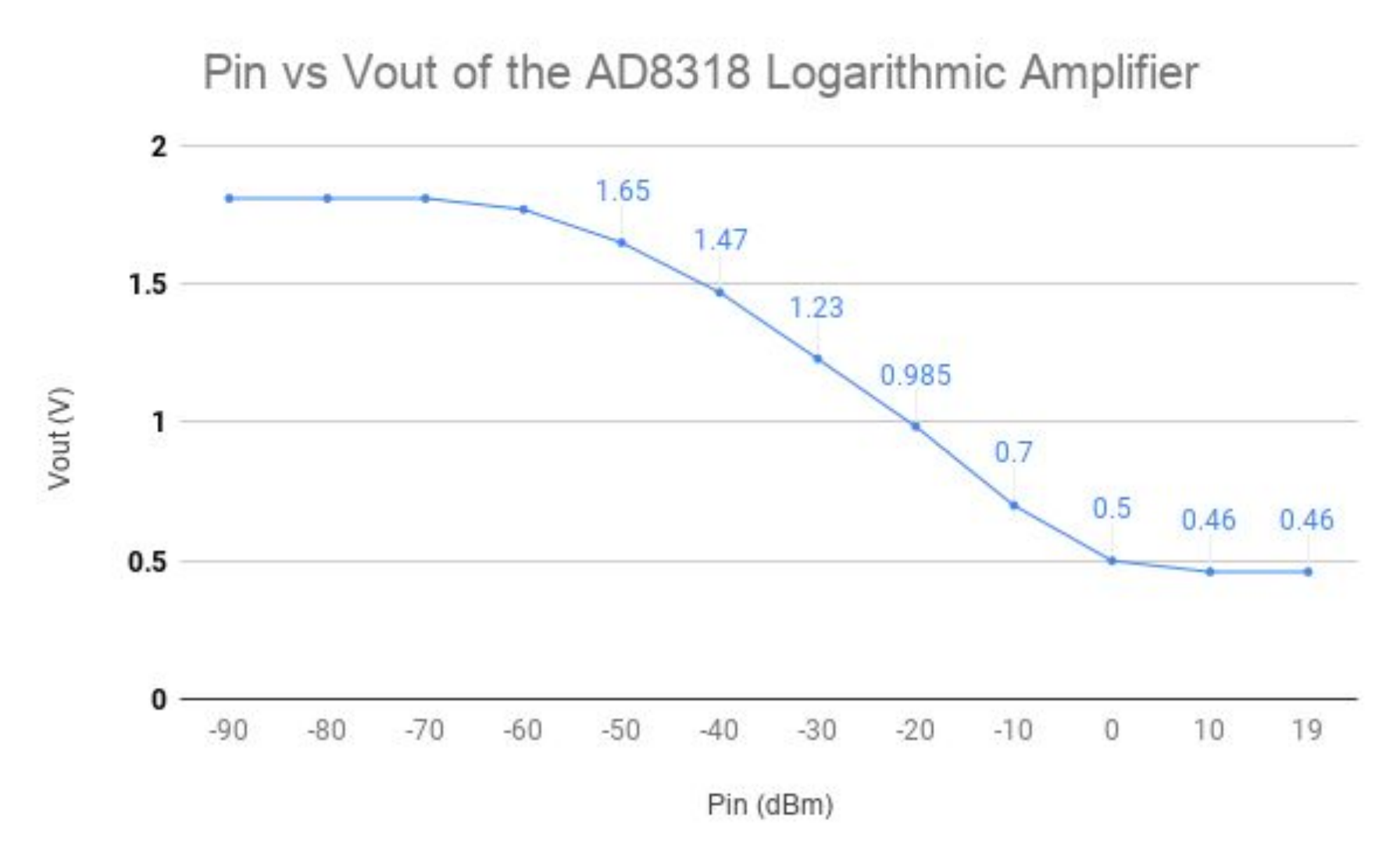
- Received power is about -60 dBm
  - -60 dBm when right above receiver
  - -63 dBm when at an angle of 45^o

$$P_R = \frac{G_T G_R \lambda^2}{(4\pi R)^2} P_T$$

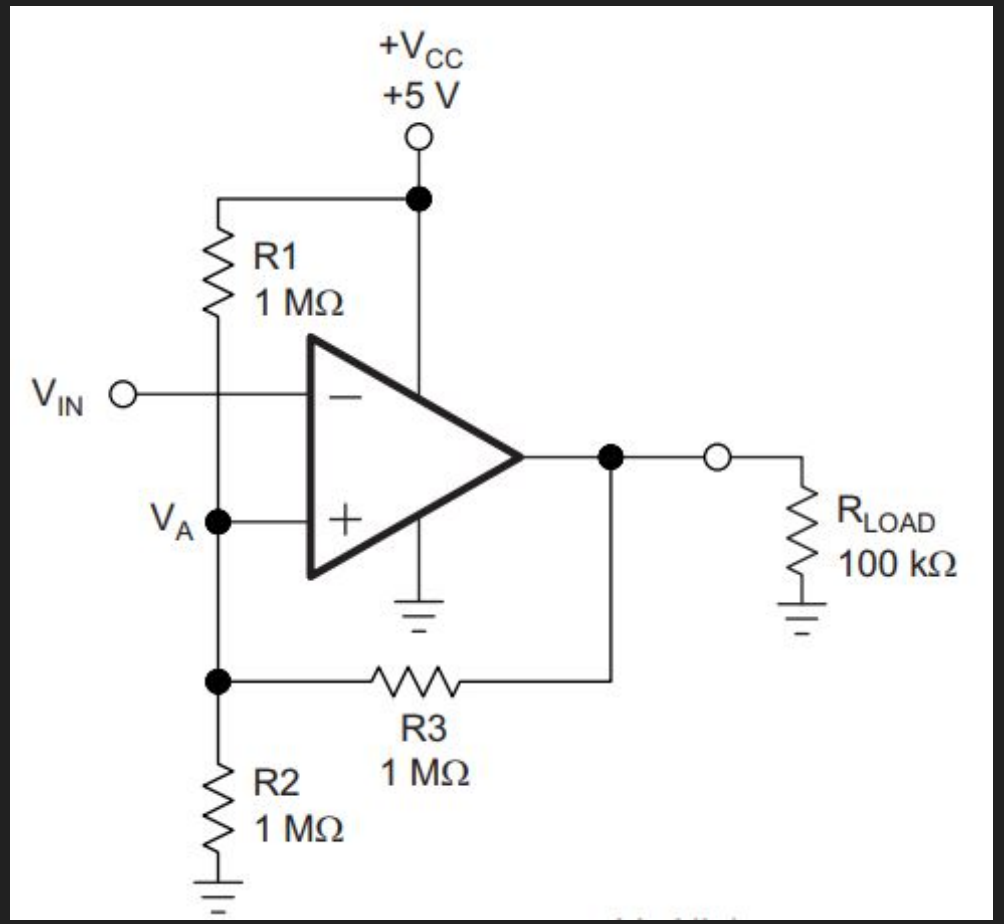
RF Front End Results & Analysis (First Stage)



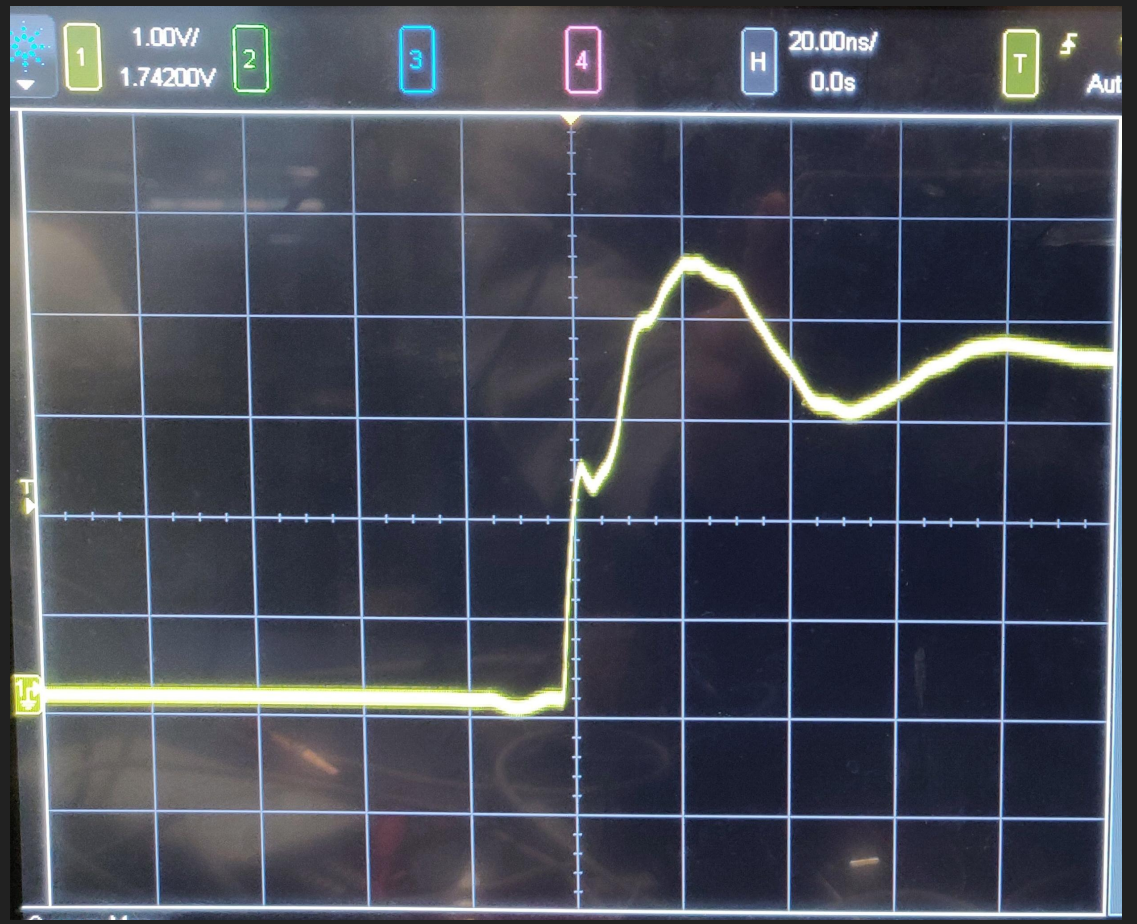
RF Front End Results & Analysis (Second Stage)



RF Front End Results & Analysis (Comparator)



TLV3201 in Inverting Configuration with Hysteresis [5]



TLV3201 Response to a 689.655 kHz Square Wave
(50% Duty Cycle)

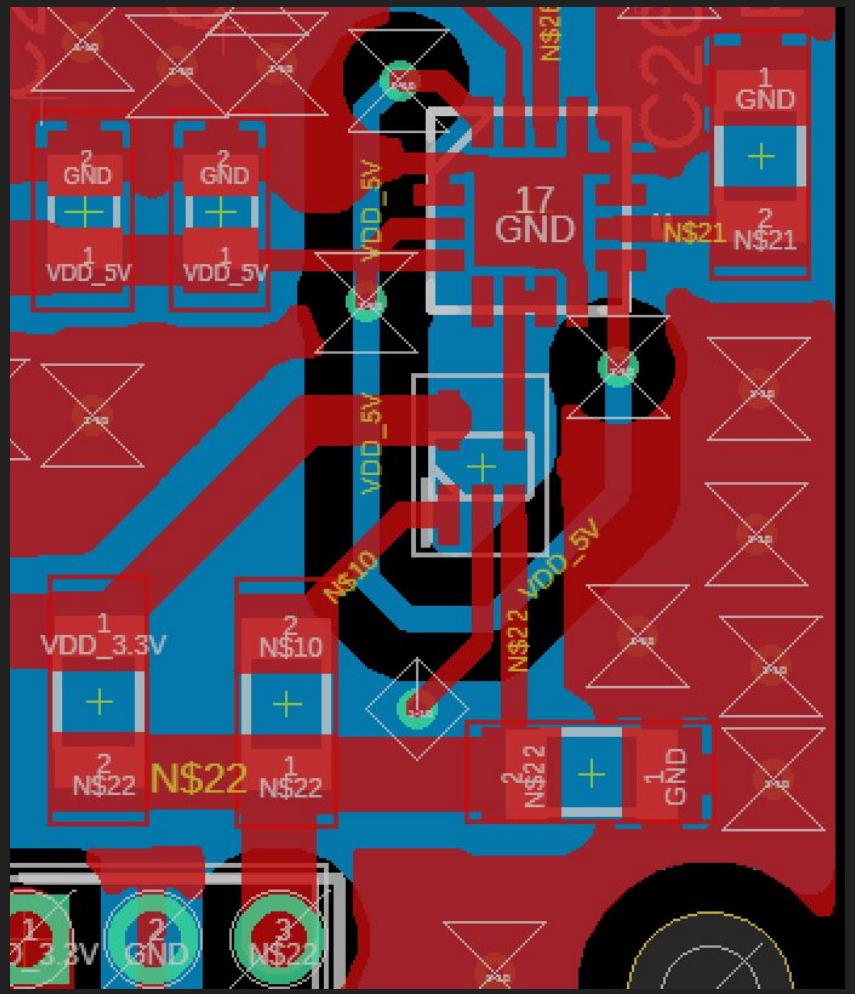
Power Module

- 48 V PoE wall adapter
- 12 V PoE splitter
- 3.3 V and 5 V voltage regulators used to power active components
- Total power consumption: 4.003 W
- Power consumption is below [2]

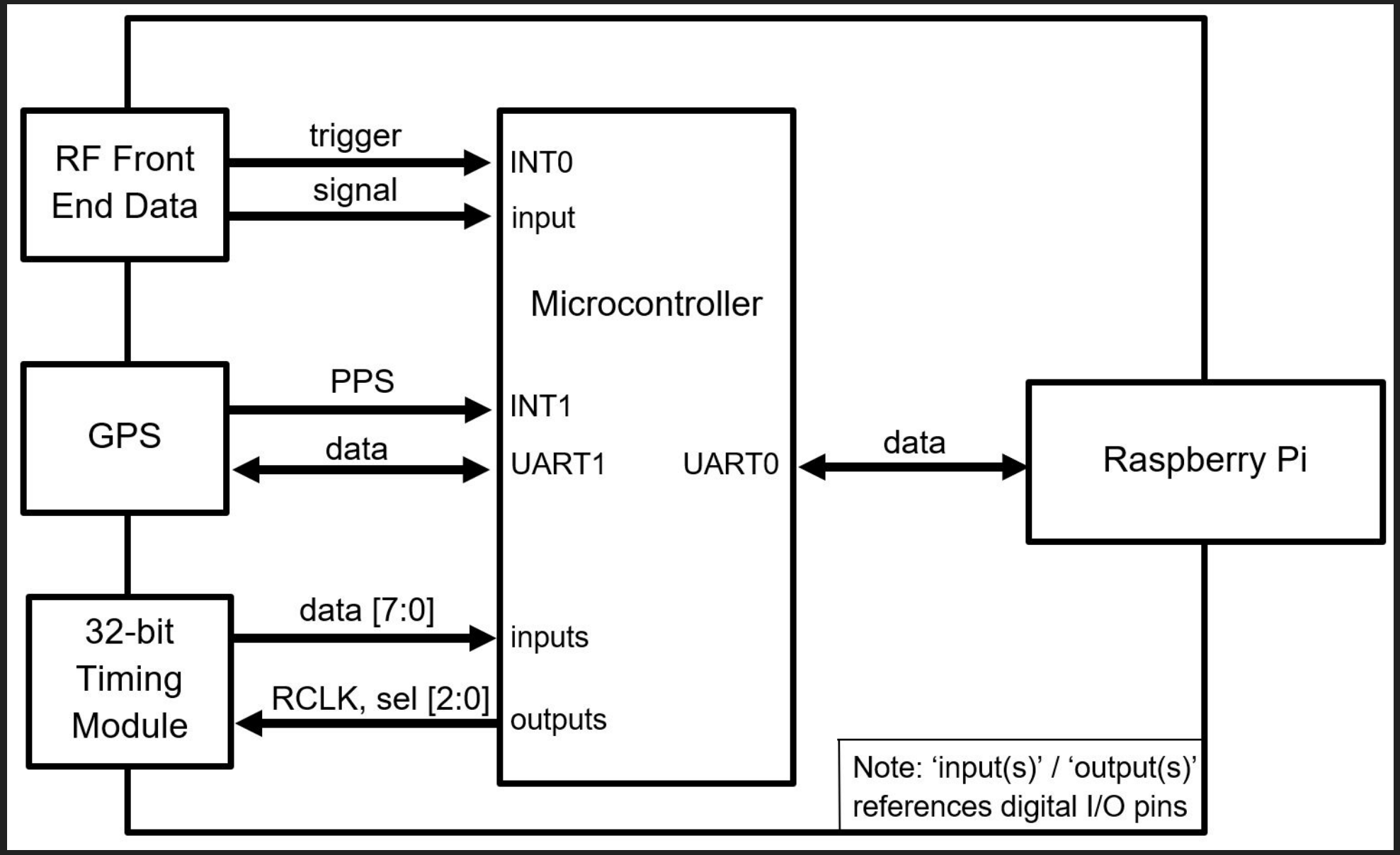
Description	Quantity	Voltage Bias (V)	Current Draw (A)	Power (W)	Subtotal
LNA	2	3.3	0.05	0.165	0.33
RF Detector	1	5	0.092	0.46	0.46
Comparator	1	3.3	0.000112	0.0003696	0.0003696
Raspberry Pi B+	1			2.5	2.5
Digital Hardware	1	5	0.122	0.61	0.61
GPS	1	3.3	0.031	0.1023	0.1023

RF Front End - Implementation Issues

- Layout
  - Log Amp
  - LNA bias pad
  - Comparator isolation
- Component biasing
  - Matching did not provide adequate input/output return loss
- Thermal Issues
  - LNA supply voltage



Control Unit



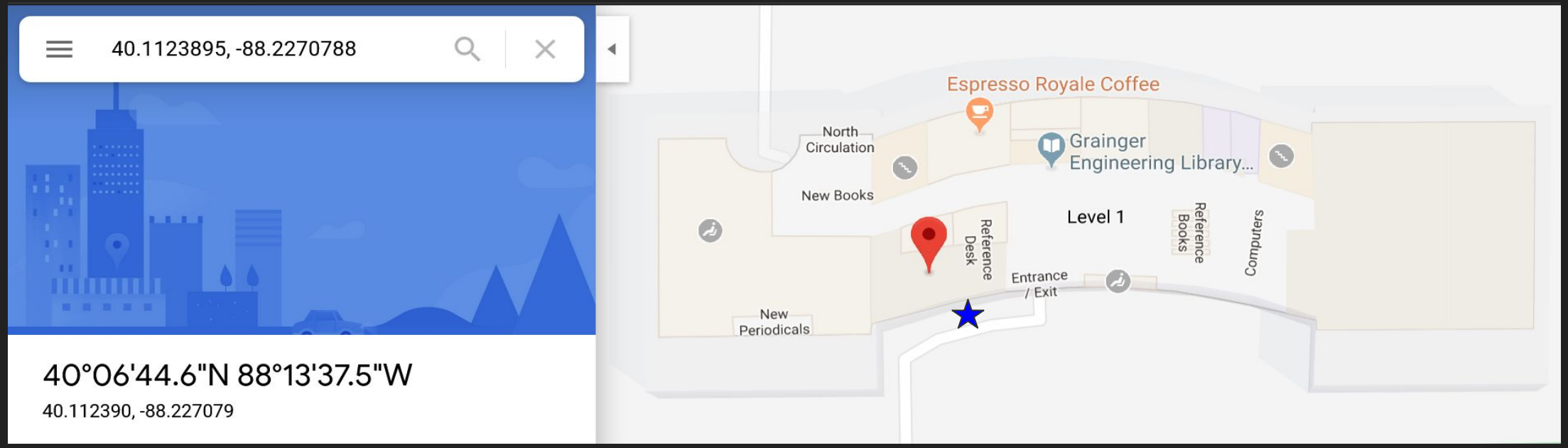
GPS Board

PPS:

Channel	Name	Value	Min	Max	Average	σ	Capture Count	Span
A	Frequency	1000 mHz	1000 mHz	1000 mHz	1000 mHz	1.176 µ...	20	Whole trace

Frequency Measurement of PPS

Location and Decoded Message:
"4,2019-04-21 19:03:25.000,401123895,-882270788,6285,660,21460,9,3580,0,209048,"



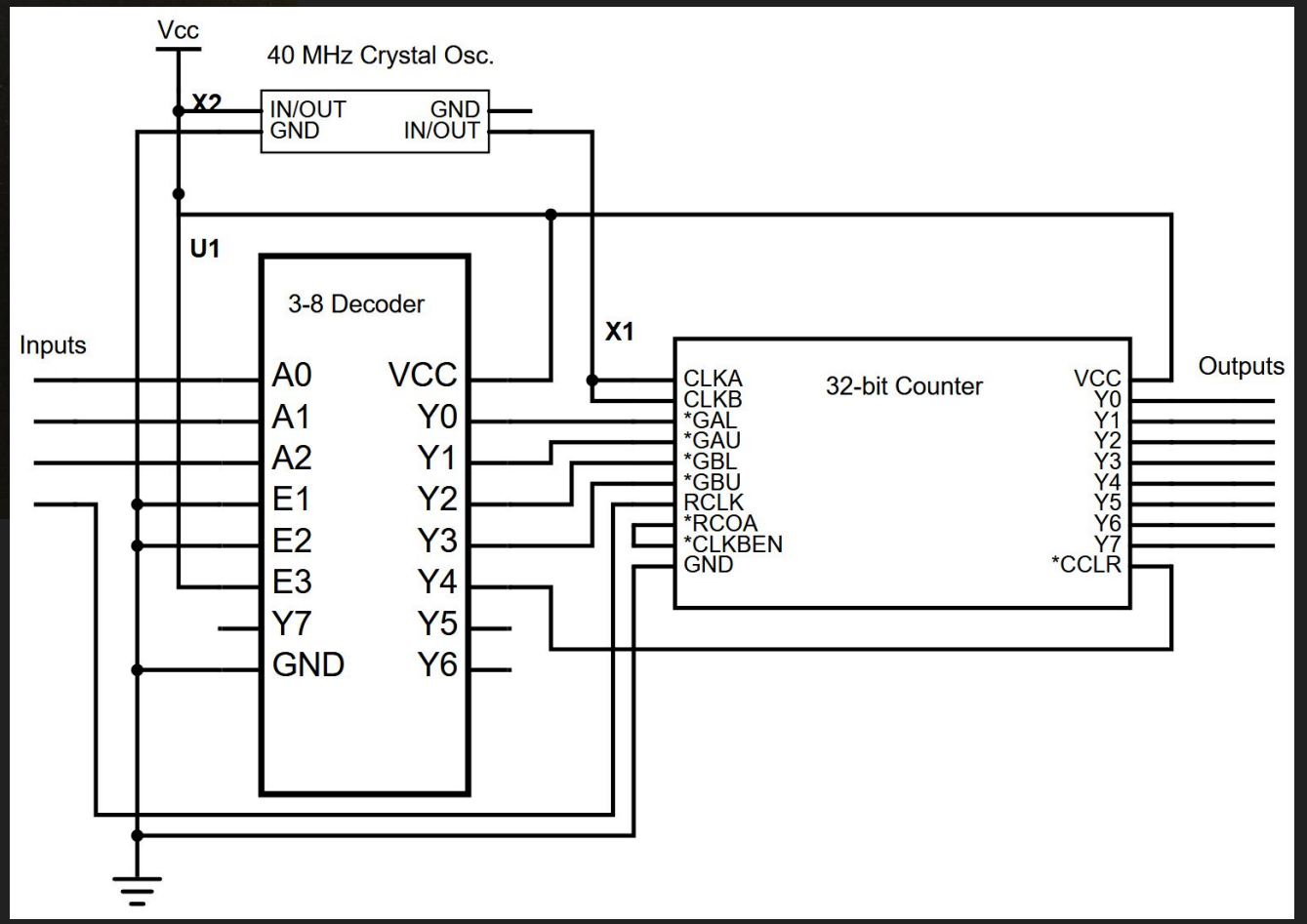
Google Map of (Latitude, Longitude) [6]

Timing Module

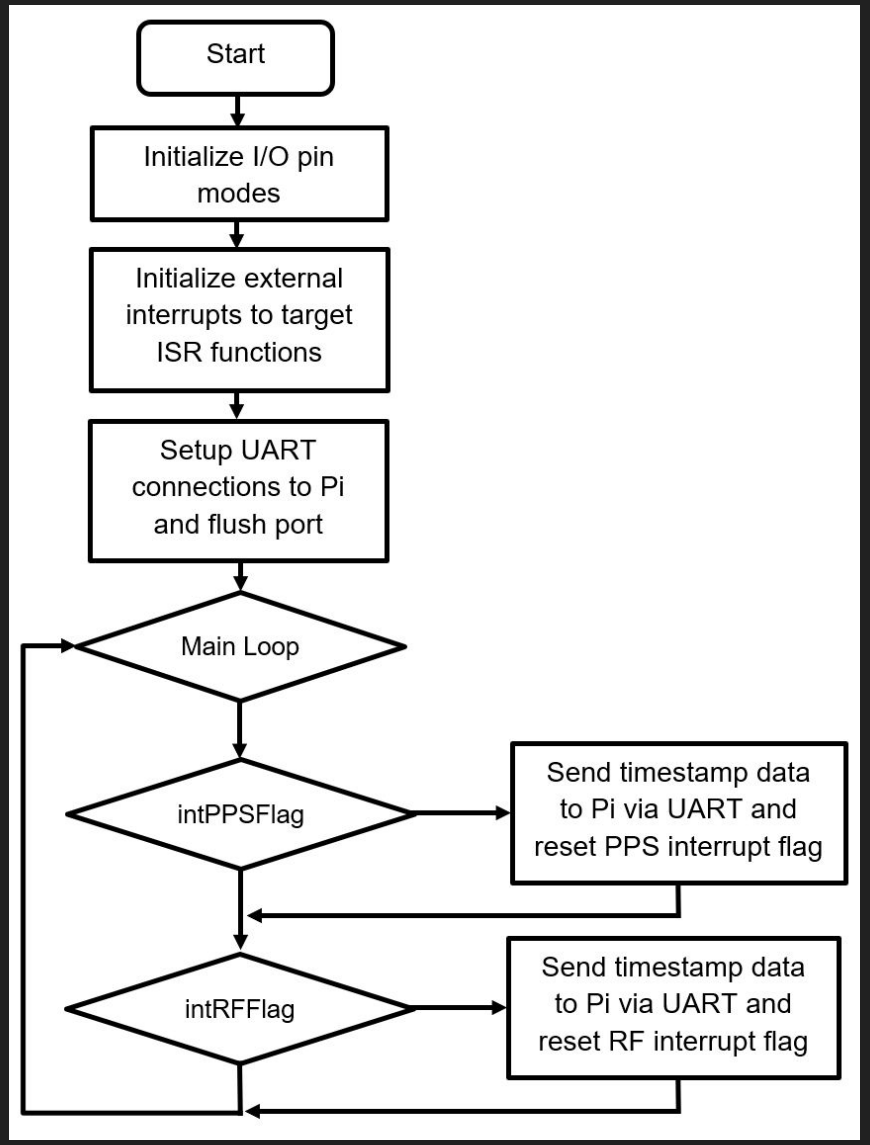
```
pi@raspberrypi:~ $ sudo python Documents/serial/serial_read.py
Timestamp at PPS interrupt 39846231
Timestamp at PPS interrupt 39855366
Timestamp at PPS interrupt 39821856
Timestamp at PPS interrupt 39820654
Timestamp at PPS interrupt 39838790
Timestamp at PPS interrupt 39762004
Timestamp at PPS interrupt 39870701
Timestamp at PPS interrupt 39813172
Timestamp at PPS interrupt 39843660
Timestamp at PPS interrupt 39809435
Timestemp at PPS intertupt 39822391
TiMestamp at PPS interrupt 33609049
Timestamp at PPS interrupt 39824723
Tieestamp at PPS interrupt 39815366
Timestamp at PPS interrupt 39820376
```

Average: 39,825,980 (995.65 ms)

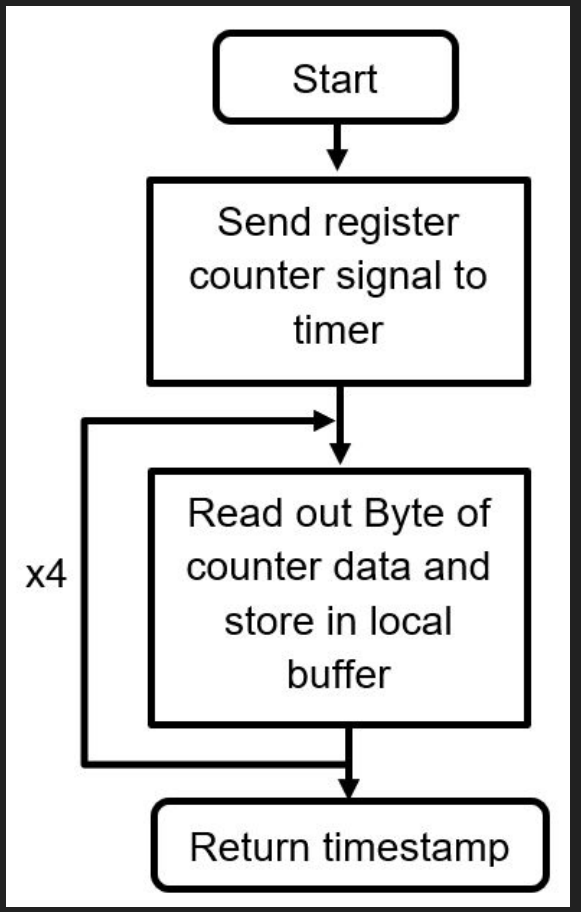
Standard Deviation: 25,587.72 (0.64 ms)



Software

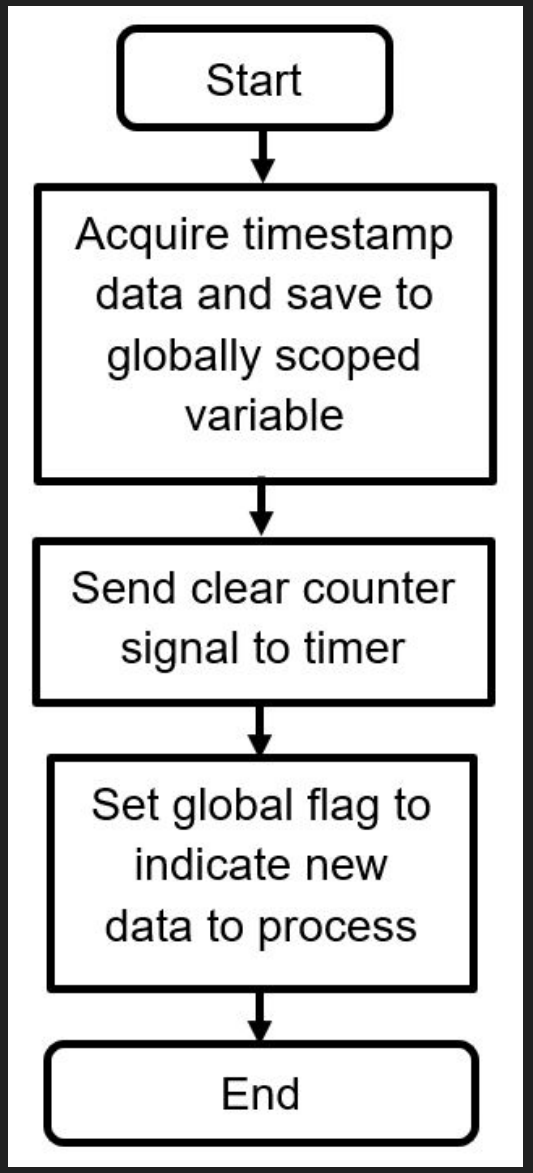


Main Flowchart

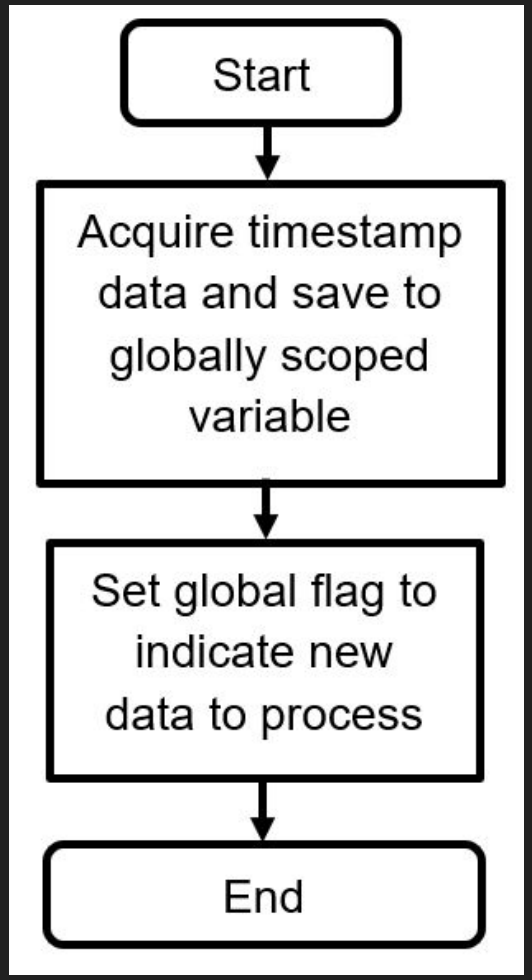


Acquire Timestamp Flowchart

Software Interrupt Handlers



PPS ISR Flowchart



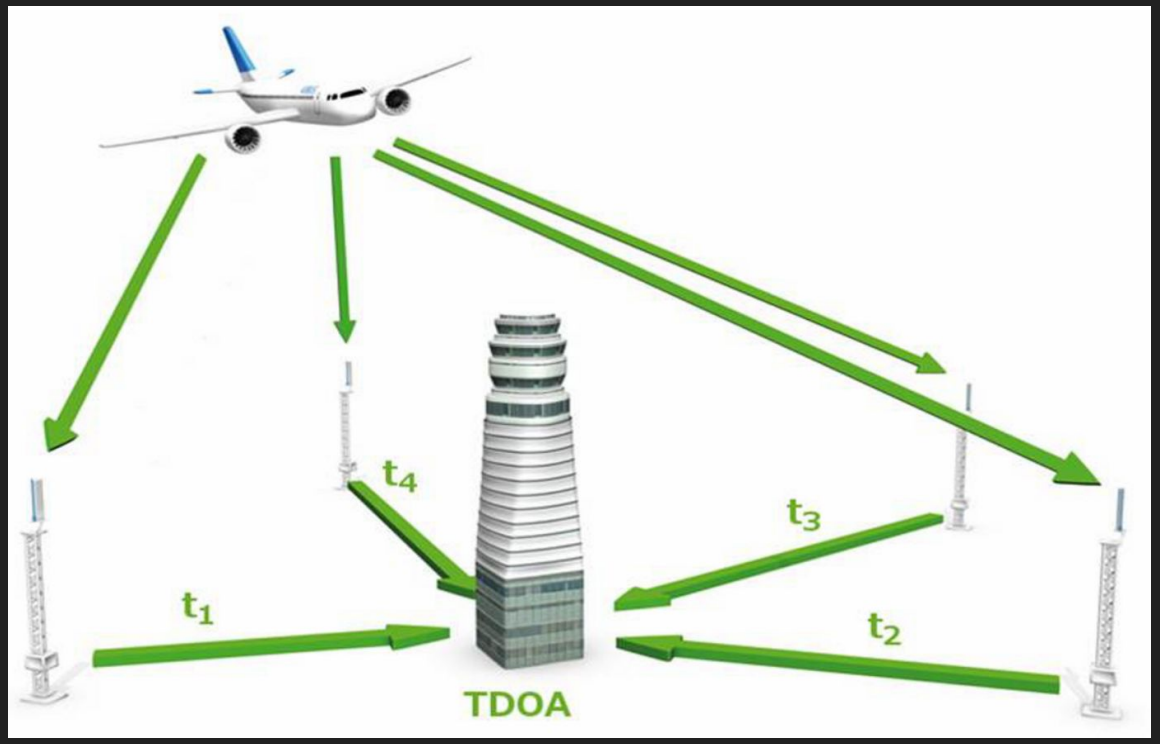
RF ISR Flowchart

Control Unit - Implementation Issues

- Microcontroller configuration issues
- ATMEGA328 limited hardware
- Arduino library incompatibility

TDOA Calculation

- Difference of distance equations can be used as a system of nonlinear equations to solve for aircraft position
- Fsolve function in MATLAB requires initial guess, which can be estimated



$$d_1 = \sqrt{(x-x_1)^2+(y-y_1)^2+(z-z_1)^2}$$

$$d_2 = \sqrt{(x-x_2)^2+(y-y_2)^2+(z-z_2)^2}$$

$$d_1 - d_2 = c\Delta t = \sqrt{(x-x_1)^2+(y-y_1)^2+(z-z_1)^2} - \sqrt{(x-x_2)^2+(y-y_2)^2+(z-z_2)^2}$$

Cost Analysis

- Grand Total: $72.72

Part number	Description	Quantity	Unit Price	Subtotal	Module
MAAL-011078	LNA	2	$5.88	$11.76	rf
TA1090EC	BPF	3	$1.50	$4.50	rf
AD8318	RF Detector	1	$10.60	$10.60	rf
M7805	5V Regulator	2	$0.57	$1.14	power
LD1117A	3.3V Regulator	1	$0.55	$0.55	power
TLV3201DCK	Comparator	1	$0.60	$0.60	digital
NEO-M8N	GPS Module	1	$15.05	$15.05	gps
GAACZ-A	GPS Antenna	1	$5.00	$5.00	gps
SN74LVC138AQPWRQ1	3-to-8 Bit Decoder	1	$0.61	$0.61	digital
SN74LV8154N	Dual 16 Bit Counter	1	$1.09	$1.09	digital
ATMEGA328-PU	Arduino Uno MCU	1	$1.95	$1.95	digital
TOYOCOM 121-049	40 MHz xtal	1	$1.12	$1.12	digital
A160L8F	16 MHz xtal	1	$0.75	$0.75	digital
OshPark pcb#1	PCB	1	$10.00	$10.00	board
	R's, L's, and C's	1	$5.00	$5.00	misc
	wires and headers	1	$3.00	$3.00	misc

Final Remarks

- Achievements
  - Fully integrated RF front end
  - Design powered by PoE
  - PPS and GPS data captured

- Problems/Considerations
  - Testing was difficult without capturing real-world data.
  - Layout with RF components had some trouble.
  - Consider developer support when choosing a microcontroller.

Future Work

- Full PCB integration
- Network implementation with multiple receivers
- Dynamic front-end
- Enclosed form-factor
- User-friendly support
  - Push buttons for test and reset
  - Status LEDs
  - Web-based applications for settings and data access

References

[1] A. Costin and A. Francillon, "Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices", Media.blackhat.com, 2012. [Online]. Available: https://media.blackhat.com/bh-us-12/Briefings/Costin/BH_US_12_Costin_Ghosts_In_Air_WP.pdf. [Accessed: 29- Apr- 2019].

[2] “What is Power Over Ethernet (PoE) and what is it used for?” versatek.com [Online]. Available: https://www.versatek.com/what-is-power-over-ethernet/ [Accessed: 19-Feb-2019]

[3] C. Wolff, "SSR - The Reply Message", Radartutorial.eu. [Online]. Available: http://www.radartutorial.eu/13.ssr/sr07.en.html.

[4] Mott, "Estimation of aircraft distances using transponder signal strength information", Taylor & Francis, 2018. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/23311916.2018.1466619 [Accessed: 28-April-2019].

[5] Texas Instruments, “TLV7031 and TLV7041 Small Size, nanoPower, Low-Voltage Comparators,” TLV7031 Datasheet, [Accessed: 28-April-2019]

[6] Google Maps. (2019). 40°06'44.6"N 88°13'37.5"W. [online] Available at: https://www.google.com/maps/place/40%C2%B006'44.6%22N+88%C2%B013'37.5%22W/@40.1120095,-88.2268208,19z/data=!4m5!3m4!1s0x0:0x0!8m2!3d40.1123895!4d-88.2270788 [Accessed 30 Apr. 2019].

Questions?

Thank You!