Covert Communications Device

ECE 445 Design Document – Team 9

By

Ahmad Abuisneineh (ahmada3)

Braeden Smith (braeden2)

Srivardhan Sajja (sajja3)

TA: Evan Widloski

March 5, 2021

Table of Contents

1 Introduction

1.1 Problem and Solution Overview

During sensitive military and law enforcement operations like house raids and room clearing, it is important to have quick intra-team communication. Individuals need to be able to quickly receive and relay information, whether that is from an external command station or between members who are not within line-of-sight. Another issue, which makes typical radios unsuitable for this task, is that individuals must speak out-loud to utilize them. Likewise, to receive, the individual must either block some sensory awareness with in-ear radios or use a speaker which will produce external noise. Maintaining silence and the ability to accurately time and communicate actions is essential for the safety and success of these high-risk undertakings.

Our goal is to create a small, wearable device to complement existing communication equipment. It will produce vibrations in response to other users pressing a button on their device. We imagine placing it on a shoulder, in a vest or pocket, or on a glove. It would allow teams in these sensitive situations to develop a set vibration pattern in order to maintain real-time, one-to-many communication without external noise nor the loss of alertness.

1.2 Visual Aid

Each device will be worn on the user's body, such that the communication button will be easily accessible and the vibrations can be felt on the skin. Figure 1 demonstrates an example of where the device can be placed and the context of its usage.

***Figure 1**: Approximate Physical Design and Application of Device in a High-Risk Environment.*

1.3 High-Level Requirements

For a successful project, we expect:

- The devices must be able to communicate from a minimum of 1 km apart while within line of sight.
- The devices must be capable of remaining battery powered for 1 hour of regular operation, and 8 hours when not actively in use.
- The communication latency (timing between button press and vibration on a secondary device) must be a maximum of 2 seconds.

2 Design

2.1 Block Diagram

As shown in Figure 2, each communication device contains three subsystems accompanied by a microcontroller that integrates the subsystems together. The power regulation unit ensures that the device can be actively used for at least one hour and can be operated on standby for a full eight hours. The radio communication unit will handle transmission and receiving of signals, guaranteeing a transmission range of at least 1-5km. The I/O unit is responsible for responding only to non-accidental button presses and providing haptic feedback against the skin. The control unit, tying the subsystems together, will ensure a secure communication latency below 200ms by performing fast encryption and processing.

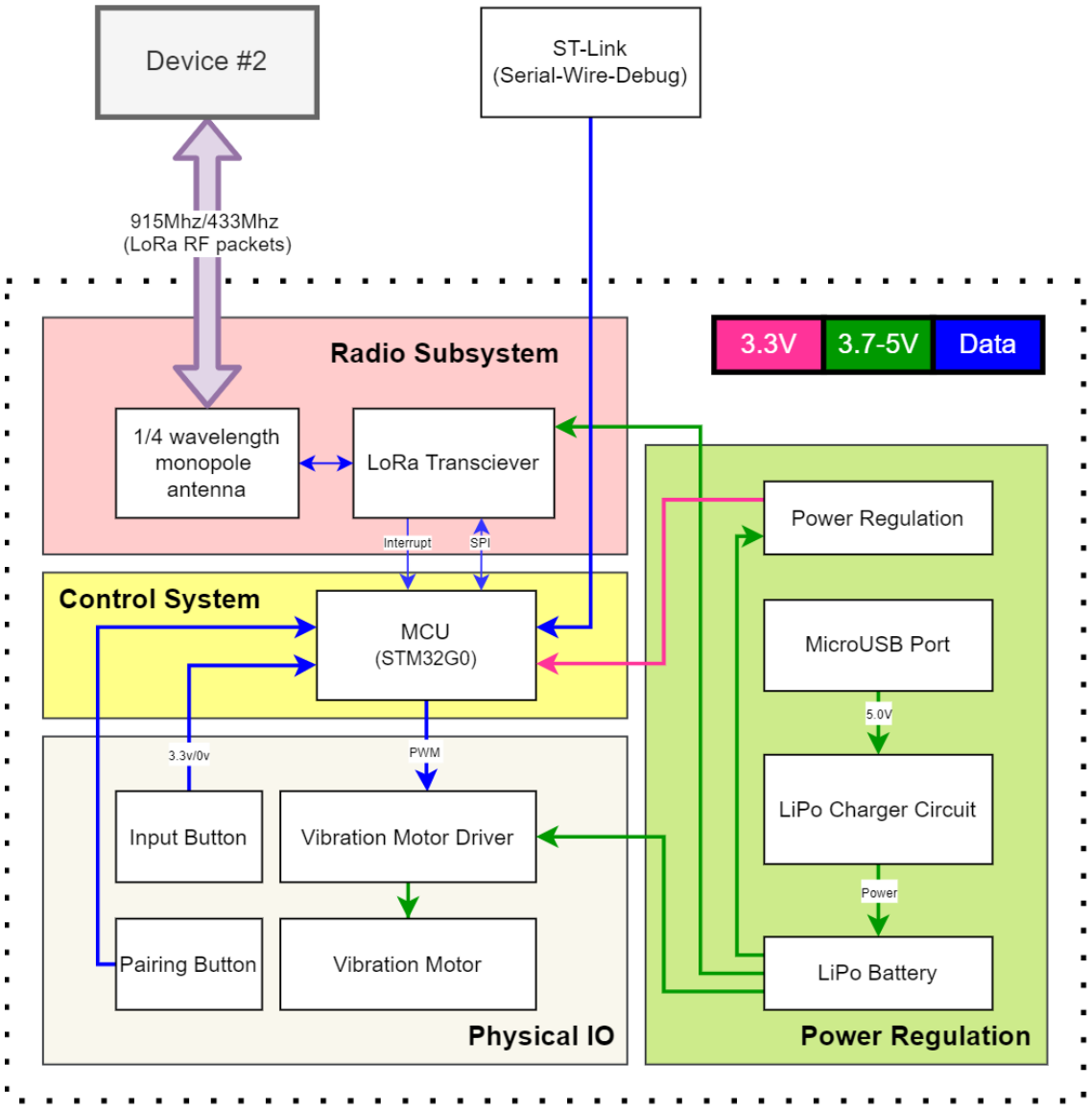

Figure 2. *High-Level Block Diagram of the Covert Communications Device.*

2.2 Schematics & PCB Design

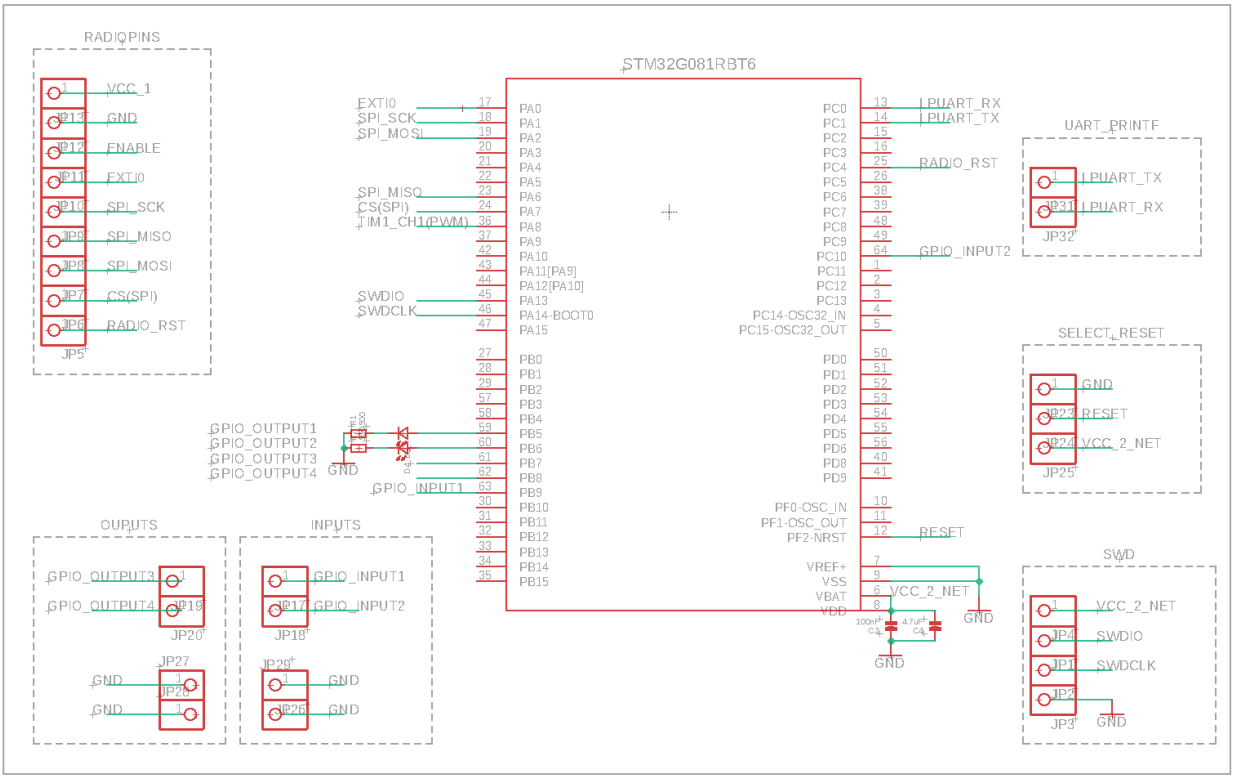

***Figure 3**: Control System, Including Corresponding Physical I/O & Module Breakouts.*

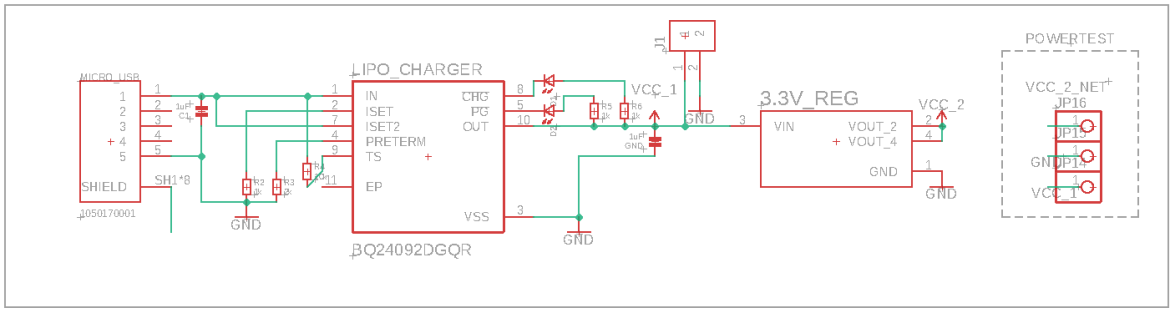

***Figure 4**: Power System & Charging Schematic.*

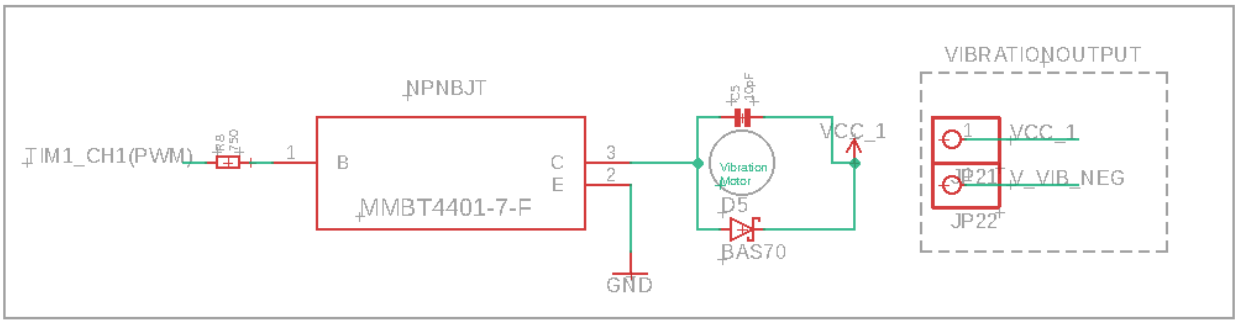

***Figure 5**: Vibration Motor Driver and Related Protection Circuitry.*

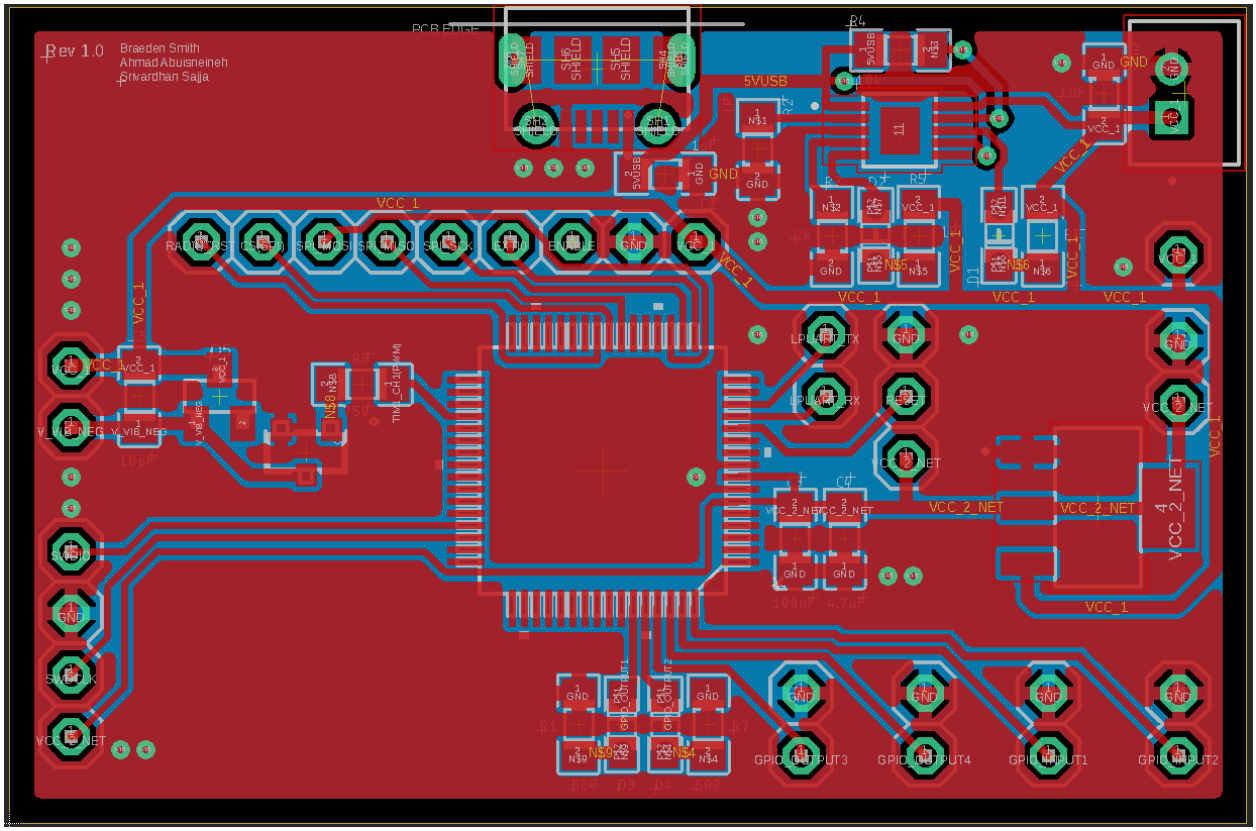

***Figure 6**: Initial PCB Layout. Dimensions: 2” x 1.32”.*

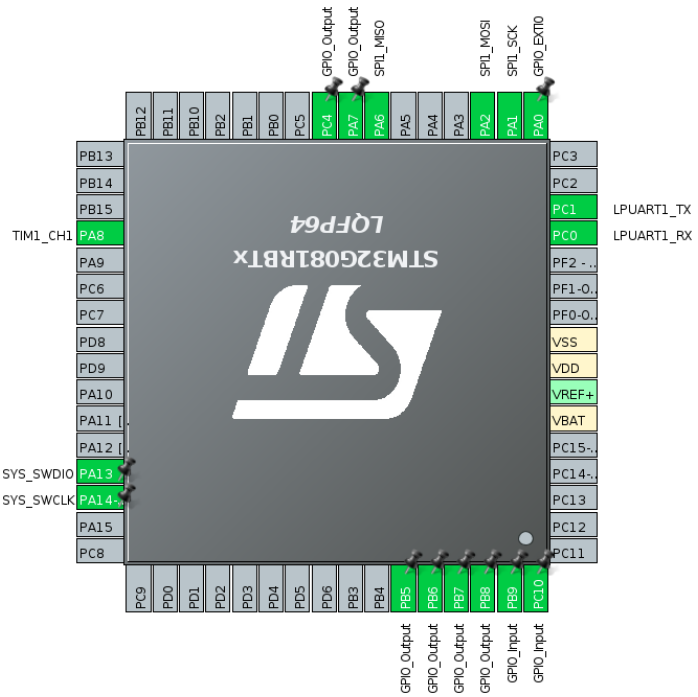

***Figure 7**: Initial STM32G0 Pin Configuration corresponding to the PCB Rotation.*

2.3 Subsystems

2.3.1 Control Unit

Input: 3.3V from regulated LDO, data from buttons, data from transceiver (SPI), external interrupts, UART, Serial Wire Debug.

Output: GPIO, PWM, SPI, UART, Serial Wire Debug.

The control unit is responsible for integrating communication between all of the other subsystems and its connections are illustrated in detail in the figure 3 schematic. We settled on a STM32G081RBT6 for a variety of advantages and the low availability of other microcontrollers. It is essential that its power draw is relatively low, so during device inactivity, we can maintain our standby goal of 8 hours. The STM32G0 series is built to have very low standby power drain, while still offering the fast processing requirements we need [1]. The relatively high clock speed 64MHz, and available memory/flash are more than required, but they give us a margin of safety for processing intensive cryptographic operations and allow us flexibility to change algorithms if we devise better methodology. The built-in true RNG and hardware AES engine are essential for maximising the security of our communications as well as the speed that devices are able to communicate. We will use the random-number generator extensively, illustrated in the software design section, and the hardware AES engine to speed up encryption/description during all LoRa packets. Other than that, the MCU offers plenty of standard PWM timers, GPIO, and interrupt-capable pins, so that the physical I/O can be connected with ease.

Table 1. *Pin Layout and Associated Signals for MCU.*

Name	Pin	Function	Signal
VBAT	6	Power	VCC_2_NET
VREF+	7		GND
VDD	8		VDD
VSS	9		GND
PF-NRST	12	Resets MCU	RESET
PC1	13	Optional printf STLink interface	LPUART_RX
PC1	14		LPUART_TX
PA0	17	I/O for communication with radio subsystem	EXTI0
PA1	18		SPI_SCK
PA2	19		SPI_MOSI
PA6	23		SPI_MISO
PA7	24		SPI_CS
PC4	25		RADIO_RST
PA8	36	PWM signal for vibration motor	TIM1_CH1(PWM)
PA13	45	Serial Wire Debug I/O	SWDIO
PA14-BOOT0	46	Serial Wire Debug Clock	SWCLK
PB5	59	General purpose output	GPIO_OUTPUT1
PB6	60		GPIO_OUTPUT2
PB7	61		GPIO_OUTPUT3
PB8	62		GPIO_OUTPUT4
PB9	63	General purpose input	GPIO_INPUT1
PC10	64		GPIO_INPUT2

2.3.2 Power Supply Unit

Input: 5.0V at 500mA (MAX), Rechargeable 3.7-4.2V LiPo Battery

Output: +3.3V for MCU, Button

+3.7-4.2V for Transceiver, Vibration Motor

LiPo constant current & constant voltage charging cycle

The power supply unit is responsible for effectively regulating the power stored and used by the rest of the components in our device. The components of this unit are carefully selected based on the needs of the device as a whole, considering voltage ratings and current draws. Our communications device receives power from the 3.7-4.2V LiPo battery. However, not every component can take 3.7-4.2V as an input, so we will have a series of components to step down the battery into other usable voltages. Furthermore, our battery stores 1200mAh of charge [2]. Since we want our device to be able to function for a minimum of one hour of active use, the circuit must draw less than 1200mA. We provide ourselves a large amount of room to go above and beyond for the “active use” requirement, although the 8 hours of passive use is a closer requirement, since our goal drain is to be <= 100mA draw while the radio is

purely in RX mode and the motor is not driven. Table 2 reflects on this requirement and ensures that our circuit consumes far less current than required.

Another critical device for our device is the LiPo battery charger. It needs to be able to accept the USB 2.0 power standard (5V at 500mA) and it has to charge the battery safely. We settled on the TI bq2409x due to its programmable current capability, status LED outputs, and safety mechanisms [3]. The entire system pulls power from the output of this chip/LiPo (see Figure 4), so it's ability to provide 500mA output current was essential to keep all the extraneous devices powered at max possible load.

Table 2. *Power Requirements for Various Devices on Board.*

Device	Voltage/Current Requirements
Lithium-Ion Polymer Battery	Outputs 3.7V-4.2V [2]
RF Transceiver	3.3-6V Draws a minimum of 150 mA [4]
Microcontroller	Requires 1.7-3.6 V Draws a maximum of 100 mA, ~25mA is expected given enabled chip features. [1]
Vibration Motor Controller	Collector−Emitter Voltage (MAX): 40 V Collector−Base Voltage (MAX): 60 V Emitter−Base Voltage (MAX): 6.0 V Collector Current: 200 mA [5]
Vibration Motor	Draws 80mA at 4V [6]
TOTAL:	Current drawn by active components: 510 mA (MAX) Voltages needed: 3.3V for MCU 4.2-3.7V for everything else

We're using a 3.3V linear regulator to step down the voltage from the battery for use in 3.3V logic level systems (powering the MCU). We are utilizing the TPS7A05 for this task. The voltage regulator is rated to output a maximum of 200 mA of current [7]. We expect our circuit to draw a maximum of 100mA on the 3.3V power rail (see table 2), which is well below this threshold. We have high flexibility if the chip needs to power additional unforscene components. The relatively high efficiency for a linear regulator and small 1uA quiescent current make it a great choice to keep our total power draw low. Table 3 shows the pin configuration of the voltage regulator.

Table 3. *Pin Layout and Descriptions for Voltage Regulator [7].*

Name	PIN	Pad Type	Description
ADJ/GND	1	input	Adjust pin for adjustable output option. Ground pin for fixed output option.
Vin	3	input	Input voltage for regulator
Vout	2	output	Output voltage for regulator (3.3V)

2.3.3 Radio Unit

Input: +3.7-4.2V from the power supply, data and actions from the microcontroller

Output: data and interrupt requests to the microcontroller

The RF transceiver and antenna combo will modulate, transmit, and receive signals on the 915 MHz frequency band. The patented LoRa (Long Range) modulation allows an increase of 2-5X distance over traditional packet radios, and can easily reach into the kilometer range with non-directional antennas [8]. We need significantly greater distance than standard WiFi or Bluetooth radios, but we also don't need to transmit much data (low bitrate requirements). LoRa radios make the perfect application fit with long range and bitrates in the 11 bps to 37 kbps range. We choose this specific breakout board because it has an on-board regulator and level-shifter for data communication [4]. This allows us to prototype with 5V or 3.3V logic level devices and not consider power regulation requirements. Refer to Table 4 for the pin layout and usage of the transceiver module. The data received by the radio unit will be encrypted via AES encryption performed by dedicated hardware in the MCU.

The bitrate/data rate of our LoRa radio system is an essential component for project success.

Since a single AES block is 128 bits in length, we need our bitrate to be no slower than ~2 kbps to have a transmission in ~60 ms or less. This gives some leeway to account for SPI, processing latency, and mode switching. It depends on a multitude of factors and will require real-world experimentation to determine tradeoffs between distance, speed and reliability. Doing some experimental exploration, we end up with a real latency as mentioned in the table 12 below, this hints at the need to 3kbps + to hit our 100ms requirement. The 3rd configuration is our current candidate as it gives a good balance of SF + BW while still hitting < 100 ms in real latency tests which includes the overhead + data rate. Some further testing will be needed with SF 6 since that required special register configuration.

Some of the factors that can be configured and directly affect the data rate are bandwidth, spreading factor, coding rate and they are directly given by this equation: $DR = SF \cdot \frac{BW}{2^{SF}} \cdot CR$. And other indirect factors that influence distance/signal integrity are transmission power, preamble length and CRC.

We can determine several plausible configurations that meet our minimum bitrate requirements as shown in the table below. The final determination must be done by experimentation about how different settings affect distance, SNR, packet loss and data rate.

Table 12. *Candidate modem configurations for LoRa radio.*

Bandwidth (BW)	500KHz	31.25KHz	250KHz	500KHz	7.8KHz
Spreading factor (SF)	11	6	9	6	12
Coding Rate (CR)	4:5	4:5	4:5	4:5	4:8
Resulting Data Rate (DR)	2.148kbps	2.344 kbps	3.516 kbps	37.500 kbps (maximum)	11 bps (minimum)
Theoretical Latency (16 bytes)	59.59 ms	54.6 ms	36.40 ms	3.41 ms	11.63 seconds
Real Latency (1 byte)	~104ms	~42 ms (SF6 testing problematic)	~53 ms	~3ms (SF6 testing problematic)	14 seconds
Real Latency (16 bytes)	~165ms	~42 ms (SF6 testing problematic)	~93 ms	~3ms (SF6 testing problematic)	23 secs

Table 4. *Pin Layout and Descriptions for Radio Transceiver [4].*

PIN Name	PIN	Pad Type	Description
Vin	1	3.3-6V	Power in. Becomes regulated down to 3.3V, so any 3.3-6V input is fine. Requires 150mA.
GND	2	VSS	Ground for logic and power
EN	3	input	Connected to enable pin of voltage regulator. Pulled HIGH to Vin by default. LOW cuts power to radio.
SPI_G0	4	output	GIPO 0 pin, aka IRQ pin, used for interrupt request notification from the radio to the microcontroller
SPI_SCK	5	input	SPI Clock pin
SPI_MISO	6	output	Microcontroller In Serial Out, for data sent from radio to processor
SPI_MOSI	7	input	Microcontroller Out Serial In, for data sent from processor to radio
SPI_CS	8	input	Chip Select. Drop LOW to start SPI transaction
RST	9	input	Reset pin for the radio: High = reset LOW = turn on

2.3.4 I/O Unit

Input: PWM signal indicating vibration pattern

Output: HIGH signal indicating a button press

To send a message over radio communication, the microcontroller first awaits a signal from the button. The button will send a HIGH signal to the microcontroller for as long as it is pressed, and will send a LOW signal otherwise. The microcontroller then sends an encrypted signal to the radio unit for transmission.

Upon receiving a message over radio communication, the device microcontroller "turns on" the vibration motor. A NPN BJT will function as a motor controller so that the motor doesn't overdraw current from the microprocessor and can instead be connected to the power supply unit directly. We selected a NPN BJT over a n-channel MOSFET after some deliberation. BJTs are more accessible from a component availability/price perspective and they are more easily driven at 3.3V logic levels. Although we sacrifice some power efficiencies, since the vibration motor will not be ON most of the time, we believe that reducing the complexity and number of external passive components is more conducive to a successful project. See table 5 for pin assignments and functionality.

A related consideration to the LoRa data rate is the "button hold" timing. Essentially the minimum timespan that a received "on" signal will vibrate the motor. The high-level requirements put our total communication latency at <= 200ms, which means we can consider this a goal of the button-hold timing. We can hold the vibration motor on for that duration everytime we receive an on signal and comfortably avoid non-existent breaks in vibration and not affect the perceptible patterns being transmitted.

Table 5. *Pin Layout and Descriptions for Motor Controller (NPN BJT) [5].*

Pin Name	Pin	Description
Base	1	Base allows current to flow between Emitter and Collector based on PWM signal from MCU
Emitter	2	Emitter - Connected to ground
Collector	3	Collector - vibration motor connects between VDD and the collector

The vibration motor does not have a pin set, but rather two wires that need a potential difference between them for the motor to start [6]. It can be conceptualized as a resistor (in series with an inductor), both in function and in a schematic, and for that reason, we will not be including a pin layout table.

Motors inherently pose the risk of creating a counter-electromotive force (back-emf) due to the electromagnetic properties of the motor, especially during on to off transitions. We plan to nullify the potential damage of this back-emf to the MCU by inserting a diode in parallel with the motor, such that no voltage spike could damage the BJT or MCU.

Similarly, motors also pose the risk of creating electromagnetic interference. We will suppress this EMI by putting a low-capacitance capacitor in parallel with the vibration motor. Together, these two changes will reduce the electromagnetic side effects of the motor, allowing it to behave almost like a resistive load.

Likewise, for the button, the circuit across its two wires is open until the button is pressed, after which the circuit is closed. We will not include a pin layout for the same reason as above. The button will close the circuit between the MCU's GPIO pins and ground. Otherwise, the internal pull up resistor will produce a high signal.

2.4 Requirements and Verification Table

2.4.1 Control Unit [12.5 Points]

Table 6. *Requirements and Verifications for the Control Unit.*

Requirements	Verifications
1. AES-128-CTR encryption and decryption on 16-byte blocks each must occur in <10ms	A. Include the official STM32 cryptographic library + enable hardware AES for MCU in STM32 CubeIDE B. Write to perform AES-128-CTR encryption and decryption on a random piece of stack memory 10,000 times C. Record the times for both operations relative to the clock speed D. Use the serial wire debug breakpoints to view time/clock cycles elapsed for the operations
2. Public key generation and key exchange using Curve25519 library in STM32 crypto must occur in <1 second taken separately	A. Include the official STM32 cryptographic library B. Write a two programs to time and do the following 100x: a. Generate random bytes for private key and execute public key generation b. Generate a shared secret from the created secret and a hardcoded public key C. Take the average times recorded by these programs
3. Ensure the STM32 can receive external interrupts and context switches to respond to them in <50µS.	A. Get two oscilloscope probes and place the oscilloscope into its highest capture rate with a rising edge trigger B. Configure the STM32 to enable rising edge external interrupt on an exposed pin, and internally pulled-down output on the other C. Write code that, when it receives an interrupt, it drives the other pin high D. Place scope on both pins, pull the interrupt high

	E. Measure the latency between the rising edges on the oscilloscope

2.4.2 Power Supply Unit [12.5 Points]

Table 7. *Requirements and Verifications for Power Supply Unit.*

Requirements	Verifications
LiPo Battery: 1. True capacity, from being fully charged (4.2V) to discharged (3.7V) should be ≥800mAh	A. Use a lithium polymer charger with constant current charge and discharge capabilities (ISDT Q6) B. Charge lipo to full (4.2V) -- discharge it at 500mA with a cutoff voltage of 3.65V, record displayed capacity. C. Now charge LiPo to full (4.2V) again at 500mA rate, record the displayed capacity
LiPo Charger: 2. LiPo charger should have protection against accidental shorts of exposed JST pins	A. Use a current limited mode on a lab power supply, set 5V, 600mA limit B. Drive the USB power pins via exposed breakout on assembled PCB C. Measure the output pin of the LiPo charger with an oscilloscope D. Short the JST connector pins E. Ensure the output pin drops to zero until power is cycled and that the 600mA limit on the power supply is not hit
LiPo Charger: 3. LiPo charger should be capable of providing 300mA throughout it's output voltage range (3.65-4.25V), while being powered by a 5.0±0.1V 500mA current limited source	A. Prior to installation. A benchtop power supply should be set to 5.0V with a 500mA current cutoff B. The LiPo charger should be configured appropriately with passive components to set the proper mode and charge rates C. A standard discharged (3.7V) LiPo battery should be plugged into the output pins D. A multimeter should be placed in series between the output pin & the battery E. Check if the current output exceeds 300mA F. Otherwise, add an artificial load via a resistor to ground in parallel with the battery. Continue to lower the resistance until the multimeter reads 300mA G. At 300mA, use an oscilloscope or multimeter to measure the voltage is above 3.65V

3.3V Regulator: 4. Regulator should be capable of supplying 3.3±0.1V at 50mA from an input of 3.7V at 400mA	A. Prior to installing the voltage regulator, place it on a breadboard, use a benchtop power supply to provide 3.7V as input B. Place a resistor of 50-66 Ohms between 3.3V output and ground C. Use a multimeter to ensure the 3.3V output does not fall below 3.15V under load.

2.4.3 Radio Unit [12.5 Points]

Table 8. *Requirements and Verifications for Radio Unit.*

Requirements	Verifications
1. Upon sending a packet on one device, it should be received on the secondary device and sent via SPI in <100ms	A. Use two 3.3V/5V logic level devices (Nucleo development board + Arduino are both options) and have each connect to a transceiver with SPI B. Setup both devices with LoRa libraries, use selected modem configuration, set one of them to TX every 200ms C. Have the transmitting device drive a GPIO pin high when it finishes transmitting D. Have the receiving device drive a GPIO pin high as soon as it receives a packet via SPI E. Attach an oscilloscope to each GPIO pin and set up single-shot capture F. Compare the time differences between each pin's rising edge over a sample size of five
2. Upon sending a packet on one device, it should be received on the secondary device if paired and euclidean distance between devices is less than or equal to 1 km with no obstructions between them	A. Use two 3.3V/5V logic level devices (Nucleo development board + Arduino are both options) and have each connect to a transceiver with SPI (at maximum output power) B. Setup both devices with LoRa libraries, set one of them to TX every 200ms C. The RX device will blink an LED everytime it receives a packet D. Walk the TX device 1km away within line of sight E. Use a video recording to ensure the RX device blinks at least once per second (it's okay to miss packets)

2.4.4 I/O Unit [12.5 Points]

Table 9. *Requirements and Verifications for I/O Unit.*

Requirements	Verifications
1. Vibrations generated by the motor should have high enough amplitude to convey the user information without the user facing any difficulty, but should be low enough to not alert targets	A. Power the vibration motor with 4.2V, to make it run at maximum battery voltage B. Install a decibel meter application similar to "Sound Meter" on a smartphone, to measure the decibel level of the motor while running C. Place phone microphone 1m away from the vibration motor D. Check with the decibel meter to see if decibel range is between 0 and 7 decibels compared to the existing noise floor
2. The addition of a small capacitor and schottky diode should reduce the back-EMF voltage spikes generated by the motor down to a negligible level (<50% its original value)	A. Drive the vibration motor from 4.2V, using a signal generator. Attach an oscilloscope probe to the motor B. Observe the voltage spike generated by the motor during the transition from 4.2V to 0V C. Use a single-shot capture on the oscilloscope and measure the amplitude of the voltage spike D. Attach the diode in the reverse orientation and capacitor in parallel and redo the previous test (see Figure 5) E. New measurements should be less than 50% of the original value

2.5 Software Design

The core software component of our project is instantiating device communication and maintaining security during regular use. We have developed a software flow which uses several advanced cryptographic patterns to ensure device chatter cannot be understood nor replayed.

First Boot & Device Assignment

We start out prior to the first device boot: a singular device within the fleet is assigned a "master" status at a fixed location within its flash memory. The software on each device is identical but behaves slightly differently based on this status. Each secondary device must be paired individually with the master device prior to normal communication.

At first boot, as illustrated in Fig. 11, every device checks whether it has an assigned or generated "master key". If it is lacking this "master key", it uses the true random-number-generator on board the microcontroller to generate and store a new 32-byte key.

Asymmetric Pairing

The pairing software flow is illustrated in Fig. 8. All devices have an internal pairing button and only two devices can be in pairing mode at a given moment: the sole master and secondary of choice. To begin the pairing process, both buttons must be pressed within a close time interval. From there, an interrupt occurs on the MCU, jumping it to the pairing code. We use Curve25519 as a Diffie-Hellman function because of its small processing requirements compared to traditional asymmetric key exchanges [9]. Each device generates a random private key and then a corresponding public key. They then exchange their public keys “in the clear” by transmitting five times with random delays, as illustrated in Figure 8. If both devices successfully receive the other’s public key, they can compute an identical “shared secret” using their own private key and the other’s public key. Now that they both have the same “shared secret”, a truncated version of that is used for the AES-128-CTR symmetric encryption. The master device will now send it’s true “master key” by encrypting it with the shared secret key. The secondary device now replaces it’s internal “master key” with the one it just decrypted.

Standard Encrypted Communication

For standard AES (a symmetric encryption mechanism) usage, we simply use the “master key” stored in memory to encrypt and decrypt messages. This is accelerated by the on-board AES hardware that is built into the device. AES is a block cipher with a minimum block size of 128 bits, therefore we must create and transmit multiples of 128 bits of content in every radio packet. Since our actual information requirements are very small, we can assume we will send only one (padded) block during each transmission. This is discussed in some detail in the radio section when determining LoRa data rate analysis.

Normal communications (of vibration state) use AES-128-CTR (counter) which is a specific mode of operation of AES, see Figure 9. We append a counter to each message that we send and the recipient will only accept messages with a counter greater than the last one that was received. This prevents what is called a “replay-attack”, where an attacker could directly resend a valid packet without needing to know the contents.

Alternative Schemes

We considered alternative pairing schemes, including a more synchronous approach. Regardless of the approach, we are left with several hard problems based on the radio system & device including: variable latency, packet loss, half-duplex communications and lack of synced clocks.

The master and secondary device must transmit public keys to each other. Only after that has successfully happened, can the master device must send the “master key”. Whether we do more asynchronous or synchronous transmissions, we have to determine retry counts & wait length because of issues mentioned previously.

In the supplemental section, Figures 14 and 15 illustrate an alternative semi-synchronous approach we may take based on the result of experimentation & software development with the radio systems.

Known Weaknesses

Although we have devised a relatively sophisticated communication & pairing protocol, there are some attacks that this system design is inherently weak to. We offer a few thoughts for potential mitigation strategies if we consider it defensible.

1) Man-in-the-middle during pairing. If an attacker is able to actively transmit to the master device during a pairing sequence, they can provide their own public key and will get sent the “master key”, from which they’ll be able to decrypt all communications.
2) Side-channel attack by viewing packet bunching. Since we are transmitting the binary “on” state when a device has a button pressed. An attacker would be able to view sections of packets being sent and determine the pattern & time that buttons were pressed without needing to read the contents. To overcome this, we will attempt to batch randomized device heartbeats that will have similar appearance to button presses but will not contain any “on” signals.
3) Man-in-the-middle during regular transmission. Although the data will be encrypted, an attacker who can receive and jam the RF spectrum will be able to retransmit valid “on” packets at any pace or time they would like, precluding a successful packet arrival from the jammed source. This is not a really defensible threat without extreme additional complexity because we’re transmitting binary data not information, a target can actually be affected by delayed or time differed arrival.
4) Pure RF jamming. This would prevent the arrival and transmission packets and is hard to defend from. Spreading factor, CRCs, variable bandwidth, and high transmit power set up in the radios will help against some amount of external interference, but otherwise directed, powerful jamming is indefensible without alternative technology like FHSS radios.

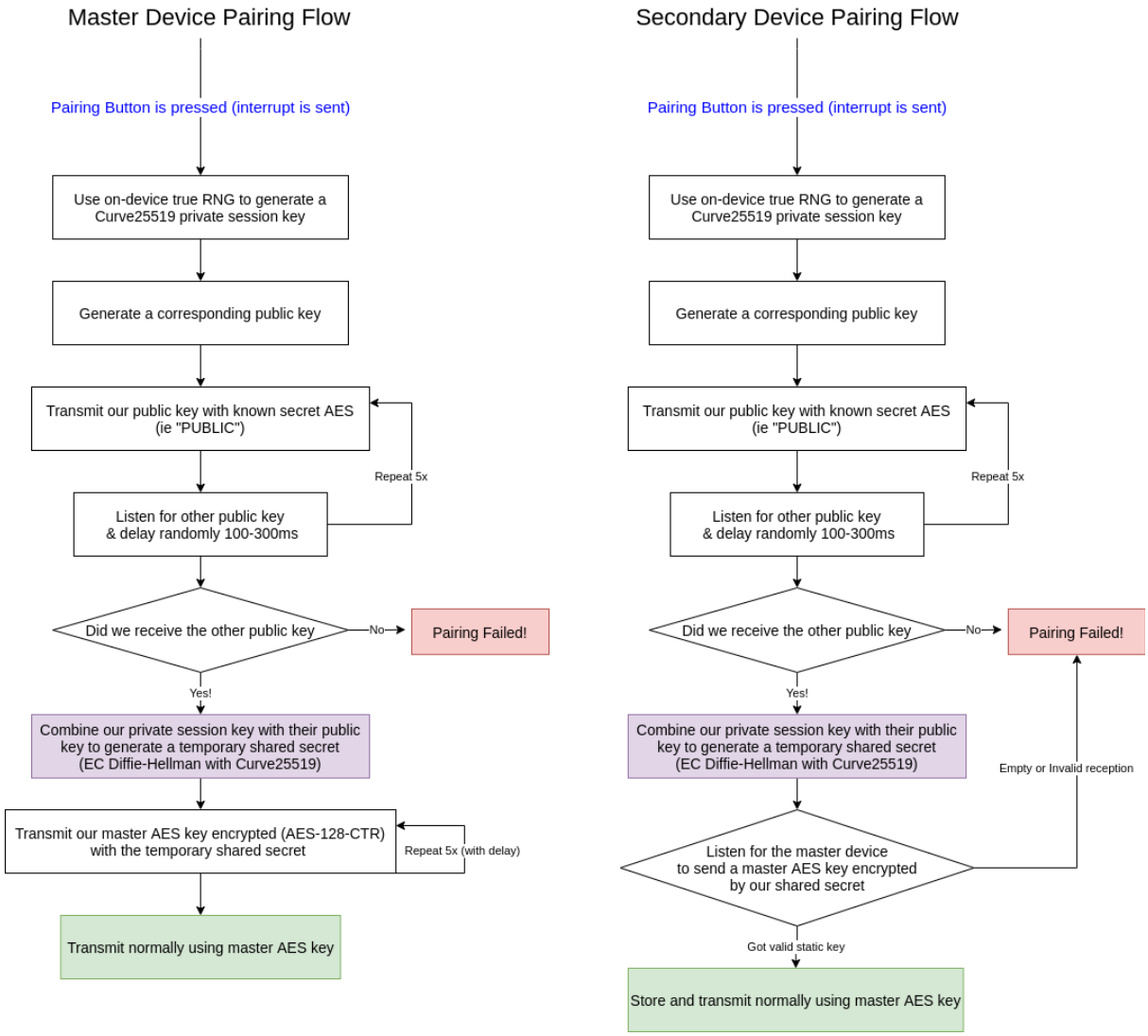

***Figure 8**: Software Flow for Multi-Device Pairing Using Elliptic-Curve Cryptography.*

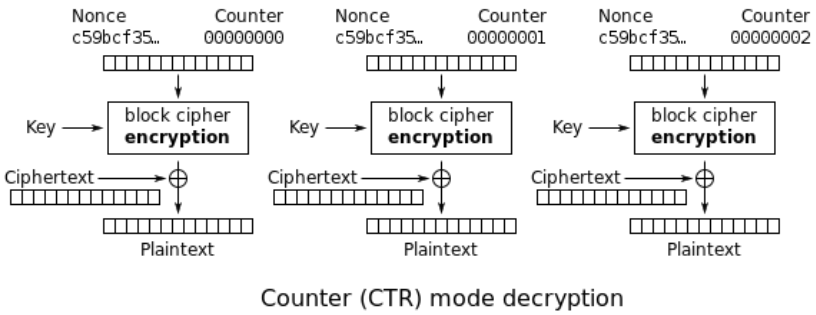

***Figure 9:** AES CTR Mode of Operation, to Avoid Valid Vibration Data Being Resent by an Attacker [10].*

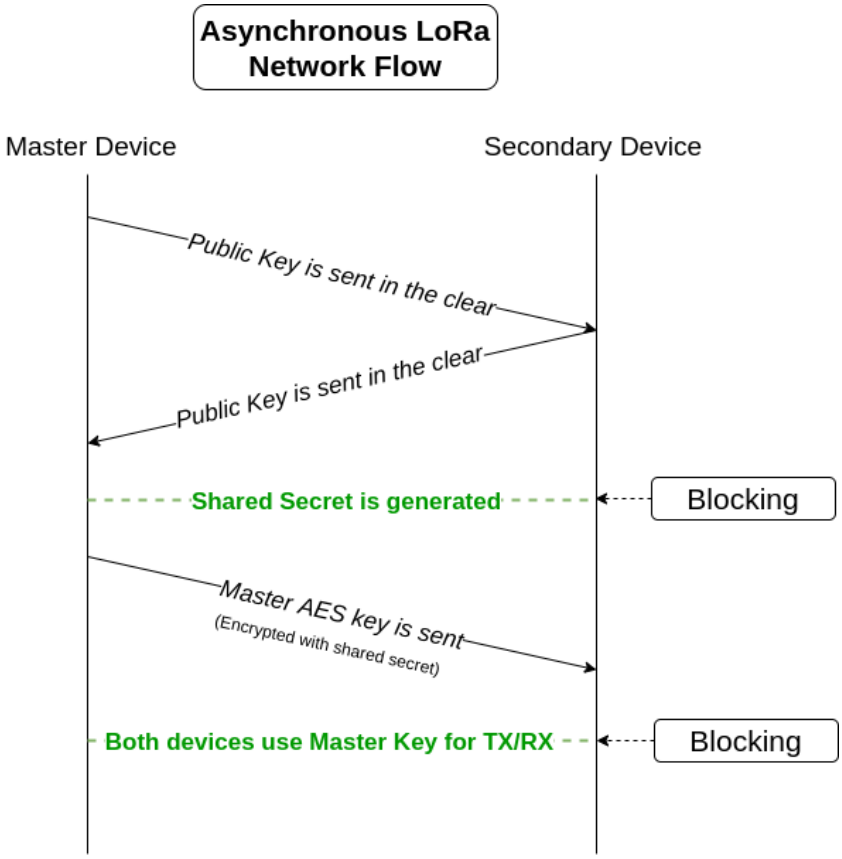

***Figure 10**: Asynchronous LoRa Network Flow for Pairing.*

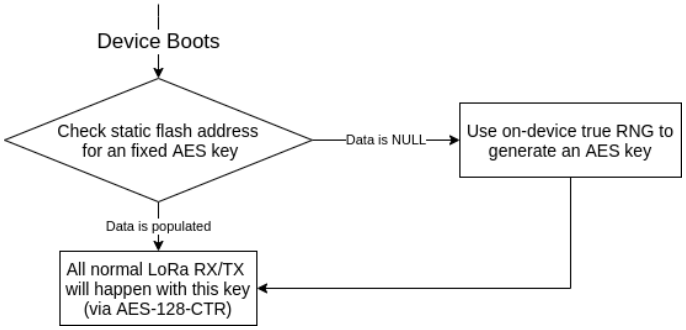

***Figure 11**: Device Boot Key Generation.*

2.6 Tolerance Analysis

One important component of the completion of our project is the ability to reliably and within specification control the vibration motor. It needs to turn on when driven via the MCU's PWM signal throughout the input voltage range, otherwise important communications may be missed, defeating the entire purpose of the device. We settled on a NPN BJT (2N3904 series) to be the core driving component

of our circuit for reasons mentioned earlier. Because of that, we need to choose appropriate base resistor values to avoid drawing more than 5mA (and ideally as little as possible) from the GPIO pins on our MCU, while also being certain that our collector-to-emitter current can drive our vibration motor load, whether in active or saturated mode.

Using the KVL equations for a BJT in active mode:

$$V_{BE} = V_{in} - I_B R_{MCU} \tag{1}$$

From the datasheet: $V_{BE(Sat)} = .65V\ to\ .95V$[5].

We also know from the STM32 details that: $V_{in} = 3.3V$ and we must have $I_B < 5mA$ strictly.

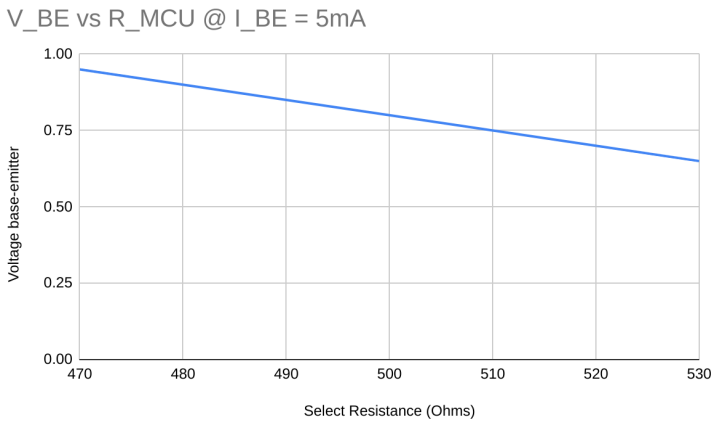

***Figure 12**: Highest permitted base current (5mA) over base-emitter voltage range.*

Furthermore we can use KVL and the definition of a BJT to model collector-emitter relationships:

$$V_{CE} = V_{CC} - I_C R_{Load} \tag{2}$$

$$I_C = \beta I_B \tag{3}$$

The MMBT3904 datasheet also tells us the worst case $h_{FE}(\beta) = 30$ and $V_{CE} = 0.2V$ to $0.3V$ [5], as the current approaches $I_{C(Sat)}$ [5]. The motor specification resolves a load of 60mA at 3V, 80mA at 4V and 100mA at 5V [6], so we can approximate it as a resistive load of 50 Ohms. Our V_{CE} varies from 3.7-4.2V because it is driven from nominal battery voltage for a LiPo [2].

$$V_{CE} = V_{CC} - I_C 50\Omega \tag{4}$$

$$I_C = 30 I_B \tag{5}$$

Taking the two extremes of voltage (V_{CC}, V_{CE}), $4.2V - 0.2V = 4.0V \; and \; 3.7V - 0.3V = 3.4V$. We can model the possible ranges to select an efficient and appropriate base current.

$$3.4V = 30 I_B 50\Omega \tag{6}$$

$$4.0V = 30 I_B 50\Omega \tag{7}$$

This leaves us with a result of $2.2mA \; to \; 2.6mA$base current (I_B). We now consider what resistances allow each of those currents to flow into the base of the transistor from a 3.3V logic level.

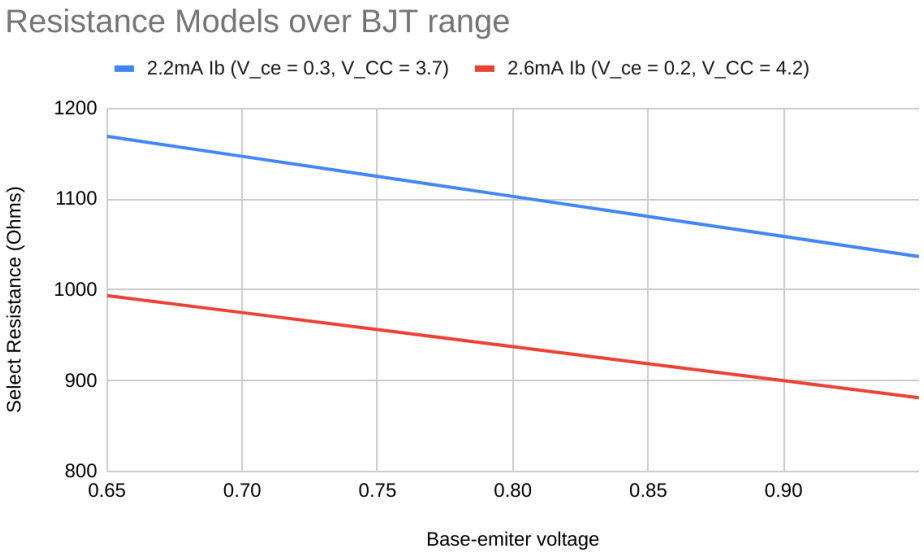

***Figure 13**: Lines are the Models of Max+Min Voltage Drop Across the Load and the Resistors Available.*

Based on the results of our two models, since we want to minimize our base current while still being confident it will drive the motor at its rated current, we want to select a R_{MCU} between 530Ω to 880Ω. The GPIO pin will source >= 2.6mA while not exceeding our hard maximum of 5mA in any conditions.

3 Costs and Schedule

3.1 Cost Analysis

A typical salary for a UIUC BS Computer Engineering graduate is $96,992/yr, or about $50/hr. We expect the three of us to work on this project for about 10 hours per week each, leading to an estimated labor cost of $60,000.

$$3\,persons * 10\frac{hours}{person*week} * 16\,weeks * 50.00\frac{dollars}{hour} * 2.5 = \$60,000 \quad (8)$$

Our parts costs during development are as follows in table 10:

Table 10. *Parts List, Quantities, and Costs.*

Part No	Supplier	Description	Price Per Unit	Quantity	Net Price
NUCLEO-G071 RB	Digikey	Discovery Board	$10.99	1	$10.99
STM32G081RB T6	Mouser	Microcontroller	$3.85	5	$19.25
ST-LINK/V2	Digikey	ST-Link	$22.60	1	$22.60
455-1704-ND	JST Sales America	JST Connector	$0.17	5	$0.85
1201	Digikey	Vibration Motor	$1.95	3	$5.85
1010	Adafruit Industries	Buttons	$5.95	1	$5.95
SMMBT3904LT 3G	Microchip Technology	Motor Controller	$0.50	2	$1.00
258	Adafruit Industries	Battery	$9.95	2	$19.90
296-41204-6-N D	Texas Instruments	LiPo Charger Chip	$1.36	2	$2.48
MMBD101LT1 GOSDKR-ND	ON Semiconductor	Schottky diode	$0.29	5	$1.45
TPS7A05	Texas Instruments	3.3V LDO	$0.62	4	$2.34
WM1399DKR-ND	Molex	MicroUSB Female port	$0.83	5	$4.15
1528-1667-ND	Adafruit Industries	Transceiver	$19.95	2	$39.90
n/a	Digikey	Misc. Resistors + Capacitors	$10.00	1	$10.00
4269	Adafruit Industries	Antenna	$0.95	2	$1.90
Total Price:					**$138.27**

For crucial or sensitive parts, such as the microcontroller, several duplicates as a precaution, in the case that one becomes broken during development. For other circuit components, such as the antenna, only two are needed for development, because they cannot break as easily. We plan to assemble two fully functional boards during development, but will leave room for revisions along the way.

We anticipate the total cost of this project's prototype to be:

$$\$60,000 + \$138.27 + \$60,138.27 \tag{9}$$

3.2 Schedule

We plan to allocate our time on this project as follows in table 11:

Table 11. *Weekly Schedule Until 5/3.*

Week	Braeden	Ahmad	Sajja
2/8/2020	Conceptualize design		
2/15/2020	Submit RFA and create Project Proposal		
2/22/2020	Create design document		
3/1/2020	Create circuit schematic and PCB layout Create Design Document Order initial components	Create design Document	
3/8/2020	Design Review Order additional components	Design Review Validate Initial PCB Design	Design Review Validate Initial PCB Design
3/15/2020	Finalize rev 1. PCB Orders	Design and source external casing & select physical IO	Get development board running STM32 crypto library & benchmark
3/22/2020	Begin populating PCB Create and order rev. 2 PCB	Begin populating PCB and testing R+V	Get both LoRa transceivers communicating. Finish R+V software checks.
3/29/2020	Debug initial PCB & populating rev. 2 Assist with software development	Construct final casing and begin assembly Assist with software development	Develop software prototype and run it on hardware prototype (if feasible)
4/5/2020	Finalize software prototype Begin combining elements and final in-case construction using Rev 2. PCB		
4/12/2020	Debug & leeway week Plan Demo		
4/19/2020	Debug & leeway week Mock Demo		
4/26/2020	Demo project		
5/3/2020	Prepare final presentation and final report		

4 Ethics and Safety

One of the many dangers with electronics lies within batteries. They can leak, and when put under certain conditions, they can become explosive. Lithium-ion batteries specifically are not too flexible and pose a major risk in devices subjected to wear and tear. In order to comply with ethical design (IEEE code of ethics #I.1), we decided to use a Lithium-Ion Polymer (LiPo) battery [11]. We believe the LiPo battery already adds many benefits to our project, but safety is our main concern. LiPo batteries are more flexible than traditional lithium-ion batteries and have a smaller chance of exploding [12]. The usage of the LiPo battery ensures a safer product for the consumer.

Not only do batteries pose a risk to consumers, but components connected to the battery do as well. Overheating is not uncommon in electronics, and when integrated circuits or other miscellaneous chips are not properly configured, they can easily become a fire hazard. We will minimize this risk in our circuit design through various implementations, such as properly limiting current throughout the circuit such that no component draws an unsafe amount nor exceeds its thermal specification. We will also utilize a LiPo battery that contains a built-in over-discharge prevention circuit, which ensures that the batteries cannot be drained lower than 3.0V. The design practices put together will ensure maximum electronic safety for consumers.

Additionally, in the physical design of our product, we will avoid sharp edges on the PCB and other components that could potentially puncture the Lithium-ion cell to avoid the severe fire risk [13]. We will also include a 3D-printed casing that will protect and insulate the internal circuit and battery. This design decision minimizes the risk of accidental battery punctures.

Radio Frequency (RF) transmission is a form of radiation, or energy passing through the air and objects in the area. The higher the energy is, the more damage can be done. Relative to other frequencies, radio frequency waves have a low amount of energy and does not ionize (i.e., have molecule-altering effects that may damage tissue and DNA). However, the associated biological effects of RF energy are thermal: exposure to very high levels of RF radiation can be harmful due to the ability of RF energy to heat biological tissue (like the effects of a microwave oven). Lower (non-thermal) levels of RF radiation have no proven harmful biological effects on humans. However, further research is needed to confirm this [14].

To comply with IEEE code of ethics #I.1, we will be using a low-powered, long-range transceiver to transmit and receive signals on our device [14]. According to the FCC, “because of the low power levels used, the intermittency of these transmissions ("push-to-talk"), and since these [hand-held, portable] radios are held away from the head, they should not expose users to RF energy in excess of safe limits”, so we expect our RF transmissions to be ethical and safe [14]. The transceiver that we will use will be FCC certified for use as a module in device integration, so there is no concern about the bands nor the power the device will use [4].

We were initially concerned about the privacy of information sent over the air. If the information is confidential, it may be a violation of certain privacy laws or contracts. However, after some consideration, we concluded that, given that the user(s) will have their own vibration language, they can make their code “unbreakable”, or gibberish to prying eyes. In addition to using a coded language, the device will perform an highly secure asymmetric key exchange during pairing and then use industry standard AES-CTR encryption on data, to further obfuscate packets in the air.

This product may be misused by students in exams. Such usage would be an academic integrity violation. As true to IEEE #1., we will uphold the highest standard of integrity by staying true to our plans: developing a covert communications device [11]. The name already suggests use for an academic integrity violation, no matter the implementation.

Unfortunately, we cannot stop students from cheating on exams. There are already a plethora of devices and techniques available: if a student wants to cheat, he, she or they will have the means. Our covert communications device will be no different than, for example, a student using wireless earphones under his/her hair. The ethical issue of students cheating on exams with our device is a responsibility on the students' part to stay true to their academic integrity agreement. We do not have a solution for this otherwise.

To mitigate the safety concerns of our project, we can give consumers a warning: the device in question contains lithium-ion batteries and should not be smashed, crushed, or otherwise damaged. We will also warn consumers to be wary of flying on an airplane with this device and to abide by the TSA's rules on batteries on flights. We may also include a lab-safety notice about the usage of long-range radio frequencies in this device. This way, users cannot unintentionally harm themselves or others with this product, as well as abide by state and federal regulations.

5 Supplemental Material

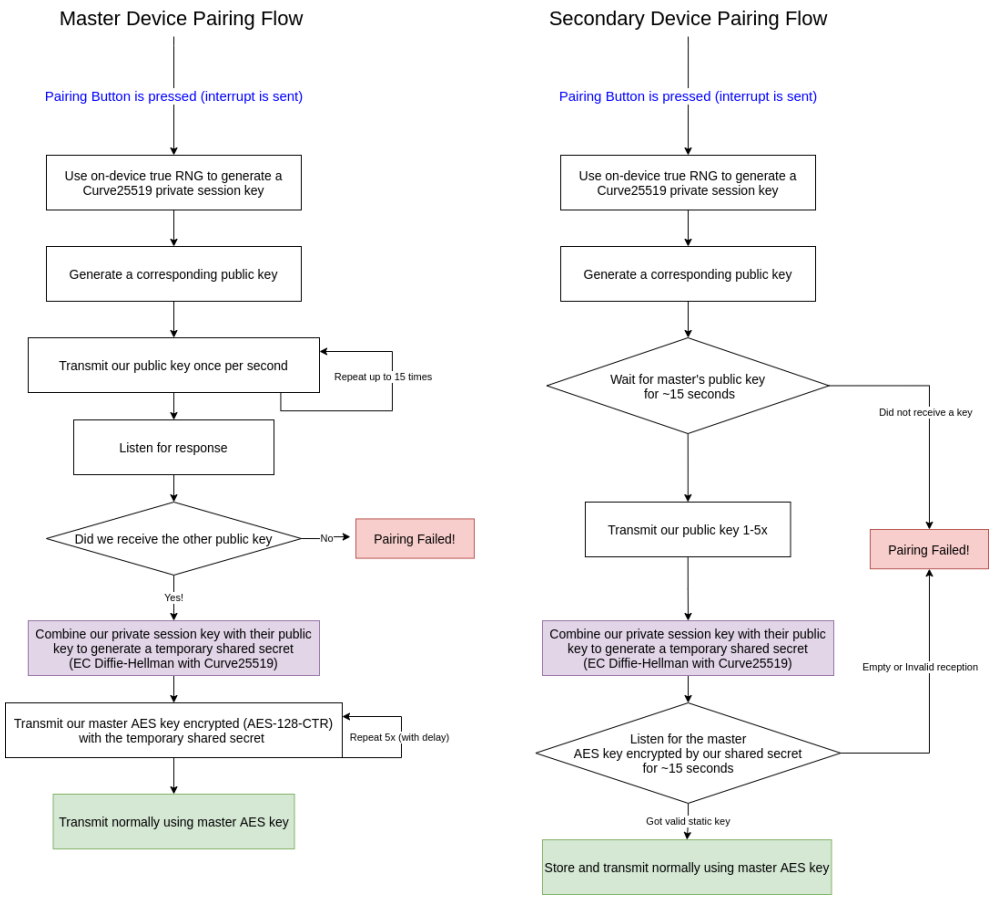

***Figure 14**: Semi-synchronous alternative pairing flow.*

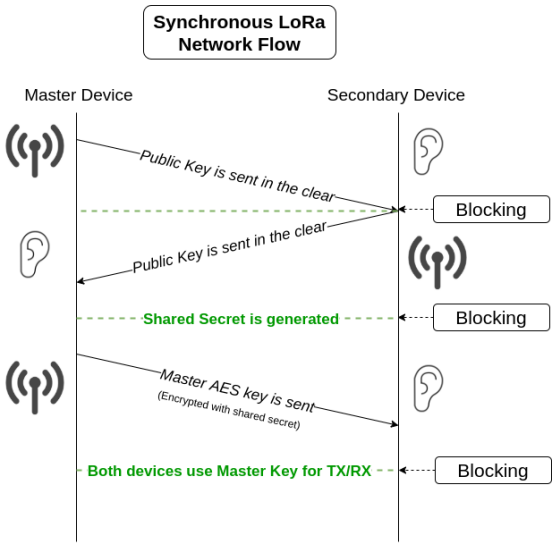

***Figure 15**: Semi-synchronous network transmission flow.*

6 Citations

[1] "STM32G081RB (Mainstream Arm Cortex-M0+ MCU)," *STMicroelectronics*. [Online]. Available: https://www.st.com/en/microcontrollers-microprocessors/stm32g081rb.html. [Accessed: 05-Mar-2021].

[2] A. Industries, "Lithium Ion Polymer Battery - 3.7v 1200mAh," *Adafruit Industries*. [Online]. Available: https://www.adafruit.com/product/258. [Accessed: 05-Mar-2021].

[3] "BQ24092 (Single-Input, Single Cell Li-Ion and Li-Pol Battery Charger)," *Texas Instruments*. [Online]. Available: https://www.ti.com/product/BQ24092. [Accessed: 05-Mar-2021].

[4] "Adafruit RFM95W LoRa Radio Transceiver Breakout - 868 or 915 MHz," Adafruit Industries. [Online]. Available: https://www.adafruit.com/product/3072. [Accessed: 05-Mar-2021].

[5] "SMMBT3904LT3G," DigiKey. [Online]. Available: https://www.digikey.com/en/products/detail/on-semiconductor/SMMBT3904LT3G/8538914. [Accessed: 05-Mar-2021].

[6] A. Industries, "Vibrating Mini Motor Disc," Adafruit Industries. [Online]. Available: https://www.adafruit.com/product/1201#technical-details. [Accessed: 05-Mar-2021].

[7] "TPS7A05 1-µA Ultralow IQ, 200-mA, Low-Dropout Regulator," *Texas Instruments*, Feb-2018. [Online]. Available: https://www.ti.com/product/TPS7A05.

[8] "Semtech SX1276," *Semtech*. [Online]. Available: https://www.semtech.com/products/wireless-rf/lora-transceivers/sx1276. [Accessed: 05-Mar-2021].

[9] D. J. Bernstein, "A state-of-the-art Diffie-Hellman function," *Curve25519: high-speed elliptic-curve cryptography*, 15-Oct-2005. [Online]. Available: https://cr.yp.to/ecdh.html. [Accessed: 04-Mar-2021].

[10] “Block cipher mode of operation,” *Wikipedia*, 04-Jan-2021. [Online]. Available: https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation. [Accessed: 01-Mar-2021].

[11] “IEEE Code of Ethics,” IEEE. Jun-2020 [Online]. Available: https://www.ieee.org/about/corporate/governance/p7-8.html. [Accessed: 18-Feb-2021].

[12] Macfos, “Lithium Ion Vs Lithium Polymer Battery: Latest Detailed difference,” Lithium-ion Battery vs Lithium-polymer Battery, 03-Feb-2021. [Online]. Available: https://robu.in/lithium-ion-battery-vs-li-po-battery/. [Accessed: 18-Feb-2021].

[13] “What To Do With A Punctured Lithium Ion Battery,” Custom Lithium ion Battery Pack. [Online]. Available: https://www.large.net/news/89u43pe.html. [Accessed: 19-Feb-2021].

[14] “RF Safety FAQ,” Federal Communications Commission, 13-Oct-2020. [Online]. Available: https://www.fcc.gov/engineering-technology/electromagnetic-compatibility-division/radio-frequency-safety/faq/rf-safety#Q20. [Accessed: 18-Feb-2021].