Covert Communications Device

By

Ahmad Abuisneineh
Braeden Smith
Srivardhan Sajja

Project Proposal for ECE 445, Senior Design, Spring 2021
TA: Evan Widloski

18 February 2021

1 Introduction

1.1 Objective

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. The secondary condition, which makes typical radios unsuitable for this task, is that individuals must speak out-loud to utilize them, and to be a recipient, you must either block some sensory awareness with in-ear radios or use a speaker which will produce external noise. Maintaining silence and being able to accurately time and communicate actions is essential for the safety and success of these high-risk undertakings.

Our goal with this project is to create a portable device that can produce vibrations in response to other users pressing a button on their device. We imagine that it could be placed on a shoulder, in a vest, in a pocket, or on a glove -- and would allow teams in these sensitive situations to develop a set vibration patterns that would allow them to maintain real-time, one-to-many communication without external noise nor the loss of alertness.

1.2 Background

Internal and external communication during events like SWAT raids or military operations are essential for the safety of those involved, to coordinate movements and time various elements. The teams need to both communicate to one another and receive/send information and updates to external command teams. The typical existing solution is to use in-ear radios and a push to talk microphone. [1][2] While this is functional, two core problems arise depending on the situation. Firstly, if the mission requires some level of silence, then the radios can only be used as outward-in communication, as the user cannot speak out loud. Secondly, having in-ear radio systems, even if they have ambient noise amplification, lessen then ability of a user to hear their surroundings, especially directionality of potential threats.

The research and work that goes into special operations communications is advanced, and we want to offer a supplemental solution that would act in addition to existing market technologies.

1.3 Physical Design

The device, from the user's perspective primarily consists of a single casing with 4 components: a transmitter unit, a receiver unit, a command generator unit, and a haptic feedback generator unit. The device would be placed on the body, close to the skin, where the user can easily comprehend the instruction received, and be able to reach to send instructions back, as demonstrated in Figure 1.

A location on the body such as the bicep, chest, or thigh, easily accessible by one's hand, would be optimal to quickly create commands to send to other receivers nearby.

Figure 1: *Physical Design, Application of device in high-risk environment*

1.4 High-Level Requirements List

For the project to be complete, we expect:

- The devices must be able to communicate at from a distance greater than 1km within line of sight.
- The devices must be capable of remaining battery powered for 1 hour of regular operation, and a full business day when not actively being used.
- The communication latency (timing between button press and vibration on a secondary device) should be below 100ms.

2 Design

2.1 Block Diagram

Each communication device needs three main subsystems, accompanied by a microcontroller that integrates the subsystems together. The subsystems are the power regulation unit, the radio communication unit, and the input/output unit. As the names sound, the power regulation unit will take battery power, and convert it into multiple different voltages that are used by the modules in the circuit. The radio communication unit will handle transmission and receiving of signals, as well as the encoding/decoding of those signals. The input/output unit will be straightforward, having a button to send vibrations, and a motor to create vibrations.

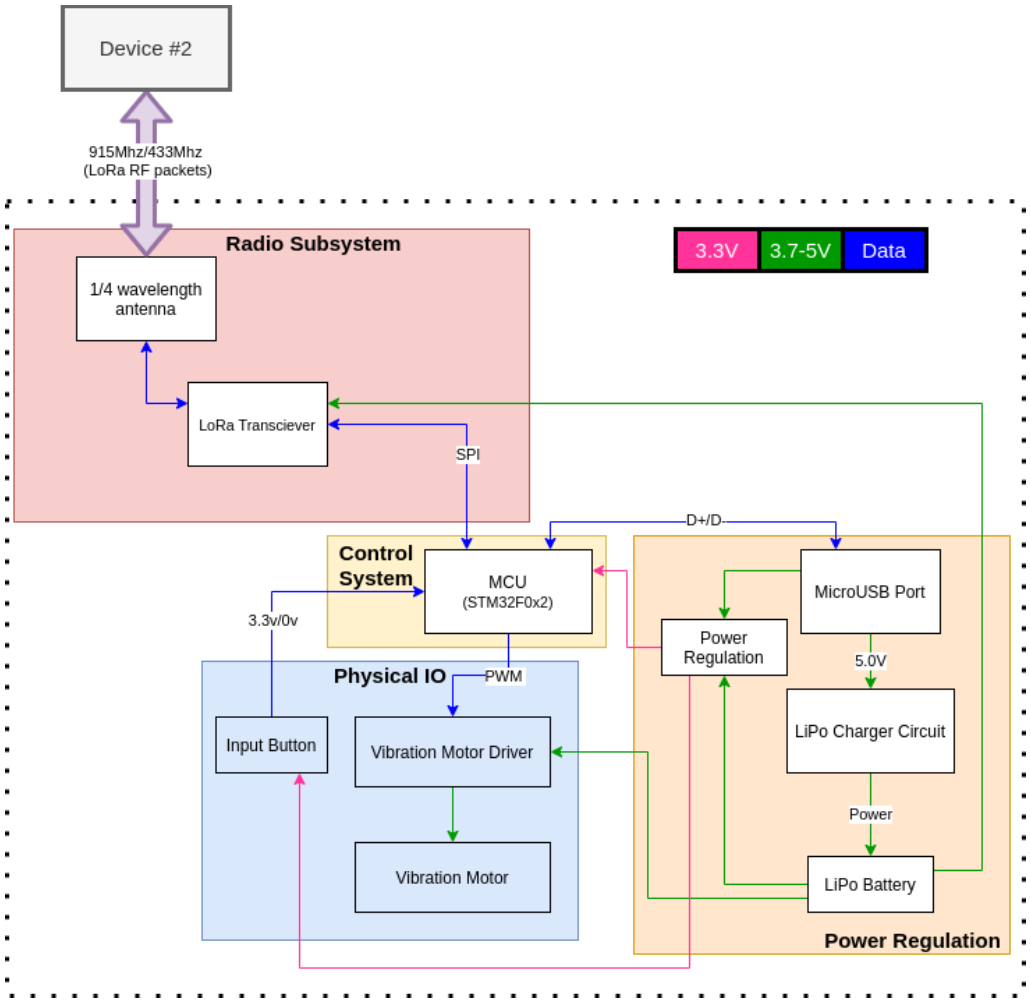

***Figure** 2: High Level Block Diagram*

2.2 Functional Overview and Block Requirements

A brief description of the function of each block in the block diagram along with a highly detailed block description is as follows. This index the componentized relationship to other blocks and to the high-level goals. Per block requirements are specified as they relate to individual elements but are equally applicable to the block subsystem I/O.

2.2.1 Radio Subsystem

Data from the MCU will be transmitted over the electromagnetic spectrum via radio frequency waves. We will use a singular transceiver to send and receive signals, as well as an antenna to extend our range of communication to a useable distance. The transceiver choice and operating mode is important to meet our goal latency because we need received data to be sent to the MCU in the minimal possible timeframe.

LoRa Transceiver: The LoRa (Long-Range) transceiver will be responsible for transmitting and receiving packets that contain information about vibration state. It will communicate via SPI to the MCU and will

simply relay packets to and from. It will have its own voltage regulation on board, so it will be supplied the same general rail (3.7-5.0V) power. It is responsible for transmitting on the correct frequencies and at sufficient power to meet our goal of 1km LOS. The internal packeting is essential to keep our total latency <100ms.

Requirement: Upon receiving an entire packet, it should be delivered via SPI in <50ms.

¼ Wavelength Antenna: Attaching an antenna to our transceiver is required to avoid damage to the transmitter. The antenna must be tuned to the correct frequency (the correct length) to minimize RX/TX loss. For space and weight requirements we are likely to use a simple monopole antenna (normal-mode helical or solid-core wire).

Requirement: The antenna should increase our transmission range to a workable range, 1-5km.

2.2.2 Physical IO

The physical I/O subsystem will allow the user to communicate with the device's control unit: the user can hit a button to send a signal to control unit, and the control unit will send a signal to the motor controller to create a vibration that the user will feel. Essentially, the I/O subsystem is the user's gateway to the communication device. It connects logic-level (3.3V) IO to the MCU GPIO pins and uses the main power rail to drive the motor without burdening the LDO.

Input Button: The main button on the front of the device will be held down to create a vibration signal. The vibration will follow the duration of the button press.

Requirement: The button should be designed such that it would be difficult to trigger accidentally.

Vibration Motor Driver: The motor driver will be a simple CMOS chip that allows the vibration motor to be powered straight from the battery source, while still being controlled by a PWM wave from the microcontroller.

Requirement: The motor driver should be able to endure regular use without overheating.

Vibration Motor: The vibration motor will be the primary output source to the user. Once a signal is received, the motor will trigger, creating a vibration that matches the duration and pattern in the received signal. We plan on using a vibration motor can be felt through the skin, preferably stronger than a cell phone vibration.

Requirement: The vibration should be adjustable in software and able to be felt through at least two layers of clothing -- it should also not be excessively audible.

2.2.3 Control System

The control system will receive signals from the user via a button and convert those signals into a form usable by the radio subsystem (including performing AES encryption round on the packet data). It will also receive response signals from the radio subsystem and decrypt/convert those signals into PWM signals used by the vibration motor controller. Essentially, it will allow for the different subsystems to communicate with each other. We will design our control system to be the most efficient such that there is negligible latency in communication. It must do all of this while not placing an excessive drain on the limited battery power available on-board the device.

MCU: Our control system is based off the MCU and its inputted/outputted signals. We will be using the STM32F0x2 (ARM M0) microcontroller. We believe it will provide the resources we need to cache button presses, convert it into a signal that can be transmitted, and decode that signal on the receiving end. This microcontroller also contains flash memory that we will use to reprogram it during development.

Requirement: The MCU should be capable of public-key cryptographic exchange (ECC via ED25519) in < 2 seconds (with keygen, sign, verify taken separately).
Requirement: The MCU should be capable of performing a round of AES encryption/decryption in <10ms.
Requirement: The MCU should be capable of sinking and sourcing >=5mA with its GPIO pins.
Requirement: The MCU should be capable of operating at <25mA current consumption while remaining in normal running mode and not driving any external IO.

2.2.4 Power Regulation

The power system is the heart of the device. It shoulders the responsibility of keeping all the other components powered and within specification. It provides two output rails 3.3V and 3.7-5.0V depending on the other subsystem's specifications. It also must be capable of effectively charging and discharging the LiPo battery so that operating time goals can be met in normal and standby mode.

Requirement: No individual component may exceed 60C during charging, discharging to avoid potential LiPo hazards

Power Regulation: This block is responsible for stepping down the voltage from the battery / micro-USB port for use in the 3.3V logic level systems (powering the MCU) with an LDO (low-dropout regulator). It also keeps current from flowing into the battery or into the USB port when both are connected simultaneously (likely through Schottky diodes).

Requirement: When supplying 3.3V to the MCU, under a load of 25mA, voltage ripples must be < 0.1v PP

Micro-USB Port: This durable physical port is used to deliver 5.0V and initiate the charging of the LiPo battery when it is connected externally.

LiPo Charger Circuit: The LiPo Charger Circuit is responsible for recharging the LiPo battery and connects the Micro-USB port and the LiPo battery. The pure efficiency of this circuit can be disregarded if normal thermal temperatures are maintained.

Requirement: The LiPo charger must be capable of charging at 0.1 to 0.4 C (for our chosen 1200mAh battery that is 120mA to 480mA).
Requirement: It must be able to handle USB specification ongoing ripple of +-5% on the 5v rail without damage to itself or the battery.

LiPo Battery: The lithium-ion-polymer battery will power the entire circuit while the radio transmits ~10% of the time for at least one hour. A 1200mAh capacity battery would be the best fit for optimizing space and usage time.

Requirement: The LiPo battery, in standby mode, must last 8 hours of discharging until it reaches a nominal 3.7 V under no load.
Requirement: The LiPo battery should not add excess weight or take excess space in the device containment.

2.3 Risk Analysis

The highest risk component to the success of this project is the integration and use of the control system. Not only does the hardware selection have stringent requirements, but properly integrating it with all the other systems in the design phase as well as programming/debugging it will likely be our biggest hurdle due to its complexity and centrality in our project.

From a purely hardware perspective, there are many datasheet-specific entities that are required to use a standard microcontroller, including proper decoupling capacitor choices, locations, and various pull-up/pull-down resistors for the numerous external pins. We also must ensure that the differential data pair from the USB port has the correct impedance and conforms to the USB 2.0 specifications. Furthermore, we must take the correct approach to program the device, which likely involves exposing and correctly using Serial Wire Debug (SWD) pins to a header and taking a careful look at how the built-in bootloader can allow programs to be flashed via USB.

From the software side, we lean heavily on the microcontroller to be able to communicate over SPI with the transceiver to decode and encode (and perhaps encrypt/decrypt) packets that the radio can then use. We also need to have good control over and repurpose several pins into GPIO to drive and receive data from the physical IO (which is why our requirements point out the ability to source and sink 5mA).

The risk here stems mostly from the complexity of the control system as a unit in addition to how it acts as the central hub for the rest of our device. To reemphasize the tolerances for the MCU we pinpointed in the block analysis, at a minimum, we require the MCU to perform AES encrypt/decrypt round in <10ms to maintain the latency requirements between button press until vibration starts. We additionally need it to be capable of public-key cryptographic exchange (ECC via ED25519) in < 2s if we end up desiring to "handshake" devices to exchange an initial key. We also require that it has current draw at <25mA in normal operation to help maintain our battery requirements including stand-by drain and active-use drain.

3 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 [6]. 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 [3].

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, and by using diodes to prevent current from flowing in an unintended direction. We will also utilize a LiPo battery that contains a built-in over-discharge prevention circuit, which ensures that the batteries discharge at a safe and predictable rate. 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 contact the exposed Lithium-ion cell to avoid the severe fire risk of a puncture. [4]

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 be sure [5].

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 [5]. 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 [5]. The transceiver that we will use will be FCC certified for use as a module in device integration, so we do not have to worry about the bands nor the power the device will use.

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 AES encryption algorithm 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 [6]. 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 out there: 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.

References

[1] "How technology is transforming in-ear headsets," Police1, 02-Nov-2018. [Online]. Available: https://www.police1.com/police-products/communications/headsets-earpieces/articles/how-technology-is-transforming-in-ear-headsets-revQsRhZt0NPONJs/. [Accessed: 19-Feb-2021].

[2] M. Perin, "5 Technologies To Improve SWAT Communications," Officer. [Online]. Available: https://www.officer.com/tactical/swat/article/21071376/5-technologies-to-improve-swat-communications. [Accessed: 19-Feb-2021].

[3] 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].

[4] “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].

[5] “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].

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