Touchless Proximity Lock

ECE 445 Design Document Check

Brant Bedore, Jason Hackiewicz and Talita Barbosa

Group 45

TA: Madison Hedlund

2/25/20

1 Introduction

1.1 Objective

Home security systems play a crucial role in protecting the population's homes and valuables around the world. The vast majority of these systems are mechanical in nature and are designed for simplicity and ease of use. However, ten million people around the world live with Parkinson's disease which causes tremors that impair the ability to perform physical tasks [1]. Many others suffer from arm amputation, loss of arm motion due to paralysis or stroke, and other various arm and hand motion impairments. These disabilities among others hinder the user's ability to use these mechanical locking systems. For example, someone with Parkinson's disease would have trouble putting a key into the lock on their front door due to their tremors.

For this purpose, we have taken on the task of developing a touchless proximity lock system. Current electronic locking systems on the market require some sort of touch to the device whether it is a user interface input or RFID scan. Our technology differs by striving to be fully touchless in operation. The user's electronic key will unlock the door without the necessity of touch. This solution could be applied in the households of people with disabilities to simplify the operation of their home security systems while helping them become more independent despite their impairment.

1.2 Background

Many keyless lock systems have been developed both for home and hotel use. Despite this, keyless locking systems still require touch in order to be operated. Homes have many options, such as the keypad system, which requires a password to enter the house from the outside and has a manual lock from the inside [2]. Operating the keypad interface would still be troublesome for our target audience. Another popular alternative to keyed locking systems are "smart locks" which have the ability to be locked and unlocked using a cell phone or similar electronic device. These devices often use wifi communication in addition to a software application to control home security [3]. However, the locking system unlocks using phone operation which holds it back from being a truly touchless device. Other electronic alternatives exist as well such as the use of Radio Frequency Identification (RFID) technology associated with a keycard but these also require the user to touch the card to the locking system. Similarly, there are magnetic key cards, which use a magnetic strip to unlock the door. These, despite being a cheaper option, can be damaged easily and, again, are not entirely touchless [4].

1.3 High-Level Requirements

- HLR-1: The home security system shall operate without the user needing to pick up, hold or manually operate the key device in their hands.
- HLR-2: The security system shall unlock when the key is located within a distance of within ten feet from the locking device.

- HLR-3: The security system shall not be unlocked unintentionally by a passing user from inside the home.

2 Design

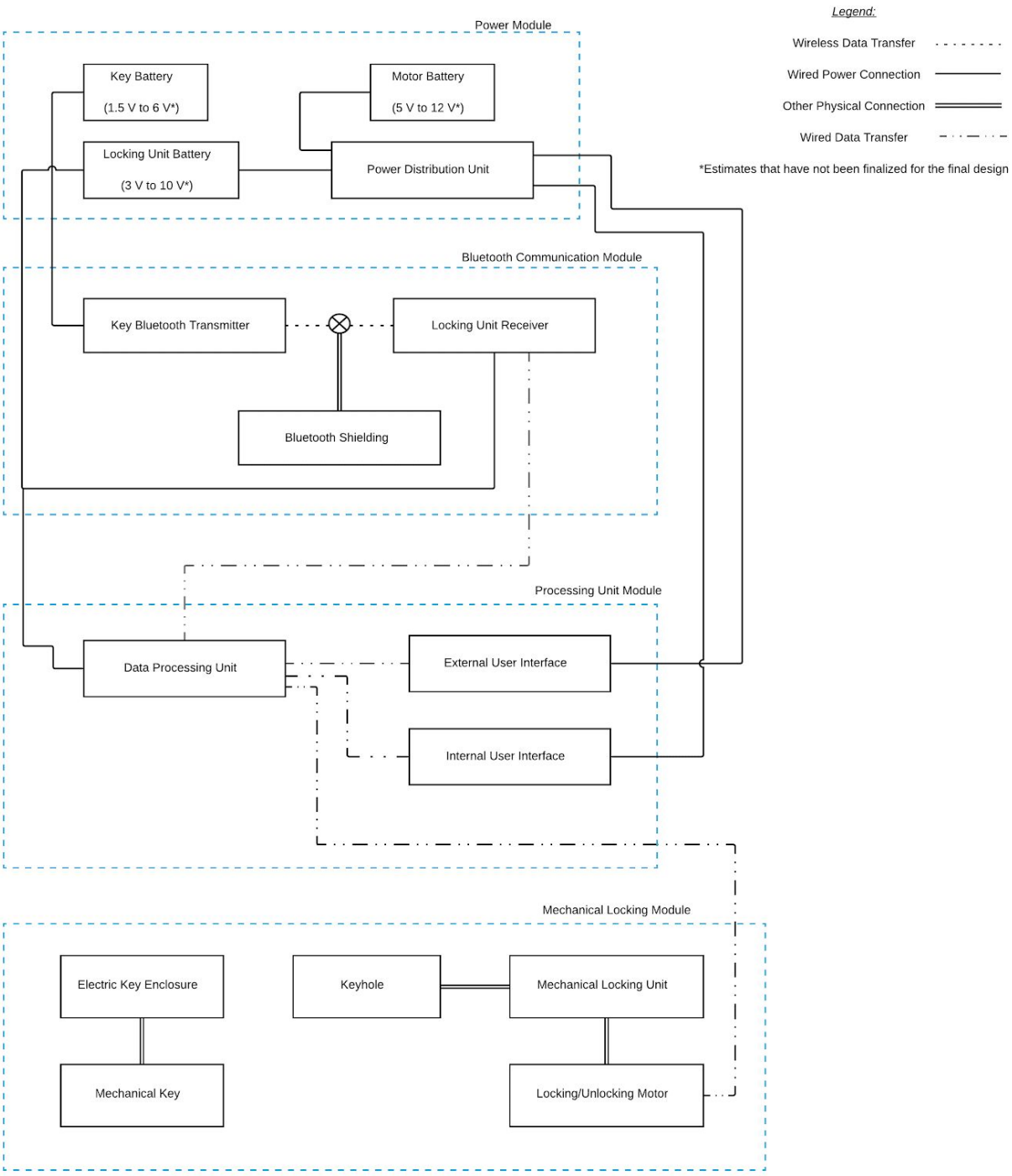

Figure 1 - Block Diagram of the Proximity Lock

A design overview is conducted over the following sections to clarify how each module and block of the system operates. Before beginning, it is important to establish the nomenclature associated with the system. There are two primary physical devices associated with the system: the key and the locking unit. The key is a small electronic device which could be easily carried in a pocket or purse. The locking unit is a device that directly interfaces with the door and its lock. The locking unit features the electronics required to process the locking operation as well as the physical interfaces necessary to carry out this task. The locking unit features a printed circuit board to handle data and power distribution as well as the connections to the various user interfaces. A servo motor is also included as part of the locking unit to control a deadbolt lock when the lock command is engaged.

There are four main modules which compose the system: a power distribution module, a Bluetooth communication module, a processing unit module and a mechanical locking module. The power distribution module supplies power to each electrical device in the system via a collection of batteries and wire routing. All of the necessary Bluetooth communication components are included under the Bluetooth communication module. The processing unit module contains the printed circuit board (PCB) which processes and interprets data. This module also encompasses the data processing and communication with the user via an external and internal user interface. These devices include small LED based displays to alert the user if there is some change in the device's functionality. Interfaces between the electrical components and the physical world are handled by the mechanical locking module. This module includes the physical enclosures that house the key and locking unit as well as the devices required to physically lock the door, like the servo motor. Also included in this module are alternative methods to unlock the door mechanically in case the system fails such as the mechanical key and its associated keyhole.

2.2 Bluetooth Communications Module

To fully realize the touchless component of the proximity lock system, adequate communication must occur between the user and the system. Integrating the touchless aspect into this area is a particular challenge as there must be some way for the locking unit to recognize whether the door should be unlocked or not. For this reason, processing will occur via a Bluetooth transmission and reception device. Bluetooth is a low power radio standard in which two paired devices can transmit data over a short range. A small network between the paired devices called a piconet is formed which detects nearby Bluetooth devices and their associated addresses [5]. Once the devices are paired, they will cause the motor to rotate, unlocking the door in the process. For this system, the Bluetooth transmitter will be a component of the key and the the receiver will be a component of the locking unit.

2.2.1 Bluetooth Key Transmitter

Functionally, when the user steps within a certain range of the Bluetooth receiver while carrying the transmitter on their person, the door will automatically unlock. The Bluetooth module chosen is the HC-05 Bluetooth 2.0 Serial Pass-Through Module by DSD Tech. This module can receive 3.6 V to 6 V, which is within the expected input voltage, and can be connected to an Arduino for control, which will be described in another section of this document. The advertised range is 10 meters (32.8 feet), and power consumption of around 0.0025W, which fits the required low power consumption. This could

possibly be lowered even more by setting the programmable transmission speed, which is 38400 baud by default, to be lower. Lowering the power consumption, however, is not totally necessary for the success of this project, given that the default rate is already very low.

This device will be able to transmit data by being programmed as the master. The transmission itself can be processed with low amounts of data transferred as the only data that needs to be processed is a signal to lock/unlock the door. This is accomplished by the nature of the chosen Bluetooth module, which sends only one bit of information at a time according to the transmission speed. The device will constantly send small amounts of data to the paired device as long as it is on. When the locking unit is detected within the range of the transmitter, an “unlock” signal will be sent to the receiver, which will be done by having a loop on the arduino code that constantly sends a logic "1" to the transmitter.

Because the device is supposed to remain in the user’s pocket, the transmission component should be kept to a relatively small size. The HC-05 module is very small and, even paired with an arduino and battery, could easily fit into a pocket.

2.2.2 Bluetooth Locking Unit Receiver

The same Bluetooth module will be used for the locking unit, but, this time, as the slave. The Bluetooth receiver waits for a signal to be sent by the transmitter and then proceeds to process the signal. The receiver will constantly be checking for the “unlock” signal until it is received by the transmitter. This is the default of this module, and its receiving speed has to match the transmission speed of the master Bluetooth module. As mentioned before, the speed determined the refresh rate of the module, which can be programmed.

Once a signal is taken in by the receiver from a paired transmitter, the device will send a signal to the control PCB (Arduino) to power the unlocking motor. This is challenging because our project requires that the Bluetooth connection is made within 10 feet, but Bluetooth signals can have a range of about a kilometer, and the chosen module can range up to 32.8 feet. However, we can make sure our device has a smaller range and will not interfere with other signals from industrial, scientific and medical devices [5]. This solution would be to control the range with the "state" pin on the HC-05 Bluetooth Module, which has a value of 1 while the device is connected (ON), and 0 while disconnected (OFF). Once the ON state is established at 32 feet, the Arduino can delay the signal sent to the motor by adding a timer, which would only unlock the door at around 10 feet. The average walking speed can range between 0.94 meters per second to 1.43 meters per second [6], so the timer will be between 4.8 seconds to 7.4 seconds. This process can be seen in Figure 1.

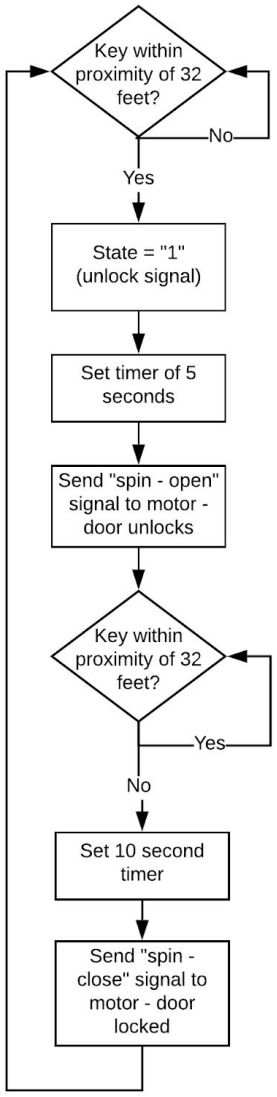

Figure 2 - Pseudocode of locking/unlocking signal routing

Likewise to the transmitter, the power needs to be kept low, which is achieved by the low power consumption of the HC-05 module, along with the possibility of lowering the transmission and receiving speeds to make it even lower, as previously mentioned.

Requirements	Verification
BCM-2: The Bluetooth receiver shall receive the unlock signal within 10 feet of the user approaching the door, without the user having to operate the key using their hands.	A. The key shall be inside of the user's pocket, who shall walk towards the lock starting at approximately 20 feet away. Once within 10 feet, the lock shall unlock. B. A distance of 20 and 10 feet shall be measured beforehand, and these will be marked on the floor by a post-it.

2.2.3 Bluetooth Shielding Device

A reasonable concern with a device like the one proposed is security from the inside of the home or apartment. It would be an undesirable function of a home security system for the door to unlock when a user passes by while carrying a key on the inside of the home. For this reason, a Bluetooth signal shielding device will be applied to one side of the receiver, on the inside of the door. This will function as a Faraday cage, blocking the magnetic field and disrupting the radio frequency that the Bluetooth devices use to communicate. With this device applied to the receiver, the device will only receive signals to unlock the door from outside and prevent unlocking the door when already inside the house. Faraday cages can be constructed simply using a mesh of conductive materials. The shielding device will be built with this principle out of relatively simple and cheap malleable metal.

Requirements	Verification
BCM-3: The Bluetooth shielding device shall stop signals from being interpreted on the shielded side of the receiver and shall allow signals to pass through on the other side.	A. The key shall begin in the user's pocket while the user stands 5 feet away from the locking unit on the shielded side of the Faraday cage. B. The user shall walk around to face the non-shielded side of the receiver while maintaining a 5 foot radius to test if the door unlocks and the signal is not disrupted from that side. C. Modifications will be made in accordance with the thickness and geometry of the cage to cause disruption when desired.

BCM-4: The shielding device shall not interfere with the operation of other components of the touchless proximity lock system.	A. Wired communication will be used instead of wireless for all non bluetooth communication. B. Components will be unit tested when in close proximity to the Faraday cage. C. The full system will be tested with the Faraday cage in place to confirm unwanted disturbances occur.

2.2.4 Arduino

An Arduino Uno will be used to control and power both Bluetooth modules, as well as sending signals to the motor for the door to be unlocked. Therefore, we will have two total Arduinos, one for the key, and one for the locking unit. Since these devices are bulky, we will build one on the control PCB that will provide the same capabilities. For that, we will need an Atmel ATmega328 chip, which is the microcontroller in an Arduino, LEDs for testing, wires, capacitors, resistors, a voltage regulator, a button to be able to reset the program and a clock crystal [7]. These parts are listed in detail later on this document. These will essentially work as an Arduino, being able to connect to the Bluetooth modules and be programmed in the same way, through the IDE.

.

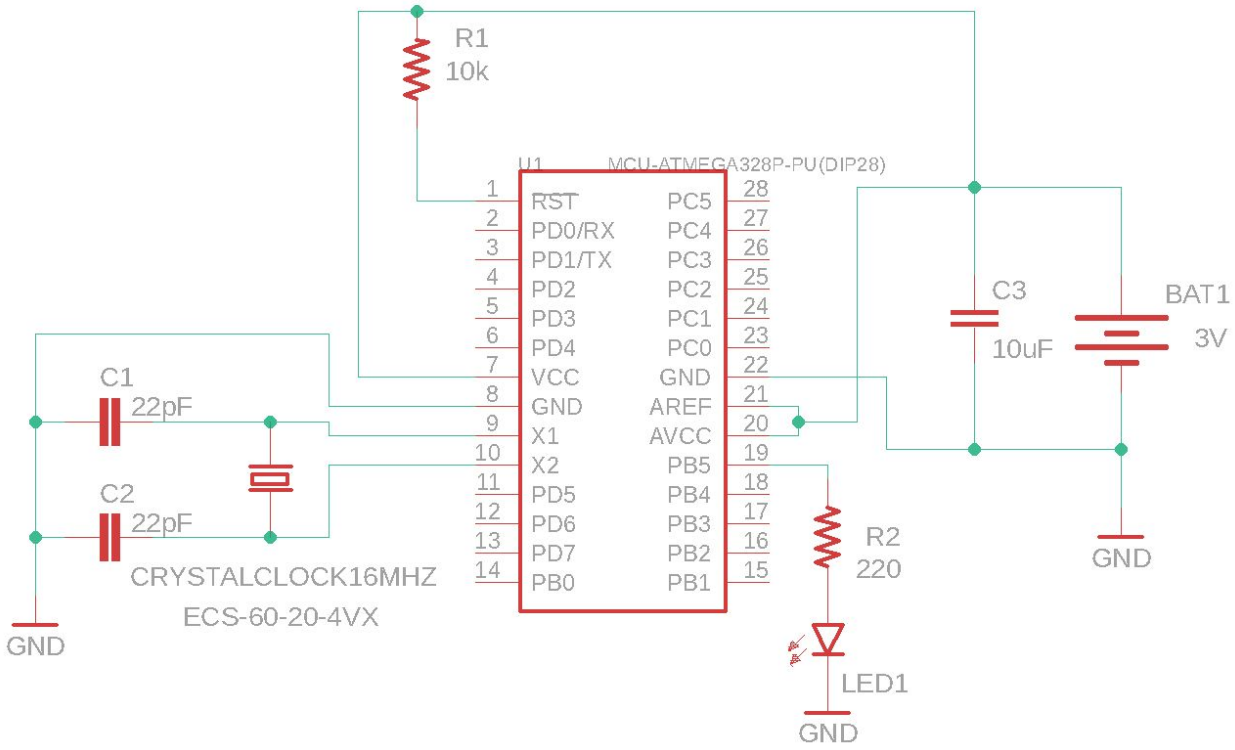

Figure 3 - Arduino on breadboard schematics

They will be powered with a coin battery of 3 V and a capacity of 1000mAh. The microcontroller chip on the Arduino can consume a lot of power, even when not performing any tasks. We are able to optimize this system, however, to have low power consumption by using the JeebLibrary to make the microcontroller sleep for a few seconds [7].

2.4 Mechanical Locking Module

Interfaces between physical components and electrical signals are bridged via a mechanical subsystem. Included in this module are electrical housings for both the key and locking unit as well as a modified deadbolt lock. This modified deadbolt is designed to automatically lock using a servo motor positioned to apply sufficient torque to the rotational component of the deadbolt. Important priorities considered during the design of this module included size of components, speed of unlocking capabilities and ability to sufficiently perform its mechanical task.

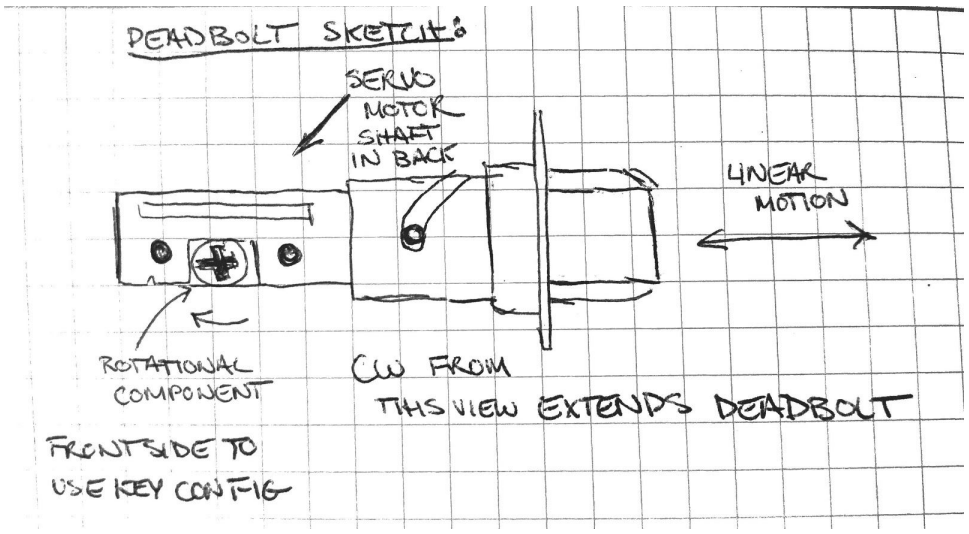

Figure 4: Sketch of prototype deadbolt (Side View)

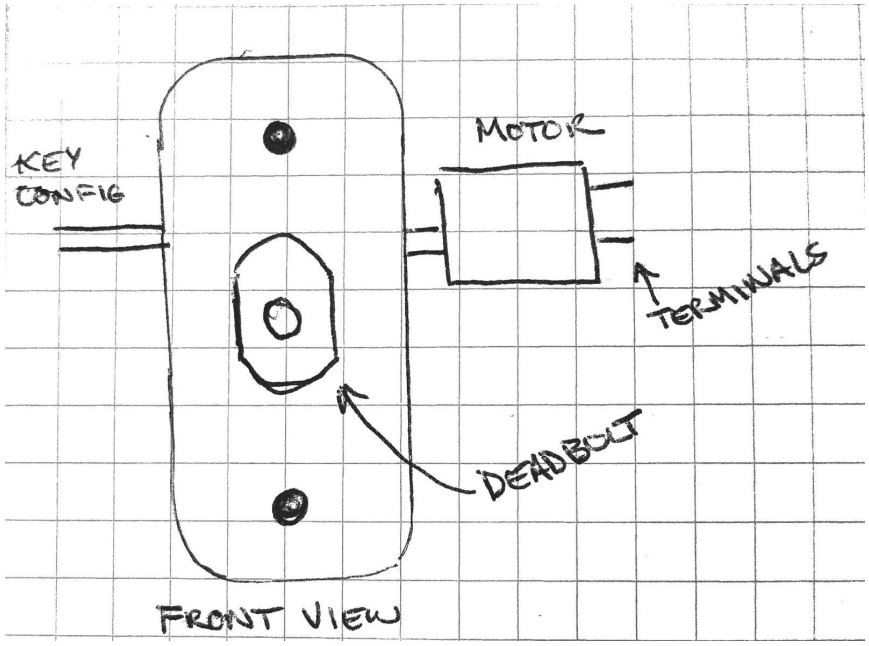

Figure 5: Sketch of prototype deadbolt (Front View)

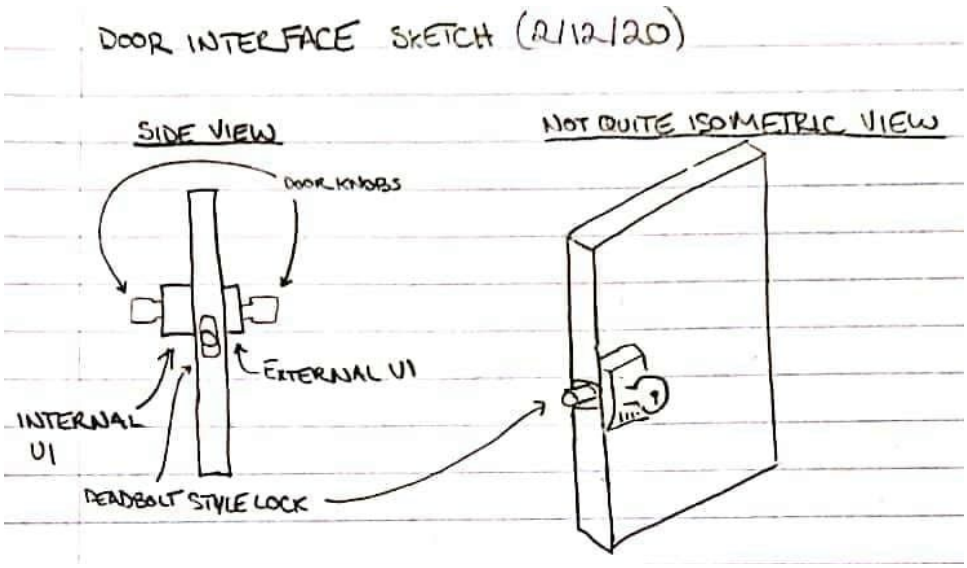

Figure 6 - Sketch of the Mechanical Locking Module

2.4.1 Key Enclosure

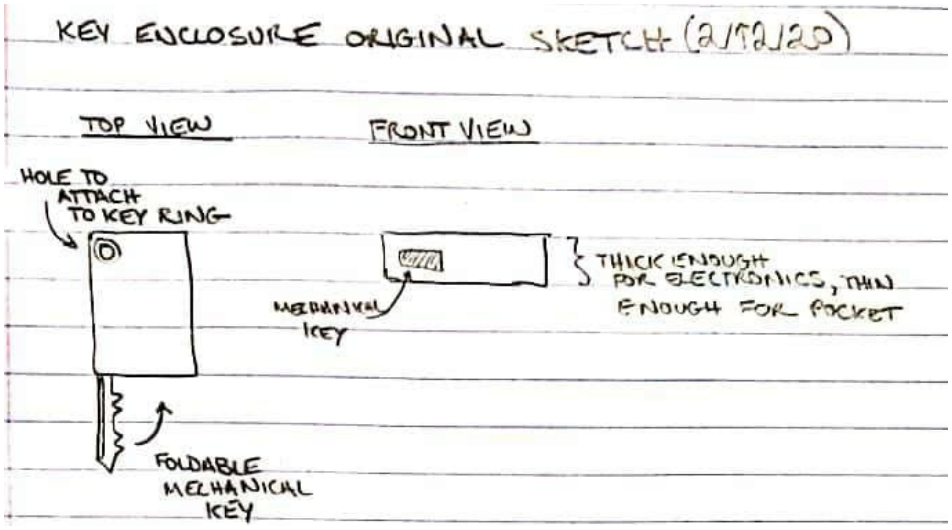

Figure 7 - Initial design of the Key Enclosure

While not mechanically complex, the key enclosure's design is important for housing the electronics to control the entire system. For this reason, the enclosure will be composed of a simple modified electrical project box. The project box selected must be large enough to contain the Bluetooth transmitter but small enough to fit in the users pocket. Small holes will be drilled into the project box such that an LED

can be mounted and wired to the inside without compromising protection. This LED will be used to display if the electronic key has twenty percent or less battery remaining.

Requirements	Verification
MLM-1: The key enclosure's size shall be small enough to fit into a pocket (10 inches deep by 8 inches across) or purse and shall be considered a priority in its design.	A. The project box chosen shall be smaller than 6 in X 3 in X 2 in. B. The project box will be put into the users pocket during testing and demonstration to prove hands free operation.
MLM-2: The key enclosure shall surround the electronics such that electronics cannot be touched while key enclosure is fully assembled.	A. All holes drilled for routing wires will be kept under a radius of 5mm to prevent debris from entering the box. B. The electronics inside the project box shall not be able to be accessed or touched by someone using the product during demonstration.

2.4.2 Locking Unit

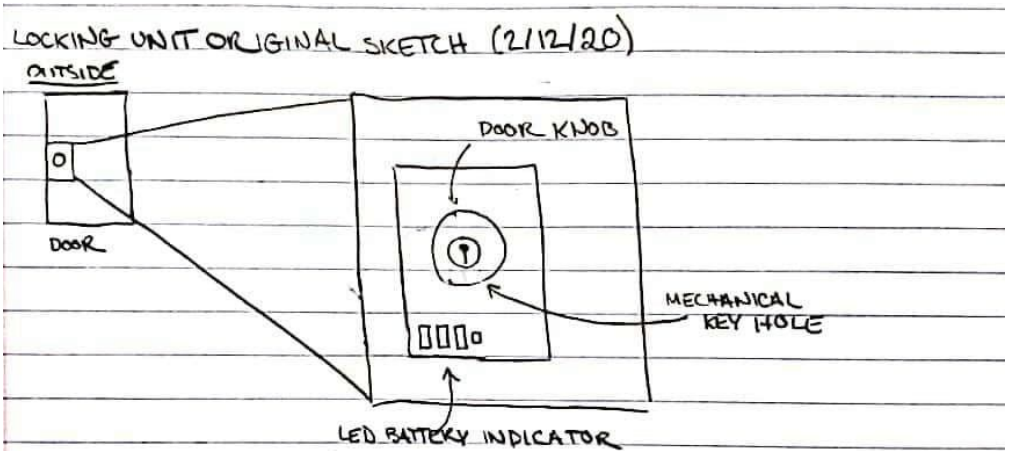

Figure 8 - Initial sketch of the outside of the door and the locking unit

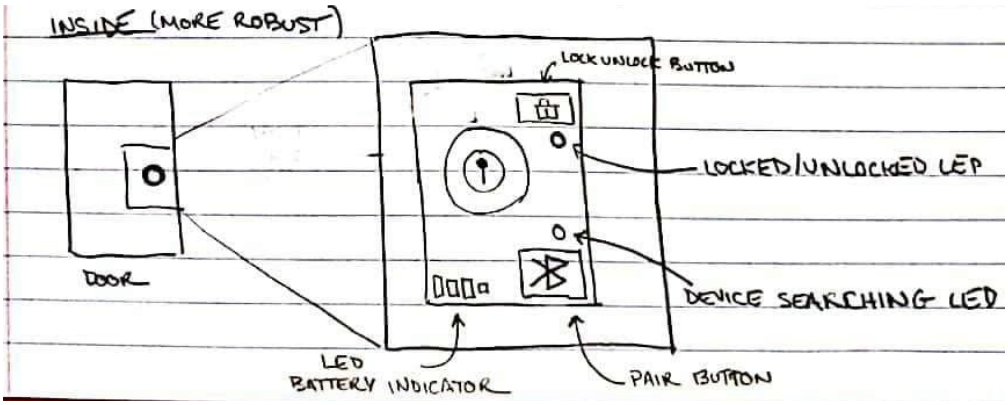

Figure 9 - Initial sketch of the inside of the door and the locking unit

The locking unit will have a servo motor that will turn the deadbolt lock once the motor receives a signal from the processing unit. If the user needs to use the mechanical key, the locking mechanism will work as a common lock and bypass the motor.

The locking unit is composed of various physical components which would be mounted on a door for the full implementation. For ease of use on both sides of the door, the locking unit is divided into an external and internal component corresponding to the external and internal user interfaces detailed above. For the external component, no buttons will be routed to the front but LEDs will be mounted to indicate the remaining battery life of the locking unit. The internal component will include a similar LED configuration but also will include a user accessible button mounted alongside the display. Additionally, the Bluetooth shielding device will be mounted around the Bluetooth transmitter in the external component of the locking unit. Mounting and enclosure of the unit will be created with the assistance of the ECE machine shop staff.

In addition to the displays and user interfaces associated with the processing unit module, there is a mechanical component to the locking unit which includes a modified deadbolt lock. Most deadbolt locks are traditionally driven by converting rotational motion to linear motion and this design capitalizes on that principle. A 12 V servo motor will be applied to drive the cylindrical hub of the deadbolt lock when given a lock or unlock signal. The motor shaft will apply sufficient torque to rotate the hub ninety degrees in order to fully extend or retract the deadbolt. To prevent damage to the deadbolt lock, the motor will not rotate further than ninety degrees. In case of system failure, the original mechanical key access will remain operational. Under failure conditions, the mechanical key will be able to rotate the lock by backdriving the motor through the cylindrical hub. While speed of operation will be considered for the motor, the torque parameter was prioritized in the motor selection process to ensure the torque is large enough to actuate the deadbolt.

Requirements	Verification
MLM-3: The servo motor shall supply at minimum 5% more than the sufficient torque required to rotate the deadbolt cylindrical hub.	A. The operating torque shall be carefully considered as a design choice and verified using observed stall torque and DC motor's linear relationship between speed and torque if necessary. B. The servo motor shall be tested before mounting to the locking unit by using the shaft to drive the cylindrical hub.
MLM-4: The servo motor shall rotate 90 degrees per lock/unlock motion with a tolerance of plus or minus 5 degrees.	A. During Arduino software development, motion shall be programmed to rotate exactly 90 degrees and adjusted accordingly. B. The rotor shall be marked and rotated through one unlock and lock cycle and the angle will be measured. C. The motor shall be positioned to rotate the deadbolt and observations shall be taken for signs of stalling such as odd sounds or noticeable wear.
MLM-5: The user shall be able to use a mechanical key to operate the deadbolt lock in case of a system failure by backdriving the motor.	A. The machine shop shall be notified of plans to include backdriving capabilities to the motor. B. The motor shall be positioned for the user to backdrive via rotation of the rotor. A multimeter or oscilloscope shall be attached to the motor terminals to identify if backdriving the motor will have a significant electrical effect. C. After mounting, the mechanical key will be inserted while the power is off. The user will turn the key to test if the door can be both locked and unlocked.

5 Safety and Ethics

Ethical considerations were taken during the birth of this project to ensure no parties were harmed in its development. In particular, each item of the IEEE Code of Ethics Section 7.8 was carefully adhered to [8]. The proximity lock system is designed with the intent to develop a technology that could be applied to help users with a particular focus on users with disabilities. While we believe the concepts applied to this device are unique to the market, we understand that most of the technology used to do so is not. For this reason we do not intend to become in conflict with other parties by commercializing this

product. All of the data reported here and in future documentation is submitted to the best of our knowledge and all work and studies completed for this project will be reported honestly in the design document and our respective engineering notebooks. In this endeavour, studies will be conducted transparently with professors for the technological betterment of society. Any outside sources used will be properly cited in adherence to the IEEE guidelines. While the device is targeted toward an audience with disabilities, it does not discriminate as the intent is to assist people in their daily lives and can effectively be used by a person without a disability. This device is intended to be used for improving the lives of its audience and not for any action of a malicious nature. The following section contains information in regards to several ethical and safety concerns in regards to the project in addition to their proposed solutions.

Radio communication devices often have restrictions on use. However, Bluetooth frequencies are used as a standard for industrial medical and scientific in a range of 2.4 GHz to 2.483 GHz. Because the Bluetooth devices will operate within this standard, legality of developing the device should not be an issue.

One concern with any electronic security device is the possibility of an intruder confiscating the information necessary to hack the device. Bluetooth is a radio based technology and frequencies can be intercepted allowing unwanted guests to obtain personal information. However, by only exchanging information with trusted paired devices and applying device level and service level security, the threat of someone breaking in is minimized [5]. In addition, encrypted data using an algorithm such as AES can be used to protect the unlock signal sent from the Bluetooth key. While this solution maximizes security, it also increases the amount of data transfer and is more taxing on the battery and power system.

Another concern in regards to security would be the situation in which the user misplaces their key or another person obtains the key. A solution to this would be a method to remotely disable the Bluetooth key from being able to manage the locking system. This could be done from another Bluetooth device like a cell phone or computer when close to the door. Because the focus of this project is to develop the Bluetooth technology with touchless capabilities and not developing a complex encryption algorithm or remotely disable a Bluetooth device, we believe this aspect of the design is beyond the scope of the project in its current form.

The final security concern worth mentioning is the ability to unlock the door by standing a certain distance away from the locking device. Issues arise if a user is within the proximity but does not want to unlock the door. For this reason we implemented the Bluetooth shielding component as a part of the Bluetooth communication subsystem.

Safety of the product developers and users was a primary consideration taken in the construction of this design in accordance with the IEEE Code of Ethics Section 7.8 [8]. All devices involved in the system perform their tasks with low power usage so the voltages that will be used should not pose any danger to the user or developer. The most dangerous component of the locking unit are the devices associated with the mechanical design, namely the servo motor and the deadbolt lock. If mishandled, a user could cause harm to their fingers if the motor locks or unlocks without the user knowing. However, many locks operate with a deadbolt system and are relatively safe when used properly. The locking motor would be

contained within the locking unit and would not be accessible to the user. Torque associated with this servo motor just needs to be sufficient to shut the deadbolt and therefore the torque should slightly exceed that level. With careful assembly and construction in the senior design lab the developers should be kept safe during the devices construction. Because there are no plans to commercialize this product, it is necessary to develop a manual for user safety at this time.

References

[1] E. Naqvi, “Parkinson's Disease Statistics,” Parkinson's News Today, 06-Aug-2018. [Online]. Available: https://parkinsonsnewstoday.com/parkinsons-disease-statistics/. [Accessed: 13-Feb-2020].

[2] B. Hubbard, “The 10 Best Keyless Door Locks,” The Architect's Guide, 07-Jan-2020. [Online]. Available: https://www.thearchitectsguide.com/articles/best-keyless-door-locks. [Accessed: 13-Feb-2020].

[3] “Best WiFi and Bluetooth Smart Door Locks: 2019 Listings and Reviews,” Postscapes, 13-Dec-2019. [Online]. Available: https://www.postscapes.com/wireless-door-locks/#remote-locking. [Accessed: 13-Feb-2020].

[4] “How Do Hotel Door Locks Work?,” GoKeyless, 03-Sep-2019. [Online]. Available: https://www.gokeyless.com/blog/how-do-hotel-door-locks-work/. [Accessed: 13-Feb-2020].

[5] C. Franklin and C. Pollette, “How Bluetooth Works,” HowStuffWorks, 11-Nov-2019. [Online]. Available: https://electronics.howstuffworks.com/bluetooth2.htm. [Accessed: 13-Feb-2020].

[6]“What Is the Average Walking Speed of an Adult?,” Health Line. [Online]. Available: https://www.healthline.com/health/exercise-fitness/average-walking-speed#average-speed-by-age. [Accessed: 25-Feb-2020].

[7]“How to Run and Arduino for Years on a Battery,” Open Home Automation. [Online]. Available: https://openhomeautomation.net/arduino-battery. [Accessed: 25-Feb-2020].

[8] “IEEE Code of Ethics,” IEEE. [Online]. Available: https://www.ieee.org/about/corporate/governance/p7-8.html. [Accessed: 13-Feb-2020].