Touchless Proximity Lock

ECE 445 Design Document

Brant Bedore, Jason Hackiewicz and Talita Barbosa

Group 45

TA: Madison Hedlund

2/21/20

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 Visual Aid

Figure 1 -Simple visual diagram of how a user would operate this device. Once the user approaches the door, the door will unlock so that the door is open by the time they reach the handle.

1.3 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].

Electronic assistive devices have been commonality in the homes of people suffering from physical disabilities since the invention of the electronic hearing aid using Alexander Graham Bell's telephone technology. At the dawn of personal computers, several applications of text to speech technology are applied in modern computer systems to allow visually impaired users to read. Even more impressive are Smart Brailler devices which assists blind users by providing the tools necessary to type digital documents [5]. Today, many technological advancements such as the growth of wireless communication have contributed to simplified applications of everyday tasks. Specifically, Bluetooth has numerous applications for short ranged communication. Bluetooth technology was developed over 20 years ago as an alternative to high power, long distance communication. By making use of the 2.4 GHz to 2.485 GHz frequency range, digital communication was made possible for low power systems at a small distance [6]. This protocol is particularly useful for assistive devices as they can be manufactured for consumers for home use at low costs. Several Bluetooth systems working together can significantly impact the way that a handicapped user performs tasks we take for granted.

1.4 High-Level Requirements

- HLR-1: The security system shall unlock and lock 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 ten feet while directly in front of the locking unit.
- HLR-3: The security system shall not be unlocked unintentionally by a passing user behind the locking unit within a distance of two feet.

2 Design

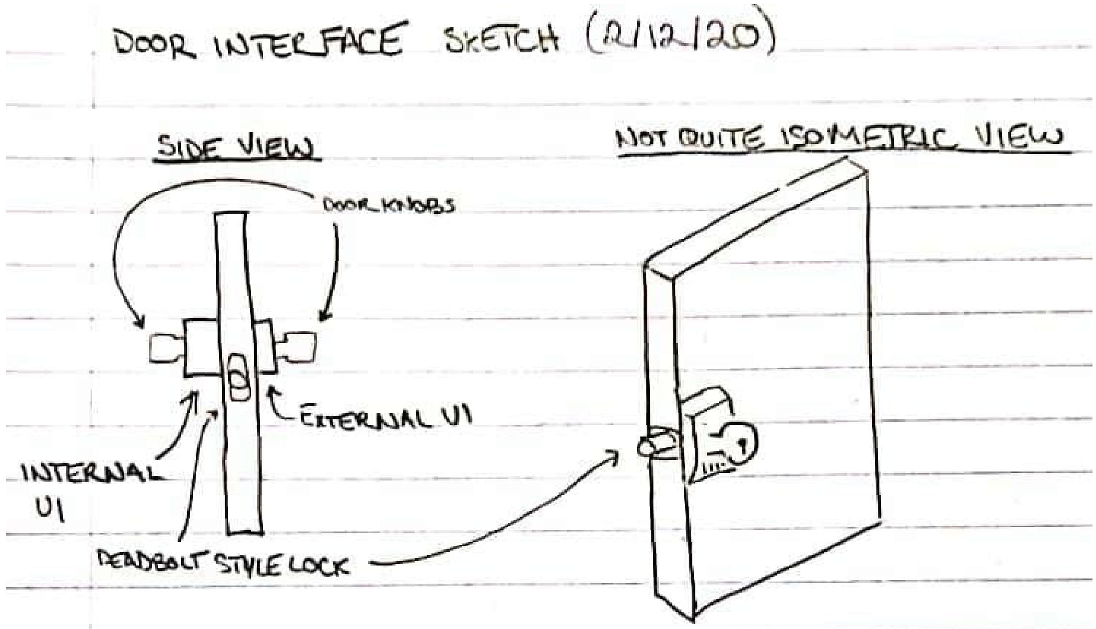

Figure 2 - First sketch of design idea and how the electronic components would interface with a door.

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.

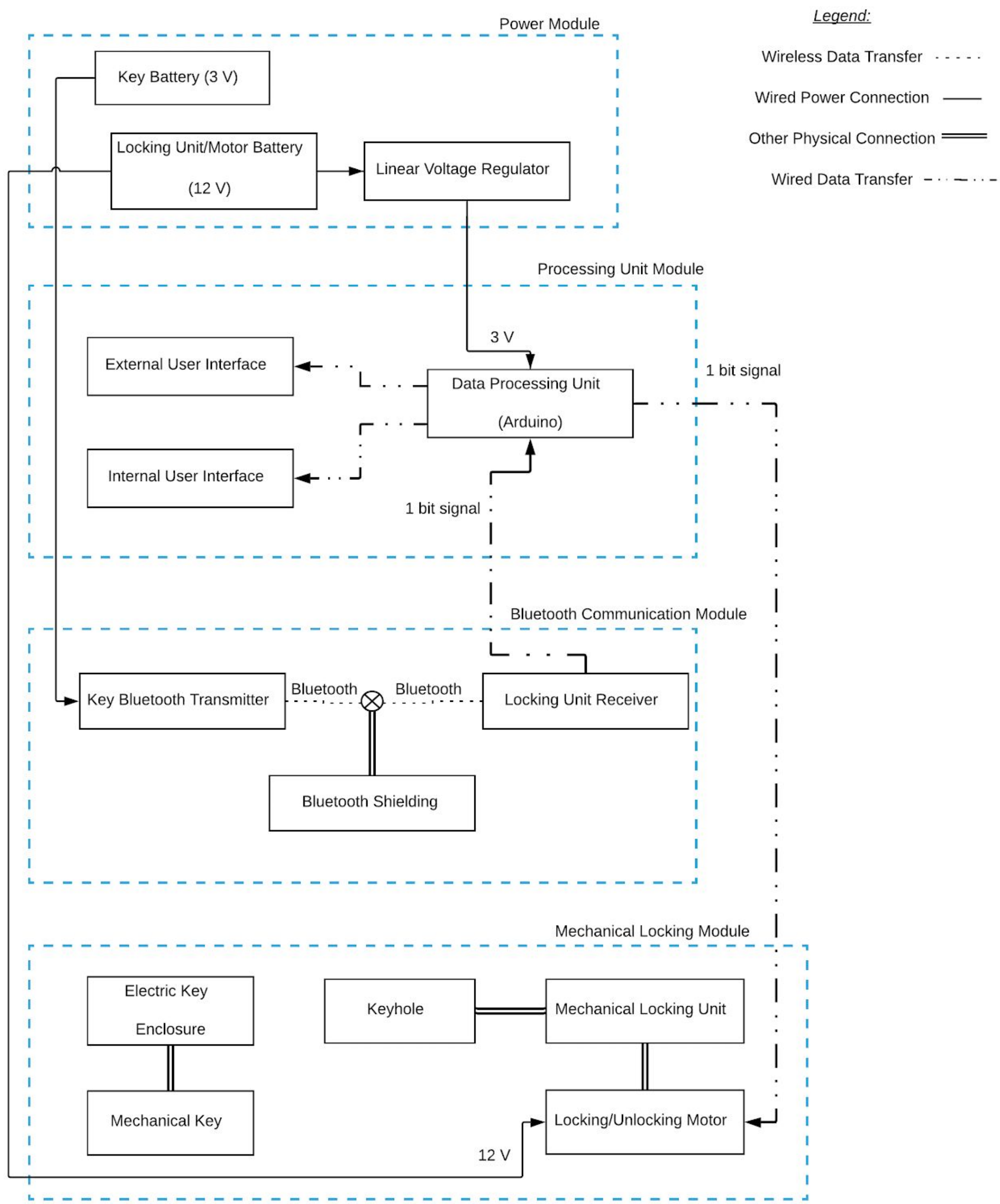

Figure 3 - Block Diagram of the entire Touchless Proximity Lock system. This is composed of four modules: Power, Bluetooth Communication, Processing Unit and Mechanical Locking.

2.1 Power Supply Module

Each electrical device associated with this system will require power to be able to run. The power supply module is composed of several batteries and power distribution wires to supply the power necessary for each individual component.

2.1.1 Batteries

In order to operate the electronic key and locking unit, two seperate power supplies are necessary. The key will have its own battery and will only have to power the PCB, which will control the Bluetooth transmitter. Even though the transmitter will be constantly sending signals, its power consumption will be small since the power consumption of the HC-05 [7] Bluetooth module is very low, and will be connected to the 5 V pin on the ATmega328p. The battery on this module is, therefore, powering the PCB, which can have a coin battery of 3 V, since the current drawn is around 0.2mA [8]. The schematic of how the battery is connected to the PCB is shown in Figure 5 in section 2.3.1.1.

The power supply for the locking unit will also be battery operated. Many components on the locking unit will need power, such as the PCB, which will have the Bluetooth receiver connected to its 5 V pin, and the LEDs that are used for the user interface. For this reason, the expected voltage necessary for this power supply is slightly higher than the battery necessary for the key. It was decided to have one 12 V battery for this unit, since it needs to power the motor as well. Since the PCB cannot receive that much voltage, it will be stepped down to 3 V by a linear voltage regulator, which was chosen to be the MCP1702 by Microchip.

Requirements	**Verification**
PSM-1: The key battery shall supply an input voltage of 1.8 V to 5.5 V to power the PCB that drives the Bluetooth in the key, which makes it connect to the receiver.	A. The Bluetooth modules shall connect when they are within proximity of each other, which will be visible by the synchronized blinking pattern on their respective pairing LEDs.
PSM-2: The locking unit shall supply a voltage input of 12 V to power both the motor and the PCB that drives the Bluetooth and control signals.	A. The Bluetooth modules shall connect when they are within proximity of each other, which will be visible by the synchronized blinking pattern on their respective pairing LEDs. B. The ATmega328p shall receive the connected signal and send the unlock

	signal to the motor, both signals shall be able to be seen through the serial monitor. C. The motor shall spin and unlock the door once unlock signal is received.

Table 1 - Requirements and verification for Power Module in regards to batteries.

2.1.2 Power Distribution Unit

Power distribution is only necessary for the locking unit. Since there will be only one battery of 12 V for all its components, there is a need for a linear voltage regulator to step down the voltage for the PCB used to drive the Bluetooth.

Requirements	Verification
PSM-3: The voltage from the 12 V battery shall be distributed to the PCB, which will receive 1.8 V to 5.5 V, and to the motor, which should receive 12 V.	A. The linear voltage regulator output voltage shall be measured with a multimeter. B. The input voltage from the motor shall be measured with a multimeter

Table 2 - Requirements and verification for Power Module in regards to distribution.

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 [10]. 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 will be provided by the ATmega328 chip on its 5 V pin and 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 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 IDE 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 PCB and battery, could easily fit into a pocket.

Requirements	**Verification**
BCM-1: The Bluetooth transmitter shall send 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.

Table 3 - Requirements and verification for Bluetooth Communications Module in regards to key operation.

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 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 [10]. 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 PCB on the locking mechanism 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 [11], so the timer will be between 4.8 seconds to 7.4 seconds.

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 receiver shall send a spin signal to power the unlocking motor once the Bluetooth receiver receives a signal from the paired transmitter.	A. The Bluetooth modules shall flash their respective pairing LEDs synchronously when connected to each other. B. Motor shall spin once spin signal is received, unlocking the lock. C. The Bluetooth modules shall connect when they are within proximity of each other, which will be visible by the synchronized blinking LED pattern on both Bluetooth modules

Table 4 - Requirements and verification for Bluetooth Communications Module in regards to the locking unit.

2.2.3 Bluetooth Shielding Device

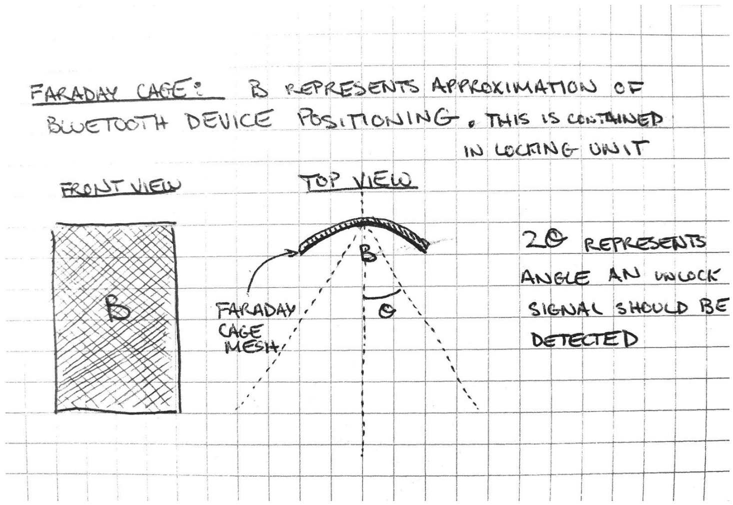

Figure 4 - Sketch of The Bluetooth shielding device using the Faraday cage concept.

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 several pieces of aluminum mesh. This mesh will be constructed to cover one side of the receiver and prevent signals being received from behind the receiver. By nature, a Faraday cage has a destructive nature toward electrical signals so the geometry of this component is vital to its success. By bending a simple rectangular sheet to have a slight curve, the angle in which the user can unlock the door will be restricted such that only a user walking toward the door can unlock it. After defining a plane that follows the path directly across from the HC-05 receiver, an angle can be defined to represent a range on either side of the plane that a signal can be detected. An example of this geometry can be seen in Figure 4.

Requirements	Verification
BCM-3: The Bluetooth shielding device shall allow signals to be received from a key directly in front of the receiver and at minimum 15 degrees from this plane on both sides.	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 directly behind the receiver. The lock will be in the locked state. B. The user will walk counterclockwise in a 5 foot radius around the locking unit until reaching the 15 degree mark. If the locking unit enters the unlocked state as expected, this requirement is verified.
BCM-4: The Bluetooth shielding device shall disrupt unlock signals from the key when directly behind the receiver and at a minimum of 90 degrees from this plane on both sides at a distance of at least 2 feet from the receiver.	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 directly behind the receiver. The lock will be in the locked state. B. The user will walk 90 degrees clockwise, followed by 180 degrees counterclockwise. If the receiver does not receive an unlock signal, this requirement is verified.
BCM-4: The shielding device shall not interfere with the operation of other components of the touchless proximity lock system.	A. All non-bluetooth data routing, such as the unlock/lock and spin signals, shall be designed using physical connections instead of other wireless signals to prevent disruption from the shielding device. B. Each component in the processing unit module will be unit tested in the position it will be in relation to the shielding device. This is done to ensure each device operates as expected without interference caused by close proximity to a conducting material. C. The full system will be tested with the Faraday cage in place to confirm unwanted disturbances occur.

Table 5 - Requirements and verification for Bluetooth Communications Module in regards to the shielding device.

2.3 Processing Unit Module

A small central processing unit subsystem is implemented in order to route data and communicate information to the user. This subsystem will be directly attached to the mechanical locking subsystem and would be composed of a few small displays as well as a data processing PCB. This unit will handle the received signal, decode it and send a signal to the lock motor to change it to its unlocked position. The processing unit will also contain a timer of ten seconds after the door is shut to lock the door behind the user.

2.3.1 Data Processing PCB

The data processing circuit board is the device that regulates and processes the signals and power needed to operate the system. This PCB is composed of the idea of an "Arduino on a breadboard", in which the ATmega328p microcontroller is built on a PCB, such as described in section 2.2.4.Through the software in it, we will ensure that all signals are routed to the correct place.

2.3.1.1 Data Routing

A PCB with the ATmega328p microcontroller 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, there will be two total PCBs, one for the key, and one for the locking unit. Since these devices are bulky, they will be built into the control PCB that will provide the same capabilities as a full Arduino. Therefore, we will need an Atmel ATmega328 chip, which is the microcontroller in an Arduino, LEDs for testing, wires, capacitors, resistors and a clock crystal [12]. These parts are listed in detail later on this document and were chosen with a minimal design in mind. 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.

.

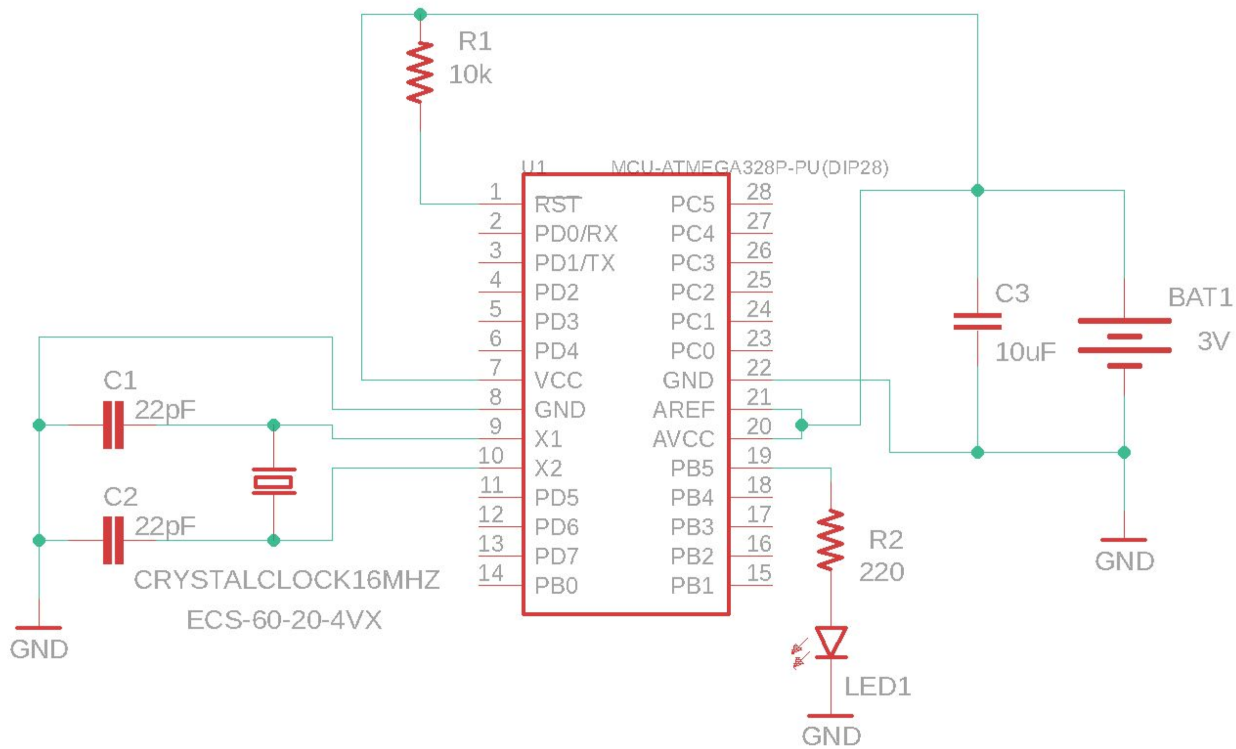

Figure 5 - Mock Arduino microcontroller device schematic.

The schematic on Figure 5 consists of an ATmega328p chip on the center, which is the Arduino's microcontroller. Each pin on the chip corresponds to a pin on the Arduino, may it be digital, analog, ground or voltage. Pin 1 is reset, and it is connected to VCC through a resistor. Pins 7, 20 and 21 are connected to VCC. Pins 9 and 10 are connected to a 16 MHz crystal clock, which provides a clock signal to the microcontroller. Pin 19 is connected to an LED for testing purposes.

The board will be powered with a coin battery of 3 V on the key, while the locking unit will be powered by a 12 V battery with a linear voltage regulator that will step down the voltage to 3 V. The ATmega328p 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 at a time [12].

In order to process the unlocking command, data must be communicated between the Bluetooth receiver and the locking system. The connection which routes the unlock signal from the Bluetooth receiver to the PCB will be established by the state pin on the Bluetooth module. If the transmitter is within proximity to pair with the receiver, the state pin will be valued "1", which represents the unlock state. As described in section 2.2.2, there will be a timer between 4 and 7.4 seconds such that the door unlocks only within 10 feet, and, once the timer is up, a signal will be sent to the motor so it can spin, unlocking the door. The state will change to "0" when the key is not within proximity anymore, which, again, will set a timer of 10 seconds and then send a signal to the motor to lock the door.

In addition to this, the ATmega328p also routes data associated with the external and internal user interfaces. For example, the internal user interface would have an LED which alerts the user if the door is in the locked or unlocked state. This PCB would route the data to change this display when the state of the door changes. Another example of this would be the lock/unlock button present on the internal user interface. Once pressed and detected by the microcontroller, the latter will send a signal to the motor so it can spin. Here, the motor will have to spin to the opposite position it is currently in, which means the microcontroller will track the position of the motor at all times. More details about the software involved that will control and route all these signals are described in section 2.6 of this document.

Requirements	**Verification**
PUM-1: The data processing PCB shall update an LED to display the lock/unlock status of the door such that it appears instantaneously to the user on the inside of the door.	A. The user shall be in proximity and unlock the lock, at which point the LED shall shine a green light representing the unlock status. B. The user shall go to the other side of the lock, and, after the set lock timer, the motor should spin to lock the door and the LED shall shine a red light representing the lock status.

Table 6 - Requirements and verification for Processing Unit Module in regards to PCB Data Routing.

2.3.1.2 Timer

To prevent the door from remaining unlocked for an excessive amount of time, and also give the user some time to open the door for someone or grab something quickly outside, a timer will be implemented. Once the Bluetooth signal is lost, the door will unlock after 10 seconds. This can be done by setting a timer after the key has lost connection with the lock, which can be controlled by the state pin on the Bluetooth module.

Requirements	Verification
PUM-3: A timer shall be implemented into the locking unit which will lock the door automatically after ten seconds when the key is out of range.	A. The user will unlock the lock by being within proximity B. The key shall be put into a metal cage such that the Bluetooth connection is lost, at which point a timer shall be set C. The door shall lock before the timer hits 10 seconds

Table 7 - Requirements and verification for Processing Unit Module in regards to the timer.

2.3.2 External User Interface

Two devices will be integrated into the locking unit for relaying information to the user: an external user interface (EUI) and internal user interface (IUI). LEDs will be on both sides of the door so that users on either side can be notified about the state of the locking system. However, the information displayed on the external user interface will be different from the internal interface due to the confidentiality of some of the information. For example, a user would not want the lock status of the door to be on the external user interface as it would alert possible intruders that the door is unlocked. Therefore, data displayed on the external user interface would only include an LED-based battery indicator.

This LED battery level indicator will also be applied on the key. be achieved through a series of 5 resistors and 5 LEDs. The LEDs will be connected to each other by anode connecting to cathode, and a 1KΩ resistor between each of them. The positive node of the battery will be connected to the resistors and the ground to the first LED [13]. Since there are 5 LEDs, the indicated battery level will be around every 20%.

Requirements	Verification
PUM-4: The external user interface shall use light emitting diodes to display battery life to the user. The status shall be updated for every 20% of the battery lifetime.	A. Batteries with different voltage levels, representing each 20% of 12 V, shall be connected to the battery life indicator and to a multimeter. The number of LEDs that light up shall correspond with different voltage levels.

Table 8 - Requirements and verification for the Processing Unit Module in regards to the External User Interface.

2.3.3 Internal User Interface

The internal user interface will be more comprehensive than its external counterpart but will serve the same function of relaying information to the user. Similar to the EUI, the internal user interface will feature a battery indicator so that the user is aware when the batteries will need to be replaced. The same system for the battery level indicator will be used. There will also be an LED indicator which lets the user know if the door is in the locked or unlocked state, as described in section 2.3.1.1.

A lock/unlock button will also be featured on this user interface, which lets users control the lock from the inside and permanently unlock it if they wish to do so. This feature will be accomplished by, upon the press of the button, a signal being sent to the motor so it can change its position. Thus, if the motor is in the "locked" state, it will change to "unlock" and vice versa.

Requirements	Verification
PUM-4: The internal user interface shall use light emitting diodes to display battery life to the user. The status shall be updated for every 20% of the battery lifetime.	A. Batteries with different voltage levels, representing each 20% of 12 V, shall be connected to the battery life indicator and to a multimeter. The number of LEDs that light up shall correspond with different voltage levels.
PUM-6: The internal user interface shall feature a button to lock/unlock the door. This shall be able to be accomplished at all times when the key is not in proximity, no matter the position of the motor.	A. With the door locked and the key out of proximity, the user shall press the lock/unlock button and the door shall unlock. B. With the door unlocked and the key out of proximity, the user shall press the lock/unlock button and the door shall lock.

Table 9 - Requirements and verification for the Processing Unit Module in regards to the Internal User Interface.

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 DC 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.

2.4.1 Modified Deadbolt and Demonstration Mount

The most essential component to the success of the mechanical system is the modified deadbolt itself. As previously explained, this device capitalizes on the rotational capabilities of the deadbolt by driving a small 12 V DC motor to turn a cylindrical hub. This hub takes the torque applied by either the user turning the key manually or the DC motor to convert rotational motion into linear actuation. With assistance from the ECE Machine Shop, the deadbolt along with the various other physical components will be mounted for demonstration purposes. To protect the components from harming the user or becoming damaged, communication with the machine shop will be frequent.

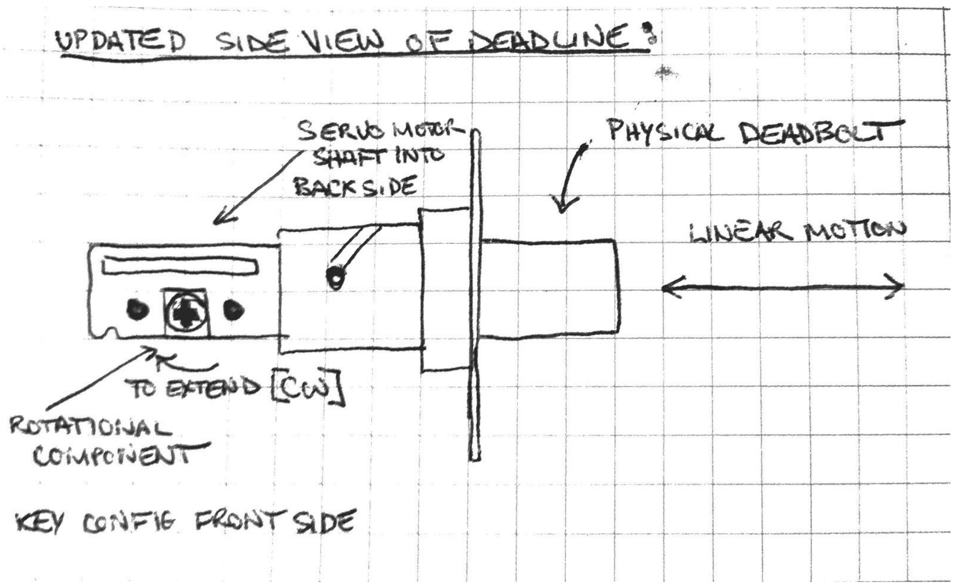

Figure 6 - Sketch of mechanical deadbolt. The rotational component will be driven by a DC motor to automatically transition between the locked and unlocked states.

2.4.2 Key Enclosure

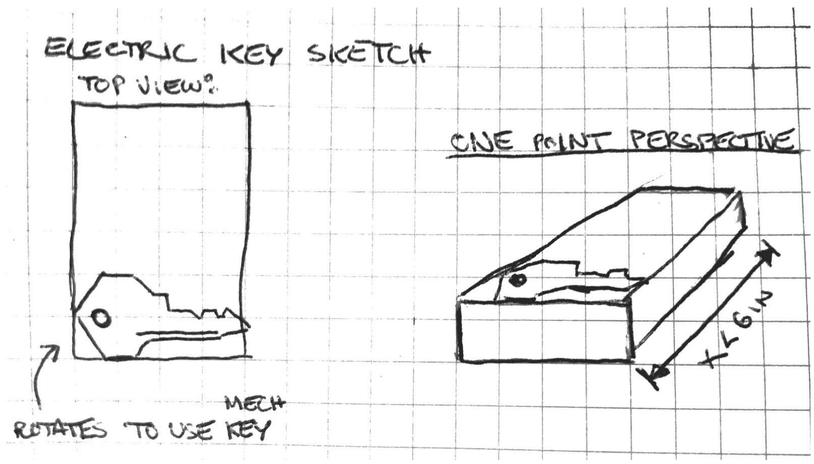

Figure 7 - Sketch of electronic key enclosure. This device stores the keys electronic components and has the mechanical key attached on top for easy access.

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. The mechanical backup key will be attached directly to the electronic key such that the user would not need to carry more than a single device for unlocking the door.

Requirements	**Verification**
MLM-1: The key enclosure's size shall be small enough to fit into a pocket or purse and shall be considered a priority in its design.	A. The project box chosen shall be smaller than 6 in X 4 in X 2 in. B. The project box will be put into the users pocket during testing and demonstration to prove hands free operation.

Table 10 - Requirements and verification for the Mechanical Locking Module in regards to the key enclosure.

2.4.3 Locking Unit

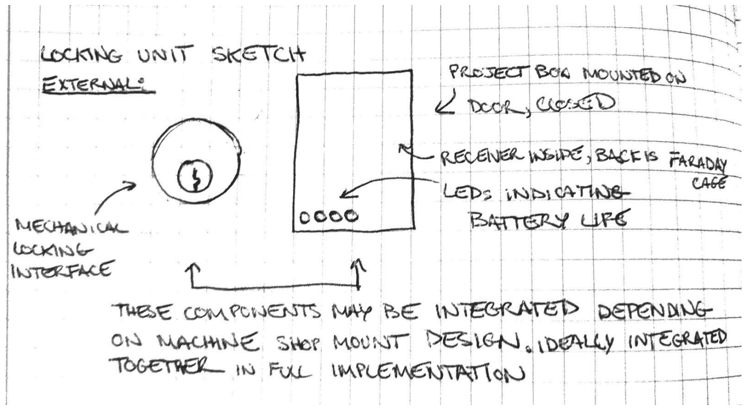

Figure 8 -Sketch of the components involved in the external part of the locking unit. These devices will be placed on the outside of the door and electronics will be kept safely inside an enclosure.

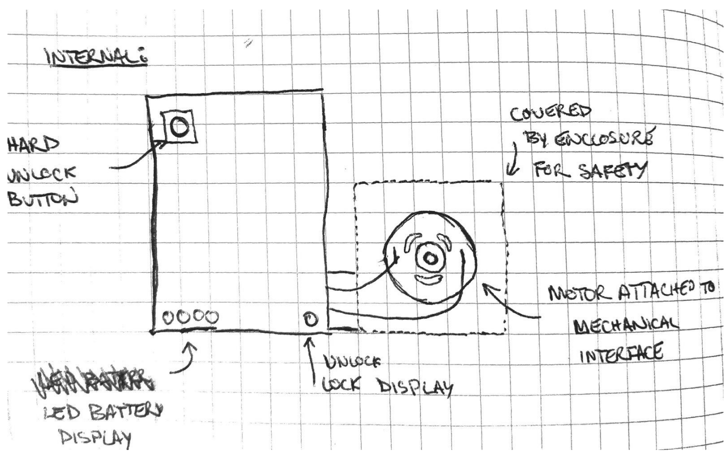

Figure 9 - Sketch of the components involved in the internal part of the locking unit. These devices will be placed on the inside of the door and electronics will be kept safely inside an enclosure. Additionally, the motor is stored here which spins the rotational component of the deadbolt.

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.

In addition to the displays and user interfaces associated with the processing unit module, there is a mechanically driven component to the locking unit which includes the modified deadbolt lock and motor. 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 sufficient torque 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 IDE 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.	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.

Table 11 - Requirements and verification for the Mechanical Locking Module in regards to motor operation.

2.5 Software Overview

The software was described in many sections of this document, but, here, it will be described in full, as a pseudocode. The software will be loaded into the ATmega328p chips on the PCBs, therefore, there will be two different files, one for the key and one for the locking unit. It will be used to control the Bluetooth, the motor and the manual lock/unlock button.

2.5.1 Locking Unit Software

The locking unit specific software will handle the locking and unlocking through Bluetooth, the motor control and its tracking and the manual lock/unlock manual button on the internal user interface. The software will be written in the Arduino IDE.

2.5.1.1 Locking and Unlocking with Bluetooth

The goal of this part of the software is to create a connection with the transmitter and control the lock. The receiver unit will constantly look for the transmitter to make a connection. Once they are connected, the state pin of the Bluetooth module will change to “1” (unlock signal). Since the HC-05 Bluetooth module has a range of about 32 feet and we only want the unit to unlock within 10 feet, we will set a timer of about 6.09 seconds. This time was set given the average walking speed of humans, considering the user will be walking towards the door and it will only unlock within the limited distance.

Once the timer is up, a signal, “spin open”, will be sent to the motor for it to spin towards the unlock position, and it will stay that way until the key is out of proximity, because of the Faraday cage on the inside or being far away enough, in which case the pin state will be “0” (lock signal). When the receiver and transmitter are disconnected, there is a timer of 10 seconds until a signal, “spin close”, is sent to the motor so it can lock. This timer is set in case the user needs to have the door open for some time, either to let someone in or grab something quickly outside. After that, the receiver will constantly look for the transmitter again. The pseudocode is shown in Figure 10.

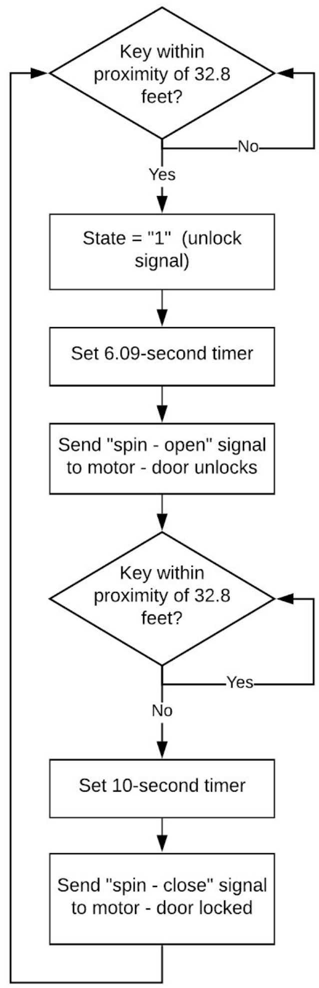

Figure 10 - Pseudocode for locking and unlocking using Arduino based Bluetooth software. This includes the logic required for the key to correctly lock and unlock the door when desired.

2.6.1.2 Motor Control and Lock/Unlock Manual Button

The software will also have a global variable which will keep track of the state of the motor, called locked and unlocked. This will be useful when using the lock/unlock manual button on the internal user interface, which will have to turn the motor to the opposite state it is currently in, i.e, if it is on the locked state, it will go to unlocked and vice versa. The global variable will update every time the motor signal spin open or spin close are sent.

2.6.2 Key Software

The software for the key is not as complex as for the locking unit, since its only task is to connect to the receiver. Therefore, the only code needed is for it to constantly send its signal such that it can be paired with the locking unit.

2.7 Tolerance Analysis

An important tolerance for this project is the consideration of the Bluetooth range and its power consumption. The proximity lock requires the Bluetooth to have low range and low power consumption while still having a strong and fast connection between the receiver and transmitter modules. In terms of range, the best type of Bluetooth device found for this task was a Class 3 device, which has a range of about 10 meters (32.8 feet) [14]. However this is still too much for the 10 foot (about 3 meters) constraint for this project. Since there is a software component to the lock, it was decided that adjustments could be made in the Arduino code.

The chosen Bluetooth module, HC-05, is rated for 10 meters [15], and has a state pin that is 1 when connected and 0 when disconnected from another Bluetooth device. Using this to our advantage, and given that we are using an Arduino, we can connect both modules at 10 meters, but only unlock the door when the user hits the 3 meter mark, by estimating their walking speed. According to Healthline [11], the average speed of a human changes with age, being the fastest 1.36 meters per second and the slowest 0.94 meters per second. Considering that a person would have to walk 7 meters, it is found through equation 1 that they would take, on average, 6.09 seconds to do so. Therefore, there will be a timer of 6.09 seconds between the Bluetooth modules connection and the actual unlocking.

$$\frac{1.36+0.94}{2} = 1.15 meters/s\ (average) \rightarrow \frac{1 second}{1.15\ meters} \times 7 meters = 6.09\ seconds \tag{1}$$

Another consideration is power consumption. The Class 3 Bluetooth type mentioned before is the one that consumes less power, at 1 mW [14]. However, usually, in Bluetooth modules' datasheets, the power is measured in dBm (decibel-milliwatts), and that needs to be converted to Watts for an easier calculation, using equation 2.

$$P(watt) = \frac{10^{\frac{P(dBm)}{10}}}{1000} \tag{2}$$

The HC-05 Bluetooth module can have an output range of -4 dBm to +6 dBm [7], and, by plugging it into equation 2, as seen in equations 3 and 4, the output power can range from 0.000398 W to 0.00398 W, which is very low and very suitable for this project.

$$P(watt\,from\ -4\ dBm) = \frac{10^{\frac{-4}{10}}}{1000} = 0.000398\ W \quad (3)$$

$$P(watt\,from\ +6\ dBm) = \frac{10^{\frac{6}{10}}}{1000} = 0.00398\ W \quad (4)$$

3 Costs

$$\frac{\$}{hour} \times 2.5 \times hours\ to\ complete\ =\ TOTAL \quad (5)$$

Our development costs are $45/hour and each team member is working at an estimated 6 hours/week. We consider the work done is approximately considered over 70% of the 16 week semester. Giving a total estimated cost of:

$$3 \times \frac{\$45}{hour} \times \frac{8\ hours}{week} \times \frac{16\ weeks}{0.7} \times 2.5\ =\ \$61,714 \quad (6)$$

In our design, the machine shop will only be responsible for modifying an existing lock and mounting the necessary components to the locking unit. We estimate a total of roughly 15 hours of labor from the machine shop. Considering they charge a rate of $50/hr, the estimated labor cost is:

$$15\ hours \times \frac{\$50}{hour}\ =\ \$750 \quad (7)$$

Description	Manufacturer	Quantity	Cost
Deadbolt Single Cylinder Antique Brass	Amazon	1	$12.39
HC-05 Bluetooth Module	DSD Tech	2	$15.27
Stainless Steel Wire	TIMESETL	1	$7.99

Mesh			
DC Brushless Gear Motor 65 RPM	Bemonoc	1	$25.88
2430 3V Lithium Coin Battery	Duracell	2	$5.37
Coppertop Duralock MN1500-B4 AA LR6	Duracell	2	$9.00
MCP1702-3002E/TO Voltage Regulator	Microchip Technology	1	$0.48
ATmega328-PU	Atmel	2	$4.16
FG16X7R1E106KRT06 10uF ceramic capacitor	TDK Corporation	2	$1.52
FA22X7R1E226MRU00 22pF ceramic capacitor	TDK Corporation	4	$7.28
RNF14FTD10K0 10KΩ resistor	Stackpole Electronics	2	$0.20
CFM14JT220R 220Ω resistor	Stackpole Electronics	2	$0.20
LED 60-piece pack - Various colors	Chanzon (sold by Amazon)	1	$6.50
9B-16.000MBBK-B 16MHz Crystal Oscillator	TXC Corporation	2	$0.60
PR02000201001JR500 1KΩ resistor	Vishay BC Components	5	$2.25
A23 12V Alkaline 23-A Replacement Battery 23AE GP - 5 Pack	GP	1	$3.66

Table 12 - Specific component costs for project’s design.

Altogether, the estimated cost of the different components from the table above is estimated $102.75. The estimated cost of machine shop labor is $750. The estimated cost of the entire project is $62,566.75.

4 Schedule

Week	Jason	Brant	Talita
2/24	Begin Writing PCB Microcontroller pseudocode for project.	Determine approximate motor parameters necessary and order motor.	Determine specifications of Bluetooth modules, including batteries and Arduino.
3/2	Ensure Bluetooth connection between both HC-05 modules is successful. Start writing code to execute accurate control necessary for the design of the project.	Perform motor requirement verification by unit testing. Supply machine shop with components for modification and assembly. Prepare for Design Review. Soldering assignment.	Design circuit necessary, connecting the idea of the Arduino on a Breadboard with the Bluetooth and motor connections. Prepare for Design Review. Soldering Assignment.
3/9	Write code in the Arduino IDE to ensure External and Internal User interfaces are correctly set up.	Work on voltage regulation component of PCB such that the motor has sufficient torque. Continue testing devices if issues arise in the first testing phase.	Continue circuit design and test the complete design on a Breadboard. Design PCB and send it to order.
3/16	Spring Break- Document progress, outline final report draft.	Spring Break- Document progress, outline final report draft.	Spring Break- Document progress, outline final report draft.
3/23	Coordinate with Talita to ensure that breadboard testing works correctly with the Arduino code developed. Implement timer function into Arduino Code as well.	Solder PCB if ready. Check on machine shop progress. Breadboard test the entire unit to verify each component receives enough power and adjust the system accordingly. Begin verifications for	Solder PCB if ready. Test each unit to make sure they are working individually if possible. Keep testing the system on breadboard otherwise and help other team members.

		Bluetooth shielding device.	
3/30	Solder PCB if ready. Test each unit to make sure they are working individually if possible.	Solder PCB if ready. Test each unit to make sure they are working individually if possible. Ensure Bluetooth shielding verifications are met.	Solder PCB if ready. Test each unit to make sure they are working individually if possible. Help other team members.
4/6	Solder PCB if ready. Test each unit to make sure they are working individually if possible.	Solder PCB if ready. Test each unit to make sure they are working individually if possible.	Solder PCB if ready. Test each unit to make sure they are working individually if possible.
4/13	Prepare for mock demo by ensuring electromechanical components work cohesively. Assemble the system onto the demo mount.	Prepare for mock demo by ensuring electromechanical components work cohesively. Assemble the system onto the demo mount.	Prepare for mock demo by ensuring electromechanical components work cohesively. Assemble the system onto the demo mount.
4/20	Perform requirement verifications for requirements that require the entire system.	Perform requirement verifications for requirements that require the entire system.	Perform requirement verifications for requirements that require the entire system.
4/27	Make final adjustments to the system for a strong demonstration.	Make final adjustments to the system for a strong demonstration.	Make final adjustments to the system for a strong demonstration.
5/4	Prepare Final Report/Final Presentation	Prepare Final Report/Final Presentation	Prepare Final Report/Final Presentation

Table 13 - Schedule of designated tasks for each group member. This is done to ensure the project remains on pace for completion by the time of demonstration.

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 [16]. 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 [10]. 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 [16]. 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.

In addition to the electrical safety standards outlined by IEEE, it is important to also comply with the building code used in the United States. In the United states, the International Building Code (IBC) and International Residential Code (IRC) and used as the national standard for door regulations. The most important two components described by the IBC and IRC to this project are egress, which refers to exits, and electromechanical regulations. Egress is a standard to prohibit exits from being blocked in the case of an emergency. The majority of these requirements are in regards to the way that the door locks and what can and cannot be put in front of it. A deadbolt is not one of the restricted locking methods and is widely used for locking applications in buildings. Considerations were taken in the design to attempt to integrate the system into the door itself. While that might not be fully realized for the demonstration, this would be an important factor to consider for the device's full implementation. For the electromagnetic locking component of the code, it is in compliance if the device has an obvious method of use and is capable of operation with one hand. The device's design meets these requirements through the use of the mechanical backup lock which is no different than a traditional lock [17]. No long power cables will be necessary as the device is battery powered and fire code will be maintained as the device will not restrict the normal operation of the door beyond the locking and unlocking capabilities.

6 Additional Implementation Ideas

Our view for the full implementation of the device goes beyond the scope of this proposal. Some of these features we are still considering but will only be implemented if time allows as they are unnecessary for the completion of the high level and module level requirements.

For the full integration of this device into a user's home, we would imagine the key would be universal and the locking unit device could be applied to a variety of doors such as gates, car doors etc. In addition, the power supplied to the Bluetooth device would be variable to adjust the distance from the key that the locking unit can detect.

As far as the security, all concerns addressed in the ethics portion of this document would be resolved by encrypting the data and adding extra security software during the pairing process. The system would be more complex in its full iteration and would offer additional security features which could be controlled by cellular devices. For example, remote locking could be implemented to allow a friend to enter the home by unlocking the door and then immediately locking it from the phone or electric key.

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] Timetoast. (2020). *History of Assistive Technology timeline.*. [online] Available at: https://www.timetoast.com/timelines/history-of-assistive-technology [Accessed 28 Feb. 2020].

[6] Android Authority. (2020). *A quick history of Bluetooth*. [online] Available at: https://www.androidauthority.com/history-bluetooth-explained-846345/ [Accessed 28 Feb. 2020].

[7] HC-05 Data Sheet. (2020). [ebook] Available at: https://drive.google.com/file/d/0B4urklB65vaCYmxZZlJ1dmw2NzA/view [Accessed 28 Feb. 2020].

[8] megaAVR Data Sheet. (2020). [ebook] Available at: http://ww1.microchip.com/downloads/en/DeviceDoc/ATmega48A-PA-88A-PA-168A-PA-328-P-DS-DS40002061A.pdf [Accessed 28 Feb. 2020].

[9] 250 mA Low Quiescent Current LDO Regulator. (2020). [ebook] Available at: http://ww1.microchip.com/downloads/en/DeviceDoc/22008E.pdf [Accessed 28 Feb. 2020].

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

[11] Healthline. (2020). *Average Walking Speed: Pace, and Comparisons by Age and Sex*. [online] Available at: https://www.healthline.com/health/exercise-fitness/average-walking-speed#average-speed-by-age [Accessed 28 Feb. 2020].

[12] Open Home Automation. (2020). *How to Run an Arduino for Years on a Battery*. [online] Available at: https://openhomeautomation.net/arduino-battery [Accessed 28 Feb. 2020].

[13] Anon, (2020). [online] Available at: https://www.youtube.com/watch?v=ydnr3Wr6VLA&fbclid=IwAR2h-WBGxcJxpAyPxVdUZ7jnrbZo46fMDcdcs_gg0_K27nRCkl6Q3dbl_9E [Accessed 28 Feb. 2020].

[14] Science ABC. (2020). *What Is The Range of Bluetooth And How Can It Be Extended?*. [online] Available at: https://www.scienceabc.com/innovation/what-is-the-range-of-bluetooth-and-how-can-it-be-extended.html [Accessed 28 Feb. 2020].

[15] B, B. and George, L. (2020). HC-05 Serial Bluetooth Module - Tutorial. [online] electroSome. Available at: https://electrosome.com/hc-05-serial-bluetooth-module/ [Accessed 28 Feb. 2020].

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

[17] Content.assaabloyusa.com. (2020). [online] Available at: https://content.assaabloyusa.com/doc/AADSS1054873&top.pdf [Accessed 28 Feb. 2020].