Touchless Proximity Lock: Proposal

Team 45 — Brant Bedore, Jason Hackiewicz and Talita Barbosa ECE 445 Project Proposal — Spring 2020 TA: Madison Hedlund

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

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.

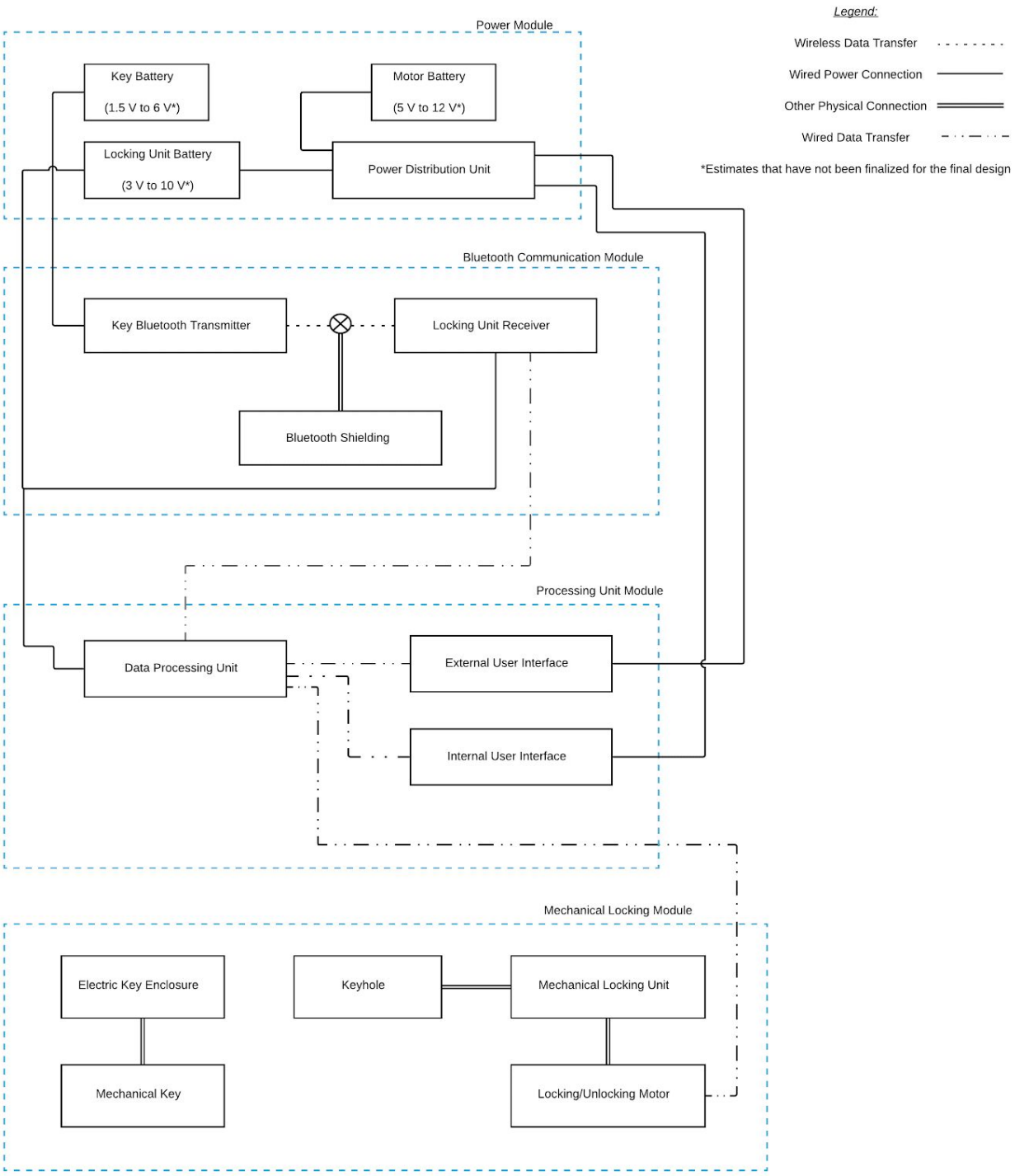

Figure 1 - Block Diagram of the Proximity Lock

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

There needs to be two separate power supplies for the key and for the lock. The key will have its own battery and will only have to power the Bluetooth transmitter. Even though the transmitter will be constantly sending signals, its power consumption will be kept small to ensure the battery lasts as long as possible. A smaller battery also allows for a smaller key enclosure so that it can fit in the user's pocket.

The power supply for the locking unit will also be battery operated. Many components on the locking unit will need power, such as the receiver 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. Voltage values have not been finalized for these batteries because it is necessary to know the requirements of each other part of the system to determine this. At this point we estimate that the voltages necessary for the key will be between 1.5 V and 6 V and the voltages necessary for the locking unit will range between 3 V and 10 V. Due to the low power consumption necessary for the receiver and LEDs, the battery will be able to last for long periods of use. The motor will have its own dedicated battery, since it consumes the most power. We estimate this battery will have the greatest voltage of the three but will still be between 5 V to 12 V.

- PSM-1: The key battery shall supply a sufficient voltage input ranging from 1.5 V to 6 V to power the components of the key.
- PSM-2: The locking unit shall supply a sufficient voltage input ranging from 3 V to 10 V to power the components of the locking unit.
- PSM-3: The motor battery shall supply a sufficient voltage input ranging from 5 V to 12 V to power the servo motor.

2.1.2 Power Distribution Unit

A printed circuit board will be located inside of the locking unit and serves the function of processing data and routing power to each device in an organized fashion. This would include sending the appropriate voltage to the external user interface, the internal user interface, the Bluetooth receiver and locking/unlocking motor. Because these devices would require different amounts of power, a combination of resistors would be used to scale the voltage from the locking unit battery to the appropriate level. These resistors would be integrated as part of the PCB.

2.2 Bluetooth Communications Module

To fully realize the touchless component of 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. While Bluetooth signals can have a range of about a kilometer, by supplying a lower power of about 100 mW, the range can be reduced such that the device only operates in a small area and does not interfere with other signals from industrial, scientific and medical devices [5]. This criteria will be satisfied by a Class 3 Bluetooth transmitter which has a range of one to ten meters. 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. Because the device is supposed to remain in the user's pocket, the transmission component should be kept to a relatively small size. 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.

- 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.

2.2.2 Bluetooth Locking Unit Receiver

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. 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. The motor will activate and the door will become unlocked. Likewise to the transmitter, the power will be kept low in order to reduce the range of operation.

- BCM-2: When the Bluetooth receiver takes in a signal from a paired transmitter, the receiver shall send a signal to power the unlocking motor.

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.

- 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.
- BCM-4: The shielding device shall not interfere with the operation of other components of the touchless proximity lock system.
- BCM-5: The shielding device shall not impact the functionality of nearby devices not associated with the proximity lock system.

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.

2.3.1.1 Data Routing

In order to process the unlocking command, data must be communicated between the Bluetooth receiver and the locking system. There will be a connection which routes the unlock signal from the Bluetooth receiver to the PCB. From this point the signal will be interpreted and perform the correct action based on the command received. In addition to this data, the PCB also routes data associated with the external and internal user interfaces. For example, the internal user interface would have an associated display which alerts the user if the door is in the locked or unlocked state. This circuit board would route the data to change this display when the state of the door changes. Another example of this

would be the current battery life of the locking unit which is displayed on both the internal user interface and external user interface. After detecting a change in the current battery life of the device, the PCB would route the data to change an LED display alerting the user that the device will need its batteries replaced soon.

- PUM-1: The data processing PCB shall update an LED to display the lock/unlock status of the door such that it appears instantaneous to the user on the inside of the door.
- PUM-2: The data processing PCB shall process data to update the battery life at least once every five minutes.

2.3.1.2 Timer

To prevent the door from remaining unlocked for an excessive amount of time, a timer will be implemented to automatically lock the door if the Bluetooth signal is lost for more than ten seconds. This can be done by using simple timer logic and controlling the locking motor. This timer device would be built into the PCB so that the user need not think about locking the door after operation. This timer will be implemented in case the user needs the door open for some time to let someone in or grab something quickly outside.

- 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.

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). A small display will be on both sides of the door so that users on either side of the door 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. Data that would be displayed on the external user interface would only include an LED based battery indicator.

- 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.

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. There will also be an LED indicator which lets the user know if the door is in the locked or unlocked state. A few buttons will also be featured on this user interface but these will only be necessary for setting up the device and letting in users from the inside. Because Bluetooth devices must be paired, there will be a button which would allow the Bluetooth receiver to establish a pairing with the transmitter. There will

also be an LED indicator which would flash at 1 Hz to indicate that the locking unit is searching for other devices to pair with. Pressing the pair button again will end the device search. Another button that would be featured here is a manual lock/unlock button allowing a user inside the door to unlock it for someone else. This button could also be used as a way to test the locking motor to ensure it is working properly.

- PUM-5: The internal user interface shall use light emitting diodes to display information such as the battery life to the user. The status shall be updated for every 20% of the battery lifetime.
- PUM-6: The internal user interface shall feature a button for pairing the locking unit and key at the time of first use. When this button is engaged at the same time as the pairing button on the key, the devices will pair together and will become functional for unlocking purposes.

2.4 Mechanical Locking Module

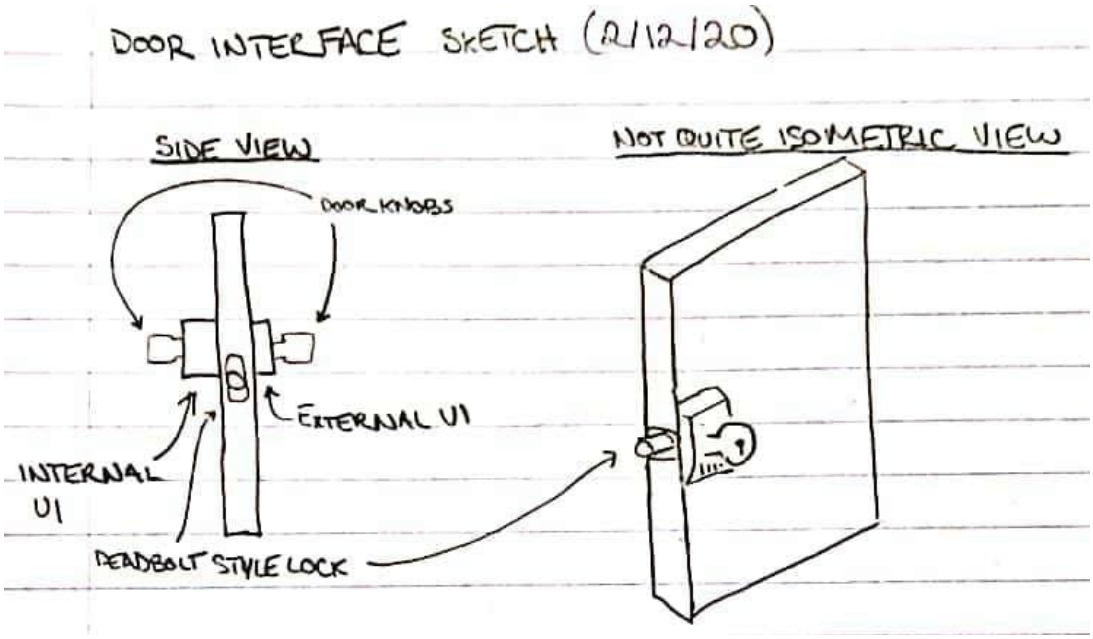

Figure 2 - Sketch of the Mechanical Locking Module

The proximity lock system must be able to interface with the physical world and does so using the mechanical locking system. This includes several components on both the key and locking unit which allow the user to complete the unlocking task hands free. The key's mechanical component would be composed of an enclosure for the electrical key components which interfaces with a mechanical backup key. The locking unit will have enclosures for both the external and internal electronics as well as a motor to turn the deadbolt to lock the door.

2.4.1 Key Enclosure

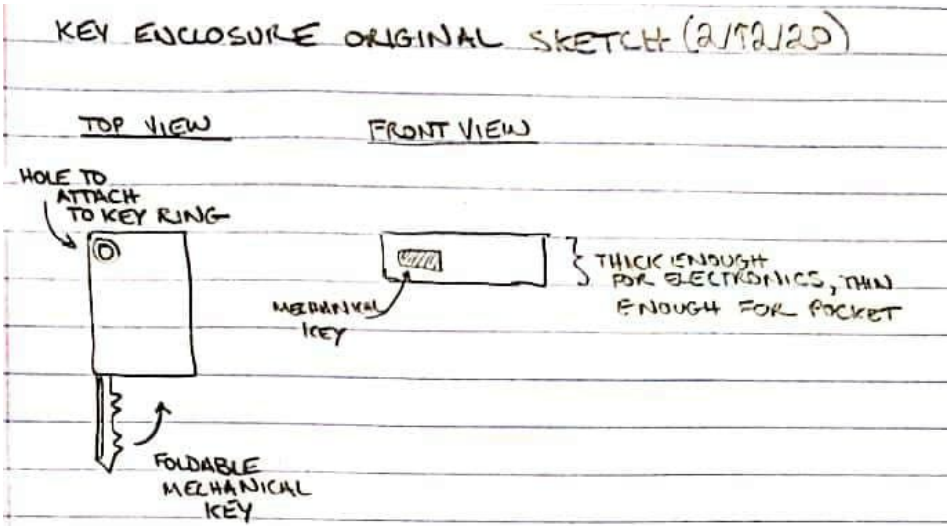

Figure 3 - Design of the Key Enclosure

For the user to avoid inconvenience while using the touchless proximity lock system, the key enclosure will be kept to a relatively small and flat size such that it would fit in a pocket or purse. The enclosure also houses a foldable mechanical key in case the device runs out of battery or malfunctions. There will also be a small hole at the top of the enclosure to attach a key ring. The device will have its internal electronics safely secured so that no dirt of external particles will interfere with the device's components. For ease of use, the key will also be composed of a light plastic material. Another feature on the enclosure would be a small low power red LED which would illuminate to indicate the device has a low battery. A button will be on the surface of the key which allows the key to be paired with the locking unit when both buttons are pressed and searching for nearby devices.

- 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.
- MLM-2: The key enclosure shall surround the electronics such that electronics cannot be touched while key enclosure is fully assembled.

2.4.2 Locking Unit

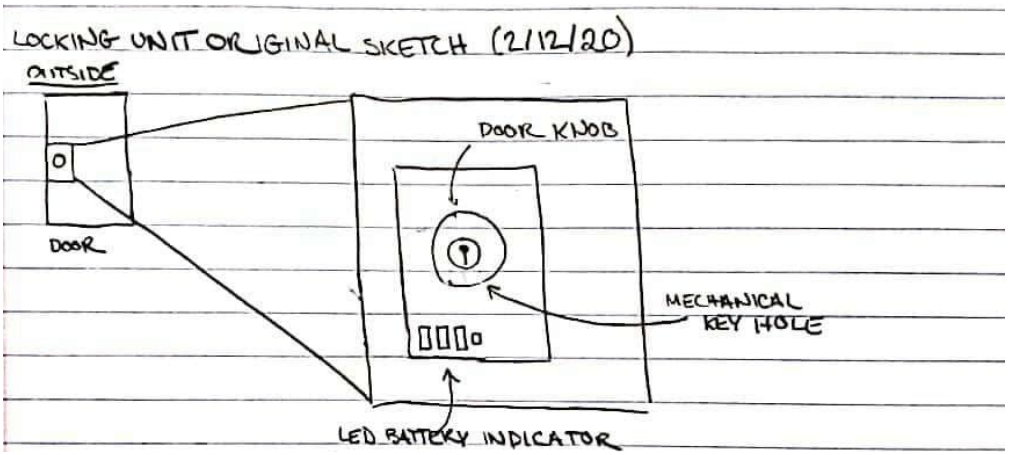

Figure 4 - Sketch of the outside of the door and the locking unit

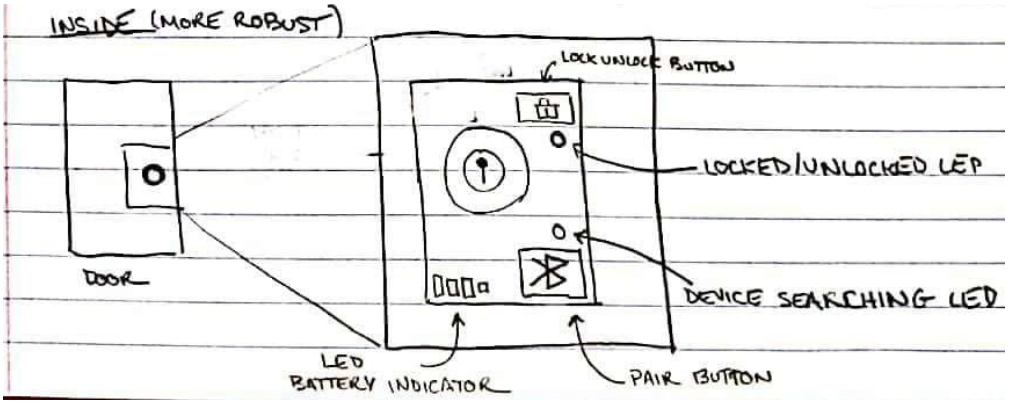

Figure 5 - Sketch of the inside of the door and the locking unit

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.

- MLM-3: When a signal is processed to unlock the door, the servo motor shall rotate to retract the deadbolt lock.
- MLM-4: The user shall be able to use a mechanical key to operate the deadbolt lock in case of a system failure.

2.5 Risk Analysis

	Low Risk	Mid Risk	High Risk
Low Severity	Mechanical Locking Module		
Mid Severity		Processing Unit Module	
High Severity	Power Module		Bluetooth Connection Module

Table 1 - Risk Analysis: green - low, yellow - moderate, red - high

Upon considering the design of the system, the power module has the highest severity of failure along with the Bluetooth connection module. If power is removed from the devices it would cause a critical system failure. For this reason, much attention was put into lowering the risk of this failure. Warning LEDs signal the user when batteries need to be changed and optimizations are being considered to lower the overall power usage thereby elongating battery lifetime. While the power module can have modifications made to reduce the associated risk, the Bluetooth connection module has more limitations on the the ability to reduce risk. The Bluetooth connection is integral to the functionality of the system as a whole but suffers from being an interruptible wireless data transmission system. If interference is caused by outside devices, the bluetooth component could fail resulting in a critical failure. Careful considerations will be made in attempts to minimize the risk of failure for this module. The processing unit module falls into the medium risk and severity categories. Small failures in the wiring or construction of the processing unit module's PCB could cause module level requirements to fail but some of the high level requirements would still function. An example of this would be a failure in the lighting of the battery level LED. While this would not cause any of the high level requirements to fail, module requirements such as PUM-4 would fail. Because the processing unit is physically the most complex module, there is a medium amount of risk associated with it. The mechanical locking module has the lowest severity and risk. The mechanical locking system's locking unit will be retrofitted to an existing deadbolt door lock which should operate as intended. In addition, while the enclosures are meant to protect the internal electronics, they would not directly contribute to a system failure. The mechanical key and keyhole should also be operational after repeated use just like every mechanical lock used on current home security systems. The highest area of risk for the mechanical component is the interface between the lock and motor. Despite general motor wear, once the motor is in the proper position it will take numerous uses to cause a failure.

3 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 [6]. 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 [6]. 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.

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