USER SPECIFIC FIREARM LOCKING SYSTEM

By

Steven Bettenhausen

Yong Seok Lee

Andrew Weller

Final Report for ECE 445, Senior Design, Spring 2012

TA: Jane Tu

02 May 2012

Project No. 12

Abstract

The objective of this project is to increase firearm safety by creating a simple and portable system that allows only authorized personnel to unlock and operate a firearm. This system is not intended to stop the theft of firearms; rather, it helps prevent the accidental firing of the weapon. While the firearm is locked, the trigger cannot be pulled and the magazine cannot be removed. The system consists of two main components: the control unit, a user-interfacing subsystem separate from the firearm, and the firearm unit, a subsystem attached to the firearm that physically puts the weapon into the proper state. Persons attempting to use the firearm must scan their fingerprint on the control unit. A successful scan allows the user to unlock the firearm for a user-selected duration. The unlock signal is then transmitted wirelessly to the firearm unit which places the weapon into the proper state.

Even though our project worked as intended, we could have made improvements. If we had used better wireless antennas, our wireless range could have increased greatly. Also, smaller and more efficient parts could have been used on the firearm unit to decrease its size and increase the life of the power supply.

The total cost of the project came out to be $26,523.83 which was $5239.63 lower than the initial estimate. This discrepancy is discussed in the cost section of this report.

Contents

1. Introduction

The objective of this project is to increase firearm safety by creating a simple and portable system that allows only authorized personnel to operate a firearm. This system is not intended to stop the theft of firearms; rather, it helps prevent the accidental firing of the weapon. While locked, the firearm's trigger cannot be pulled and its magazine cannot be removed. The system consists of two main components: the control unit, a user-interfacing subsystem separate from the firearm, and the firearm unit, a subsystem attached to the firearm that physically puts the weapon into the desired lock or unlock state, Figures H.2 and H.3 in Appendix H show the completed units. Persons attempting to operate the firearm must first scan their fingerprint on the control unit; a successful scan allows the user to unlock the firearm for a user-selected duration. The unlock signal is then transmitted wirelessly to the firearm unit which places the weapon into the proper state.

1.1 Purpose/Usefulness of Project

The purpose of this project is to increase firearm safety by preventing unauthorized use of a firearm. Instead of requiring a bulky and expensive gun safe to restrict access to a weapon, this system creates a portable and user friendly way to allow gun owners to have control over the firearm's operators. While in lockdown, the trigger cannot be pulled and the magazine cannot be removed, rendering the firearm useless. Since this system can be readily unlocked with the scan of a fingerprint, the firearm is operational in seconds. Should the firearm need to be used in an emergency, our system removes the stress of having to remember the combination to a gun safe. Most importantly, this system allows for quick access to the firearm while removing any danger of leaving it out.

1.2 Project Functions

This project functions as an added safety measure for firearm owners by defaulting the firearm into a locked state that prohibits the removal of the magazine and the firing of the weapon. Any persons wishing to operate the firearm must scan their fingerprint on fingerprint scanner located on the control unit. A successful scan puts the firearm into the emergency unlock state, a timed unlock of ten seconds, in case the user needs immediate use of the firearm. Unless the user is still operating the firearm, it will return to the locked state after the ten seconds conclude and the user will go through a menu displayed on the LCD screen. The menu provides options for fingerprint management and locking/unlocking the firearm. The fingerprint management options include adding and deleting fingerprints while the lock/unlock options include selecting the time of the unlock state and overriding the unlocked state. Once the firearm has been unlocked, the locking mechanisms move so the user can fire the weapon and remove the magazine. When the desired time for the unlocked state is reached, the firearm returns to the locked state unless the user is still holding the firearm. This feature is controlled by a pushbutton sensor that is depressed while the firearm is being held. As long as the firearm continues to be held, it will remain unlocked. Immediately after the firearm is released, it returns to the locked state until the user sends another unlock command from the control unit.

1.3 Blocks/Subprojects

The design is broken down into several subsystems that each has its own functions to perform. The implemented subsystems were:

1.3.1 Fingerprint Scanner

The fingerprint scanner is used to record and compare fingerprints from users. The scanner is controlled by I/O signals from the microcontroller via the scanner's GPIO ports. The scanner outputs a signal to the microcontroller relaying if the fingerprint scan was successful or not.

1.3.2 User Interface

The user interface accepts prompt-based inputs from the user for the time unlock and fingerprint management options. The user responds to prompts by entering commands on a keypad, providing inputs to the control unit's microcontroller.

1.3.3 Control Unit Power Supply

The control unit power supply converts a +9V DC source to +5V and +3.3V with respect to ground to power the other subsystems in the control unit. The supply also prevents spikes in current and voltage that could damage the other subsystems.

1.3.4 Control Unit Microcontroller

The control unit microcontroller communicates with all the control unit's devices. It commands the LCD display, processes user inputs, and generates the wireless locking and unlocking signals.

1.3.5 Wireless Transmitter and Receiver

Consisting of a transmitter in the control unit and a receiver in the firearm unit, the wireless unit relays the decisions made in the control unit's microcontroller to the microcontroller on the firearm.

1.3.6 Pressure Sensor

The pressure sensor is used to determine when a user is holding the firearm. As long as the firearm is being held, indicated by the depressing of the sensor's pushbutton, the firearm will remain in the unlocked state.

1.3.7 Locking Mechanisms

The locking mechanisms mechanically put the firearm into the proper state based on the digital signals sent to it from the firearm unit's microcontroller.

1.3.8 Firearm Unit Power Supply

The firearm unit power supply converts a +9V DC source to +5 V with respect to ground to power the subsystems in the firearm unit. The supply also prevents spikes in current and voltage that could damage the other subsystems.

1.3.9 Firearm Unit Microcontroller

The firearm unit's microcontroller receives the lock, unlock, and timer signals from the wireless receiver and generates the digital signals to be sent to the locking mechanisms to put the firearm into the desired state.

2 Design

2.1 Control Unit

2.1.1 Control Unit Power Supply

Initially the power supply was to be constructed by placing four AA batteries in series. With each battery supplying +1.5 volts, the supply would have a total output of +6 volts. To check if this voltage would correctly power the control unit's components, their datasheets were consulted. It was found that the LCD display [1], wireless transmitter [2], and microcontroller [4] each require +5V volts to run properly while the fingerprint scanner runs on a +3.3V input [5]. This meant that the +6V output from the supply had to be regulated to those voltages. This was done by placing a voltage regulator with a +5V output at the output of the AA batteries. The regulator's output was fed to the LCD, microcontroller, and the wireless transmitter as well as to another voltage regulator with a +3.3V output which was used to power the fingerprint scanner. For proper operation of the voltage regulators, capacitors were attached to their inputs and outputs. The values of these components were selected because they were used in a similar voltage regulator circuit [6]. LEDs were also added to the regulator outputs to visually show then the power supply was providing power. Before the fingerprint scanner was connected to the circuit, the components were powered correctly; however, once the fingerprint scanner was placed in the circuit, it was found that the batteries did not supply enough voltage and current to run the subsystems concurrently. The batteries were unable to handle the 168 mA current draw during a fingerprint scan. After looking at several other battery configurations, the decision was made to go to a 9-volt battery as the primary source since it would be able to operate the subsystems simultaneously, outputting up to 280 mA of current, while providing enough power for several hours of usage. Finally, a toggle switch was included so that the battery could be connected and disconnected easily to prevent the continuous draining of power.

2.1.2 User Interface

The user interface was designed to create a way for the firearm's operator to easily manage user fingerprints and unlock and lock the firearm. The interfacing is done via a LCD display that prompts the user and a keypad that allows the user to respond to these prompts.

The chosen LCD display is a 16 character by 2 line display with a HD44780 Hitachi controller [1]. Utilizing the capability to display 32 characters at a time allows the created prompts to be very detailed. The character data for these prompts is sent on data lines, 4 bits at a time, from the control unit's microcontroller. A prewritten code [7], [8] is used to display the proper characters on the LCD display. For proper communication with the microcontroller, the register select (RS), read/write enable (E), and read/write select (R/W) pins are connected to the microcontroller's I/O ports, as shown in Figure A.1 in Appendix A.

The keypad chosen is a 16 key conductive rubber keypad [9]. This particular keypad was selected because its keys consist of the numbers 0-9, the letters A-D, the '#' key, and the '*' key. Having many keys allows each one to have its own specific function in the menus. Communicating the user inputs to the microcontroller is done by connecting the keypad's outputs to eight I/O pins on the microcontroller;

these connections are shown in Figure A.1 in Appendix A. Since the keypad behaves as a switch matrix, its pins had to be probed systematically to determine which key was being pressed. An algorithm was created and called by the read_keypad() function which returns a number between 0 and 16 as shown in Table B.1 in Appendix B. The microcontroller begins this process by sending high voltage to the first four keypad pins and reading the value of the other four pins. When the microcontroller reads a high voltage on one of these pins, a key is pressed and the algorithm switches off power to the first four pins one by one until the input to the keypad is no longer high. At this point, the key that was pressed is identified and its value is returned to the main function.

The user menu is designed using a case statement so that the navigation within the program is simple and efficient. The acceptable keys are listed at each prompt along with the corresponding result of each key press. Only acceptable key presses allow the user to navigate through the menus, all other key presses are ignored. To make traversing the menu easier on the user, only two main tracks were created. In the fingerprint management track, the user is able to add or delete acceptable user fingerprints while the locking and unlocking track allows the user to input the duration of the unlocked state or override the unlock state to lock the firearm. While moving through the user menu, appropriate messages such as “scan successful” or “unlocking for 100 seconds”, are displayed on the LCD display for two seconds to give the user status updates. While these messages are displayed, no user inputs are accepted. The complete flowchart of the user menu can be found in Figure C.1 in Appendix C.

2.1.3 Wireless Transmitter and Receiver

The communication between the control unit and firearm unit was chosen to be done wirelessly. This would allow the firearm to be separate from the control unit, making the firearm unit small and unobtrusive while still allowing for the interactive user interface and fingerprint scanner to be used. The wireless communication was done using Linx HP3 series receivers and transmitters because they are easily configured to communicate with the PIC microcontroller. Another benefit of these components is the 902 MHz to 927 MHz RF frequency range over which they can communicate [10]. To transmit the signals 916 MHz Linx antennas were chosen. For proper communication with the antennas, the transmitter and receiver were set to an operating frequency of 916 MHz, the closest channel that is able to be set with parallel ports to the antennas’ center frequency. This was done by configuring the I/O ports CS0, CS1, and CS2 on the transmitter and receiver to the operating frequency.

The next step was to set up the RS-232 serial communication between the transmitter and receiver via the putc function in a prewritten piece of code [7], [8]. In the code, the receiver is always on and waiting for the transmitted byte to be sent. The default signal is high, and the data is sent by first sending a low start bit, then sending the 8 data bits from the least significant bit to the most significant bit. The transmitted data, the lock and unlock signals, are 8 bits and 32 bits respectively. The extra three bytes in the unlock signal are due to the three extra characters for the unlock time duration.

Because the microcontroller has only one serial transmit pin, and both the transmitter and fingerprint scanner use serial communication, glue logic was needed to enable the fingerprint scanner or the transmitter separately. This was done by using two OR gates that were each fed with an enable input which would only enable the scanner and transmitter when low. Figures A.1 and A.2 in Appendix A show the complete connections for the transmitter and receiver.

2.1.4 Fingerprint Scanner

The fingerprint scanner's complex function, to scan and store fingerprint data, led to the decision to purchase a premade component. An optical scanner was chosen because they are easier to use and have fewer problems than slide scanners. The selected scanner, NITGEN FIM5360, comes with its own microcontroller which allows the comparing of fingerprint data to be done on the scanner unit. Another feature of this scanner is the internal memory and the ability to output a unique identification number serially for each fingerprint [5].

Initially, communication with the microcontroller was to be done by connecting the transmit-to-host serial port of the fingerprint module to the UART input pin of the PIC. The signals input back to the scanner from the microcontroller would be first passed through a two-input OR gate because the microcontroller would have to communicate serially with both the wireless transmitter and the fingerprint scanner modules. Unfortunately, issues arose with the serial communication so the decision was made to use the five GPIO ports to communicate with the control unit's microcontroller, see Figure A.1 in Appendix A. The Identify, Register, and Delete ports are input to the scanner and the Pass and Fail ports are output to the microcontroller. Code was then developed and integrated into the user menu that brings the three input I/O lines from high to low to activate the various commands. The Identify function compares the user's fingerprint to the database of fingerprints already in the system and drives the Pass output low if the fingerprint is in the system or it drives the Fail output low if the fingerprint is not in the system. The Register function compares the user's fingerprint to the database of fingerprints already in the system and drives the Pass output low if the fingerprint is not in the system or it drives the Fail output low if the fingerprint is already in the system. Fingerprints that are not already stored in memory are added to the memory. The Delete function compares the user's fingerprint to the database of fingerprints already in the system and drives the Pass output low if the fingerprint is in the system or it drives the Fail output low if the fingerprint is not in the system. Fingerprints stored in the system's memory are removed.

2.2 Firearm Unit

2.2.1 Firearm Unit Power Supply

Initially the power supply was to be constructed by placing multiple +3.3-volt watch batteries in series. This configuration was ideal because it would keep the supply relatively small, a desired characteristic since it would be attached to the firearm. The number of batteries needed would be decided by the total voltage and current required by the firearm unit's subsystems. The datasheets for the receiver and microcontroller revealed that for proper operation the wireless receiver [3] required 17 mA and +5V and the microcontroller [4] needed 220 µA and +5V. Testing on the locking mechanisms' motors revealed that they ran while the voltage across their terminals was between +3.5V and +12Vwith a nominal 60 mA current draw. Unfortunately, this large current draw by the motors made the arrangement of several watch batteries in series not viable since the number of batteries it would take to deliver the required current would make the supply too large. After looking at several other battery configurations, the decision was made to go to a 9-volt battery as the primary source since it would be able to operate the firearm subsystems simultaneously while providing enough power for several hours of usage.

Recalling the voltage requirements of the subsystems, particularly the +5V needed by the microcontroller and wireless receiver, the power supply needed a way to regulate the voltage sent to these components. This was done via a voltage regulator with a +5V output. Supplied by the 9V battery, the regulator lowers to voltage to +5V which is sent to the microcontroller and wireless receiver ensuring they always have the correct voltage to operate. For proper operation of the voltage regulator component, capacitors and resistors are attached to its input and output. The values of these components were selected because they were used in a similar voltage regulator circuit [6]. The final configuration of the supply can be seen in Figure A.2 in Appendix A and shows the 9-volt battery, labeled as Vcc, feeding into the voltage regulator which is outputting to the microcontroller, wireless receiver, and locking mechanisms.

2.2.2 Pressure Sensor

The pressure sensor's simple function, to detect when a user is holding the firearm, led to the decision to purchase a premade component. Originally this component was to be a thin sensor that would use infrared technology to detect a user. The idea was that when the firearm was held, this sensor would output a high signal to the firearm's microcontroller; but this functionally required a sophisticated sensor that cost too much to make it a viable option. The sensor's basic function, acting as a switch, led to the realization that a simple switch would work perfectly. Different types of switches were looked at, but ultimately the pushbutton switch was selected since it would act as a closed switch only when pressed. The pushbutton is located on the firearm so that when a user held the firearm the pushbutton would be depressed. The output of the pushbutton is fed to the microcontroller, with a high signal indicating the firearm is held and a low signal indicating the firearm is not being held. When pressed, the pushbutton passes through the voltage at its input directly to the microcontroller. This limited the pushbutton's input voltage to the maximum input that the microcontroller's input pins could handle, +5V.This is done by connecting the pushbutton's input to the output of the voltage regulator in the firearm's power supply. To keep the output signal to the microcontroller low when the button was not pressed, a pull-down resistor is placed at the output. This 33 kilo-ohm resistor ties the output to ground until the sensor is pressed and when that occurs, the large resistance maintains the+5V at the output. The final configuration of the pressure sensor is shown in Figure A.2 in Appendix A.

2.2.3 Locking Mechanisms

Designing the locking mechanisms' circuitry took many attempts. Initially, the circuitry would consist of both analog and digital components. The thought was that the digital components would receive inputs from the firearm's microcontroller to behave as switches to control the voltage across the motors. In this design, the analog components, polarity reversing circuitry and comparators, would be used to ensure that the motors spun properly in response to different inputs from the firearm's microcontroller. Once it was determined that the motors used in the mechanical system would require up to 100 mA of current to operate, it became apparent that this design would not work. More specifically, the logic circuitry would be unable to output the necessary current for the motors. To ensure that the motors would be supplied enough current to operate, the circuitry had to be designed using only analog components. Controlling the inputs into the motor terminals was done via analog switches. Creating the proper functionality with switches while passing through enough power to operate the motors meant that high voltage and current MOSFETs were to be used.

Once it was determined that MOSFETs would be used, the next step was determining the type and quantity of the transistors. Since both terminals on the motors need to be connected to +5V or ground, an H-bridge design was selected. This design necessitates the use of a pull-up and a pull-down network consisting of two PMOS and two NMOS transistors respectively. The pull-up network ties the motors to the output of the voltage regulator, while the pull-down network connects the motors to ground. Between the output of the voltage regulator and the pull-up network is a single PMOS transistor that controls the voltage inputted to the pull-up network. The gate of this transistor receives a signal from the firearm's microcontroller that controls when the motors were able to spin. A low signal allows the PMOS to conduct, passing through the +5V from the voltage regulator to the pull-up network, thus providing the motors the necessary power to spin. When the signal goes high, the transistor cuts-off the pull-up network from the voltage regulator and the motors do not receive enough power to operate. The output from this single PMOS is sent to the sources of the pull-up network's transistors. These transistors have two different gate inputs, one relaying the lock/unlock state and the other relaying the inverted lock/unlock state. This design ensures that one PMOS in the pull-up network is conducting at all times, necessitating the use of the PMOS between the voltage regulator and the pull-up network. Each PMOS transistor output is tied to one of the motor terminals as well as the output of one NMOS transistor from the pull-down network.

The pull-down network consists of NMOS transistors whose sources are tied to ground. The gates of these transistors are fed with the same signal as the gate of the PMOS transistor that their output tied to. This configuration ensures that one terminal is connected to ground at all times and the other is connected to either +5V or ground, allowing the motors to spin clockwise or counterclockwise, depending on the firearm's desired state. The final configuration of the locking mechanisms H-bridge is illustrated in Figure A.2 in Appendix A.

Another function the locking mechanisms circuitry performs is sending signals to the microcontroller that relays when the locking mechanisms are in the locked or unlocked state, see Figure C.2 in Appendix C and Figures H.4 and H.5 in Appendix H. Using position locators placed in the locked and unlocked positions, signals are passed to the firearm's microcontroller which uses them to control the ENABLE input, thus controlling the movement of the motors. When the motors spin to the desired state, a connection is made that passes a high signal to the microcontroller. The microcontroller reads this signal and sets the ENABLE signal high to disable the motors. Every time the microcontroller receives a new state signal from the wireless receiver, it uses these signals as a check to see if the mechanisms are in the desired state. If the corresponding state signal is high, the ENABLE signal remains high keeping the motors from spinning; otherwise, ENABLE is set low until the mechanisms move to the new position. Figure A.2 in Appendix A shows the circuitry involved in this function.

3. Design Verification

3.1 Control Unit

To verify that the control unit operated as intended, the following verifications were made: the LCD display, keypad, and user menu operated with 100% reliability; the fingerprint scanner could recognize at least ten different fingerprints; the control power supply outputs the correct voltage and current to power all the subsystems; and the wireless system would successfully transmit data in under 100 ms, up to 30 feet, with 90% reliability. The full breakdown of these specifications can be found on Table D.1 in Appendix D.

3.1.1 Control Unit Power Supply

To verify the lifetime of the control unit's power supply, a new 9-volt battery was installed and the voltage outputted to the control unit was measured at various times. Initially, the voltage supplied by the battery was measured every minute for 20 minutes. Then, measurements were taken every 10 to 20 minutes until 120 minutes had passed. During this time, the fingerprint scanner was used multiple times to simulate normal usage. After the 120 minutes were completed, a plot of voltage vs. time was made, see Figure E.1 in Appendix E, and the data points were fitted with a linear line. From this line, the lifetime of the battery could be estimated. Since the system operates until the battery voltage is under 5V, the best-fit line was used to calculate the time when the voltage reached 5V. From the best-fit line, see equation 1, the battery lasts approximately 302 minutes or 5.0 hours.

$$V_{Bcontrol} = -0.0096t + 7.9 \tag{1}$$

$$t(V_{Bcontrol} = 5) = \frac{V_{Bcontrol} - 7.9}{-0.0096} = 302.1\ minutes = 5.04\ Hours$$

As expected, the greater maximum voltage and current output of the 9V battery allows the 9V battery to last much longer than the original design which used 4 AA batteries.

3.1.2 User Interface

Verifying that the user interface was 100% reliabile was done by testing its components separately then connecting them together and retesting the entire system. The first component tested was the LCD display. Since the LCD constantly outputs new data, the easiest way to test it was by programming the microcontroller and checking that the LCD output the correct characters. Displaying alphabet and numeric characters on the top and bottom lines of the display was the first test. Apiece of code was written to program the microcontroller to output the signals corresponding to each number, letter, and symbol on the keypad and the LCD was checked to verify that the proper character was displayed.

The first step in verifying the keypad's reliability was to map each button press to the keypad's output pins. This was done by individually powering each pin with a bench top power supply, then pressing each button on the keypad and reading the voltage levels of the other pins; the results are shown in Table B.1 in Appendix B. To test the keypad algorithm, the algorithm was programmed onto the microcontroller and code was added to display the key pressed onto the LCD screen. The program called for the read_keypad() statement every second, but this did not work initially because the voltages from the keypad pins that the microcontroller was reading were found to be floating. Once pull-down resistors were placed at these pins, the LCD displayed the characters corresponding to the key that was pressed, verifying that the algorithm performed properly. The final step in the keypad's verification was checking that each keypress was only registered once, no matter how long the key was held. This was tested by writing a piece of code that created a variable which incremented every time the signals for a new keypress were returned to the microcontroller. The counter's value was displayed by the LCD to verify that it would increment only once for each keypress, regardless of its length.

Verification of the user menu was done by stepping through the menu using the keypad and the LCD display. After this functionality was verified, unacceptable keys were pressed to check that the user menu did not respond to them. As expected, the user menu was traversed only when acceptable keys were pressed.

3.1.3 Wireless Transmitter and Receiver

The first step in verifying the wireless components was to test the microcontroller output to the transmitter-ensure that the correct data was being sent to the transmitter. The oscilloscope measurement of the signal 10 (1010), shown in Figure G.1 of Appendix G, shows that the transmitter input is correct. The transmitter and receiver were then connected to their respective microcontrollers and antennas and once they were set to the same frequency, a piece of code was written that would have the control unit microcontroller send a data bit to the transmitter. To verify that the signal sent from the microcontroller was being sent to the firearm unit properly, voltage measurements were taken at the data ports of the transmitter and receiver, see Figure G.2 in Appendix G. The matching signals show that the wireless system transmission worked properly.

After the functionality of the wireless system was verified, its range was checked. Placing the two units next to each other and sending several signals to the firearm revealed that even at such a small distance, the transmission success rate was only 90%. Testing the maximum range of the wireless system was carried out by sending lock and unlock signals from the control unit to the firearm unit while gradually increasing the distance between the two units. This procedure was repeated until the firearm no longer responded to the control unit's signals. It was found that the wireless system operated with a reliability of 80% at five feet, 50% at 10 feet, and 20% at 20 feet. While the wireless range did not reach the desired 30 feet, this issue could be resolved by using better components. Fortunately, the functionality of the project was largely unaffected by the lack of wireless range. The small wireless range would only affect performance when sending signals the firearm. With the timer for the unlock state being located in the firearm's microcontroller, the firearm could be moved out of the wireless range while unlocked and still relock once the unlock time runs out. The firearm could then be moved back within the wireless range to have new signals sent to it.

3.1.4 Fingerprint Scanner

The first step in verifying the functionality of the fingerprint scanner was confirming that the outputs ports of the scanner were properly connected. Since the port pins were very small and its connector was not a standard size, the connections were made by soldering wires directly to the back of the fingerprint scanner's board, see Figure H.1 in Appendix H. After these connections were made, the GPIO pins could be tested. A piece of code was written that would change the I/O line to the identify pin from high to low every time the number “1” was pressed on the keypad. Similarly, pressing “2” and “3” would change the I/O lines from high to low on the register and delete pins respectively. The Fail and Success pin outputs were fed to the control unit’s microcontroller and two LEDs, as shown in Figure A.1 in Appendix A. The LEDs were used to show whether the fingerprint scan was successful or not while the microcontroller read the outputs to determine if the user was authorized to operate the firearm.

Next, the fingerprint scanning options were tested. The commands to identify a fingerprint, remove a fingerprint, and register a fingerprint were sent to the fingerprint scanner. These commands initiated a fingerprint scan approximately 95% of the time. The identify function and remove function were completed with a 90% success rate, but the register function worked only 50% of the time. This statistic, however, was dependent on the fingerprint being registered. Some users attempted to register their fingerprint several times before it was successful, while other users needed just one scan to register their print. This discrepancy is believed to be due to the different fingerprint characteristics of each person, making some easier to distinguish than others. Another possible explanation is that the registration function required clearer scans in order to properly save the fingerprint’s characteristics to memory, whereas the identification and deletion functions likely required only a few such characteristics to match, thus increasing the success rate of these functions.

To verify that the scanner could identify the desired ten fingerprints, 10 different fingerprints were registered and saved to the scanner’s memory. Next, the identify function was done on the fingerprints and all ten were properly identified. To determine the number of fingerprints that could be saved, the scanner’s datasheet [5] was consulted and it was seen that several hundred prints could be saved, easily surpassing the desired ten.

3.2 Firearm Unit

To verify that the firearm unit operated as intended, the following verifications were made: the firearm microcontroller outputs the correct state signals to the locking mechanisms; the pressure sensor outputs a high signal when pressed and a low signal when not pressed; the firearm power supply outputs the correct voltage and current to power all the subsystems while providing enough power for 24 hours of continuous use; the locking mechanisms respond to the microcontroller’s signals in under five seconds, and they do not attempt to move into the position they are already in. The full breakdown of these specifications can be found on Table D.2 in Appendix D.

3.2.1 Firearm Unit Power Supply

To verify the life of the firearm’s power supply, a new 9-volt battery was installed and the voltage outputted to the firearm unit was measured at various times. Initially, the voltage supplied by the battery was measured every minute for 20 minutes. Then measurements were taken every 10 to 20 minutes until 120 minutes had passed. During this time, the lock and unlock signals were sent to the firearm unit multiple times to have the mechanisms move to simulate normal usage. After the 120 minutes were completed, a plot of voltage vs. time was made, see Figure E.1 in Appendix E, and the data points were fitted with a linear line. From this line, the lifetime of the battery could be estimated. Since the system will operate until the battery voltage is under 5V, the best-fit line was used to calculate the time when the voltage reached 5V, see equation 2.

$$V_{Bfirearm} = -0.0079t + 8.7 \tag{2}$$

$$t(V_{Bfirearm} = 5) = \frac{V_{Bfirearm} - 8.7}{-0.0071} = 521.1\ minutes = 8.69\ Hours$$

As can be seen from the above calculation, the battery would last approximately 521 minutes or 8.7 hours.

The lifetime of the firearm's power supply was lower than we had initially hoped. From initial current drain measurements, we speculated that the firearm unit would use approximately 30 mA of current when the motors were still and approximately 70 mA when the motors spun. Using the constant current characteristics plot [11] from the battery's datasheet, see Figure F.1 in Appendix F, the battery life would be approximately 9.5 hours, see equation 3.

$$t = 17\ hrs * \frac{5V}{9V} \tag{3}$$

$$t = 9.44\ hrs$$

The small discrepancy between the theoretical and actual lifetime of the battery is due to the estimations made in both cases. For the theoretical value, the lifetime of the battery had to be estimated by reading the constant current performance plot while the actual lifetime was calculated by using a best-fit line from several measured data points. The only definitive way to determine the battery's lifetime would be to run the system until the battery can no longer power it.

3.2.2 Pressure Sensor

Verification of the pressure sensor's functionality was done by taking measurements at the output of the pushbutton. The sensor's input was connected to a bench top power supply set to +5V to mimic the voltage that the sensor receives from the output of the power supply's voltage regulator. Using an oscilloscope, the voltage at the pushbutton's output was measured at +4.951V with respect to ground, when pressed and less than 100 mV when the button was not pressed.

These results were expected because the pressure sensor is designed to act as a switch, not dissipating any energy when closed and not allowing any power through when open. Although the pushbutton is not an ideal component, it is designed to minimize losses and behave as an ideal component. Therefore the measured voltage values were expected to be very close to 5V, when pressed, and 0V, when not pressed. Figure G.3 in Appendix G shows the average voltages for the input and output when the sensor is not pressed. The outputted voltage is non-zero due to leakage in the pushbutton, but it is less than 2% of the inputted +4.948V. Figure G.4 in Appendix G shows the average voltages for the input and output when the pushbutton is pressed. The outputted +4.951V is within the desired 5% of the inputted +4.965V.

3.2.3 Locking Mechanisms

To verify the functionality of the locking mechanisms, the inputs to the MOSFETs' gates were hardwired to simulate the signals that would be received from the microcontroller. While these signals were varied between +5V and 0V to simulate the lock and unlock signals, voltages were measured at several points in the circuit, see Table 1 and Figure 1, to verify that the motor terminals would receive different voltages when the signals changed. After the voltages at the motor inputs had been verified, the motors were connected to the circuitry to confirm that the MOSFETs were able to pass through enough power to operate the motors. After this was validated, the microcontroller was connected to the mechanisms' circuitry to test upper-level functionality. Signals were sent from the microcontroller to place the locking mechanisms into the lock or unlock state, and once the motors moved to the proper position the signal was repeated. When the signal was sent for the second time, the locking mechanisms did not try to move into the position they were already in. As expected, the repeated signal did not cause the locking mechanisms to move. To verify that the mechanisms responded to locking and unlocking signals in less than five seconds, the mechanisms were placed into the lock/unlock state and then the unlock/lock signal was sent. When the second signal was sent, the locking mechanisms were observed to begin to move without a noticeable delay.

The locking mechanisms functioned as anticipated. They responded to the locking and unlocking in under the required five seconds and they did not try to move into the position they were currently in. The response time was not expected to be an issue since the datasheets for the MOSFETs [12], [13] indicated that the maximum delay of their configuration would be approximately 170 ns, see equation 4.

$$t_{+\ terminal} = t_{-\ terminal} = \max(2 * t_{PMOS}, t_{NMOS}) \tag{4}$$

$$t_{+\ terminal} = t_{-\ terminal} = \max(2 * 85\ ns, 90\ ns) = \max(170\ ns, 90\ ns) = 170\ ns$$

When this was tested, the delay between a new input and the motors spinning was not noticeable which was expected since humans cannot perceive a delay on the order of nanoseconds.

Table 1. Locking Mechanism Testing

Enable	L/U	INV_L/U	A	B	C	D	Movement
0V	0V	5V	5V	5V	5V	0V	Unlocking
0V	5V	0V	5V	5V	0V	5V	Locking
5V	X	X	X	X	0V	0V	None

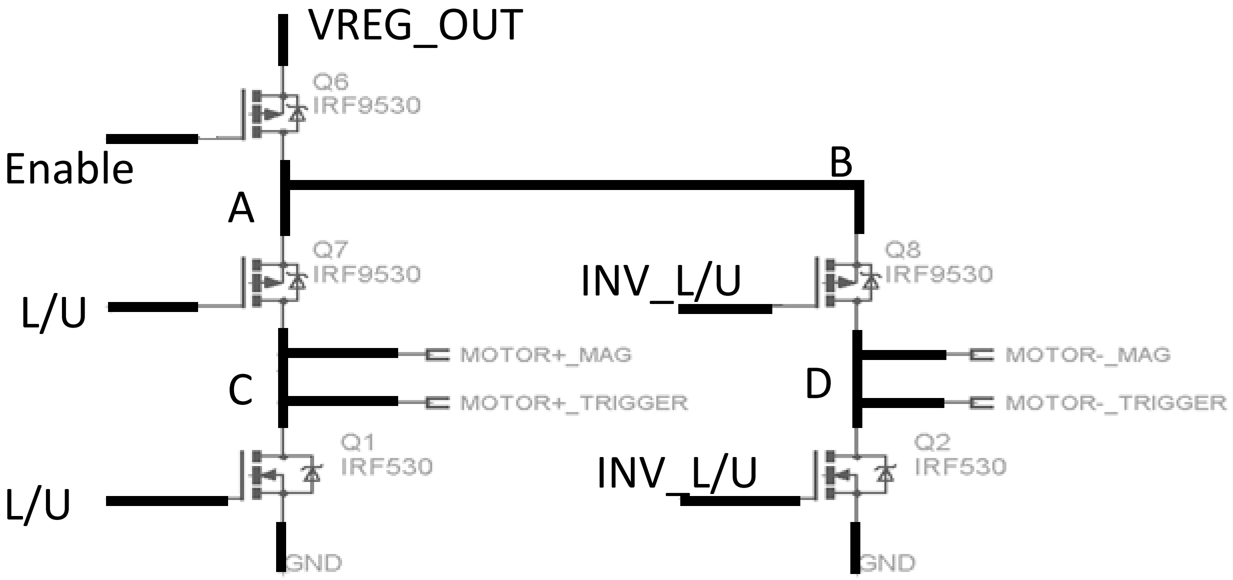

Figure 1. Locking Mechanisms Testing Circuit

4. Costs

The costs of creating the firearm locking system are broken down into the parts cost and the labor costs. The initial estimation of the project's total cost was $31,763.46 with $31,000 coming from labor costs and the remaining $263.46 coming from the parts. The final cost of this project came to be $26,523.83 with $26,250 coming from labor costs and $273.83 coming from the parts.

4.1 Parts

The breakdown for the costs of the control and firearm units can be seen in Tables I.1 and I.2 of Appendix I. The firearm unit cost $74.94 and the control unit cost $198.89, leading to a total parts cost of $273.83. The initial estimation of the parts' cost was $263.46 which is about $10 less than the final cost. The difference comes from the addition of parts that were not in the initial design, such as resistors, capacitors, and voltage regulators.

4.2 Labor

The estimated salary was set at $35 per hour which is approximately the hourly pay of a beginning engineer. The time spent working together and individually came out to be about 100 hours per person for a group total of 300 hours. Equation 5 was used to determine the total labor costs of this project which came to $26,250.

$$\text{Labor Cost} = \text{Ideal Hourly Salary} \times (\text{Hours Spent} + \text{Shop Hours}) \times 2.5 \qquad (5)$$

This number is roughly $5,000 less than the initial estimation because the total time spent working was about 60 hours fewer than the estimated time.

Before this project could make a profit, 262 units would have to be sold at $100 above production cost, or $373.83. While this is not extremely expensive, it would most likely cost too much to become a mainstream solution to increase firearm safety. Setting the price to $300, while increasing the number of units to be sold before a profit is made, would make this system much more affordable to the consumer.

5. Conclusion

5.1 Accomplishments

When demoed, this project successfully performed the desired function, increasing firearm safety. The final design has the potential to be used as a prototype for a consumer product. The user interface, which provides the user with the option to lock or unlock the weapon and allows the user to input new authorized users or remove old ones, creates a simple way for even the least experienced users to maximize the system's functionality. Using a fingerprint recognition system to authorize users makes the firearm secure and extremely difficult to tamper with. Finally, the firearm unit is small enough that it does not interfere with the positioning of the user's hand while still performing the desired function. This was accomplished by placing the larger components on a unit separate from the firearm.

5.2 Uncertainties

Although our design functioned successfully, a few parts in the system could be changed to increase performance. The range of the wireless transmission was not as far as we would have liked. Initially, we hoped to have a range of 30 feet, but the components we used only gave us a reliable transmission range of 10 feet. Another issue that arose was the fingerprint scanner's serial interface. The initial design called for the scanner to interface with the control unit's microcontroller via serial communication, but the outputs never correctly functioned so the GPIO interface was used instead. The serial interface would have been convenient to fine tune the fingerprint scanner options and to store the fingerprints in our own system. Although the serial interface could have added more capabilities, such as storing user names, with the GPIO interface the system could still perform the essential functions: identifying, adding, and removing fingerprints.

5.3 Ethical considerations

The purpose of this project, improving firearm safety, reflects the first code of the IEEE Code of Ethics [14] which refers to "making decisions consistent with the safety, health, and welfare of the public" [14]. Too often stories come on the news where someone was shot because they or someone else was not handling a firearm properly. Our system will help to prevent these accidents by only allowing authorized users to operate the firearm through the "appropriate application" [14] of technology. Taking advantage of modern technologies such as fingerprint scanners and wireless transmitters/receivers this project creates a system to help "avoid injuring others" [14] through inappropriate firearm usage. Finally, if our work is "honest and realistic in stating claims […] based on available data" [14] this project will fulfill its intended purpose: improving firearm safety.

5.4 Future work

To enhance the marketability of this project, some minor adjustments would need to be made. Smaller and more powerful antennas would be used to greatly increase the wireless capabilities up from the current 20 foot range. The components on the firearm unit would be replaced with smaller and more efficient ones to reduce the size of the unit and to increase the battery life. The size of the control unit could also be decreased by purchasing a LCD display without buttons attached to it. Along with the above changes, a sturdier housing must be added for this project to move from a simple prototype to an actual, consumer ready design.

References

[1] LCD Front Panel Set, web page. Available at: http://www.piclist.com/techref/io/LCD/panel1.html.

[2] *HP3 Series Transmitter Module Data Guide,* datasheet, Linx Technologies, 2011. Available at: http://www.linxtechnologies.com/resources/data-guides/txm-900-hp3-xxx.pdf.

[3] *HP3 Series Receiver Module Data Guide,* datasheet, Linx Technologies, 2008. Available at: http://www.linxtechnologies.com/resources/data-guides/rxm-900-hp3-xxx.pdf.

[4] *PIC16F882/883/884/886/887*, datasheet, Microchip Technology Inc., 2009. Available at: http://ww1.microchip.com/downloads/en/DeviceDoc/41291F.pdf.

[5] *NITGEN FIM5360: Stand-Alone Fingerprint Identification Device with Built-in CPU,* datasheet, NITGEN Co., 2011. Available at: http://dlnmh9ip6v2uc.cloudfront.net/datasheets/Sensors/Biometric/FIM5360_DataSheet_v1.04.pdf.

[6] D. Block, "GE423 Mechatronic Homework Assignment #3," class notes for GE 423, Department of General Engineering, University of Illinois at Urbana-Champaign, Feb. 22, 2012.

[7] Custom Computer Services, Inc., *CCS C Compiler Package*, 2007.

[8] C Compiler Reference Manual, Custom Computer Services, Inc., 2011. Available at: http://www.ccsinfo.com/downloads/ccs_c_manual.pdf.

[9] *Series 96 Standard Keypads*, datasheet, Grayhill Inc., 2008. Available at: http://www.grayhill.com/catalog/keypads_96.pdf.

[10] *ANT-916-PW-LP,* datasheet, Antenna Factor, 2008. Available at: http://www.linxtechnologies.com/resources/data-guides/ant-916-pw-lp.pdf

[11] 9V Battery (EN22), datasheet, Energizer. Available at: http://data.energizer.com/PDFs/EN22.pdf.

[12] *N-Channel MOSFET (MTP4N80E)*, datasheet, On Semiconductor Corp., 1996. Available at: http://www.datasheetcatalog.org/datasheet/on_semiconductor/MTP4N80E-D.PDF.

[13] *P-Channel MOSFET (NTP2955)*, datasheet, On Semiconductor Corp., 2006. Available at: http://www.onsemi.com/pub_link/Collateral/NTP2955-D.PDF.

[14] IEEE Code of Ethics, web page. Available at: http://www.ieee.org/portal/pages/iportals/aboutus/ethics/code.html.