ARDUINO INTEGRATED PORTABLE RFID BICYCLE LOCK

An Undergraduate Research Scholars Thesis

by

JORDAN THOMAS LEWALLEN

Submitted to the Undergraduate Research Scholars program
Texas A&M University
in partial fulfillment of the requirements for the designation as an

UNDERGRADUATE RESEARCH SCHOLAR

Approved by Research Advisor: Dr. Jiang Hu

May 2016

Major: Electrical Engineering

TABLE OF CONTENTS

ABSTRACT

Arduino Integrated Portable RFID Bicycle Lock

Jordan Thomas Lewallen
Department of Electrical & Computer Engineering
Texas A&M University

Research Advisor: Dr. Jiang Hu
Department of Electrical & Computer Engineering

The purpose of this research is to design a multi-purpose electronic lock for bicycles and motor scooters. This engineering project will develop a battery-powered device that can function both as a touchless electronic lock and, if necessary, a traditional mechanical lock. In order to conquer this task, I will generate a lock design that will be secure while also allowing convenient owner access to the internals to change the battery when it inevitably loses charge. Security, convenience and ease of use are the highest priority design criteria. With this device, it will be possible to synchronize existing electronic card keys tag as used in some apartments and store it within device memory, which will reduce the number of keycards/keys that must be carried around on a daily basis. Data logs will also be stored to determine time-of-day and date when a bike lock was unlocked or broken and, therefore, making it easier to track down the missing property on campus and around town.

CHAPTER I

INTRODUCTION

Universities and large cities such as Texas A&M and Houston prove challenging to get around. Walking can be time consuming and searching for a convenient parking lot with available spaces can be a gamble, not to mention cost prohibitive. Bicycles and motor scooters are natural forms of transportation for students and urban residence [1]. Good locks exist, but they are often challenging. It can be difficult to maneuver your body around a rack full of bicycles to find the tiny key hole, precisely insert the key, and retrieve the open lock. Engineers should be able to design a more convenient device.

Modern electronics have provided new capabilities to make life simpler. Cellular telephones, wireless computer routers and automobile key fobs are a few examples of modern electronics that have made life faster and easier. A properly designed wireless, electronic bicycle lock using a radio-frequency identification tag (RFID) would remain safe and be more convenient [2, 3]. Besides the "touchless" convenience factor, there are several additional features that would make such a lock even more valuable. For example, having the ability to synchronize an existing RFID from your apartment complex or office building, and use it as your bicycle key could reduce the number of card keys you would need to carry. As an ancillary attribute, this modern electronic lock could also help should your bicycle get stolen since 1.5 million bicycles are stolen every year [4]. A properly programmed electronic bicycle lock would record the date and time the lock is broken. Police could use this recorded time and date to immediately scan time-stamped security camera footage for recorded evidence.

Therefore, the purpose in this research is to use existing technology, such as RFID, to design a multi-purpose bicycle lock that would make it easier to unlock without the physical obstacles that a mechanical bicycle lock presents. The lock would be programmable to authorize additional security cards to be used and it would record information helpful to police to recover a stolen bike.

CHAPTER II

METHODS

Radio-Frequency Identification (RFID) card reader implementation

After evaluating design specifications, it is important to select a card reader that withholds three key standards: size, range, and power consumption. Due to dimensional requirements (ensuring lock portability), the reader should not exceed a maximum area of 8-10 square centimeters. By maximizing the effective range of the card reader, the device would contribute to a more convenient locking/un-locking experience. Therefore, installing a card reader with a range greater than 100mm would be optimal. Lastly, implementing a card reader that consumes power efficiently would prevent the consumer from having to replace the battery as often, therefore, power consumption should be kept below 2-5V/50 mA.

ID-Innovations RFID reader

ID-Innovations offers two variations of their RFID Card Readers: ID-2LA and ID-12LA. It is important to select the device that optimizes the three standards: size, range, and power consumption.

ID-Innovations ID-2LA & ID-12LA

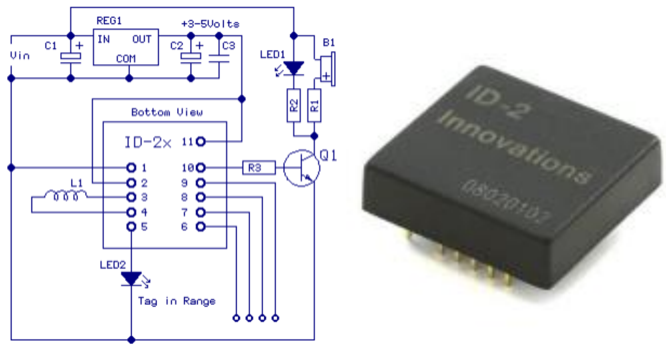


Figure #1. ID-Innovations ID-2LA circuit diagram (Left) and device (Right).

While the ID-2LA is (dimensionally) the smallest of the three, a 3rd party antenna must be soldered onto pins 3 and 4 for the reader to function properly (see Figure 1 above). This external component was considered since it would allow a controlled placement of both the reader and the antenna separately in order to optimize signal strength. Fortunately, the lock design will not interfere with signal strength as a plastic enclosure was considered (signal interference will be discussed more thoroughly later on), therefore, the ID-12LA was employed within the design for its larger read range.

Battery composition and implementation

Due to voltage restrictions specified by the ATMEGA328 and the ID-12LA RFID Card Reader, the system should not exceed a 5V limit. Therefore, there were few alternatives that this design could be implemented with. In an attempt to produce a consumer-friendly device, the objective was to utilize a battery that was readily available in most markets. Due to current and reliability limitations, an alternative voltage source above/below 5V would have to be considered.

Step-up v. step-down switching/linear regulator

A voltage regulator is a component specifically designed to maintain a consistent voltage level. Two forms of regulators were considered for this design: Linear and Switching.

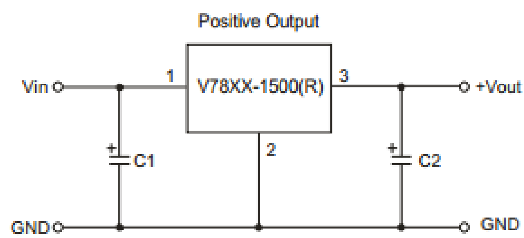
A linear regulator employs an active (ex: Bipolar Junction Transistor (BJT)) device controlled by a large-gain differential amplifier. By comparing the output voltage with a specific reference voltage, this linear regulator adjusts the allowable voltage to maintain a constant voltage. Given an input and output voltage, a linear regulator's power dissipation is directly proportional to its output current. As a result, efficiencies for linear regulators sit near 50% as nearly half of the energy in the battery would be converted to waste heat. However, this regulator does have the advantage of low noise at the output of the system.

A switching regulator converts a DC input voltage to a switched voltage which is applied to a BJT or MOSFET switch. This switched output voltage is filtered and sent back to the circuit that controls the power switch so that the voltage remains constant regardless of load current and input voltages. Using optimal components, a switching regulator (with voltage & current values matching a specified range) will be able to reach peak efficiencies near 90% and drive higher current loads. However, output noise is much higher than the linear regulator.

It is important to take into account individual component specifications in order to identify any conflicting parameters. Three core components were given priority:

ID-Innovations ID-12LA RFID Card Reader datasheet states that a linear regulator is the ideal power supply for the reader to work properly. Switching power supplies are increasing in popularity, but this form of power supply can present several problems for the card reader. First and foremost, the switching frequency must not be close to a multiple of the frequency of operation (125 KHz) or interference will reduce the reading range. Also, switching power supplies output voltage ripple (or noise as mentioned earlier). For respectable range, the output ripple should be no larger than 2mV peak-to-peak, which can be very demanding on switching power supplies. Next, the bicycle lock's primary locking mechanism operates a Zon Hen Open-Frame solenoid which requires a (comparatively) large current draw over a short period of time. Finally, the bike lock should be sustainable for long periods of time, thwarting the consumer from purchasing a new battery often. As a result, this would require a very efficient power regulation component. With these considerations in mind, a switching regulator was used within the design.

Following the decision of a switching regulator, it was important to determine whether the regulator should step the voltage up or down within the system. While in operation, a switching regulator forms an inverse relationship with current. If a voltage is dropped, the current increases (step-down). Conversely, if voltage increases, current is dropped (step-up). As mentioned earlier, high current draw and power efficiency are of paramount importance within this design, therefore, a CUI Inc. V7805-1500 step-down switching regulator capable of converting voltages greater than 6.5V and outputting 1.5A (with a typical switching frequency of 340 kHz) was selected for the design.



Part Number	C1 (Ceramic Capacitor)	C2 (Ceramic Capacitor
V7805-1500	10μF/25V	22μF/16V

Figure #2. (Top) Typical application circuit utilizing the CUI Inc. V7805-1500 step-down switching regulator. (Bottom) Recommended capacitance values for use within the system.

The capacitor at pin 1 (C1) is used to reduce voltage transients on the input of the regulator and improve output voltage stability (although it may not be necessary when using a battery as a power source). The capacitor at pin 3 (C2) reduces transient voltage fluctuations on the output terminal cause by rapid changes in the load current. By limiting the design to a step-down switching regulator, as seen in Figure 2, the system ultimately restricts the voltage source selection to 9V batteries.

Radio frequency signal interference with switching regulator

As discussed in further detail below, the final bicycle lock design will employ a switching regulator. Unfortunately, switching power supplies are associated with radio interference. These power supplies function at high frequencies that approach the RF spectrum (conversely, linear power supplies do not run at such high frequencies which would result in less interference). Due to the “fast” switching, harmonics of the switching frequency generated by under-damped oscillations (a signal containing excess “noise” when initiated, this noise is reduced slowly over time, until the desired signal is set, seen in Figure 3) will result in RF complications.

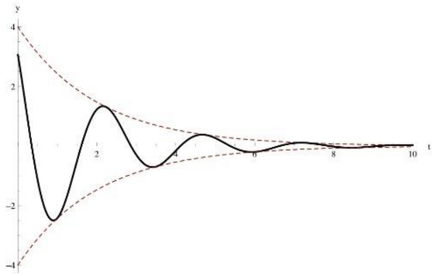


Figure #3. An example of an underdamped signal, this waveform characteristic affects RF signal read range.

Battery saving methods

While experimenting with the preliminary design, current was drawn continuously from the power source until the battery was removed within the system. Regulating power consumption within a device that runs full-time while only operating a few times a day is inefficient and would be an inconvenience to the consumer (considering that the battery would only last a few hours). In an effort to maximize battery life and efficiency, a few software and hardware enhancements were implemented within the design.

Mechanical Power Slide-Switch vs. Button Switch

Figure #4. Mechanical slide switch (Left) and Button Switch (Right)

The first fix was the implementation of a mechanical power slide-switch, observed in Figure 4. While slide-switches are not as convenient (or as aesthetically pleasing) as a conventional power button, slide-switches operate under less current draw due to the lack of a de-bouncing circuit. A slide switch "mechanically" connects two wires together (no extra components necessary).

What is a de-bouncing circuit?

Simple push buttons will generally produce false open/close transitions when pressed (example in Figure 5 below). This is usually due to mechanical/physical issues within the design. As a result, OFF/ON transitions are determined as multiple presses in a short period of time which, as a result, may fool the software that is continuously checking to see if a button is pressed.

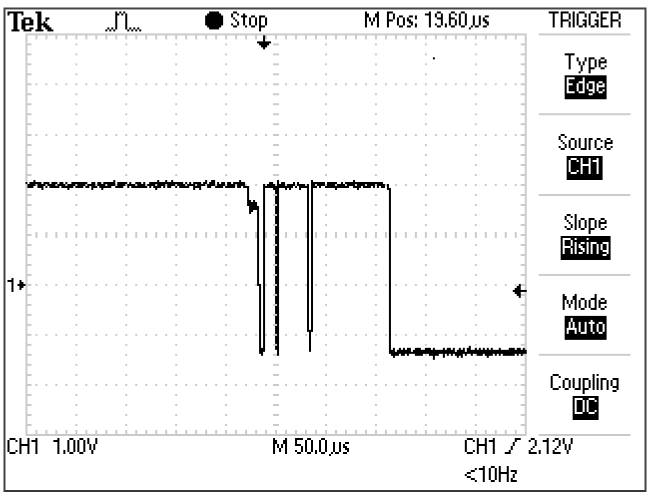


Figure #5. Oscilloscope output of a system without a de-bouncing circuit (note the several dips in the signal output).

One drawback of the slide switch (when compared to the button switch) is the likelihood that a consumer will forget to turn the switch OFF after unlocking/locking their bicycle. The push button does not face the issue since the button will remain OFF unless specifically pressed ON. In order to counter this issue, additional Arduino programming was necessary.

System timeout software enhancements

By observing test results, the average unlock time per trial (power ON stage to LOCK stage) was 10 seconds. When employing additional Arduino code, it was possible to program the system to enter a low power sleep mode if a time threshold of 25 seconds was met. At this point, the microcontroller assumes that the user forgot to turn off power via the slide switch and will enter sleep mode to preserve battery power. By sliding the switch back to its initial OFF position, the Arduino will completely shut off and will be ready to use the next time a bicycle need to be locked/unlocked.

Dead battery replacement method

As with any (non-wired) battery powered devices, there will inevitably come a time when the battery within the device will need to be replaced. This brought up an interesting question. How can a user access the battery in a device that is designed to be tamper-proof? The two concepts that were considered are stated below.

Direct key access

The first concept employed a mechanical "key" unlock, similar to what can be found on a common bicycle lock. Except in this case, when a user inserts and twists the key, the rotational movement will pull back the rod inside the solenoid (instead of a metal stud), allowing the U-bar to be removed from the lock.

Moving bar concept

The second concept proves to be more complex. This time, the U-bar is connected by a horizontal bar at the top. One end of the U-bar extends into the base of the bicycle lock, while the other end contains two metal segments: the RFID segment and the mechanical segment. These two segments are connected via a traditional mechanical lock. By using the RFID method, both segments will be released via the solenoid. However, if the battery in the bicycle lock dies, the user can insert a key and detach the lower segment from the U-bar. As a result, the U-bar will only be connected at one end. This will allow the user to "pivot" the bar so that the battery compartment can be accessed via the three sleeve design. While this design was not employed, it was deemed appropriate to include both unlocking mechanisms.

Key locking mechanism: Solenoid

Figure #6. 5v solenoid component

A solenoid, displayed in Figure 6, will be used as the primary locking mechanism within the design. Solenoids are composed of two features: A rod (typically called an armature) and a coil of wire around the rod. When a large current flows through the coil of wires, a magnetic field is formed around the wire. More coils in the wire results in a larger magnetic field flowing around the coil and through its center in a "donut" shape. When current flows through the coil, the rod moves to increase the flux linkage by closing the air gap between cores. The solenoid is typically spring loaded (as this one is) to retract the rod when current stops flowing through the coils. Utilizing a solenoid has many convenient functions such as the speed at which the rod is pushed and pulled (a fast locking and unlocking mechanism) and no mechanical moving parts thus, the odds of the solenoid breaking are quite slim. One deterring factor of a solenoid is the hefty amount of current that is necessary for the solenoid to function properly. Conventional 9V batteries do not store large currents.

Requirement of a Schottky diode

Figure #7. “Fly-back” Schottky Diode

As mentioned earlier, a solenoid comprises of two primary features: a rod and coil of wire around the rod. In order to “push” this solenoid forward, a large current is induced through the coils. The current through the coil generates a magnetic field strong enough to push the solenoid forward. Since an inductor (the solenoid) cannot change its current instantly, the flyback diode provides a path for the current when the coil is switched off. Otherwise, a voltage spike will occur causing arcing on switch contacts or possibly destroying switching transistors. Therefore, a Schottky diode was applied to the system (see Figure 7).

External crystal oscillator

While the ATMega 328P has a maximum oscillating frequency of 20 MHz, the design originated from an Arduino board running at an oscillating frequency of 16 MHz. Thus, an external crystal oscillator was necessary. Application of an external oscillator requires two capacitors in parallel with the crystal. It is important to calculate the proper values of the parallel capacitors, failure to do so will result in a poorly functioning circuit.

Calculating crystal capacitance values

In order to obtain accurate results from the crystal, it is important to match the capacitors to the selected crystal (this varies from model to model). Fortunately, it is trivial to calculate the proper capacitors for the crystal. After examining the datasheet, the Load Capacitance (CL) was discovered to be 20 pF. The two parallel load capacitors must match this Load Capacitance with the following formula:

$$C_L = \frac{C_1 * C_2}{C_1 + C_2} + C_{stray} \tag{1}$$

As mentioned earlier, C1 and C2 are the two capacitors in parallel with the crystal. Stray capacitance is the addition of excess capacitance that every component contains (trace, lead, PCB component, etc.). Thus using equation 1, the use of two 22 pF ceramic capacitors (in parallel) will be necessary to properly load the crystal oscillator.

RFID tag (125 KHz)

Another selling point for this device is the ability to store multiple key tags within device memory and to sync existing cards (ex. Apartment RFID tags) to help cut down on the number of items carried on a keyring. The Arduino Bicycle lock will come packaged with a stock passive 125 kHz RFID master card. This card can be used for two purposes when unlocking the device: Since this card is “hard-programmed” into memory as the “master card,” the device will enter write mode (the LED will flash between RGB colors) and wait for a new card to be scanned. Assuming this new card is 125 kHz, the RFID reader will read the serial off the new card and save it within the ATMega's EEPROM memory. If the master card were to be swiped again (while still in write mode), the card would act as a normal card and unlock the device. NOTE: This is the only card that can be used as a master key since the ATMega has been hard programmed with this specific serial number.

Visual operating notification

Implementing some form of visual user feedback is critical for operation of the bicycle lock. By inserting an LED within our design, this component would provide multiple forms of visual feedback. There are four stages programmed within the Arduino each stage is assigned a different color/pattern (more stages can be easily programmed as well).

Power/standby state

When the device is powered on and the reader is ready to receive a serial code, the LED is BLUE for indefinite length.

Unlock state

If the serial code read by the ID-12LA matches a code stored within the ATMega 328 IC, the LED is GREEN for 2 seconds then reverts back to its power/standby state.

Denial state

If the serial code detected by the ID-12LA does not match a serial number present in its memory, the LED is RED for 2 seconds, then reverts back to its power/standby state.

Memory write state

It should be noted that the ATMega is hard-programmed with a "master" card. If scanned, this master card will allow the user to write a new (125 KHz) card into the EEPROM memory of the IC. While it "write" mode, the LED will flash a sequence of RED, GREEN, and BLUE until a new card is read into the system. If the master card is scanned a second time while in the "write" state, the device will enter “unlock” state (LED is GREEN) and then will return to “power/standby” state.

Design schematic

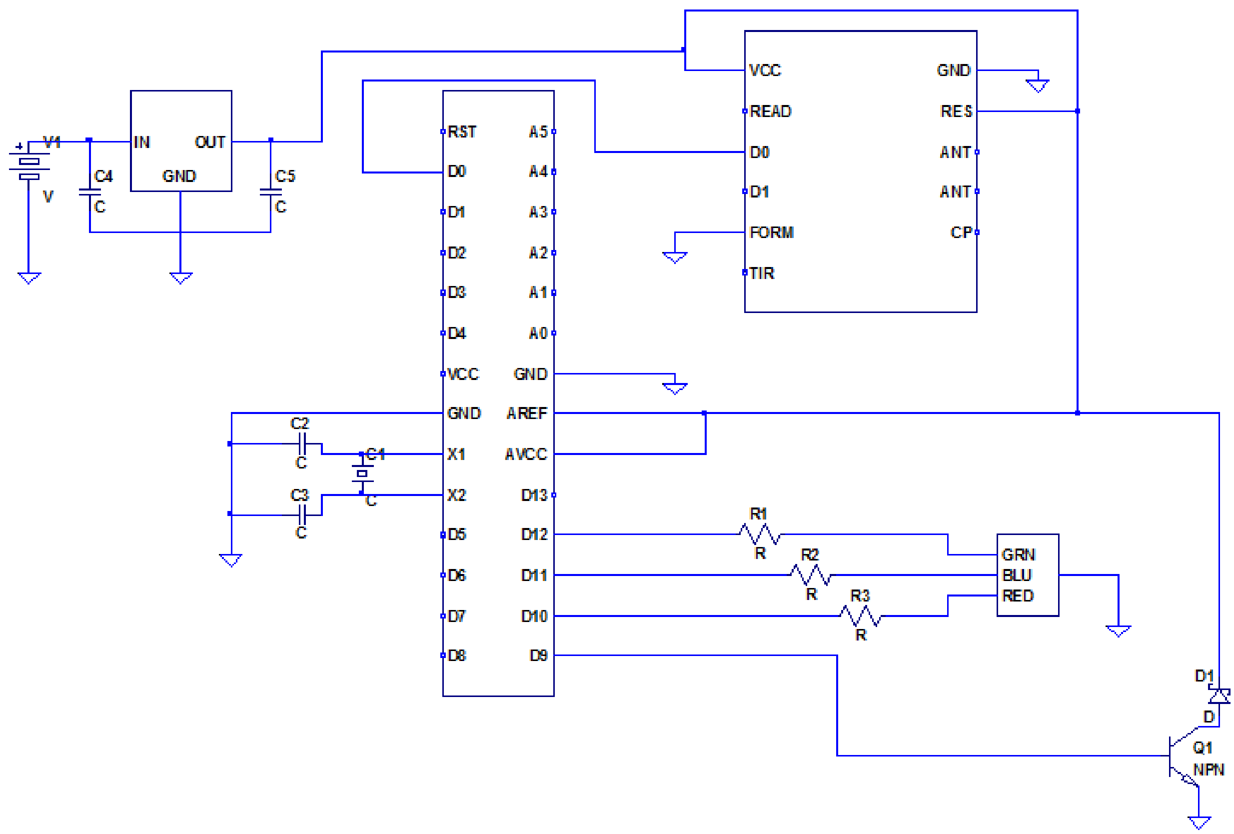


Figure #8. Bicycle breadboard design schematic

Bicycle lock “three-sleeve” design

Radio waves are electromagnetic waves that travel at the speed of light (3x10^8 m/s). There are two types of materials that affect electromagnetic waves, conductors and insulators (also called dielectrics). Most conductors are metals such as steel, copper, or aluminum. When a radio wave hits a material, some of the power is reflected by the surface and some of the power is transmitted into (and possibly) through the material. Assuming this material is metal, most of the radio power is reflected within the first few atoms. As with most bicycle locks, the external casing will be manufactured with stainless steel. The understandable benefit to using stainless steel is its resilience to forced entry. However, this project utilizes radio frequencies that are affected by such metals. As a result, the three-sleeved design averts this complication by incorporating a plastic enclosure on the left hand side, thus allowing radio frequency communication.

Figure #9. Three sleeve design demonstration.

Figures 8 and 9 demonstrate how the lock and Arduino will be assembled. (From left to right) Plastic RFID enclosure, power button (red), central housing component, stainless steel enclosure. The RFID reader and battery can be observed above the central housing component.

CHAPTER III

RESULTS

Battery lifetime results

As with any battery powered electronic device, extending battery life was a top priority. After implementing software and hardware power saving concepts, it was time to see how the bicycle would last in a lab environment. The first test featured was included as a control. In this test, maximum power ON time was examined. The device would be left in a fully functioning state until the battery crossed the 7V threshold. This threshold was set since the voltage regulator is not able to regulate a voltage less than 7V down to 5V (the operating voltage of the system).

Alkaline 9V battery

The battery to be tested was a household 9V alkaline battery rated at 595 mAh. Device function ceased to continue after surpassing the 110-minute threshold. See Chart 1 below:

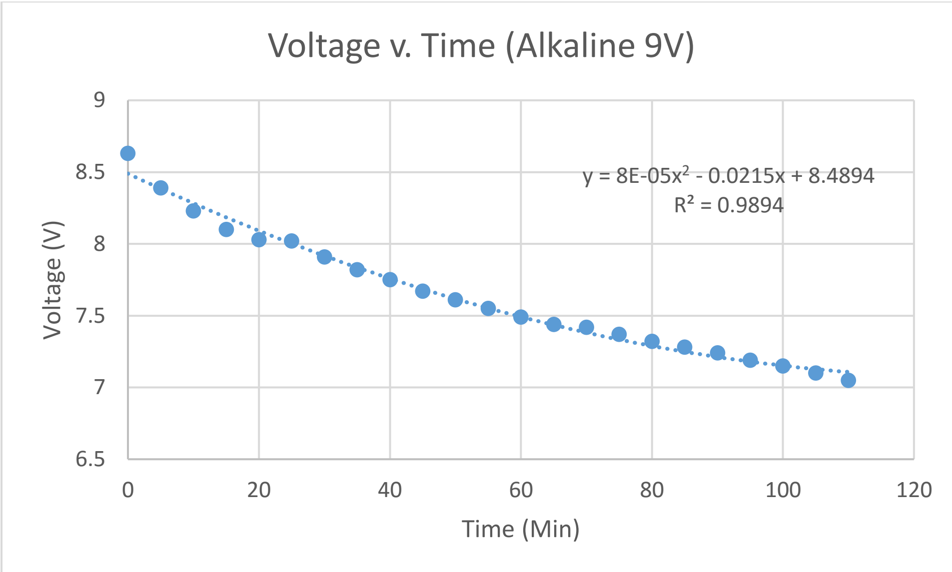


Chart 1. Duracell 9V alkaline battery voltage v. time test results. 120 minute test period.

Assuming an average device ON time of 15 seconds and lock use 2 times a day:

$$\frac{110\ min}{1} * \frac{60\ sec}{1\ min} = 6{,}600\ seconds \tag{2}$$

$$\frac{6600\ sec}{1} * \frac{1\ unlock}{15\ sec} = 440\ unlocks \tag{3}$$

$$\frac{440\ unlocks}{1} * \frac{1\ day(s)}{2\ unlocks} = 220\ days \tag{4}$$

Therefore, the average consumer will have to replace the battery every 220 days.

Lithium Ion 9V battery

For the second iteration of experimentation, an Energizer Lithium Ion 9V battery was used.

Following similar voltage specifications, the differing factor is the mAh rating, set at 750 compared to the Alkaline 595 mAh rating. This sizeable increase in current capacity is directly related to battery ON lifetime as observed in the Chart 2 below.

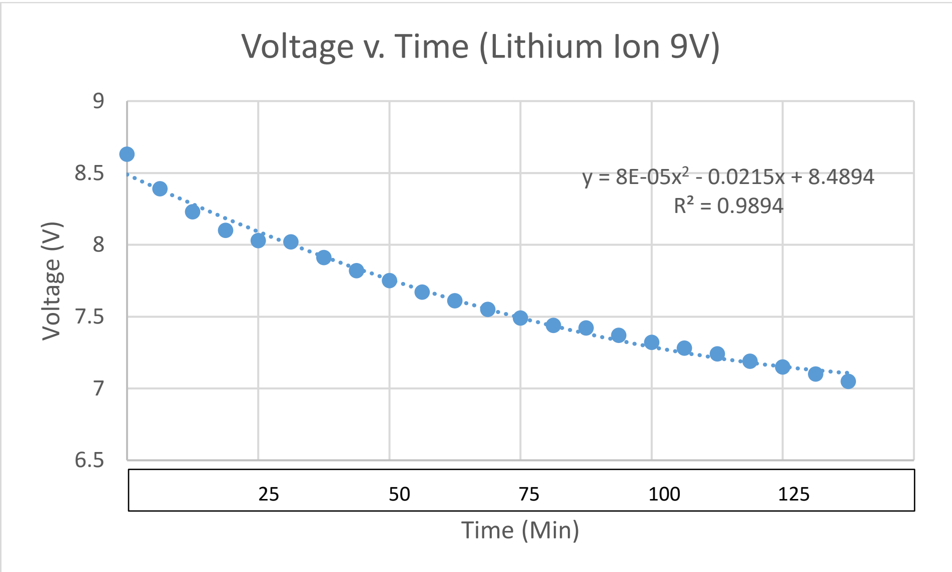


Chart 2. Energizer 9V lithium ion battery voltage v. time test results. 120 minute test period.

Following similar calculations, battery lifetime for the lithium ion 9V battery is incresed to 130 minutes. As a result, total unlocks (given 2 unlocks per day) is now:

$$\frac{Battery\ Lifetime}{2\ Unlocks} = 260\ days \tag{5}$$

Therefore it would be plausible to include a lithium ion battery upon final product shipment. In the future, other battery technolgies will be explored such as polymer lithium-ion.

Production specs and design

With a fully-functioning bicycle lock premeditated on a breadboard, the production design was to be considered. Due to the nature of a lock, it is important that the design was to be built around security and rigidity. Therefore, the majority of the lock was to be produced from hardened steel. The only exception was to be the plastic sleeve for the wireless RFID sensor (reasoning explained in the methods section). Figure 10 highlights the mechanical emergency key access (in case of battery failure) and an overhead view of the RFID, LED, and 9V battery compartments in the central steel enclosure.

Figure #10. (Left) View of the side where direct access to the mechanical lock (in case of battery failure) is placed. (Right) Overhead view displaying RFID reader, LED, and 9V battery compartments.

Figure 11 displays a cross-sectional view of the central enclosure with all components in place (not shown is the Arduino placement and wiring between components). This view also presents a detailed perspective into the unique three-sleeve design (plastic sleeve [left] and steel sleeve [right]). The solenoid rod extends into the socket, which can be observed on the right-hand side of the U-bar in the figure below. When the tag is scanned and accepted, the solenoid retracts, this will allow the user to remove the bar from the central enclosure. On the left-hand side resides a compressible power switch which powers on the components for wireless use.

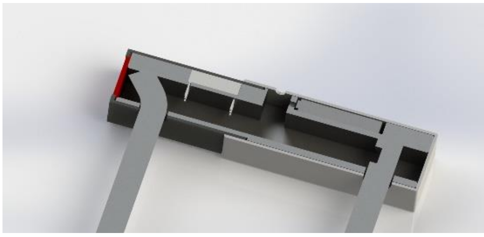


Figure #11: Cross-sectional view displaying the "three-sleeve" design, allowing access to the battery compartment

Figure 12 below present two extruded models of the bicycle lock components and their respective placement.

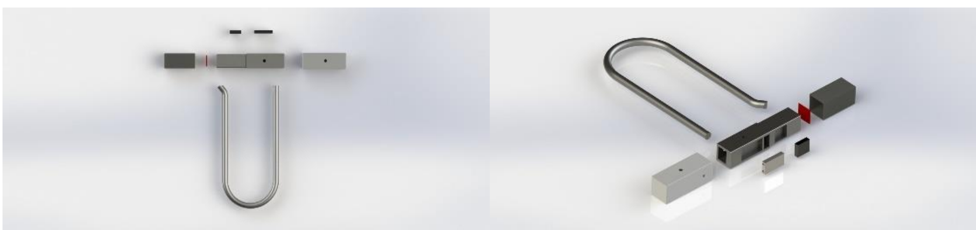


Figure #12. Exploded-view renders featuring component placement

Figure 13 shows the device in the "locked" position for an understanding of how the device will look on a day-to-day basis.

Figure #13. Side and top views of the preliminary lock design

CHAPTER IV

CONCLUSION

Completion of the prototype design thus concludes the research determined for the Wireless Arduino RFID Bicycle Lock. The resultant device provides many advantages for the consumer. With the addition of wireless technologies, the bicycle lock prevents the user from key insertion when secured in a storage rack by use of a scanning tag. While wireless communication is intended, this bicycle lock design also allows for traditional "lock and key" operational methods. The implementation of lock/unlock timestamps allows the consumer to determine when the bike was used by an unknown handler. The timestamps can then be forwarded on to local authorities for surveillance tape monitoring to observe property tampering. Finally, the incorporation of card-syncing allows the user to scan pre-existing RFID cards to lessen the total cards carried on a key fob. Upon unit testing, a respectable battery lifetime of ~220 days was examined, thus proving efficient and adequate performance on the consumer end. Fortunately, this design also allows for a large quantity of production scalability. As a result, there are many ways this project can be extended to implement evolving technologies. The incorporation of a custom Arduino will allow Bluetooth component compatibility. This compatibility would allow for connection to smart phone devices to provide proximity unlocking features while also allowing event tracking and battery life features. Using pre-existing technologies, a more convenient method for securely locking and accessing property was successfully fashioned.

REFERENCES

[1]M. Morris, 'City to convert lane of downtown street to bike path', *Houston Chronicle*, 2014 [Online]. Available: http://www.houstonchronicle.com/news/houston-texas/houston/article/City-to-convert-lane-of-downtown-street-to-bike-5714260.php. [Accessed: 06- Sep- 2015]

[2]G. Kulkami, R. Shelke, R. Sutar and S. Mohite, 'RFID security issues & challenges', in *2014 International Conference on Electronics and Communication Systems*, 2014, pp. 1-4.

[3]T. Hollstein, M. Glesner, U. Waldmann, H. Birkholz and K. Sohr, 'Security challenges for RFID key applications', in *3rd European Workshop on RFID Systems and Technologies*, 2007, pp. 1-12.

[4]"National Bike Registry - Bicycle Thefts Are up 10%!" *National Bike Registry - Bicycle Thefts Are up 10%!* Web. 25 Aug. 2015. <https://www.nationalbikeregistry.com/theft.html>.

[5]C. Floerkemeier and S. Sarma, 'An overview of RFID system interfaces and reader protocols', in *IEEE International Conference on RFID*, 2008, pp. 232-240.

[6]J. Muller, M. Schapranow, C. Popke, M. Urbat, A. Zeier and H. Plattner, 'Best practices for rigorous evaluations of RFID software components', in *European Workshop on Smart Objects: System, Technologies and Applications (RFID Sys Tech)*, 2010, pp. 1-10.