Portable Anti-Theft Package Container

By

Ethan Fransen

Conor Mueller

Yufei Zhu

Final Report for ECE 445, Senior Design, Spring 2022

TA: Qingyu Li

03 May, 2022

Team 44

Abstract

This paper details the design and functionality of our solution to package theft. We created a secure container armed with an alarm system triggered by motion sensors and an accelerometer. We will examine and discuss the operating characteristics of the device as well as the methods used to confirm the proper operation of the device with measurements used to support these claims. Total costs accounting for individual parts of the system as well as labor are included. Finally, the overall accomplishments of the system and its shortcomings are identified. Areas for improvement for a professional version of the product are theorized and proposed.

Contents

1 Introduction

Nowadays, ordering products online is a common practice. All sorts of items ranging from entertainment devices to fresh groceries wait at the entrance to people's homes for hours on end. Unfortunately, this leaves unguarded packages vulnerable to theft by opportunistic individuals, also known as porch pirates. In 2021 alone, porch pirates stole over 210 million packages[1]. Package theft is not only a major nuisance, but it can have drastic consequences when the stolen package contains essential items such as medical prescriptions. As the popularity of online shopping continues to grow, this problem will only become more pervasive.

Several potential solutions exist, but all come with significant shortcomings. Installing a secure dropbox is expensive and requires space that may not be available to all homeowners. Other delivery practices, like requiring a signature or picking up from a secure location are effective solutions, but they complicate the process more than necessary and can be annoying for both the customer and delivery service. Package theft is a crime of opportunity, so an effective solution must lower this opportunity while also deterring theft, not costing too much, and not complicating the delivery process.

Our proposed solution is a portable anti-theft package container. It will be purchased and deployed by online delivery companies such as Amazon or FedEx as a service for their customers. It would be an affordable, modular, and efficient solution and would help to prevent loss of revenue from stolen goods. It would also be easily controlled with a smartphone app, and generate a new stream of income for the delivery companies that use it. Figure 1 shows a visualization of our solution.

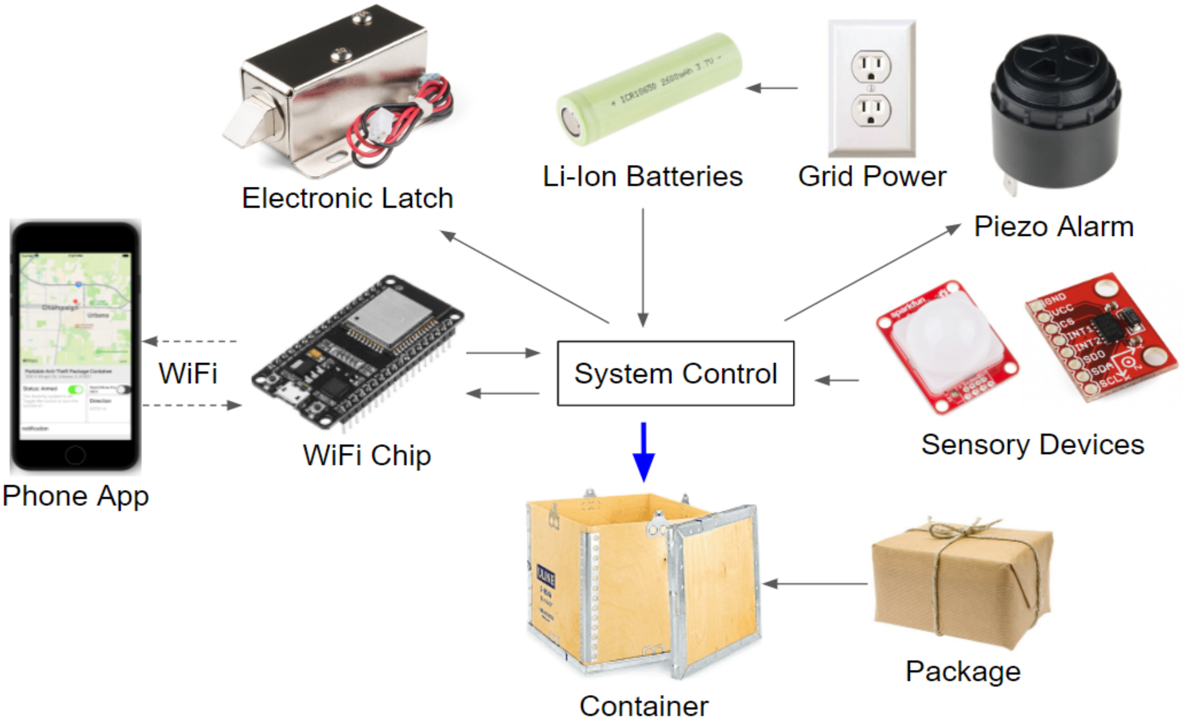


Figure 1: Design Visual Aid

1.1 Solution Subsystems

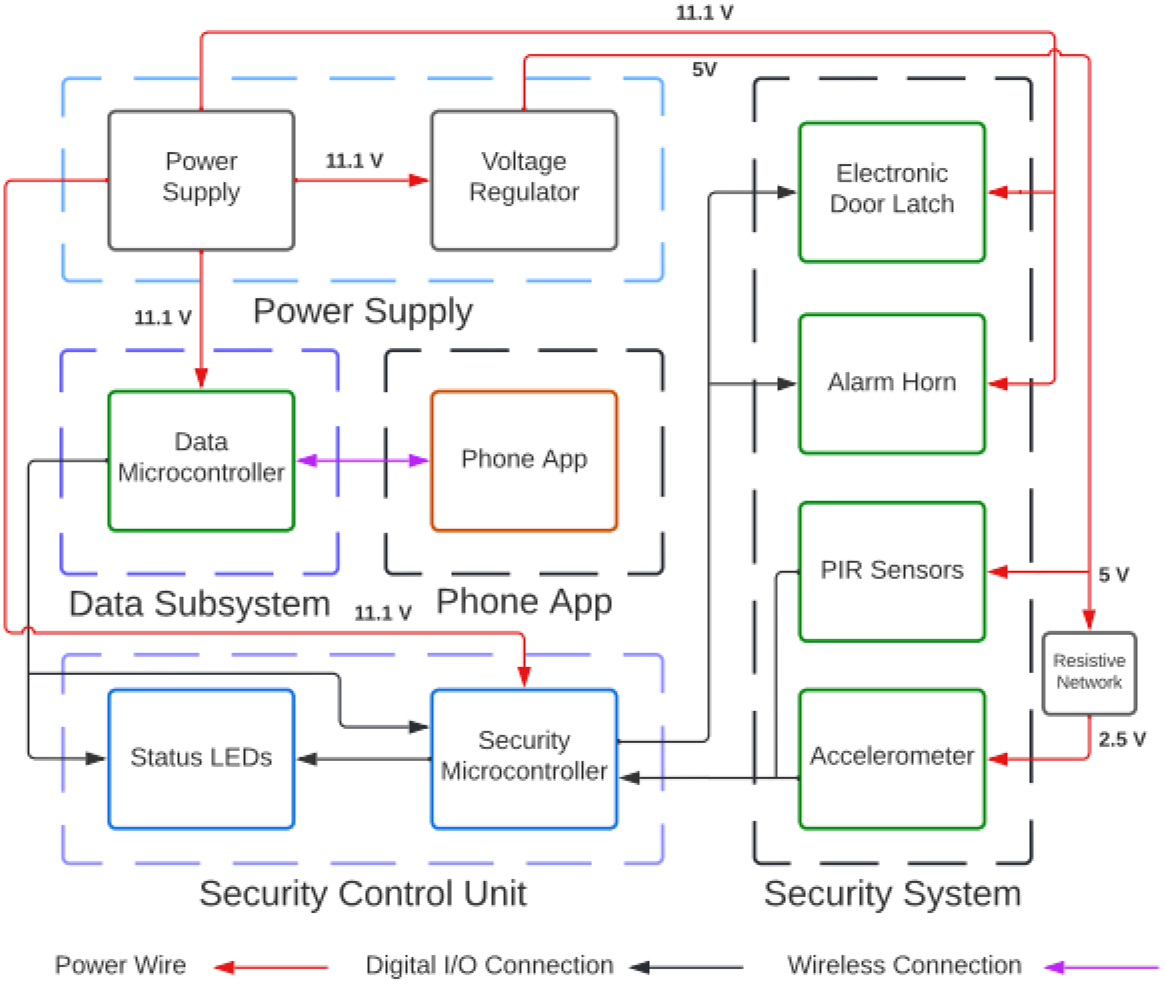


Figure 1.1.1: Block Diagram

Figure 1.1.1 shows the block diagram for our solution. The main subsystems are the power supply, security system, security control unit, data subsystem, and phone app. The power supply is responsible for supplying appropriate power to the rest of the systems. The security system includes the majority of the system inputs and outputs. It is what allows the system to actually detect potential thieves and prevent them from accessing the container. The phone app is responsible for taking user inputs and communicating wirelessly with the data subsystem. The data subsystem then communicates with the security control unit to update the security microcontroller status and move the system to the appropriate state. Figure 1.1.2 shows the state flow of the system, and highlights that the box is fail secure. The security microcontroller is the main control point for the system as it receives input from the sensors and data microcontroller, and provides output to the alarm, latch, and status LEDs.

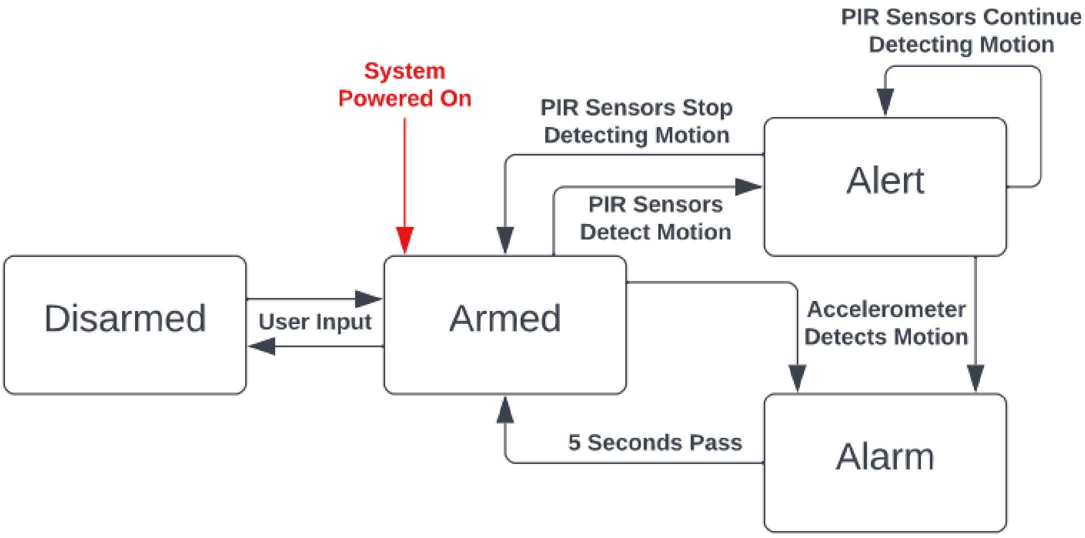

PIR Sensors Continue Detecting Motion
System Powered On
PIR Sensors Stop Detecting Motion
Alert
PIR Sensors Detect Motion
Disarmed
User Input
Armed
Accelerometer Detects Motion
5 Seconds Pass
Alarm

Figure 1.1.2: State Flow Diagram

2 Design

2.1 Security System

Much of the product design is concentrated into this system. Motion sensors and an accelerometer act as the sensory devices that step the system into higher levels of alertness. Digital I/O from these devices is used to activate the alarm located inside the container. This alarm will alert bystanders and scare any potential thieves away.

2.1.1 Electronic Latch

The door to the container is secured with a simple solenoid latch. We operate the latch using a MOSFET with our security microprocessor providing the gate voltage. The latch is connected to the 11.1V battery voltage, at which it draws 700 ± 50 mA of current. This pulls the latch back, allowing the container to be opened and the package inside accessed. As the battery voltage decreases, so does the current draw. This lowers the power consumed by the latch, but also lowers its responsiveness. We were able to open the latch at a voltage of roughly 7.5V, at which it drew 600 mA of current, but any lower than that and the latch would not receive sufficient power to operate.

2.1.2 Alarm Horn

The alarm horn acts as our means of deterrence for package thieves. Power is controlled by a BJT with our security microprocessor supplying the base current. Figure 2 depicts the connection of this device. While an MOSFET transistor similar to that used with the latch could be used here, we chose a BJT for its ease in altering the voltage delivered to the alarm. By varying the resistor value at the emitter connected in parallel with the alarm, we are able to effectively set the voltage drop across the alarm. We selected a 1 kΩ resistor, which resulted in 5.1V at 30mA being delivered to the alarm, achieving a volume of 90dB. More voltage would provide a louder alarm, but we wanted to ensure that the alarm was incapable of damaging anyone's hearing

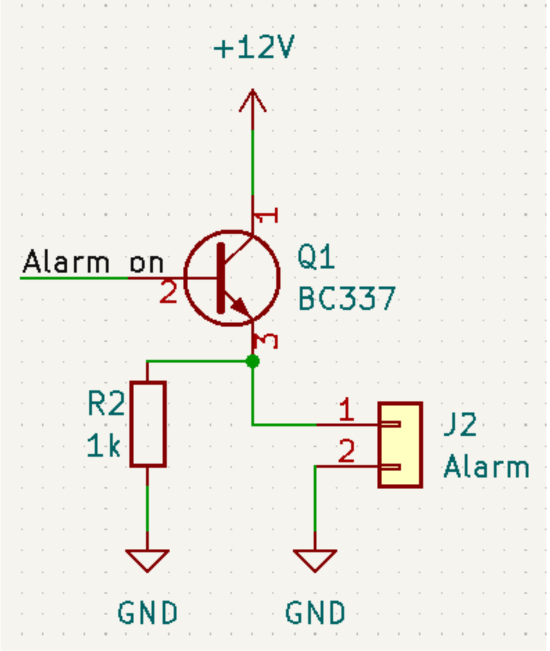


Figure 2.1.2: Alarm Schematic

2.1.3 PIR Sensors

Three PIR motion sensors, one mounted on the front and either side of the container, are used to perceive movement around the container. When movement is detected, the PIR sensor sends a digital high signal to the security microprocessor. This places the system into alert mode where an alarm chirp is sounded for a quarter second, repeating every five while motion is still being detected.

2.1.4 Accelerometer

The accelerometer acts as the main sensory element of the system. It is responsible for detecting if the container is in motion, and is the only means by which the system transitions into the alarm state. The device communicates with the security microprocessor using I^{2}C serial protocol, a simple two wire communication method. The device measures the magnitude of acceleration in the X, Y, and Z axes. If the value measured passes a certain threshold, the system will perceive this as an attempted theft and trigger the alarm[2].

The accelerometer is not rated for the 5V that we are using to power most of the other components, so we created a resistor network to drop its supply voltage to 2.5V. We also added two 4.7kΩ resistors connected from input power to the serial data (SDA) and serial clock (SCL) pins.These resistors act as external pull-up resistors to ensure proper function of the accelerometer. Figure 2.1.4 shows the accelerometer circuit schematic.

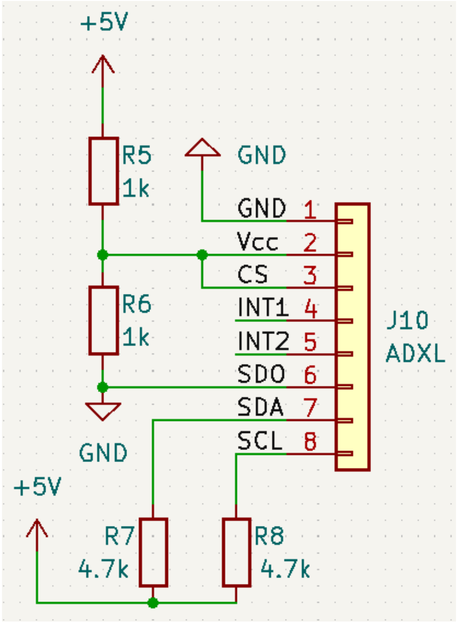


Figure 2.1.4 Accelerometer Schematic

2.2 Security Control Unit

2.2.1 Security Microcontroller

An ATmega48A microcontroller oversees all digital I/O that occurs within the security circuit. It receives input from the security devices while also providing output to status LEDs as well as the transistors for the latch and alarm.

2.2.2 Status LEDs

We use three LEDs in order to provide visual feedback to the operator on the status of the device. Power is indicated by the green LED. Armed status is indicated by the red LED. The blue LED indicates that the data microcontroller is connected to the phone app. Figure 2.2.2 shows how the lights are arranged on the front of the container.

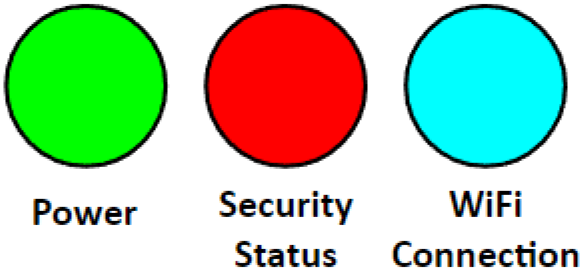


Figure 2.2.2: Status LEDs Display

2.3 Power Supply

2.3.1 Lithium ion cells

Three lithium ion cells act as the power source for the container. Due to their rechargeability and the power density characteristics, these were the optimal choice to power the system. With a nominal voltage of 3.7V per cell, the total nominal system voltage is 11.1V when we connect three cells in series.

Each cell has a 2600 mAh capacity. Connecting the cells in series does not provide any extension to battery life, but if we were to connect three more cells in parallel we would essentially double the battery life. Through an overnight test, we found that this capacity is inadequate to accomplish our high level requirements and only allows for a maximum runtime of nine hours. The results of this rest are shown in figure 2.3.1.1. Clearly, we would need to add more cells in parallel if we wish to achieve our requirement of a 12 hour runtime. Figure 2.3.1.2 shows how this new battery connection would theoretically work.

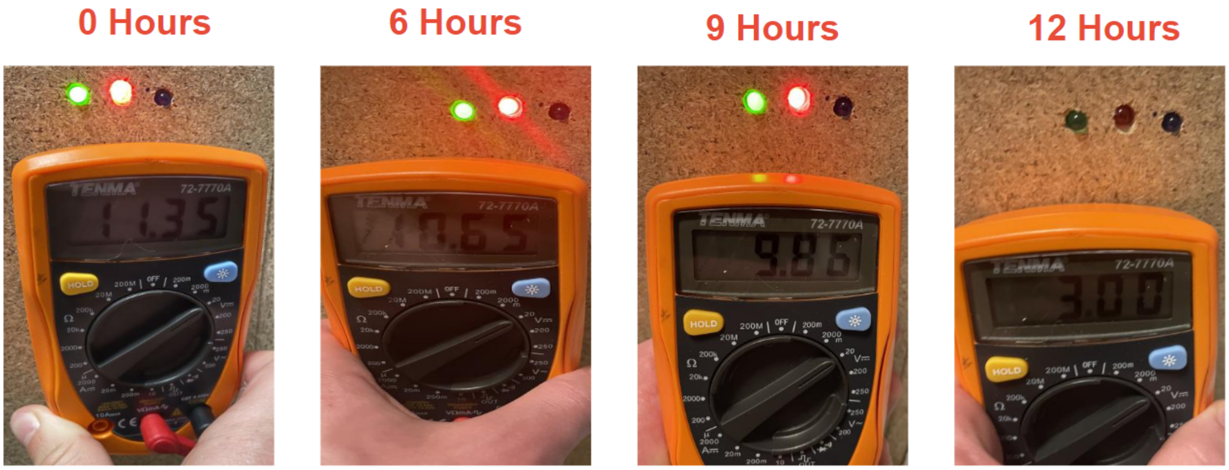


Figure 2.3.1.1: Overnight Battery Life Test

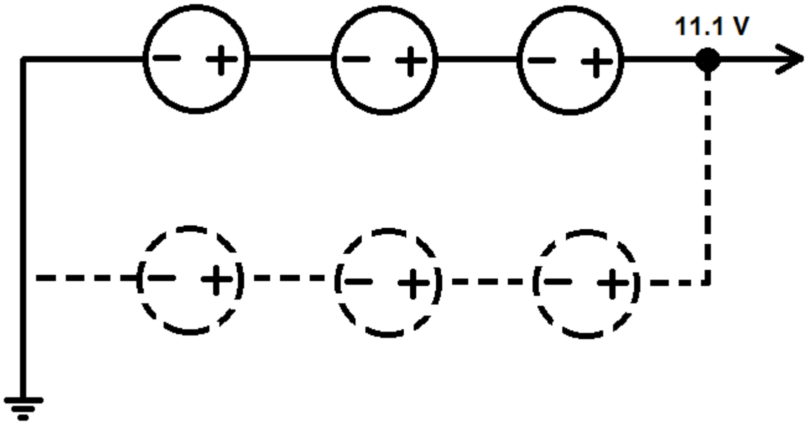


Figure 2.3.1.2: New Battery Schematic

2.3.2 Voltage Regulator

To ensure proper voltage supply to devices within the security circuit, we needed to include a 5V voltage regulator with the 11.1V battery network. The regulator has a max current output of 1.5A, which is not reached by our system even with power running to all devices simultaneously. With the current draws of all devices connected to the regulator (data taken from device data sheets), the max current output is still a magnitude of ten below the maximum rated threshold for our regulator.

$$ATmega + 3 \times PIR\,sensor + ADXL345 + 3 \times LEDs = Regulator\,output\,current$$
$$0.2mA + 3 \times 3mA + 40\mu A + 30mA + 3 \times 30mA = 100\,mA$$

2.4 Data Subsystem

2.4.1 Data Microcontroller

Remote communication and digital I/O through the phone app is controlled by an ESP32 module. The current design utilizes WiFi in order to send and receive data wirelessly between the phone app and the container. The ESP32 also connects to our ATmega security MCU at digital I/O pins 3 and 5 in order to remotely open the latch and arm/disarm the security system.

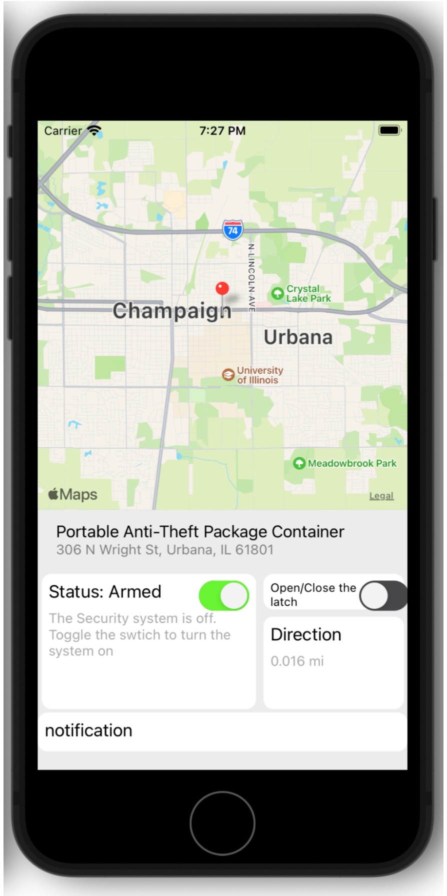
2.4.2 Cloud Data Storage

A cloud Firebase database is hosted on Google Cloud Service. This database stores some critical data including status of the security system, status of the electronic latch, and notification history of the application.

2.5 Phone App

2.5.1 User Interface

The user interface displays the system status, latch status, location of the container, distance to the container, and notification history. In addition, users can change the status of the security system and latch by toggling switches on the application. The phone app can receive alert messages when the container is in alert status. Figure 2.5.1 shows what our app UI will look like on a phone screen. While the map is mostly meaningless with the GPS tracker, it will still show the dropoff location of the container in its current application.



Portable Anti-Theft Package Container
306 N Wright St, Urbana, IL 61801

Status: Armed

The Security system is off. Toggle the swtich to turn the system on

Open/Close the latch

Direction

0.016 mi

notification

Figure 2.5.1: Phone App User Interface

2.5.2 App Coding

The app is coded by javascript using React Native framework. The app can be used on both IOS and Android systems. A NodeJS cloud server is hosted on the Google Cloud Service to process HTTP requests from the phone app and data microcontroller. The cloud server also sends notifications to the phone App.

3 Requirements and Verifications

3.1 Power System

For the power system, the desired battery output is 11.1 ± 0.2V (around 3.7V per cell), and the voltage regulator's output voltage is 5V ± 0.5V. Figure 3.1 shows the oscilloscope readings of both outputs. Both readings fall within our desired range. The voltage output of the regulator remains in this range as the battery voltage drops until the battery voltage drops below 9V. As shown in figure 2.3.1.1, this value is reached somewhere between 9 and 12 hours after activation, with the true time likely being closer to the 9 hour range considering time when the alarm is playing or the latch is open. If we add more batteries in parallel as we discussed, we can essentially double the battery life, which would allow us to meet our 12 hour requirement.

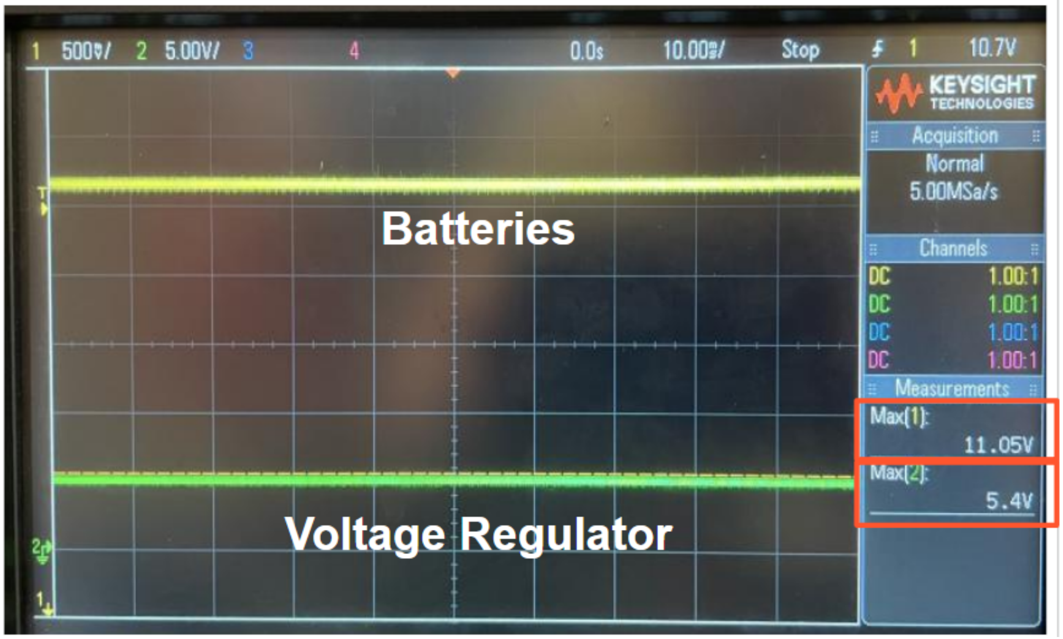


Figure 3.1: Oscilloscope Voltage Measurements

3.2 PIR Sensors

To ensure that the PIR sensors are outputting a digital high signal when motion is detected, we used an oscilloscope to the voltage from the pin to ground, with the results shown in figures 3.2.1 and 3.2.2. In the measurements, we can clearly see a near zero output when the PIR sensor is not triggered, and a 5V high output when it is.

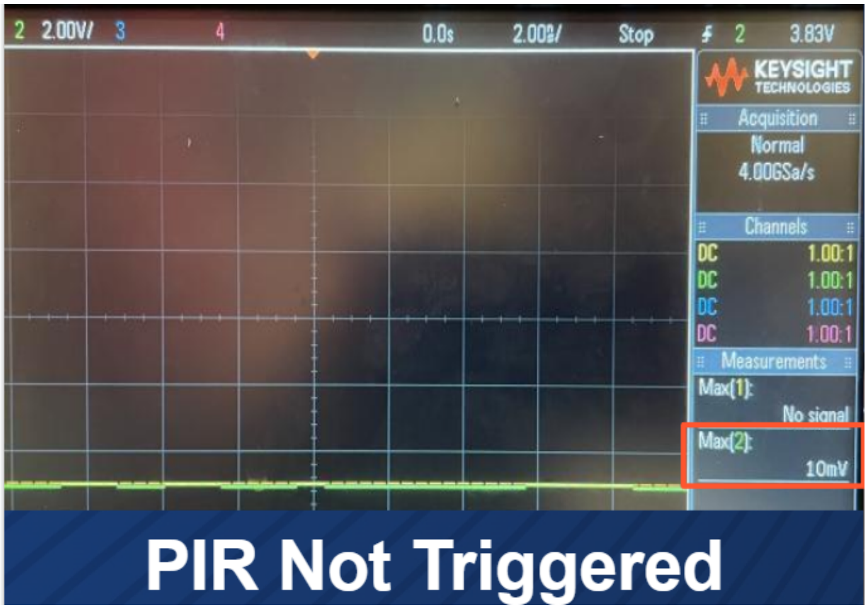


Figure 3.2.1: Oscilloscope Measurement of PIR Output Low

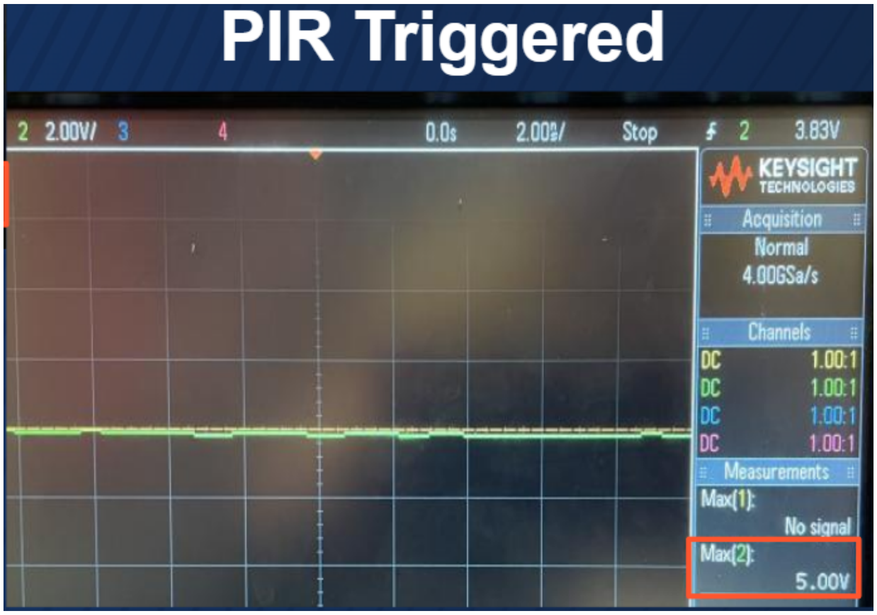


Figure 3.2.2: Oscilloscope Measurement of PIR Output High

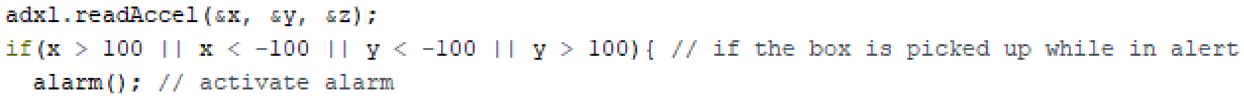
3.3 Status LEDs

Verifying the status LEDs is simply done through a visual process. While the system is powered, the green LED must remain on. The red LED must remain on while the system is armed and turn off when the system is disarmed. While the app is connected to the data microcontroller, the blue LED will remain on. Simply put, these LEDs are meant to act as verifications for the microprocessor functionality and state flow order.

3.4 Accelerometer

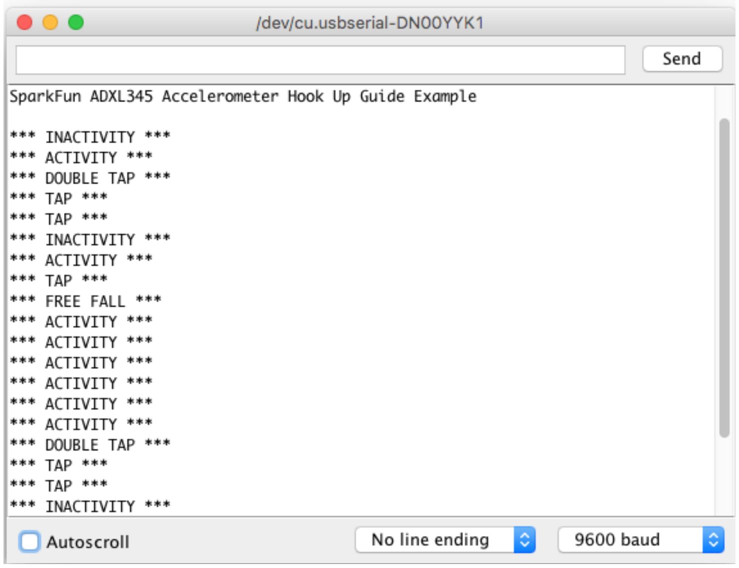
The accelerometer verification is performed with an auditory test. Should the box be moved fast enough, the user will hear the alarm activate. A successful verification indicates that the accelerometer has read the acceleration values from its memory and passed them to the security microcontroller for comparison in the code. Figure 3.4.1 shows the Arduino code snippet that calls on the accelerometer to read from memory and write these values to variables that are compared against an alarm threshold.

Verification failure indicates that either the accelerometer is connected improperly or the alarm is not functioning properly. Should the alarm function correctly in the alert state, but not in the alarm state, direct verification of the accelerometer is performed using Sparkfun's ADXL345 Library and Example Code[3]. If the accelerometer is functioning correctly, activation signals like those shown in figure 3.4.2 will appear when the accelerometer is moved.



```
adxl.readAccel(&x, &y, &z);
if(x > 100 || x < -100 || y < -100 || y > 100){ // if the box is picked up while in alert
  alarm(); // activate alarm
```

Figure 3.4.1: Accelerometer Arduino Code



```
SparkFun ADXL345 Accelerometer Hook Up Guide Example

*** INACTIVITY ***
*** ACTIVITY ***
*** DOUBLE TAP ***
*** TAP ***
*** TAP ***
*** INACTIVITY ***
*** ACTIVITY ***
*** TAP ***
*** FREE FALL ***
*** ACTIVITY ***
*** ACTIVITY ***
*** ACTIVITY ***
*** ACTIVITY ***
*** ACTIVITY ***
*** ACTIVITY ***
*** DOUBLE TAP ***
*** TAP ***
*** TAP ***
*** INACTIVITY ***
```

Figure 3.4.2: Accelerometer Output Signals

3.5 Alarm Horn

The operation of the alarm horn is verified using two auditory tests and a stopwatch. Verification tests for both the PIR sensors and accelerometer should be performed before this test, as this verification directly relies on the proper function of the mentioned devices.

The alert test is performed by triggering the PIR sensors. Should the green LED on the PIR sensors light up, the alarm will play a warning chirp for roughly one quarter of a second. The alarm will continue playing a warning chirp every five seconds as long as a PIR sensor detects motion in the surrounding area.

The alarm state test is performed by quickly picking up the container. The alarm state will be verified by the alarm playing for five seconds before turning off. Any further acceleration after this five second period will cause the alarm to once again play for a five second interval.

3.6 Phone App

Verification is achieved through the electronic latch and the red and blue status LEDs. The blue status LED indicates that the data microcontroller has established communication with the phone app and will accept user inputs. When the system is armed, the red LED will remain on. If the red LED turns off after the user disarms the system with the app, then the app is connected properly and is able to update the state flow. When the system is disarmed, the user should also be able to open the latch with the app, which can easily be verified visually.

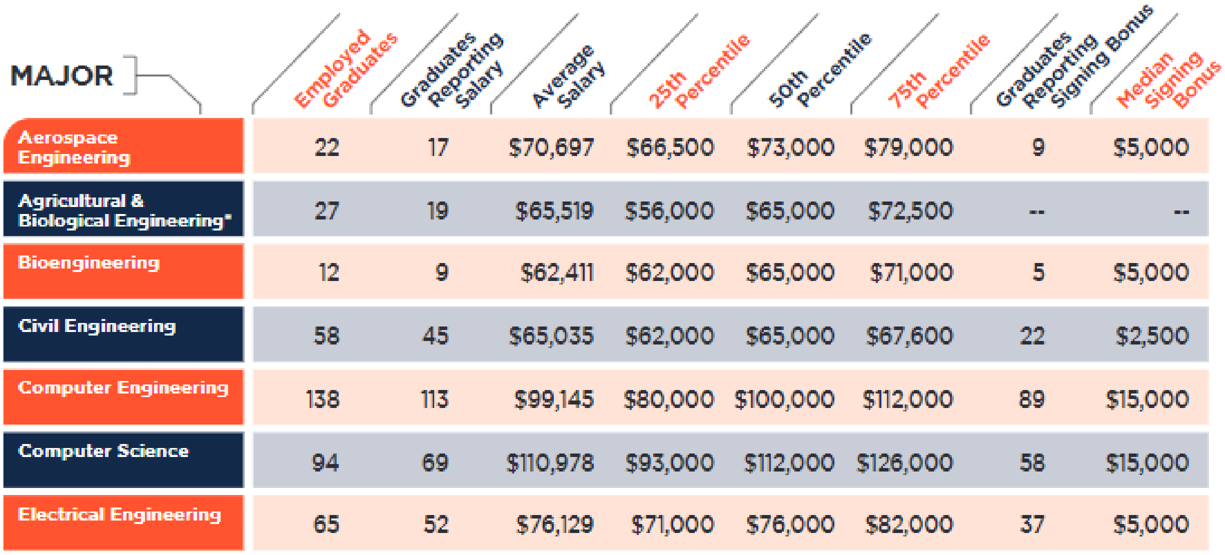
3.7 Electromechanical Latch

Verification for the latch is achieved by using the phone app to unlock the box while the system is disarmed. Functionality is verified by the latch opening and allowing the door to swing open. While the system is armed, verification is achieved by showing the latch will not unlock despite user input from the phone.

4 Costs & Schedule

4.1 Costs

4.1.1 Labor



MAJOR	Employed Graduates	Graduates Reporting Salary	Average Salary	25th Percentile	50th Percentile	75th Percentile	Graduates Reporting Signing Bonus	Median Signing Bonus
Aerospace Engineering	22	17	$70,697	$66,500	$73,000	$79,000	9	$5,000
Agricultural & Biological Engineering*	27	19	$65,519	$56,000	$65,000	$72,500	--	--
Bioengineering	12	9	$62,411	$62,000	$65,000	$71,000	5	$5,000
Civil Engineering	58	45	$65,035	$62,000	$65,000	$67,600	22	$2,500
Computer Engineering	138	113	$99,145	$80,000	$100,000	$112,000	89	$15,000
Computer Science	94	69	$110,978	$93,000	$112,000	$126,000	58	$15,000
Electrical Engineering	65	52	$76,129	$71,000	$76,000	$82,000	37	$5,000

Figure 4.1.1: Salary by Major of UIUC Graduates[4]

Our team is composed of two electrical engineers and one computer engineer. Utilizing Figure 4.1.1, which depicts the salaries of University of Illinois graduates by major, we can calculate the hourly pay rate by dividing the average salary by 1920, or the number of hours in a work year factoring in time off and holidays. Once we have this number, we can multiply by both the number of hours spent on the project and 2.5, which allows us to make a conservative estimate of labor costs. Assuming we worked on the project an average of 8 hours a week over the 16-week course, we have worked for a total of 80 hours. The results of these operations are listed below in table 4.1.1.

Table 4.1.1: Labor Costs

Member	Conor Mueller	Ethan Fransen	Yufei Zhu
Pay Rate	$39.65	$39.65	$51.64
Hours	128	128	128
Multiplier	2.5	2.5	2.5
Cost	$12,688	$12,688	$16,524.80

4.2 Parts

4.2.1 Container

For our purposes in this class, it did not make sense to invest in an expensive container material. Because of this, we simply constructed the box out of wood and screws. In order to purchase all of the materials necessary we spent roughly $50. However, if we were to continue on with this project, we would likely utilize some sort of injection molding with a durable plastic to construct the container. The initial mold would be extremely expensive, but after that we can simply inject ABS plastic to create the container. ABS plastic is quite cheap at an average cost of $0.54/lb[5]. At a density of roughly 64 lbs/ft^3, in order to create one container with a material volume of 0.12 ft^3, which we calculated in our design document, we would spend only $4.15.

4.2.2 Circuit Parts and Components

Table 4.2.2 contains the list of all the parts necessary for our project and their costs. While we spent more than this total as we purchased backup components, this is the theoretical cost per system. It is possible that we did not find or utilize the cheapest version of each component, but this is the price reflected in our system

Table 4.2.2: Component Costs

Part	Quantity	Part Number	Retail Cost
Accelerometer	1	ADXL345	$20.50
Electronic Latch	1	CABINETLOCK11	$10.95
Alarm Speaker	1	CED-ME516AQSW	$7.95
Lithium Ion Battery	6	YXY-ICR18650-A-0001	$6.50
PIR Sensor	3	NCS36000	$17.50
Security Microcontroller	1	ATMEGA48A-PU	$2.56
Data Microcontroller	1	ESP32	$10.00
Red LED	1	YSL-R531R3D-D2	$0.45
Green LED	1	YSL-R341K3D-D2	$0.45
Blue LED	1	YSL-R1047B5D-D2	$0.60
PCB	1	-	$10.00
		Total Cost	$154.96

4.2 Schedule

Week	Date	Conor	Yufei	Ethan
1	1/18 1/23	Post initial project idea	Post initial project idea	Post initial project idea
2	1/24 1/30	Lab safety training CAD assignment	Lab safety training CAD assignment	Lab safety training CAD assignment
3	1/31 2/6	Work on RFA	Work on RFA	Work on RFA
4	2/7 2/13	Work on project proposal	Work on project proposal	Work on project proposal Meet with machine shop
5	2/14 2/20	Work on design document	Work on design document	Work on design document
6	2/21 2/27	Design PCB Soldering assignment	Design the functionality and UI for the phone app Soldering assignment	Design the physical container Soldering assignment
7	2/28 3/6	Update PCB and place order	Purchase Wi-Fi microcontroller Finalize app design	Finalize component order
8	3/7 3/13	Test PCB operation Teamwork evaluation	Code app UI Teamwork evaluation	Design microcontroller connections Teamwork evaluation
9	3/14 3/20	SPRING BREAK Update PCB with revisions	SPRING BREAK Code app functionality	SPRING BREAK Assemble exterior casing
10	3/21 3/27	Finalize PCB design	Set up communications between circuitry and phone app via WiFi	Order any components still needed for circuit
11	3/28 4/3	Order updated PCB Assemble final circuit Individual Report	Ensure functionality of app communications Individual Report	Test all components Set sensor thresholds Individual Report
12	4/4 4/10	Integrate circuitry into container	Prepare demo objectives	Integrate circuitry into container
13	4/11 4/17	Make corrections and prepare for mock demo	Make corrections and prepare for mock demo	Make corrections and prepare for mock demo
14	4/18 4/24	Prepare for demo Work on presentation	Prepare for demo Work on presentation	Prepare for demo Work on presentation
15	4/25 5/1	Finish presentation Work on final paper	Finish presentation Work on final paper	Finish presentation Work on final paper
16	5/2 5/9	Get an A+	Get an A+	Get an A+

5 Conclusions

5.1 Accomplishments

We are very pleased with the outcome of our project as we were able to ensure its functionality in almost every regard. All of our subsystems worked as we needed them too, and the project concept has shown to be an effective solution to the issue of package theft. Our power supply was regulated appropriately, our sensors provided the appropriate signals to the microcontroller, our outputs functioned as desired, and we were able to fully integrate system control through the phone app. The specific requirements for each subsystem can be seen in the table in appendix a.

5.2 Uncertainties

There was only one major uncertainty with our project, and that was the duration of battery life. While the system has quite low power draw when in the armed state, which it spends approximately 95% of its time in, when we tested the duration of 3 batteries in series the system only managed to last about 9 hours. Clearly, our predictions for the power draw of the system were a bit low. This is likely due to focusing exclusively on the major components and not on internal devices like resistors and capacitors.

5.3 Ethical considerations

We all made sure to review the IEEE code of ethics before designing our project and believe that we took appropriate steps to mitigate ethical concerns. Initially, we were concerned for people’s privacy as the original design included a camera that would photograph people near the package. Ultimately, we decided to remove this element to save power and protect others' privacy. The only major concern in the project still is the lithium ion battery cells, which have the potential to start fires or explode if not handled appropriately. We isolated the batteries from the circuity and from each other in our design, which helps to minimize this risk. Some other minor concerns are the volume of the alarm and range of the sensors. Luckily, both of these metrics are variable, so we can ensure that the alarm is not loud enough to disturb the public whenever it plays a warning chirp and the sensors will not trigger the alarm unnecessarily when in a high-traffic area.

5.4 Future work

Our project has lots of room to improve, and while we currently don’t have plans to continue forward with it, there are lots of things we would love to implement if we did. First would be better container material and tamperproofing. As mentioned in section 4.2.1, we would most likely use an injection molded plastic to create the container, and we would include superior design features to make tampering with the box significantly harder. A well designed mold would also allow us to integrate our circuitry into the container itself, making it essentially impossible for a thief to access. We would also like to improve our battery supply as discussed in section 5.2. Six batteries is quite a few, especially if they have to be replaced daily. For this reason, it makes sense that we should switch to a rechargeable battery pack with a higher battery life. We would also need to create a separate delivery app with additional permissions so delivery drivers are able to arm all of the containers after delivery and know which ones to pick up after the customer has opened them. Finally, while we had to give up on the GPS tracker for our project, we would love to integrate it into the final product. This would require an integrated SIM card so the box can communicate its location with the app even when not connected to wifi, but would be worth the additional cost for final implementation.

References

[1] B. Cost, “210 million packages were stolen from Americans this year: Survey,” New York Post, 29-Nov-2021. [Online]. Available: https://nypost.com/2021/11/29/210-million-packages-were-stolen-this-year-survey/. [Accessed: 03-May-2022].

[2] Analog Devices, “3-Axis, ±2 g/±4 g/±8 g/±16 g Digital Accelerometer,” ADXL345 Datasheet. [Online]. Available: https://www.sparkfun.com/datasheets/Sensors/Accelerometer/ADXL345.pdf. [Accessed: 03-May-2022]

[3] “Sparkfun ADXL345 Hookup Guide and Arduino Code” Sparkfun. [Online]. Available: https://learn.sparkfun.com/tutorials/adxl345-hookup-guide. [Accessed: 03-May-2022]

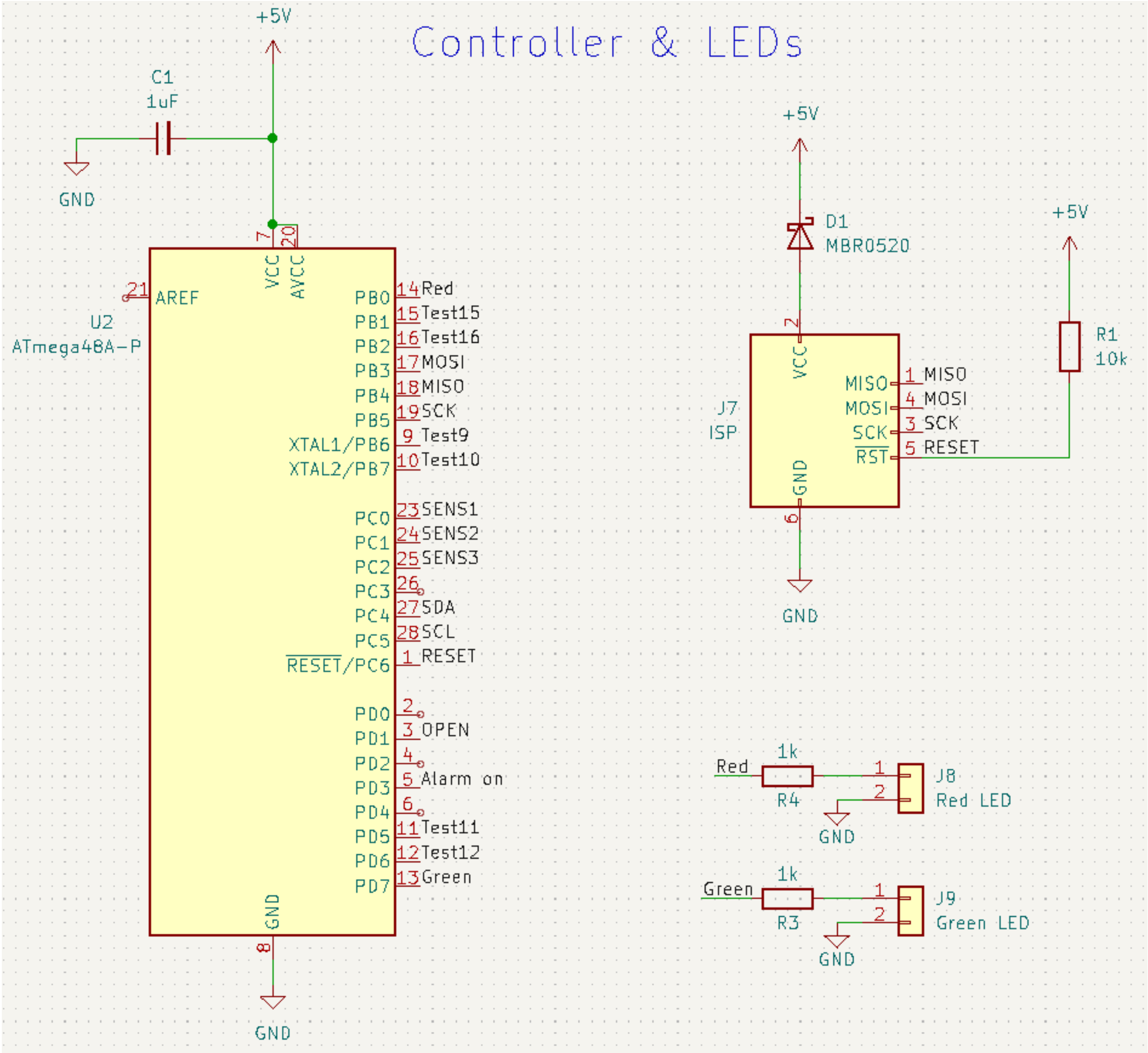
[4] “Illini Success Report,” Box. [Online]. Available: https://uofi.app.box.com/s /1t8xj69117lrsqm7753ujnrg8yyrtcwn [Accessed: 03-May-2022].

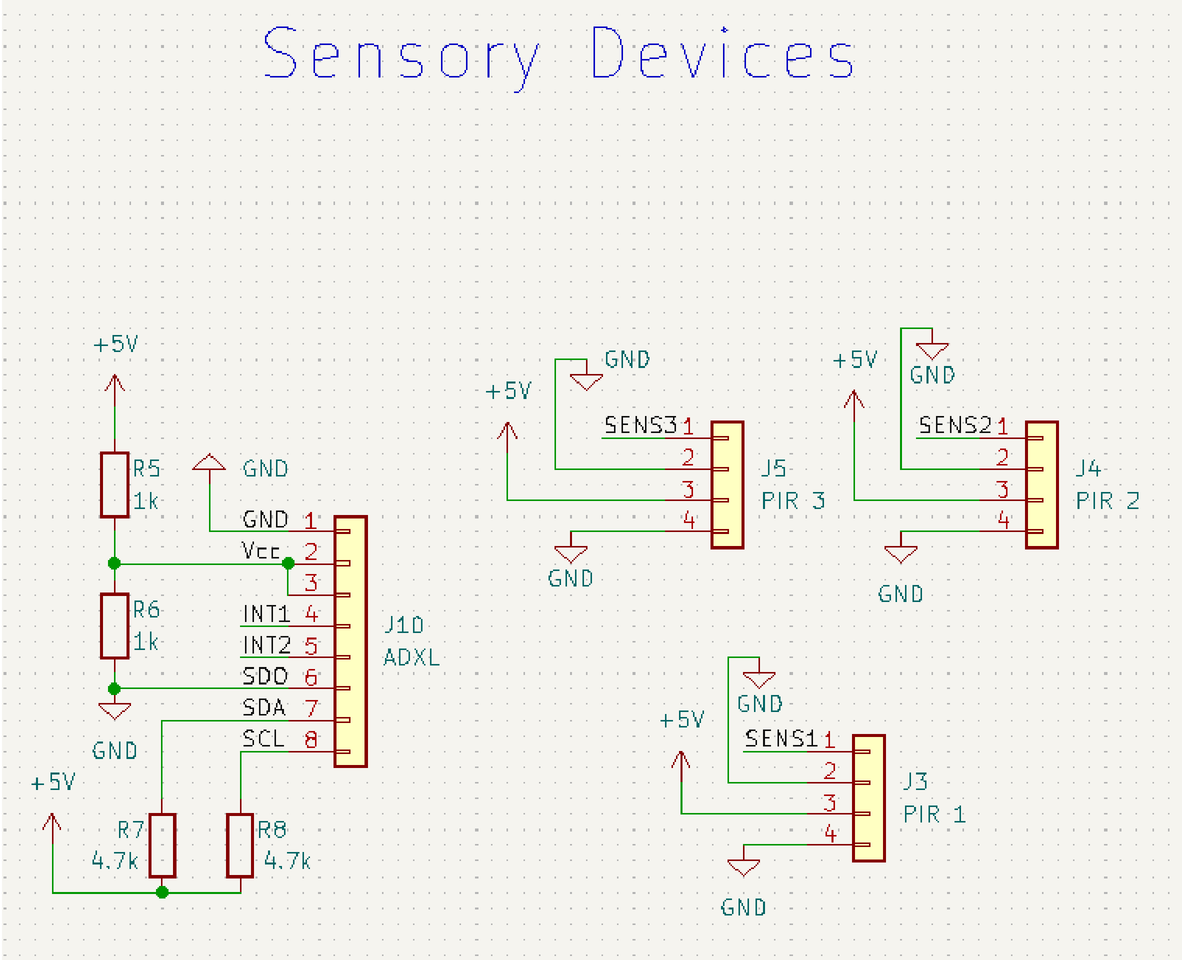
[5] T. Rogers, “Everything you need to know about ABS plastic,” Everything You Need to Know About ABS Plastic. [Online]. Available: https://www.creativemechanisms.com/blog/everything-you-need-to-know-about-abs-plastic. [Accessed: 03-May-2022].

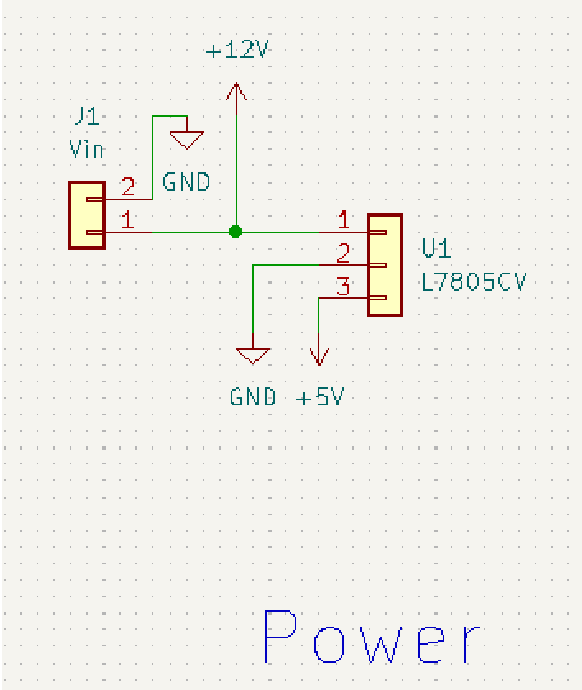
Appendix A Requirements and Verification Table

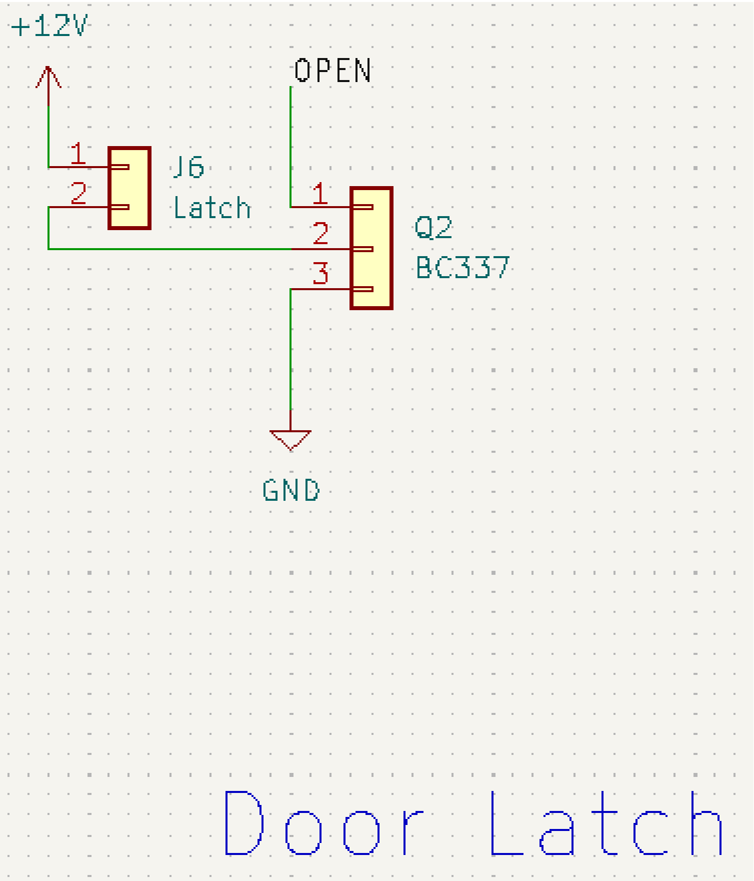
Subsystem	Requirements	Verified
Power Supply	Measure voltage output of batteries and ensure 11.1 ± 0.2 V Measure voltage output of five volt regulator and ensure 5.0 ± 0.5 V	✔
Status LEDs	Green LED turns on when system is powered Red LED turns on when system state is **Armed**, **Alert**, or **Alarm** Blue LED turns on when wireless connection is present	✔
PIR Sensors	From **Armed**, trigger PIR sensors and show update to **Alert** From **Alert**, trigger PIR sensors and show state remains as **Alert** From **Alert**, do not trigger PIR sensors and show update to **Armed**	✔
Accelerometer	From **Armed**, trigger accelerometer and show update to **Alarm** From **Alert**, trigger accelerometer and show update to **Alarm** From **Alarm**, do not trigger accelerometer and show update to **Armed**	✔
Alarm Horn	When in **Alert**, show that warning chirp is played every 5 seconds When in **Alarm**, show that blaring alarm is played for 10 seconds	✔
Phone App	Show that user input will update state to **Armed** from **Disarmed** Show that user input will open latch when in **Disarmed** Show that user input will update state to **Disarmed** from **Armed**	✔
Electronic Door Latch	When not in **Disarmed**, show that latch will not open despite user input When in **Disarmed**, show that latch will open with user input	✔

Appendix B Circuit Schematics

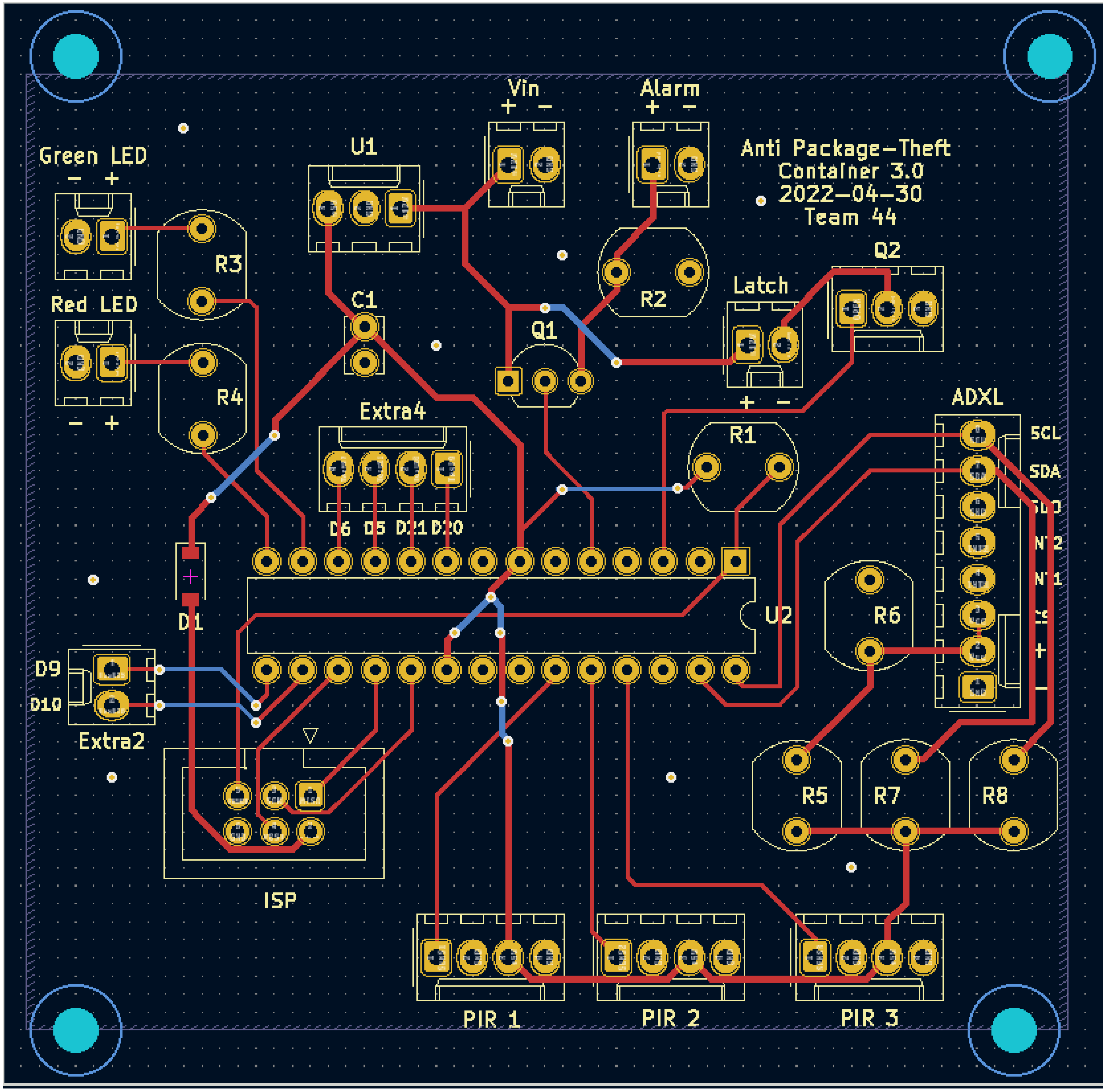



Sensory Devices
+5V
R5
1k
R6
1k
GND
GND 1
Vcc 2
3
INT1 4
INT2 5
SDO 6
SDA 7
SCL 8
J10
ADXL
GND
+5V
R7
4.7k
R8
4.7k
+5V
GND
SENS3 1
2
3
4
J5
PIR 3
GND
+5V
GND
SENS2 1
2
3
4
J4
PIR 2
GND
GND
+5V
SENS1 1
2
3
4
J3
PIR 1
GND


+12V
J1
Vin
2
1
GND
1
2
3
U1
L7805CV
GND
+5V
Power


+12V
OPEN
1
2
J6
Latch
1
2
3
Q2
BC337
GND
Door Latch

Appendix C Printed Circuit Board


Vin
+ −
Alarm
+ −
Anti Package-Theft
Container 3.0
2022-04-30
Team 44
Green LED
− +
U1
R3
Red LED
C1
R2
Latch
Q2
Q1
R4
− +
+ −
Extra4
R1
ADXL
SCL
SDA
SDO
NT2
NT1
CS
+
D6
D5
D21
D20
D1
U2
R6
D9
D10
Extra2
ISP
R5
R7
R8
PIR 1
PIR 2
PIR 3