Modularized Electronic Locker Project Proposal

ECE 445

Team #61

Joshua Nolan(jtnolan2), Jianhao Pu(jpu3), John Davis(johnhd4)

TA: Ali Kourani

Spring 2021

Table of Content

1. Introduction

1.1. Objective

Package theft is a common problem both in the US and abroad. According to a recent survey, 43% of American consumers claim they have had a package stolen in the past year[1]. As ecommerce becomes more prevalent, porch piracy will only become more prevalent. In 2020, consumers spent $862.12 billion online. This represents a 44% increase from the previous year[2]. While online shopping due to the pandemic certainly contributed to this number, our reliance on online merchants is only expected to increase over time. The objective of our project is to create a system of modular electronic lockers that can be used to protect deliveries to homes, apartments, etc. These lockers will provide a safe haven for a wide range of deliveries (Amazon, UPS, Uber Eats, etc.) as well as provide package delivery notification through a network connection. While similar solutions like Amazon Hub do exist, these systems are large, expensive, and not suitable for individual homeowners or small apartment buildings. The modular design of our electronic lockers will be able to provide affordable delivery protection for a one person household or an entire apartment building.

1.2. Background

Students living off campus without a packaging station are affected by stolen packages all the time [3]. As a result of privacy concerns and inconsistent deployment, public cameras in Champaign and around the world cannot always be relied upon. Therefore, it can be very difficult for victims to gather evidence for a police report. Most of the time, the value of stolen items is small and they are usually compensated by the sellers (Amazon and Apple are very understanding). However, not all deliveries are insured [4] and many people are suffering from stolen food deliveries during the COVID-19 crisis [5]. We need an effective solution that can protect deliveries from all vendors. The smart lockers in the market do not address expandability which makes it difficult for locker owners to increase locker capacity. We need a modular design of lockers to address such demand.

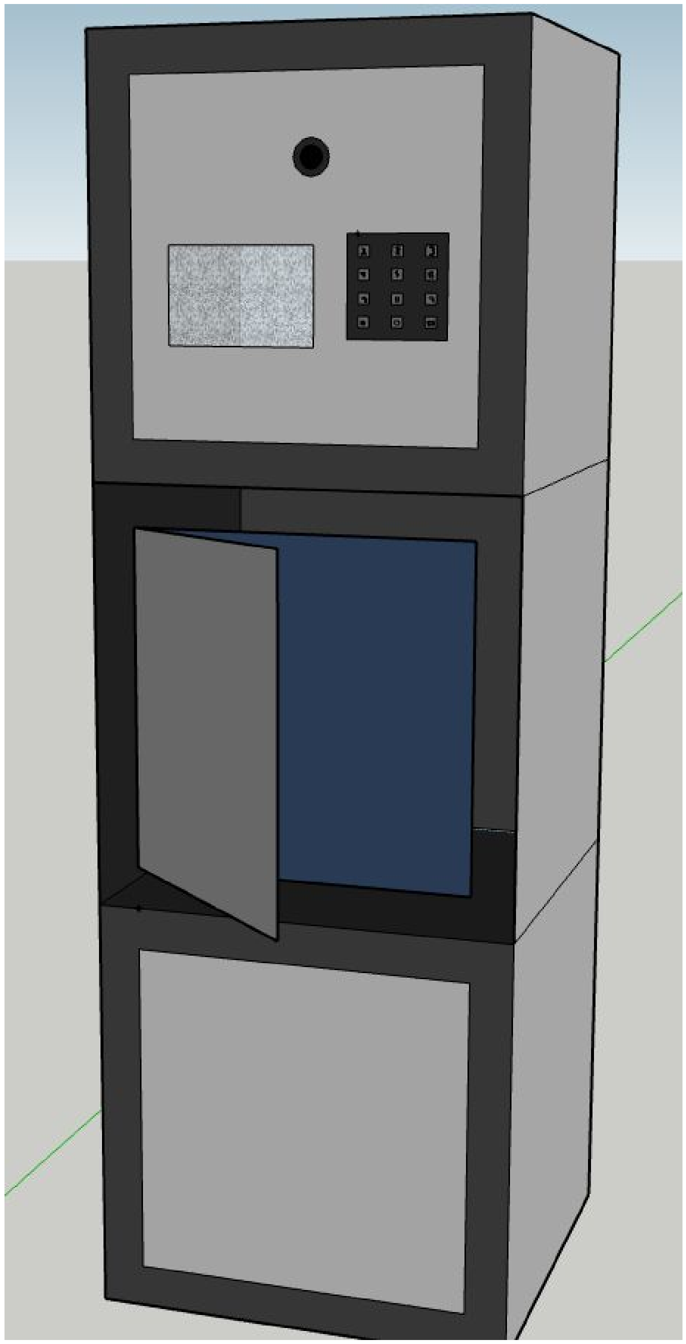

Fig. 1: Concept design of modular locker boxes

1.3. High-level Requirements

1.3.1. Connectivity

Must be able to sync pickup and retrieve password databases from cloud service every five minutes at a minimum. Package notifications and pictures taken must also be pushed to the cloud within five minutes.

1.3.2. Modularity

Modules must be compatible with each other using the same data bus and power bus. Owners simply attach modules to each other using the exposed connectors on the outside of the locker units. Our final solution must be able to support at least 3 modules in several different layouts.

1.3.3. Security

Package owners are the only ones who can open the locker in which their package resides and delivery services can only open the locker designated for that delivery.

2. Design

Our design consists of four distinct modules: a control unit, power supply, cloud server, and locker module. The control unit contains a touchscreen LED display and keypad for user input, a camera, ROM storage, a PIR motion sensor, and a Raspberry Pi. This unit is responsible for taking in user input, controlling the locker modules, and storing user data. The power supply module is responsible for supplying 12V within 3A to the system. Locker modules ensure package security and provide modularity to support numerous applications. Lastly, the cloud server module is responsible for transferring user data to the cloud as well as retrieving password information from the cloud periodically.

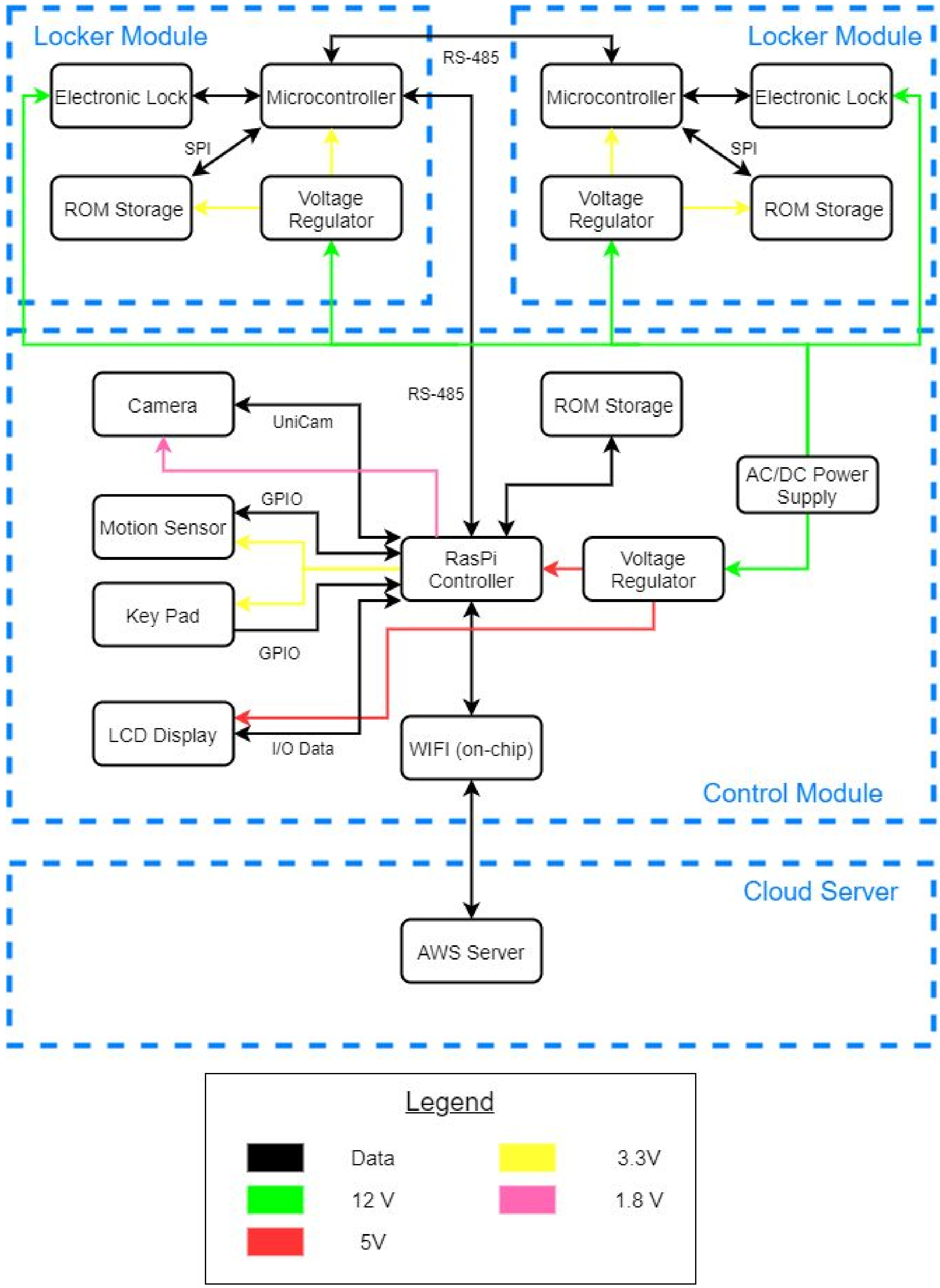

Fig. 2: Block diagram

2.1. Power Supply

The power supply will connect to a standard wall outlet to supply 12 V power within 2.5A. An AC/DC converter will be needed to supply the power to the PCBs. In the event of a critical power failure the circuit protection located on the controller PCBs will break the connection to the device.

2.1.1. Voltage Regulation

Each PCB will be receiving 12 V supply from the AC/DC converter. However, the operating voltage for ESP32 on board should be at between 2.2V and 3.6V, and the operating voltage for Raspberry Pi 4 (RPI4) should be at 5V ± 5%. The components within the Control Module, such as LCD display and RS485 drivers, also operate at these two voltages. To step down the voltage we will use voltage converters on each board for use of necessary components.

Requirement	Verification
1. Raspberry Pi 4 can run steadily for at least 15 minutes with all of its peripherals on.	1. A. Raspberry Pi can steadily run a stability test program such as GtkStressTesting for at least 15 minutes. B. Monitor can display the camera's video stream while running the stability test.

2.2. Control Module

A Raspberry Pi will work as a master on the communication bus to collect information from all locker modules, log their status and send an unlock signal to the right locker module whenever it receives a correct pickup code from the touchscreen. The Raspberry Pi will additionally interface I/O with other components such as the keypad to facilitate the operation of the whole device.

2.2.1. Raspberry Pi Main Controller

This processor is the master brain of the entire device. It is responsible for delivering lock and unlock signals to every locker module. This Raspberry Pi is also responsible for saving photos in ROM storage, sending user data to the cloud through Wifi, and handling I/O to/from the LCD display and number pad. The camera is also controlled by this device and all photo data is routed through this controller to ROM Storage.

Requirement	Verification
1. Can retrieve the user data table from the server in under 5 minutes. 2. Can send control messages over the data bus to notify the according locker module to unlock its electric lock using RS485 signal standard. 3. Can match the user-input code with valid pick-up and drop-off codes. 4. Can receive input from the touchscreen and display instructions to users.	1. A. Make a change in the cloud database. B. Time how long it takes for this change to be detected. 2. A slave device on the databus can receive a correct message in RS485 signal standard from RPI4. 3. Can recognize input from the keypad and display it on screen. 4. Can react to the touch action from the touchscreen.

2.2.2. ROM Storage

Requirement	Verification
1. Can store at least twenty 720p images. 2. Can store the user table data which includes pickup code, drop-off code and user name after it is pulled from the server by Raspberry Pi.	1. Display a sample entry of the user data table or the whole table itself. 2. Display an image stored in the ROM.

2.2.3. Camera

The camera is a security measure to protect the property of the user and to document all locker activity. Whenever the passive infrared sensor detects motion or whenever the locker is opened, an image is captured and stored in ROM.

Requirement	Verification
1. Must be able to take 720p photos whenever a locker is opened and transfer photo data to the microcontroller to be stored on a MicroSD card.	1. A. Take a picture when a person walks close. Check the MicroSD card for a photo. B. Take a picture when a locker module is opened. Check the MicroSD card for a photo.

2.2.4. LCD Display

The display is required to interface the users of the device to the hardware which the user desires to operate. The panel must convey useful information comprehensively as well as respond appropriately to the input that the user requested.

Requirement	Verification
1. Will react to touch input from the user. 2. Able to display images with half a second refresh rate or lower.	1. Respond to touch and display different content. 2. A. Code a program that changes the LCD screen when it is touched. B. Time how long it takes for the screen to change.

2.2.5. Keypad

A 12-key keypad will allow users to input the package code and retrieve their delivery.

Requirement	Verification
1. Signals from all buttons can be transmitted without error.	1. Press the 12 keys on the pad to ensure and check whether the connector has the correct signal output.

2.2.6. PIR Sensor

A passive infa-red sensor will sense whenever someone approaches the system so that the camera can take a picture.

Requirement	Verification
1. The sensor detects when someone walks within five meters of the front of the control module.	1. Walk in front of the sensor and check to see if the signal output is high.

2.3. Locker modules

The locker modules will use a spring loaded electronic lock to open only when it receives an electric signal from a microcontroller. A cheap microprocessor will be in this module to pick up messages addressed to itself from the bus and unlock the electronic lock within its module. The locker modules will also conceal the required wiring to enable modularity to other modules. Each locker module will have exposed pin-like connectors on every side so that they can easily be attached together in multiple orientations, shown in Fig. 3. Lockers will also have latches by which they can be secured together.

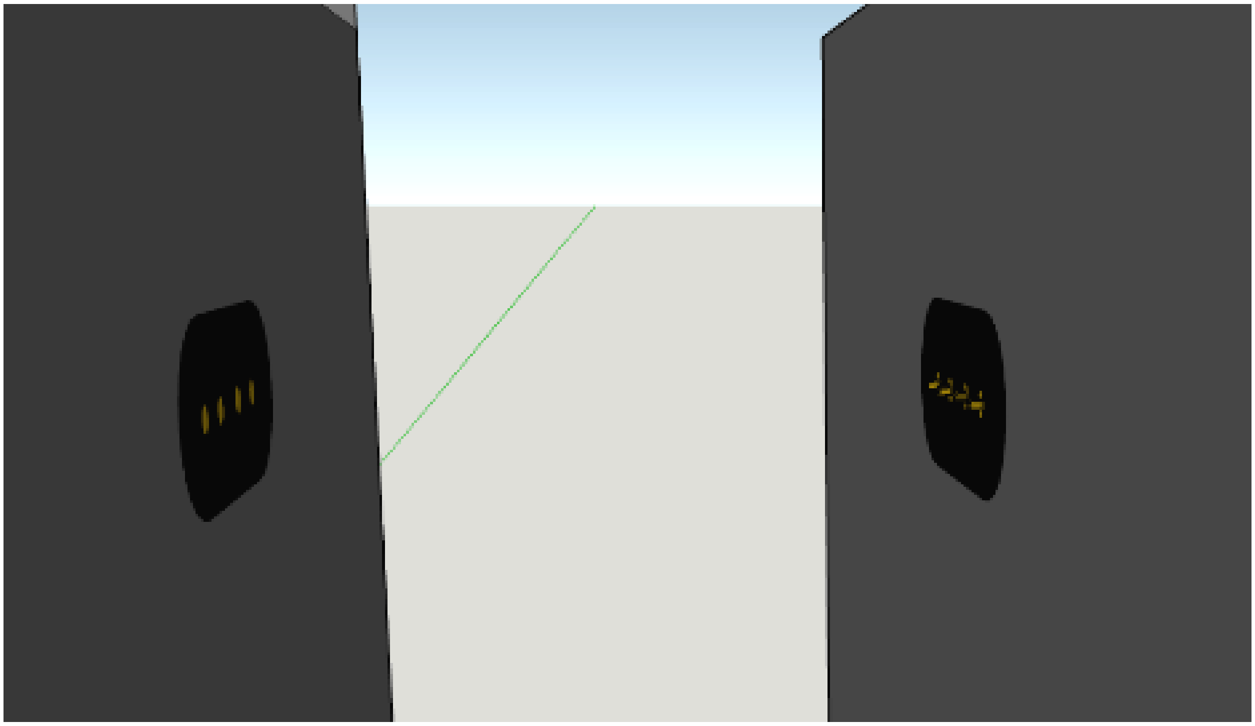

Fig. 3: Example pin connection between locker modules

2.3.1. Microcontroller

The processor component that we will be using on the slave boards will be identical to the master board to save complexity of designing more PCBs. However these boards will only include functionality for opening the lock and communicating with the other boards in the device.

Requirement	Verification
1. Able to send unlock signals to its associated locker. 2. Able to communicate with the Control Unit over the databus in RS485 signal standard.	1. A. Code the slave microcontroller to send an unlock signal to its associated lock B. Verify that the lock opens 2. A. Send an unlock message over the data bus to the slave microcontroller B. Verify that the associated lock opens

2.4. Software

The software for this project will include the hardware level code to transfer data between controllers. This also includes the transfer of data from sensors to be processed by controllers. Finally, software design will include the transfer of data from and to a cloud server hosted on AWS. The flow of this data throughout the system can be seen in Fig. 4 below.

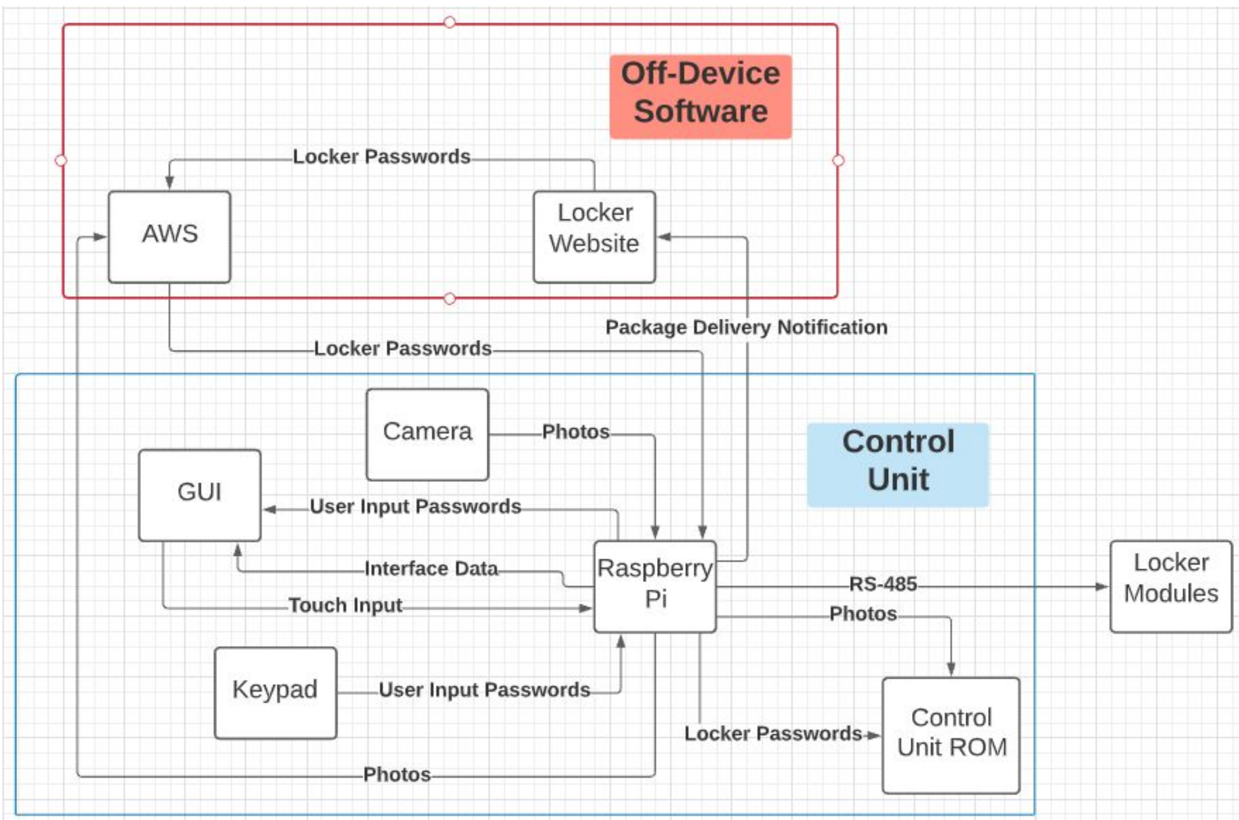

Fig 4: Software Data Flow

2.4.1. Cloud Storage/Database

The cloud database or storage will save a table of deposit/pickup code, package status and also store all pictures taken by the lockers as a security measure.

Requirement	Verification
1. Store locker images for up to two weeks 2. Store user data table	1. A. Upload an image to the cloud through the API the RPI4 will be using. B. Check the storage/database for the new image. 2. A. Change a user pick-up code on the locker website B. Display the user data table from cloud storage/database and verify that the pick-up code has changed.

2.4.2. Web Page Frontend

The cloud service will provide users with a website as a frontend to check package arrival status and update deposit/pickup code.

Requirement	Verification
1. Let users log in with their deposit codes. 2. Let users change their deposit and pickup code once they log in. 3. Let the user check whether or not there are any packages stored in the locker for them.	1. Use the deposit code to log in. 2. A. Change its deposit code and pickup code B. Log back in using the newest deposit code and check the new pickup code. 3. A. Open the locker door using a deposit code B. Verify that the website says there is a package ready for pick-up.

2.4.3. User Interface

The user interface will be based on RPI4, take input from users and provide instruction to use the locker system.

Requirement	Verification
1. Gives users and delivery services clear instructions for deposit and pickup of packages. 2. Secure state machine that does not have undefined behavior.	1. A person without prior experience with this locker system can finish deposit and pickof of a package following the instructions on the display. 2. Try all possible user behavior and the system should function normally.

2.4.4. Data Bus and Device Addressing

The data bus will be using RS485 signal standard for the locker modules and control module to communicate with each other. Each locker module will be assigned its bus address in configuration mode so that the control module can send unlock instruction to specific locker modules.

Requirement	Verification
1. Locker modules can be assigned a distinct address. 2. Locker modules can recognize a message directed to its address.	1. Configure a locker module to an non-default address. 2. A. Send an unlock message on the bus to the lock with the non-default address mentioned above. B. Verify that the locker opens.

2.5. Schematics

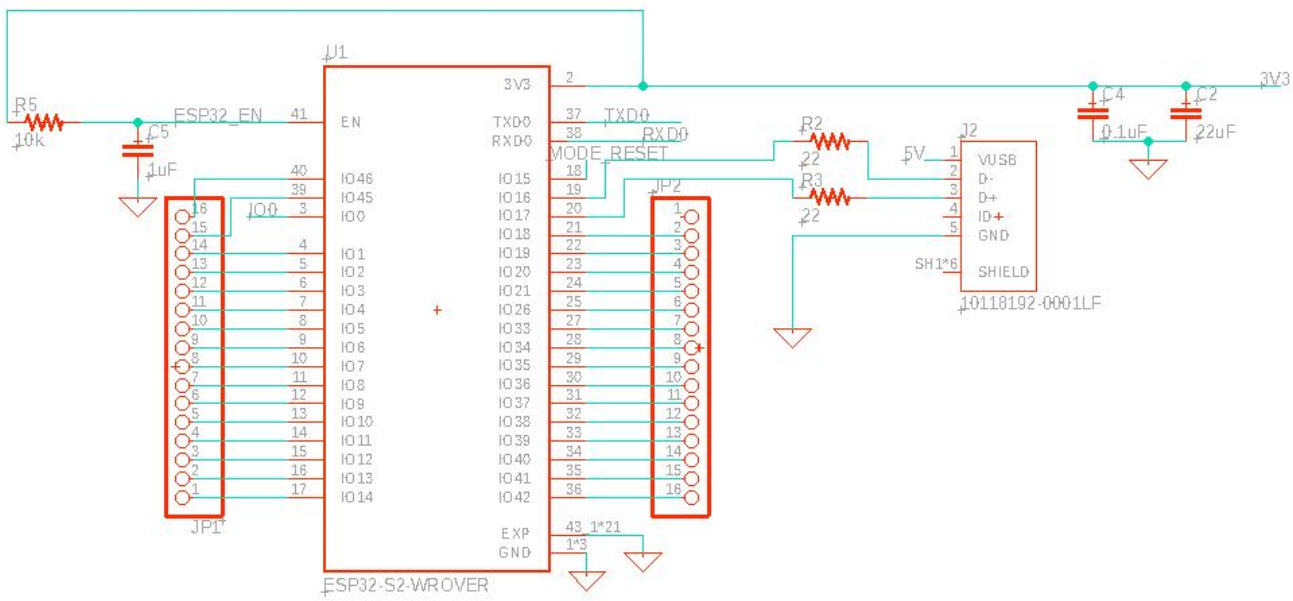

Fig. 5: ESP32 Chip with USB Connector

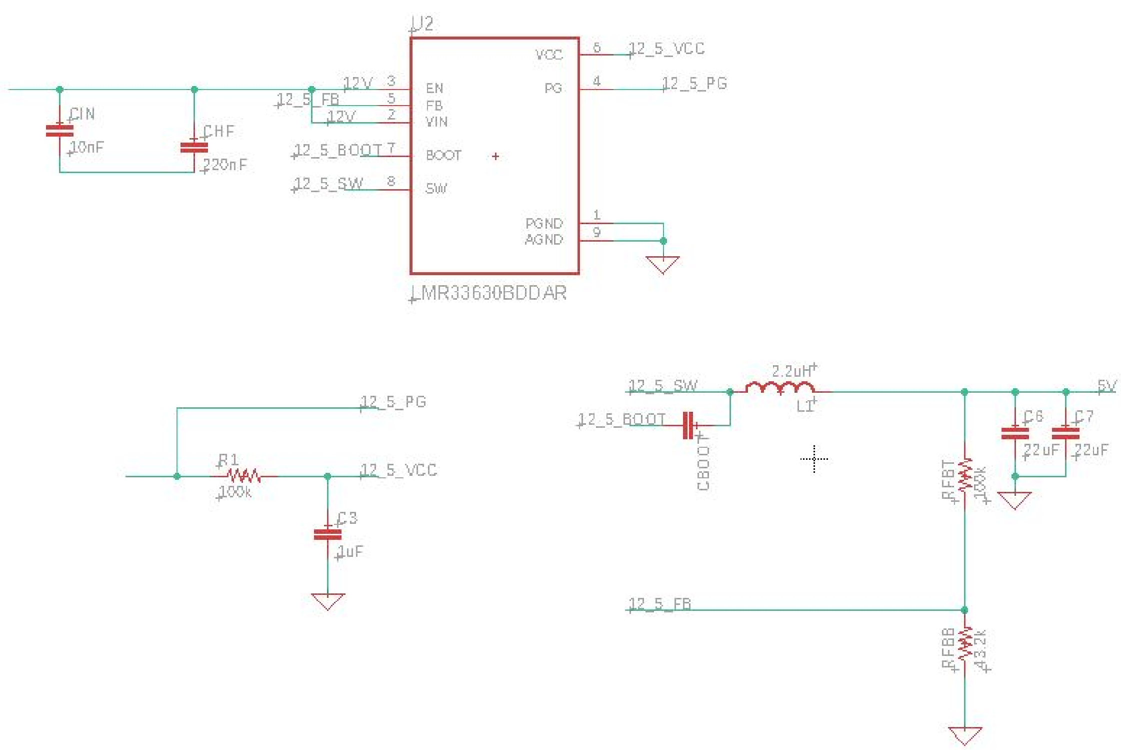

Fig. 6: 12 V to 5 V Voltage Regulation

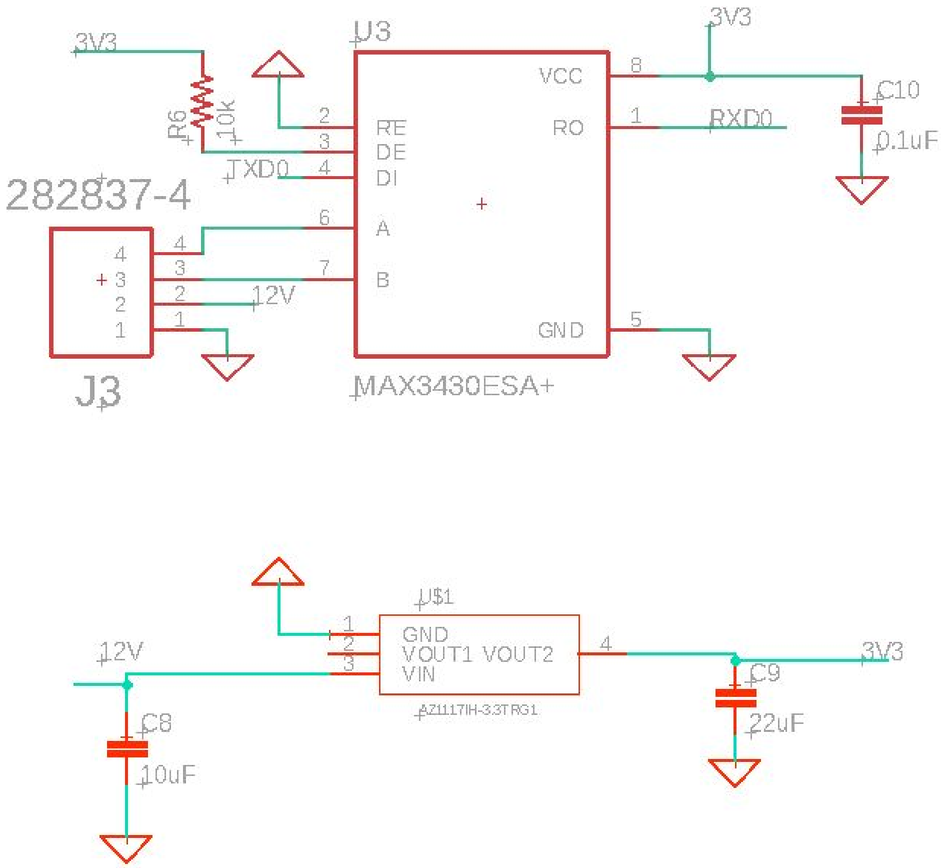

Fig. 7: RS-485 Transceiver Circuit

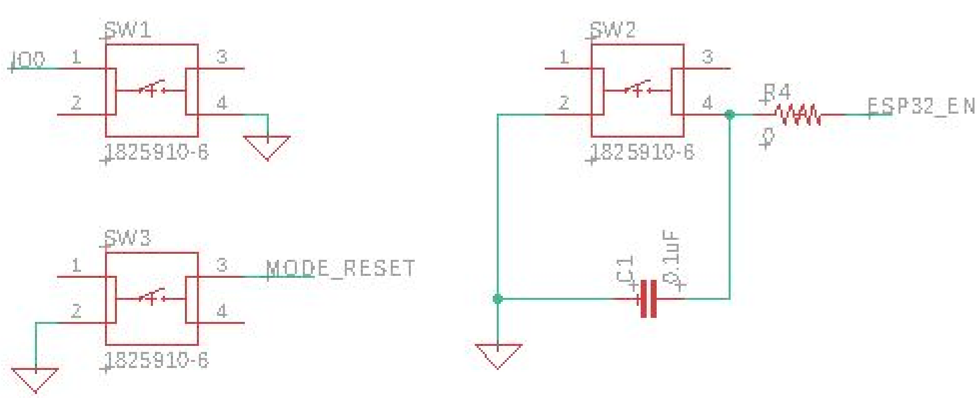

Fig. 8: Buttons to Reset and Flash Program

2.6. Tolerance Analysis

An important tolerance that we have considered is the interference that the communication between microcontrollers experience. The RS485 standard was left intentionally open for designers to implement solutions to power loss and distortion.

RS485 uses two cables which connect the receivers and drivers. However when these cables are parallel the current creates a magnetic field which creates interference with the signal shown below in Fig. 9. We will be using twisted pair cabling when wiring the bus in order to reduce the noise created by magnetic fields.

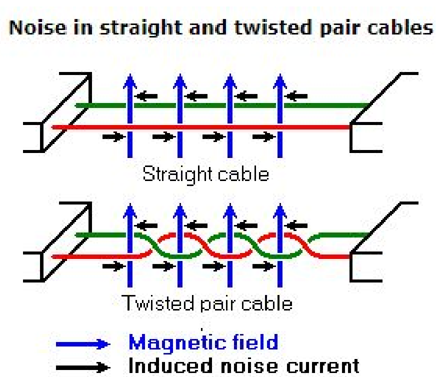

Fig. 9: Magnetic field lines and noise current in the RS485 data line [7]

Another issue in the RS-485 is transmission reflections. The reflection coefficient, Γ describes the amplitude of the initial signal that is reflected back through the transmission line. The TIA/EIA-485 standard [7] [8] specifies a characteristic impedance of 120 Ω, driver impedance of 60 Ω, and 12 kΩ minimum input impedance.

$$\Gamma_1 = \frac{Z_L - Z_0}{Z_L + Z_0} = \frac{12{,}000\Omega - 120\Omega}{12{,}000\Omega + 120\Omega} = 98.0\% \qquad \text{Eq. 1a}$$

$$\Gamma_2 = \Gamma_1 \cdot \frac{Z_L - Z_0}{Z_L + Z_0} = 0.980 \cdot \frac{60\Omega - 120\Omega}{60\Omega + 120\Omega} = \; -32.7\% \qquad \text{Eq. 1b}$$

Using Eq. 1 and Eq. 1b, it is shown that the reflections of the first two reflections create large magnitude reflections. However, we also know that the propagation time of the line is approximated [9] as 5ns/m. We do not expect the bus to exceed 5m in length so we can expect 25ns of propagation time. At approximately 500 Kbps on the transmission line, there is 2000 ns between bits which allows for ample time for the reflection to decay.

At such relatively short transmission lengths we do not expect transmission reflections to cause issues, however if noise does become a problem the most common solution is impedance matching. In particular a parallel configuration, shown in Fig. 10 below, where R_T matches the characteristic impedance of the line.The value R_T should not be greater than 10% larger than the characteristic impedance of the line as outlined in TIA/EIA-485 standard [7]. If other issues arise there are other filtering techniques that are well documented in the TIA/EIA-485 documentation. We will monitor our communications bus using an oscilloscope to assure that our signals fit within specified limitations.

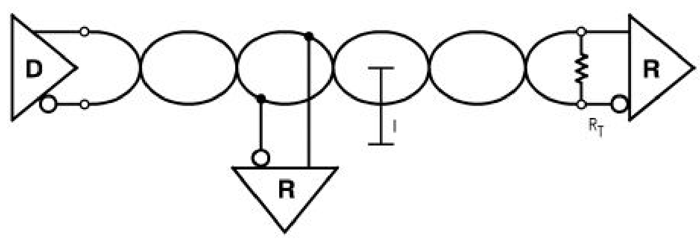

Fig. 10: Parallel Termination Configuration

3. Costs

We estimate the salary of an engineer to be $50/hr to work on this project for 10 hrs per week for 12 weeks. For 3 engineers and an overhead factor of 2.5, we estimate the development costs to be

$$3 \bullet \frac{\$50}{hr} \bullet \frac{10hr}{wk} \bullet 12wk \bullet 2.5 = \$45,000$$

The quoted cost of the construction of the 3 boxes is $150 in the machine shop. The majority of our costs lie in the control module locker and as a commercial product each locker owner would only have to purchase one of these. Each locker module would be much cheaper to purchase than the control module for the entire system.

Part Name	**Quantity**	**Cost**
Microcontroller	2	$2.20
Raspberry Pi	1	$35

12v to 3.3V regulator	3	$1.14
12v to 5.5V regulator	1	$2.35
MicroSD card holder	1	$3.31
Display	1	$17.80
Connector (between boxes)	20	$6.30
Camera	1	$8.19
Touchpad	1	$4.50/s
110V to 12V Power Supply	1	$14.90
PCBs	5	$20.10
PIR Sensor	1	$14.19
Total		$129.98

4. Schedule

Week	Josh	Jack	Jake
3/7/21	Create Touchscreen GUI	Physical Locker Design	Code AWS database
3/14/21	Finish Touchscreen GUI/Code Website	Locker hardware layout	Code Website
3/21/21	Work on communication between AWS, website, and hardware	Get camera to take picture based on PIR sensor output	Retrieve password data from AWS and store on ROM in real time
3/28/21	Finish software communication	Assemble hardware in lockers	Use RS485 to communicate between microcontrollers and open locks
4/4/21	Get proper locker to open when a correct password is input	Store camera images on ROM and periodically push to AWS	Finish RS485 communication
4/11/21	Debug GUI/Software	Debug hardware and sensors	Debug bus and AWS database
4/18/21	Ensure subsystems work together	Ensure subsystems work together	Ensure subsystems work together
4/25/21	Debugging/Stress Testing	Debugging/Stress Testing	Debugging/Stress Testing
5/3/21	Begin Report	Prepare Final Presentation	Prepare Final Presentation

5. Ethics and Safety

5.1. Ethics

This device is directly responsible for the protection of others' property. As such we acknowledge the importance of safety and privacy as outlined in the IEEE Code of Ethics, #1: “To improve the understanding of technology; its appropriate application, and potential consequences” [6]. We aim to uphold our product to standards that will improve the welfare and safety of society.

This type of electronic locker might be exploited by organized crime to exchange illegal goods and cash. In accordance with #4 of the IEEE Code of Ethics, we are committed to avoid unlawful conduct in professional activities [6]. There are multiple solutions to alleviate the risk of unlawful conduct using our lockers. For example, the locker owner can offset the legal liability by enforcing user agreement. Locker owners can also provide authorities with photos taken by the locker camera if they suspect lockers users of illegal behavior.

5.2. Safety

5.2.1. Electrocution

Since all the modules but the power supply is on 12 V, the risk of electrocution is very small. However, we still need to ground the metal casing. The 12V power supply is equipped with multiple protections against overvoltage, overcurrent, short circuit and over temperature.

5.2.2. Vandalism

Locker modules will have brackets so they can be secured together and optionally secured to a wall to prevent theft. Electronic locks will have sufficient strength so that locker doors cannot be pried open by hand.

5.2.3. Privacy

Locker passwords can be reset at any time on an associated locker website. The final product would also have a user agreement that prevents the sharing of any user images as long as their locker is used for legal purposes.

6. References

[1] PracticalEcommerce, 'Porch Piracy Is Growing', 2021. [Online]. Available: https://www.practicalecommerce.com/porch-piracy-is-growing. [Accessed: 2-18-2021]

[2] Digital Commerce 360, US ecommerce grows 44% in 2020, 2021. [Online]. Available: https://www.digitalcommerce360.com/article/us-ecommerce-sales/. [Accessed: 2-18-2021]

[3] The Daily Pensnsylvanian, 'More students have packages stolen as thieves resort to following delivery trucks', 2021. [Online]. Available: https://www.thedp.com/article/2017/04/off-campus-package-theft. [Accessed: 2-18-2021]

[4] WUSA9, 'VERIFY: Who is responsible if a thief steals your packages?', 2019. [Online]. Available: https://www.wusa9.com/article/news/verify/who-is-responsible-if-your-package-is-stolen/65-52b8f478-8aee-4cf4-951b-848f263602f4. [Accessed: 2-18-2021]

[5] BusinessWire, 'Buckle Temporarily Adds Food and Delivery Insurance Coverage to Member Policies at No Additional Cost', 2020. [Online]. Available: https://www.businesswire.com/news/home/20200506005184/en/Buckle-Temporarily-Adds-Food-and-Delivery-Insurance-Coverage-to-Member-Policies-at-No-Additional-Cost. [Accessed: 2-18-2021]

[6] Ieee.org, "IEEE IEEE Code of Ethics", 2016. [Online]. Available: http://www.ieee.org/about/corporate/governance/p7-8.html. [Accessed: 29- Feb- 2021].

[7] ti.com, "RS-485 basics: When termination is necessary, and how to do it properly", 2018. [Online]. Available: https://e2e.ti.com/blogs_/b/analogwire/archive/2016/07/28/rs-485-basics-when-termination-is-necessary-and-how-to-do-it-properly. [Accessed: 2-3-2021]

[8] lammertbies.nl, "RS485serial information", [Online]. Available: https://www.lammertbies.nl/comm/info/rs-485. [Accessed: 2-3-2021]

[9] ti.com, "RS-485 for Digital Motor Control Applications", 2003. [Online]. Available: https://www.ti.com/lit/an/slla143/slla143.pdf?ts=1614912454088&ref_url=https%253A%252F%252Fwww.google.com%252F#:~:text=Typical%20propagation%20delay%20through%20a,about%205%20ns%20per%20meter. [Accessed 2-4-2021]