Modularized Electronic Locker Project Proposal

ECE 445

Team #61

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

TA: Ali Kourani

Spring 2021

Table of Content

1. Introduction

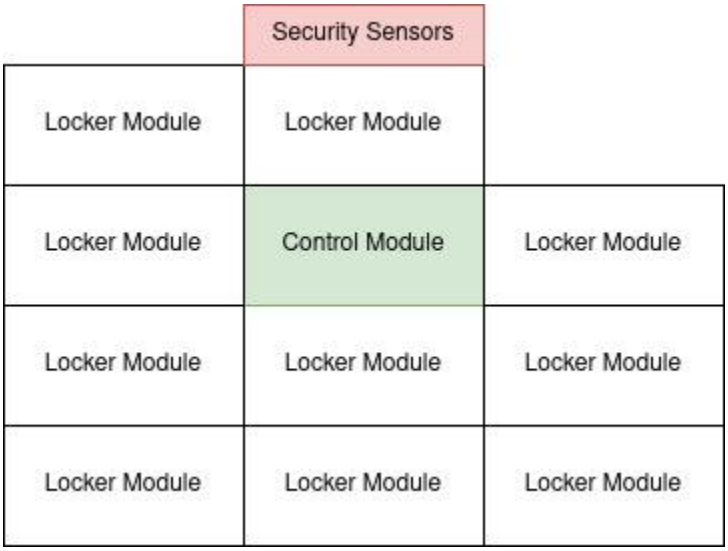
1.1. Objective

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 a low-cost solution that can protect deliveries from all vendors.

1.3. Physical Design



1.4. HIgh-level Requirements

1.4.1. Connectivity

Able to sync pickup and deposit code databases with cloud service in real-time (pulling data periodically).

1.4.2. Modularity

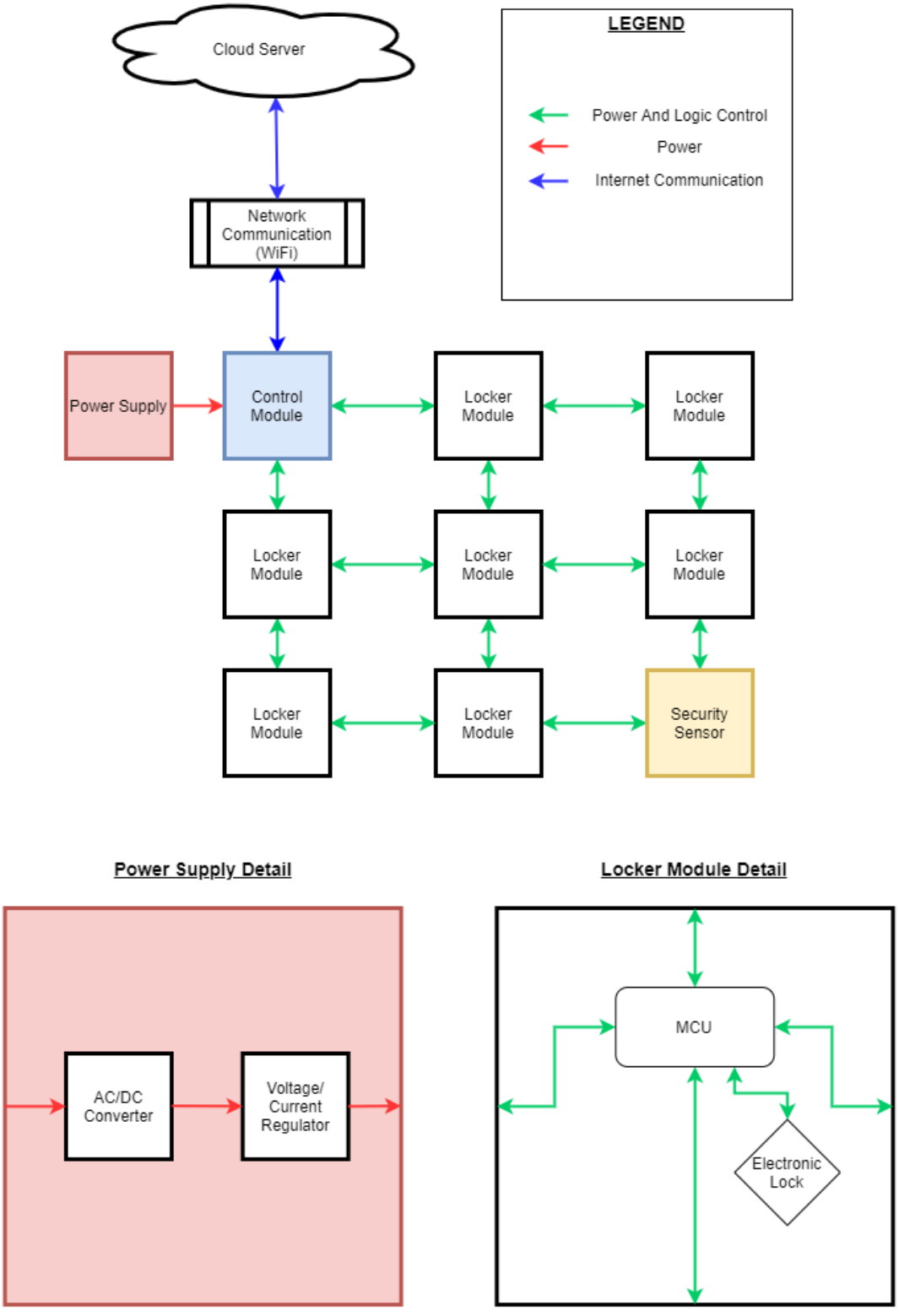
Different kinds of modules are compatible with each other using the same data bus and power bus. Our final solution can support at least 3 locker modules.

1.4.3. Security

Only package owners can only retrieve their own packages and delivery service can only open unused lockers. Each customer has their own deposit code and pickup code for theft protection.

2. Design

2.1. Block Diagram



2.2. Functional Overview

2.2.1. Power Supply

This subsystem will supply power to the entire system and should be able to do so without fault. This system ensures constant operation of the device. The power system should be able to deliver suitable power regardless of the number of additional modules added to the device.

2.2.2. Control Module

This module controls the electronic locks that allow the lockers to open. It takes input from a touchpad mounted to the locker system as well as the Network Communication Module.

2.2.3. Network Communication

The network communication will deal with communication to a cloud server. The exchanged information will include combination data, locker command data, and sensor data.

2.2.4. Security Sensors

The sensors which will be an additional module will provide additional security measures. This will include a camera that will be able to capture the surroundings of the device that will be saved by the control module. The control module will also be able to communicate with the camera to initiate a photo capture.

2.2.5. Locker modules

These modules provide the basic functionality of a locker. Each contains an electronic lock that is controlled by the control system. Lockers can be connected to each other both vertically and horizontally (stackable). The lockers will also be spring-loaded so that they automatically open once the electronic lock is disabled.

2.3. Block Requirement

2.3.1. Power Supply

This should be able to connect to a standard wall outlet to supply power to the system. An AC/DC converter will be needed to supply a custom printed PCB which will provide overcurrent and overvoltage protection. In the event of a critical power failure the power system will break the connection to the device for it's protection. The power supply will be responsible for providing constant power to the control module as well as the required power for the other modules in the system.

Requirement 1: The AC/DC adapter must be able to transform 120 V AC to 12 V +/- 5% DC to supply up to 100 W.
Requirement 2: The voltage regulator must provide 12 V +/- 5% from a 11.4-12.6 V source.
Requirement 3: The current regulator must provide up to 8 A +/- 5% and limit the current draw in the event of a short circuit or overdraw.

2.3.2. Control Module

A powerful microcontroller 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 control module should also work with the Network Communication to update its locker status and sync the deposit/pickup code database.

Requirement 1: The MCU in control module can access the communication bus (I2C/CAN) to send an unlock instruction to a specific locker module.
Requirement 2: The MCU can receive data from security sensors, save at least 5 images locally and transmit them to the cloud.
Requirement 3: The internal storage must provide both read and write speeds above 1 Mbps with a capacity greater than 5000 kB.

2.3.3. Network Communication

This module should be connected to the internet through WiFi. It will be connected to the microcontroller (part of the control module) on board.

Requirement 1: The WiFi IC must be able to communicate over IEEE 802.11b/g/n at >100 kbps with a 50 Ω nominal RF connection
Requirement 2: It must be able to communicate over SPI

2.3.4. Security Sensors

A camera will be mounted on top of the control unit and will automatically capture an image whenever a locker module is opened. This camera will be compatible with the modular connector, communication protocol and can transmit collected data to the control module through the bus.
Requirement 1: Camera can capture pictures of resolution 720p whenever users deposit and retrieve packages.
Requirement 2: Pictures can capture the appearance of users.

2.3.5. 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.

Requirement 1: Locker wiring is completely concealed
Requirement 2: Locker modules provide significant theft protection and can only be broken into using unreasonable force
Requirement 3: Microcontroller can access the communication bus (I2C or CAN) and receive the instruction from the control module addressed to itselt.

2.4. Risk Analysis

2.4.1. Bus Address Initialization

Since all the storage modules will have the same factory settings. It will be very hard to initialize the system with all the unconfigured modules connected. No matter what bus protocol we choose, the control module (master) will need to address all locker modules (slaves) distinctively. We will develop a configuration mode in the control module that uses the default locker address to reconfigure the locker module to a unique address. And we need to set up a button at each locker module to reset its address to default for debug purposes.

2.4.2. Physical Interface between Modules (Connectors)

We will have to test different connectors to find one that supports the power usage and minimize the signal noise. The connector should also be reliable and easy to connect for stackable design. The exposed

connectors should also be isolated from the bus to prevent unexpected signal and voltage inference.

3. Ethics and Safety

3.1. 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.

3.2. Safety

3.2.1. 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 and electrically isolate the power supply.

3.2.2. Vandalism

We need to find a way to secure the whole locker system right after all modules are stacked so that criminals will not break them apart.

4. 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- 2016].