ECE OpenLab Automated Equipment System

Team 12 - Abigail Starr, Aditya Bawakule, Alex Ortwig, David Hickox
ECE 445 Project Proposal - Spring 2020
TA: Dhruv Mathur

1 Introduction

1.1 Objective

The objective of this project is to create an automated checkout system that would allow students in the ECE OpenLab (OpenLab) to checkout and return equipment without requiring the assistance of a lab monitor, freeing the lab monitors to do more productive tasks during their shifts. The system will handle equipment checkout/return, logging of data, and validation the return of a piece of equipment. The system will consist of lockers that store equipment, unlock to allow access to the contents when necessary, a user identity authentication system (eg. HID Prox) that controls access, a screen for equipment selection, and an interface that logs system use.

1.2 Background

OpenLab equipment access control is a tedious process that consumes valuable time from paid OpenLab employees — time which could be spent more productively on improving the lab. There is a multistep process to checking out lab resources which includes recording i-card information, retrieving the piece of equipment, and ensuring that the equipment checked back in is complete. This process takes several minutes, is prone to human error, and is a distraction to the lab monitor.

The OpenLab has a large backlog of projects that need completion. Due to the lab monitor work schedule it is difficult enough to achieve any meaningful progress in 2 hours, much less with 30+ percent of their time going to equipment access control. The automation of the process of checking out lab equipment would allow for more uninterrupted time spent on projects for the OpenLab. Currently lab equipment is only available for checkout when a lab monitor is present; oftentimes students need to work on projects outside of these hours. Automating this system would also allow for greater utilization of the lab's resources during off-hours.

1.3 High-Level Requirements List

- The system must be able to identify whether returned equipment is within the equipment's target weight range.
- The system must validate a student's identity, check out an available item of their choice to them, associate the checkout/check in with their student ID, and make this data available to lab monitors.

- The system must lock and unlock lockers to allow access to the stored equipment when appropriate. Additionally, it should be locked in the case of power loss.

2 Design

The hardware portion of the system consists of a set of lockers with a checkout interface and user identity authentication system attached. The lockers will be locked/unlocked by the system when appropriate using magnetic locks. Additionally, each locker will be capable of measuring the weight of its contents in order to ensure that the materials were properly returned.

The software side will handle authenticating users for checkout/return, sending the commands to lock/unlock lockers using CAN (Controller Area Network), and logging all checkouts and returns. The physical interface on the device will allow users to select equipment for checkout and to report missing materials.

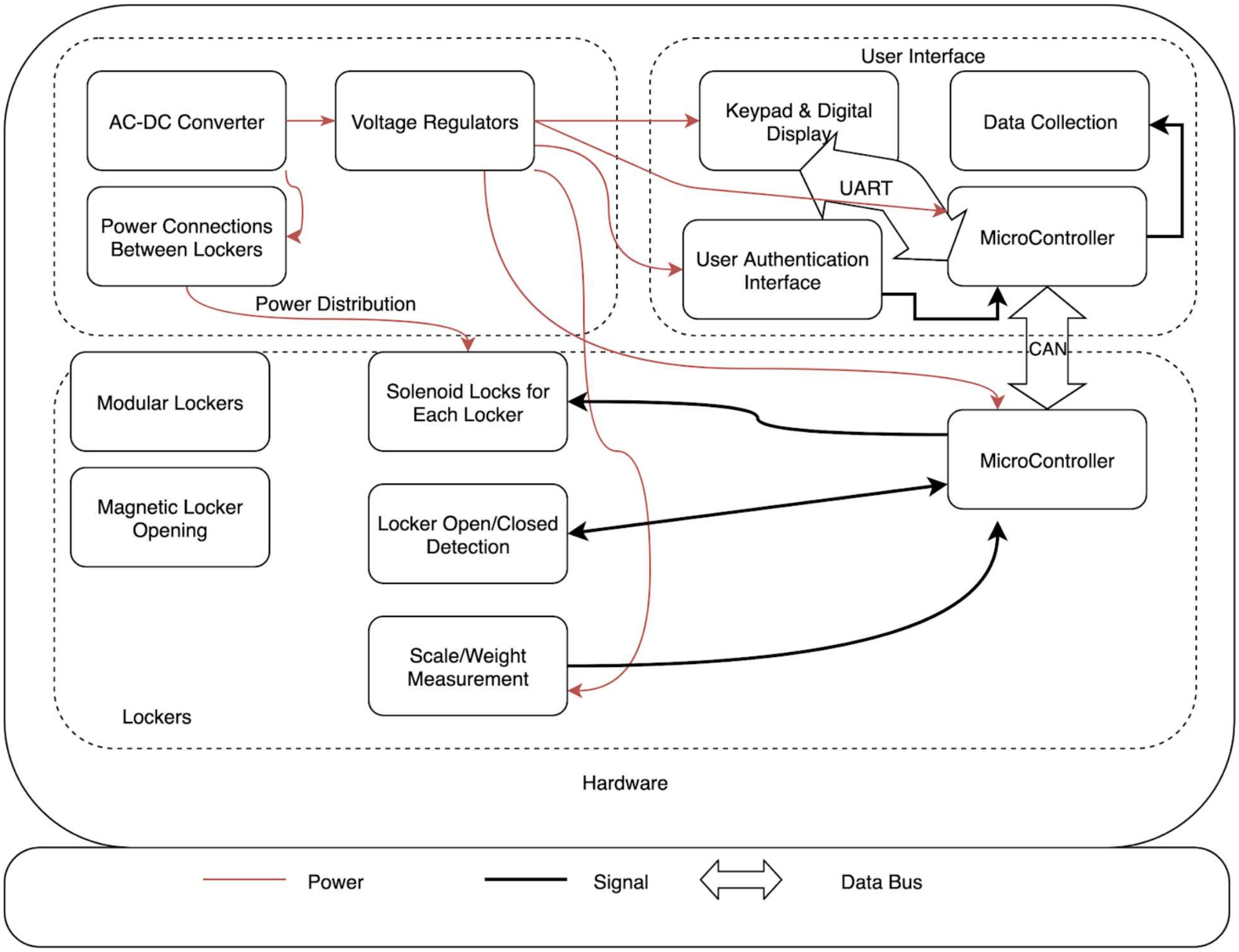

Figure 1. Block Diagram

2.1 Physical Design

Locker Dimensions:

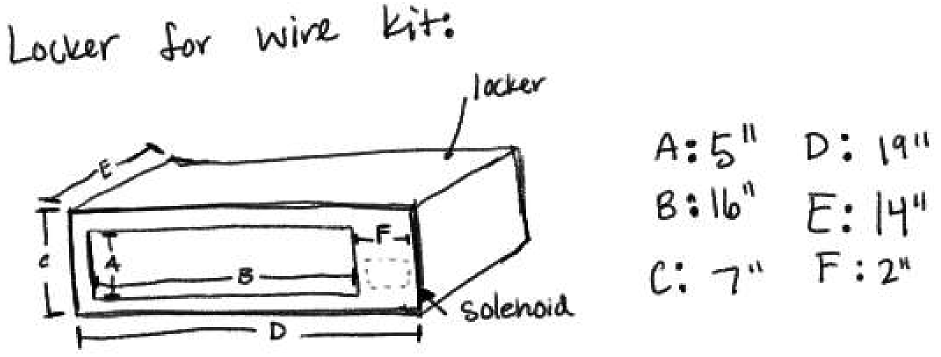

Figure 2. Locker Dimensions

There needs to be space in the locker for the solenoids and the electronics. Extra space can be created on one of the sides of the lockers to have a spot for the solenoid and the electronics, which will be protected from the user by a secondary wall, so the user cannot tamper with the electronics while the locker door is open.

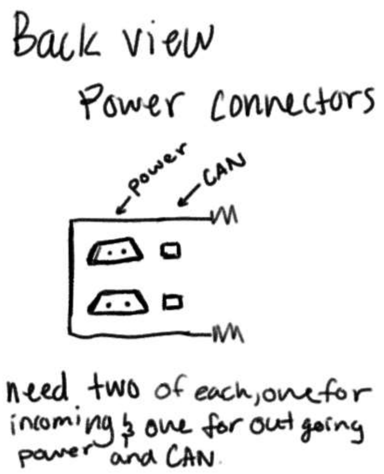
Back view
Power Connectors
power
CAN
need two of each, one for incoming & one for out going power and CAN.

Figure 3. Power Connections

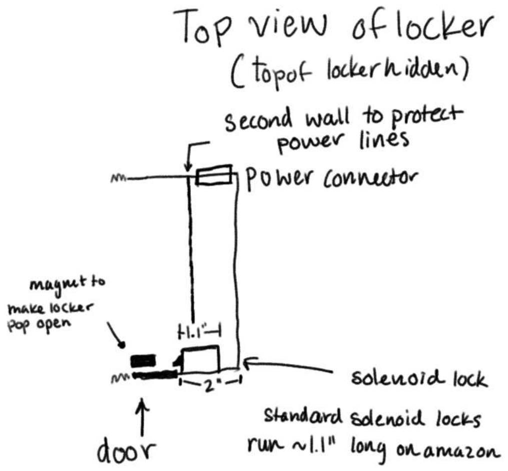
Top view of locker
(top of locker hidden)
second wall to protect power lines
Power connector
magnet to make locker pop open
1.1"
2"
solenoid lock
door
Standard solenoid locks run ~1.1" long on amazon

Figure 4. Locker Top View

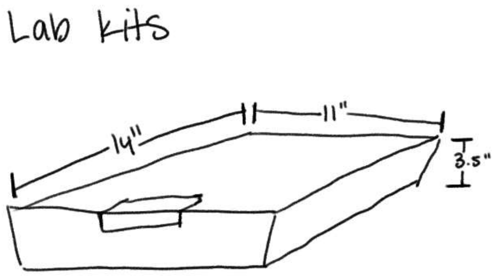

Figure 5. Standard Lab Wire Kit Dimensions

2.2 Functional Overview

2.2.1 Power Distribution

AC-DC Converter

The AC-DC converter will take in a range of 120Vrms mains AC (+\-6Vrms) from a wall outlet and output 12V DC (+\-2V) with the capability to supply at least 2A, which will be distributed to various DC-DC voltage regulators. The AC-DC converter will be a purchased item with UL certification in order to meet safety requirements.

Voltage Regulators

The voltage regulators are on-board voltage step down conversion from the 12V DC rail to the 3.3V and 5V required to power the microcontrollers and other discrete electrical components on the PCBs. The output voltage must be within 200mV of the target under no load.

Power Connections

We need to have connectors between sets of lockers that can survive 10 mating cycles, with locking connections to ensure that they will not come apart with regular use. Because the lockers are modular, we need to have a system where the power connections are not permanent and are relatively protected.

2.2.2 User Interface

Keypad

This will be for the standard user input, to control which locker the user wishes to open. This will communicate with the microcontroller, which will then process the data. The keypad will be a purchased matrix style keypad with at least 12 keys or touch locations.

Digital Display

The Digital Display will act as a visual interface between the user and the main system controller. The screen will display prompts and information to the user in order to ensure self-explanatory and easy operation of the locker system, as well as button inputs from the keypad. The display needs to be at least 16x2 characters (or 80x16 pixels) .

Microcontroller

The microcontroller will control the locking/unlocking of the lockers, take input from the keypad, and display the status on the screen. We have chosen a NXP i.MX rt 10xx with custom PCB. The master microcontroller will be connected to the keypad and Digital Display, and will send information over CAN to the microcontrollers in each locker or locker assembly that will control the locking and unlocking.

Data Collection

Data needs to be collected and logged so the OpenLab can have a record of who checks out equipment. Every interaction with the lockers will be logged into flash storage, so the lab monitors can access the logs in the case that equipment is missing or broken.

2.2.3 Lockers

Modular Lockers

A goal of this project is to be able to scale to any number of lockers in the system, so in order to do that, having modular lockers that are independent of each other is important. Each locker needs to be its own separate unit, with enough electronics to function on its own. Therefore, each locker will have its own microcontroller that can connect to the master CAN bus, and therefore be able to send and receive data from the master microcontroller.

Magnetic Locker Opening

When a locker is open we need a way for the user to be able to open the door. The locker will either have a handle and/or a spring system to pop the door open when the solenoid is triggered.

Solenoid Locks

As a security measure, the lockers need to remain locked if the power is off, and solenoid locks are a great way to accomplish this, because when they take current, they will open, and otherwise remain in the locked position. When a signal is sent over CAN to open the locker, it will unlock for 20 seconds and then lock again. Each lock will draw a maximum of 20 W from the 12v rail, and only one lock will be actuated at a time. Therefore as we scale or develop for new configurations, there is no risk of exceeding the current limit of the AC-DC converter due to simultaneous locker openings.

Scale/Weight Measurement

Each locker will have a beam-type load cell that will be used to measure the weight of the equipment inside the locker. The data from the load cell will be interpreted by the locker's microcontroller to determine a weight, and compare it to the expected weight of that specific locker. The load cell will have to support a weight of at least 2kg and be accurate within 100 grams.

Locker Closing Detection

Each locker will have a momentary switch on it, similar to an endstop detection switch. It will be simple closure detection, if the switch is closed, the circuit is complete, and the signal sent to the microcontroller will flag that the door is closed. This will be a component in the determination if the check in is complete. If an individual goes to return a piece of equipment, but does not close the locker door, then the check in will be flagged as incomplete.

User Identification Authorization

A user identity authentication system will be attached to the main console of the lockers to identify the user and therefore log the information about who is checking the equipment out.

2.3 Risk Analysis

The greatest risk to the project is the implementation of the CAN network, due to the requirement of “modularity” this requires that all of the locker modules be flashed with the same firmware but be able to be plugged into an existing system and work and be identifiable from all the other lockers.

One option is to daisy chain CAN networks allowing each locker to have a master on one side and a slave on the next. This is similar to how the popular ws2812 leds work. The issue with this is all the data that is going to any locker has to pass through each locker on its path. This increases latency, hardware implementation complexity, and software complexity due to needing universal routing code.

Another option is a single CAN bus with each new device reporting as the lowest priority device, this allows it to be configured on first install but makes it difficult to allow multiple new installations at the same time due to arbitration issues.

The last method is to have all the devices use the same priorities for messages and start the message with the device id allowing it to arbitrate and identify itself with its device id from NXP which are all guaranteed unique (similar to a mac address). This option wastes a significant amount of data in communications, lowering the data rate and increasing overhead.

The reason this is the largest risk is because every method we know of has serious issues and we need to develop a method that does not have these weaknesses. Most of the other systems we have ideas of how to design them, but for the CAN system, we have some design decisions that will seriously affect both the hardware and the software of the system.

3 Ethics and Safety

We intend to follow the IEEE Code of Ethics 7.8.1-3 and 7.8.5-9 [1]. Some of the Code of Ethics is not applicable due to the nature and methods of our project. In the case of any violations of this code we will take them seriously, especially in the case of injury of a group member or other entity. Due to our project having a physical construction component, we will emphasize the safety of the end consumer when operating our device according to the Code of Ethics 7.8.1 [1].

One concern that follows with the code of ethics currently present in the OpenLab is the potential for an abuse of the trust given to lab users to maintain the integrity of the equipment. There is the potential for certain lab kits, such as boxes of cables or tool kits, to be returned with missing or added materials, and a goal for this project is to track when such events occur in order to improve the security and availability of the OpenLab’s resources.

There are cameras in the OpenLab that are currently used to track serious theft, but it would be ideal not to use any external systems to prevent theft from the locker system. This system will work in conjunction with the security cameras and lab monitors in the case of a suspected misplacement of lab supplies so there is no chance of an accidental flagging of an innocent student which would violate injuring the reputation of others [1].

In addition to the ethical concerns, it is expected that this system be plugged into the main AC power at all times. Therefore, it is necessary to isolate the power system from the mechanical system. If there are any faults in the power system, the user needs to stay safe. For this reason we will be using an off the shelf power supply listed either by UL or ETL.

The last concern that was voiced was the fact that this could replace the lab monitors in the lab. Part of the lab's draw is the human factor of having someone always present to watch over the lab and ensure safety as well as to instruct users. This project will not eliminate the positions of the lab monitors, but free them to conduct other tasks. This system will actually not allow checkouts for certain tools until there are lab monitors present. We have the lab monitors run laser cuts and there are plenty of things that need to be done around the lab to improve the lab itself. All this system would do would be to allow the lab monitors to perform fewer menial tasks during their shifts.

References

[1] “IEEE Code of Ethics,” *IEEE*. [Online]. Available: https://www.ieee.org/about/corporate/governance/p7-8.html.