ECE OpenLab Automated Equipment System

ECE445 Design Document

Team 12
Abigail Starr
Aditya Bawakule
Alex Ortwig
David Hickox
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.

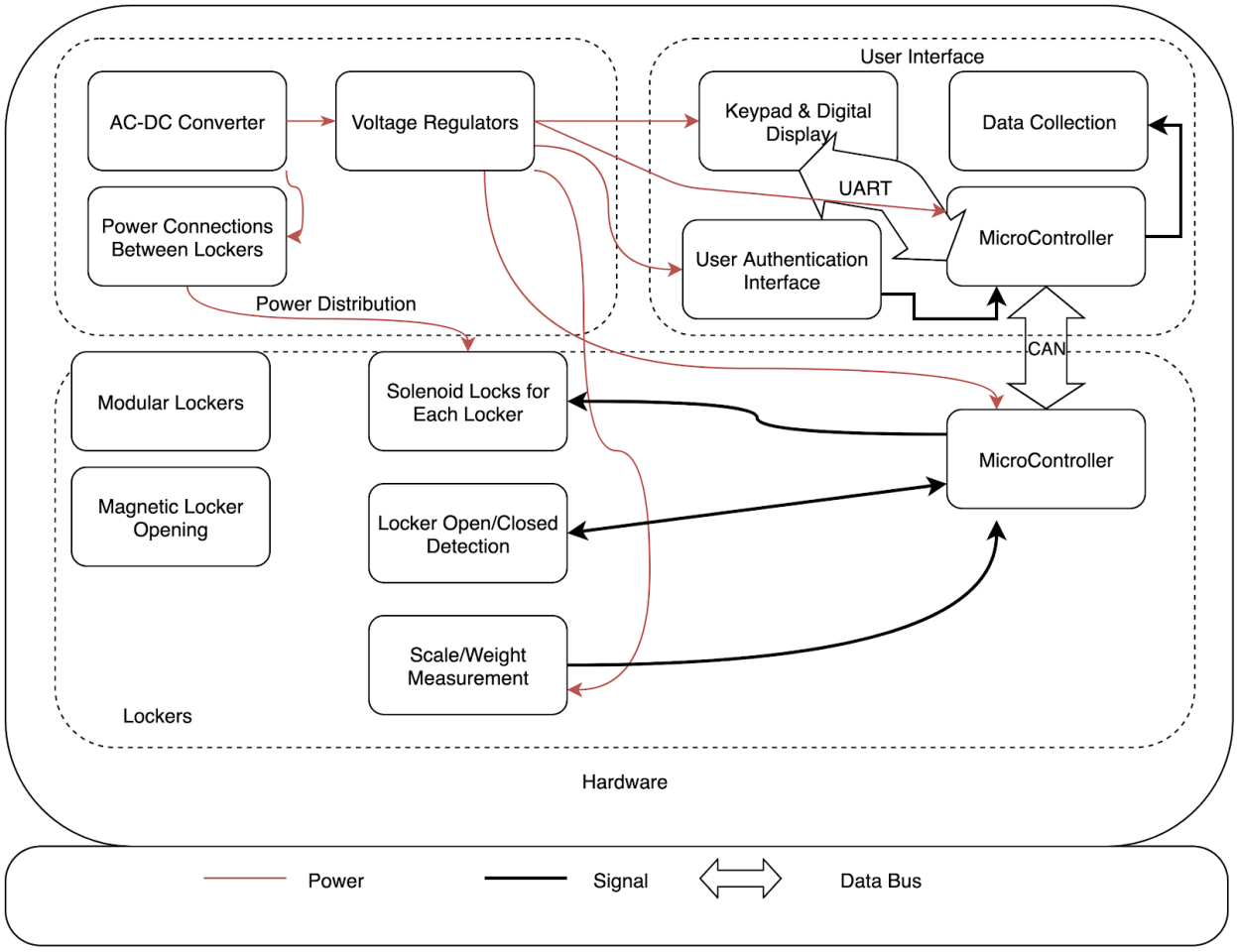


Figure 1. Block Diagram

2.1 Physical Design

Locker Dimensions:

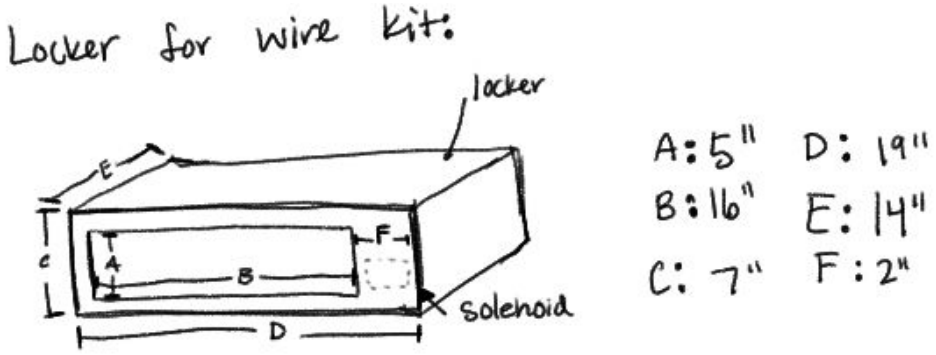


Figure 2. Locker Dimensions

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.

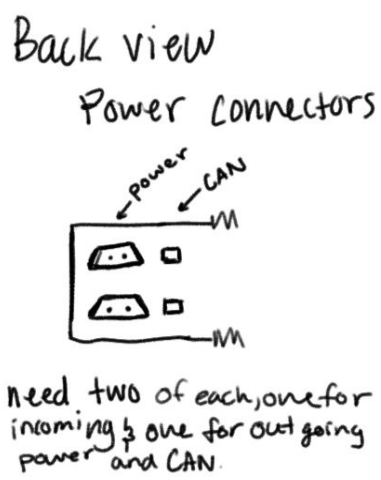


Figure 3. Power Connections

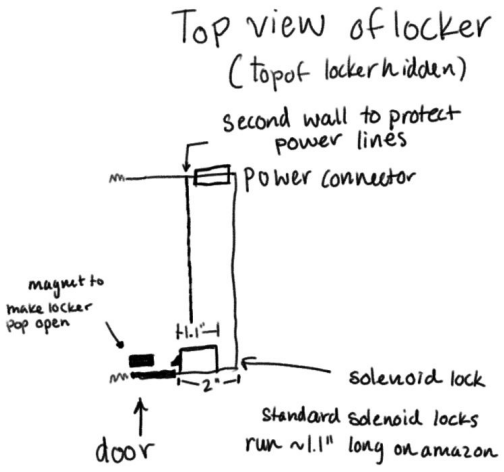


Figure 4. Locker Top View

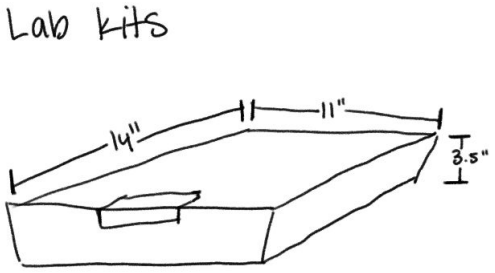


Figure 5. Standard Lab Wire Kit Dimensions

2.2 Power Distribution

2.2.1 AC_DC Converter

The AC-DC converter will be responsible for providing the locker system with a 12V DC rail from North American mains AC. The converter is one of the most important pieces of the design due to its effects on safety and system stability. The converter will be required to maintain an output of 2A for 5 minutes in case of a lock driver failure.

Requirements	Verification
1. Converter accepts an input voltage range of 114 to 126 Vrms while maintaining an output of 12V DC within a range of +\- 1V and sustaining a minimum of 2A continuous output for 5 minutes. 2. Converter is UL certified.	1. a. Use a variac to supply the converter with 114 and 126 Vrms from mains AC. b. Connect the DC output of the converter to an electric load and verify an output of 2A for 5 minutes is capable at both voltage inputs. c. Connect the DC output of the converter to a resistive load and verify the converter outputs 12V DC +/- 1V. 2. a. Verify that the converter has been certified by Underwriters Laboratories by the proper markings on the Converter.

2.2.2 Voltage Regulators

The voltage regulators will be on-board converters that step up and down the 12V rail to 3.3V, 5V, and 16V in order to power the microcontrollers, CAN bus, digital display, and authentication system. As with the other power systems in this design, these regulators will be operating 24/7 and as such will need to be designed with longevity and safety in mind. Their stability will also be crucial in maintaining stable power for the other electronics in the system.

Requirements	Verification
1. Buck converters accept an input voltage range of 11V to 13V DC and convert it to a choice of 3.3V or 5V with a tolerance of +/-0.2V. 2. Boost converters accept and input voltage range of 11V to 13V DC and converts it to 16V +/-0.2V. 3. Voltage regulators can sustain an output of at least 1A for 24 hours.	1. a. Provide the buck converter with 11V and 13V DC and verify the capability to output 3.3V and 5V within tolerance under a load of 1A. 2. a. Provide the boost converter with 11V and 13V DC and verify the capability to output 16V within tolerance under a load of 1A. 3. a. Connect one of each voltage regulators to an electronic load and verify that the regulator can sustain a 1A output at the 3.3V, 5V, and 16V for at least 24 hours.

2.2.3 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.

2.3 User Interface

2.3.1 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.

Requirements	Verification
Key pad Must have at least 12 keys with distinct output	1. Physically count the keys to ensure at least 12 are easily found 2. Press all of the keys and ensure their output is unique

2.3.2 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).

For the one LDC we have chose, it requires 3V instead of 3.3V. For that reason, there will be a separate LDO Linear Regulator that will supply power to this. This unit is expected to draw 25mA and there is a .3V difference, so the total power dissipated over this is 7.5mW

$$.3V * 25mA = 7.5mW$$

Requirements	Verification
Digital Display needs to be at least 80x16 pixels	1. Make a font that is 8x16 pixels 2. Write 32 characters to the screen, in two rows of 16, and make sure this is readable from a 1ft distance

2.3.3 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.

2.3.4 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.

2.3.5 User Identity Authentication

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. This will need to have at least fifteen unique users at any time, because that is the number of lab monitors that are staffed at any one time.

Requirements	Verification

Can accurately identify the user, a minimum of fifteen users, without mistakes.	We will add fifteen users to the system, and then have each user use the locker a minimum of fifteen times in a random order, and make sure that there are no mistakes in which user is which.

2.4 Hardware Subsystems

2.4.1 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.

2.4.2 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/magnetic system to pop the door open when the solenoid is triggered.

Requirements	Verification
1. Can push open a locker door at least 1 inch past the solenoid lock bolt.	1. a. With the locker shut and latched, send a command to the locker control board to open the locker. b. Let the locker door swing open unobstructed. c. Measure clearance of the locker door past the solenoid lock bolt and ensure it is greater than 1 inch.

2.4.3 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 2.5 seconds and then lock again. Each lock will draw a maximum of 12 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.

2.4.4 Scale and 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.

2.4.5 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 out/in is complete. If an individual goes to return a piece of equipment, but does not close the locker door, then the check out/in will be flagged as incomplete.

2.5 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.

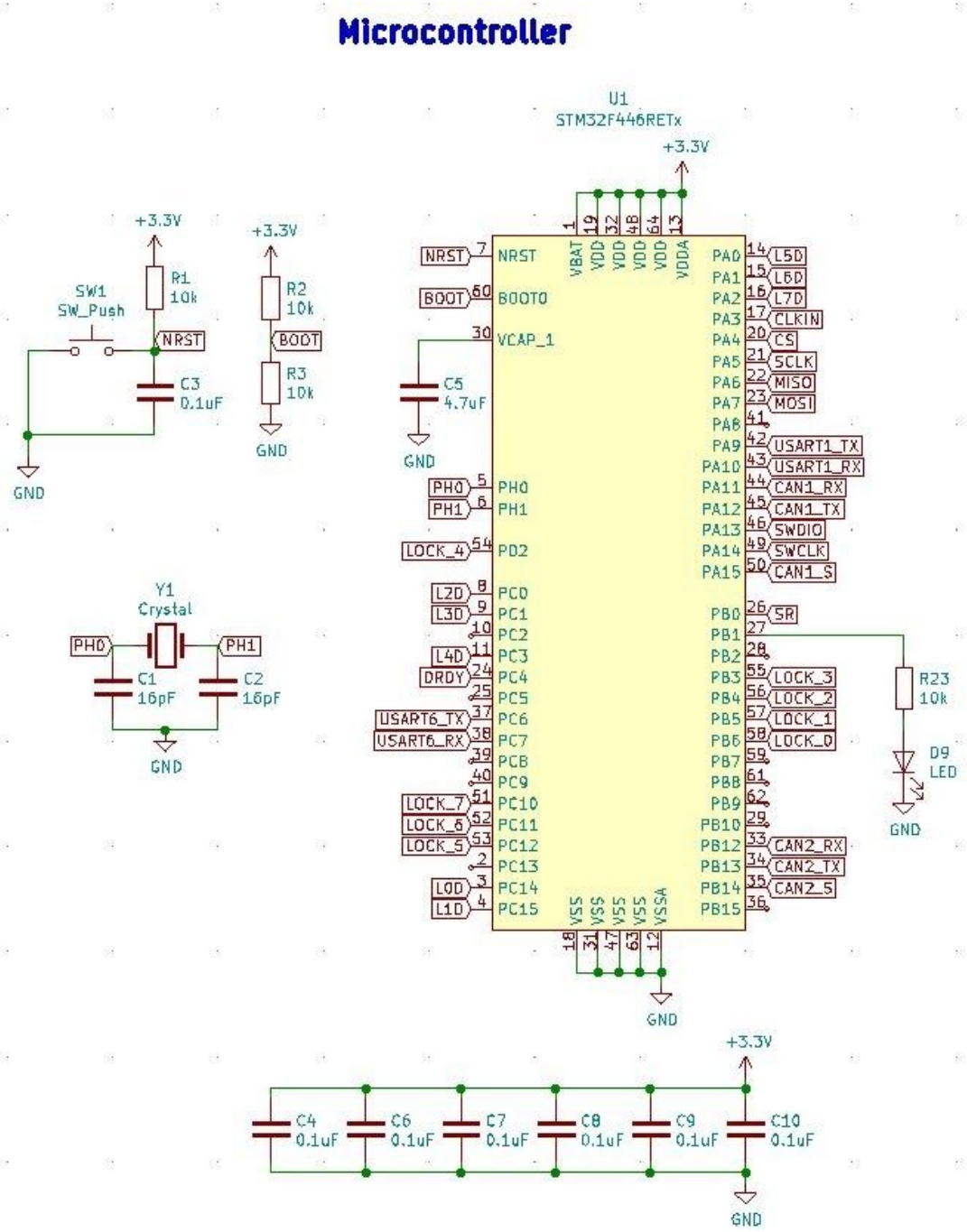
Another option is a single CAN bus with each new device reporting as the lowest priority device, this allows it to be configured on first install but makes it difficult to allow multiple new installations at the same time due to arbitration issues.

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.

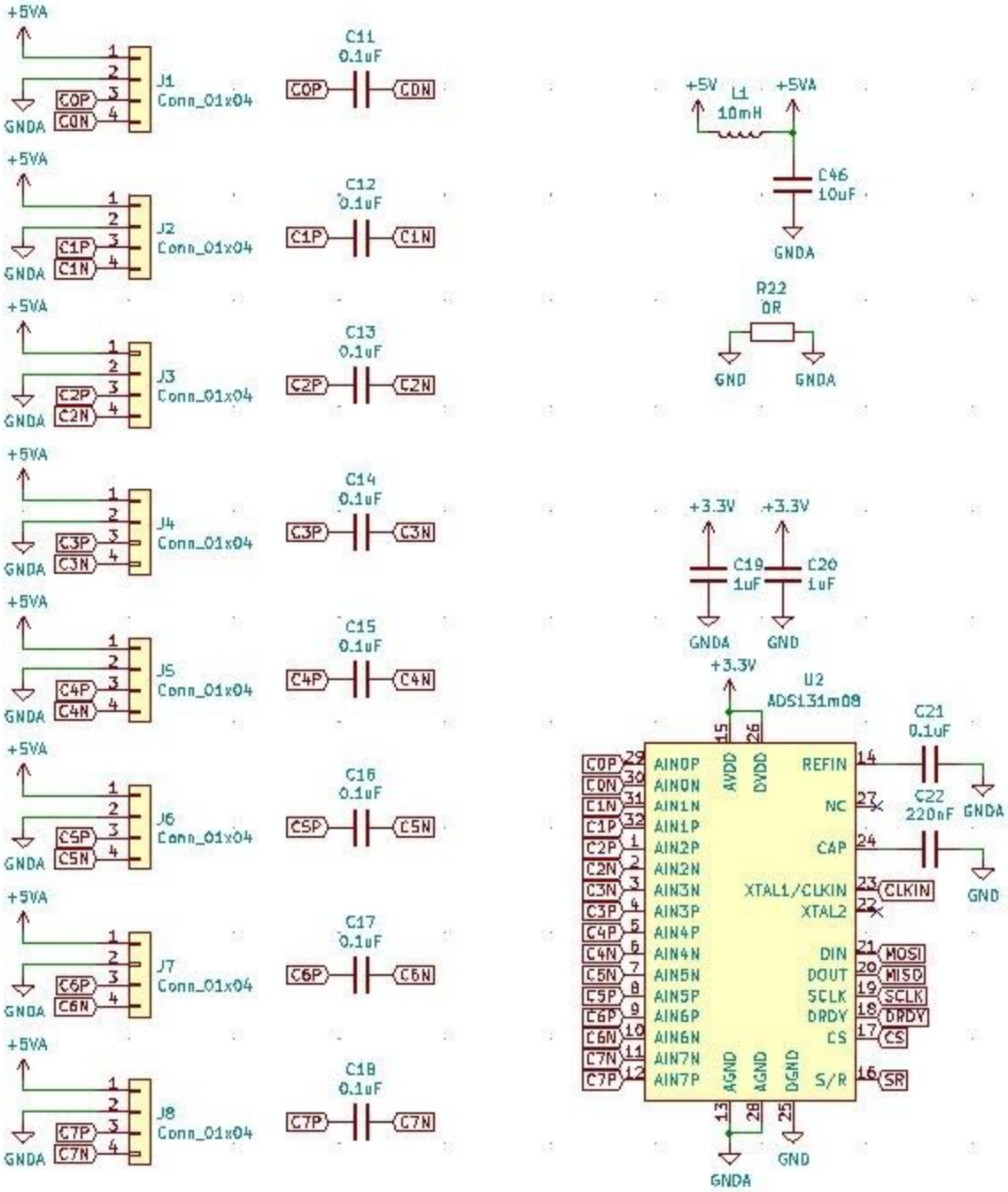
The reason this is the largest risk is because every method we know of has serious issues and we need to develop a method that does not have these weaknesses. Most of the other systems we have ideas of how to design them, but for the CAN system, we have some design decisions that will seriously affect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

2.6 Schematics

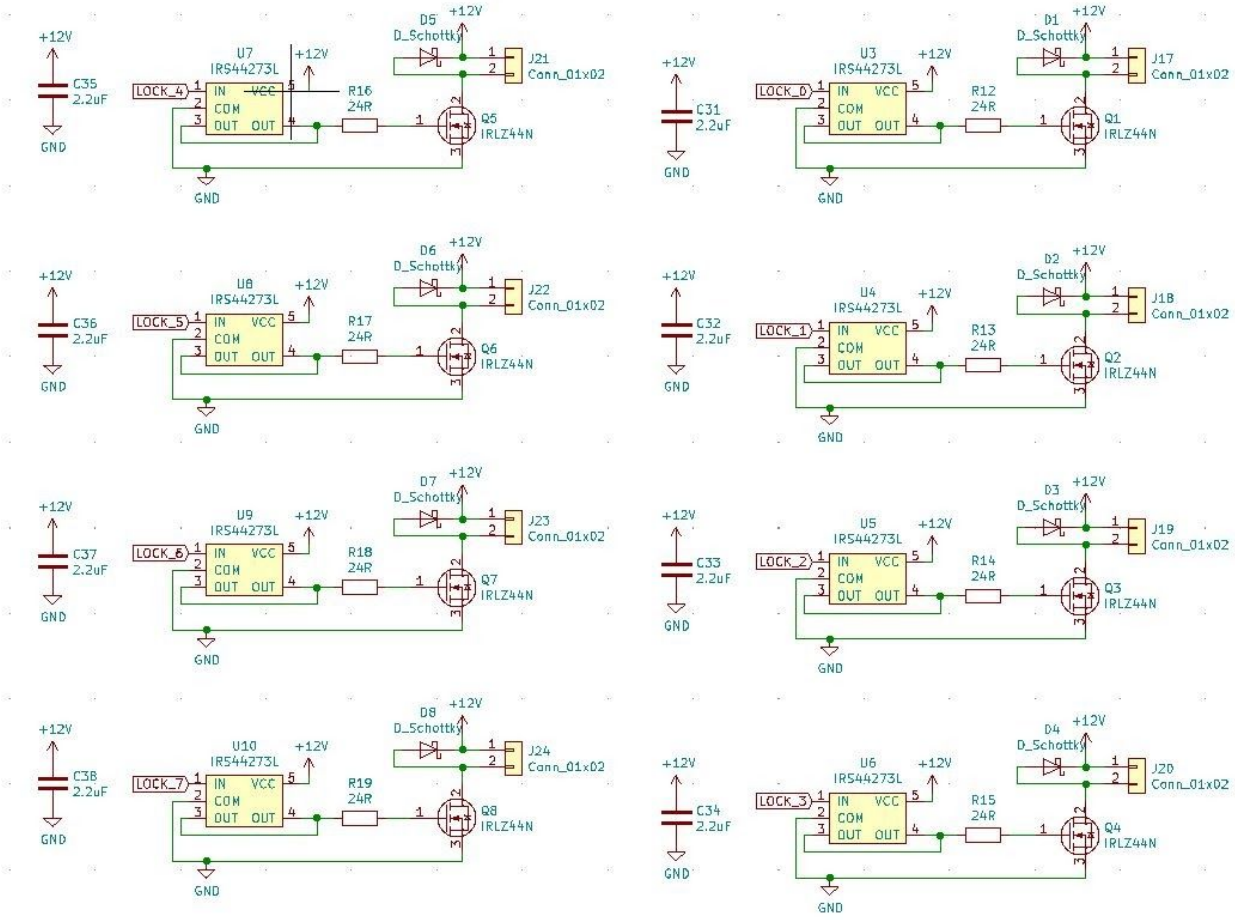
2.6.1 Locker Control Board



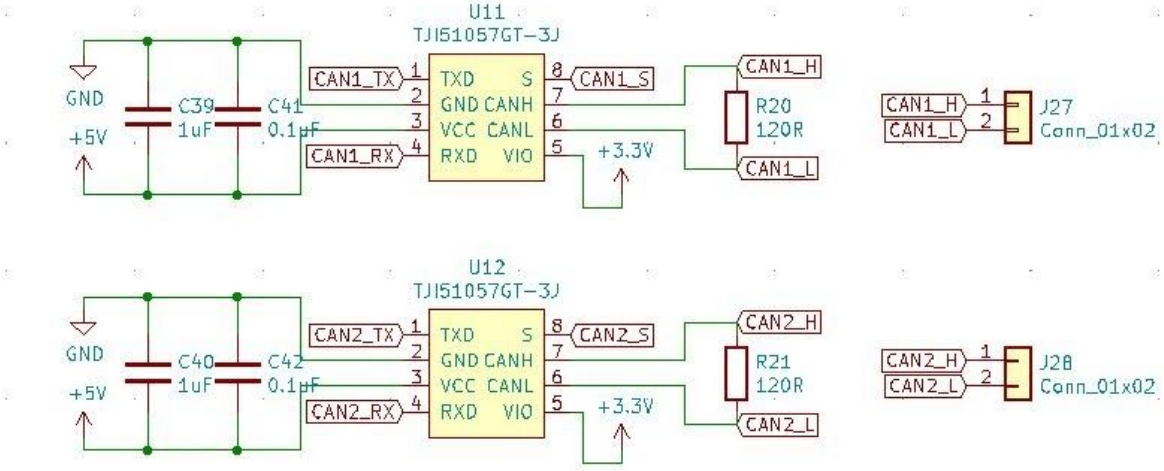
Load cell connections and ADC



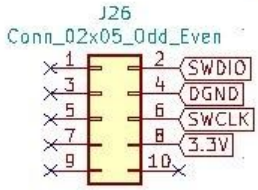
Solenoid Lock Drivers



CAN

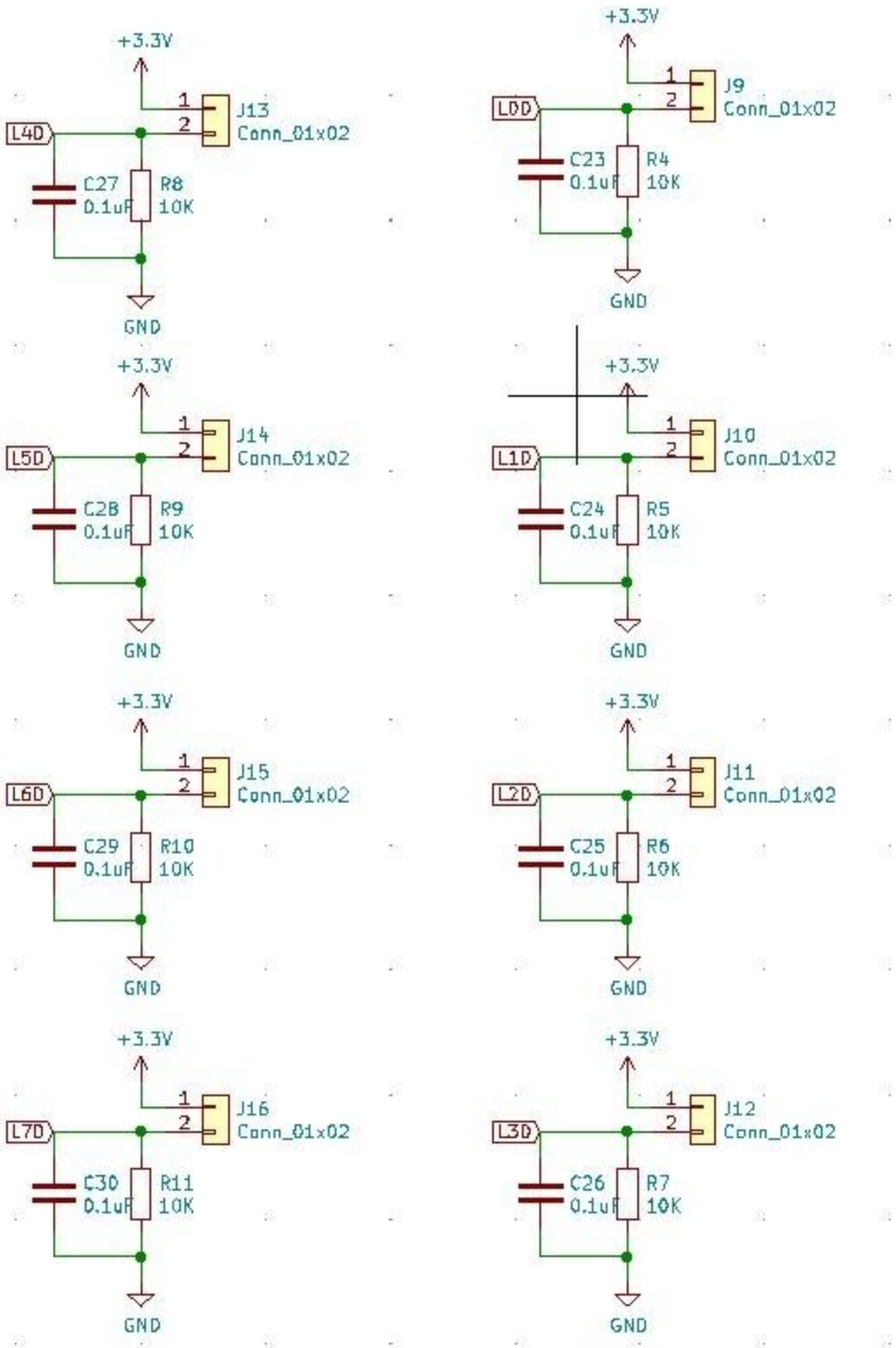


Serial Debug



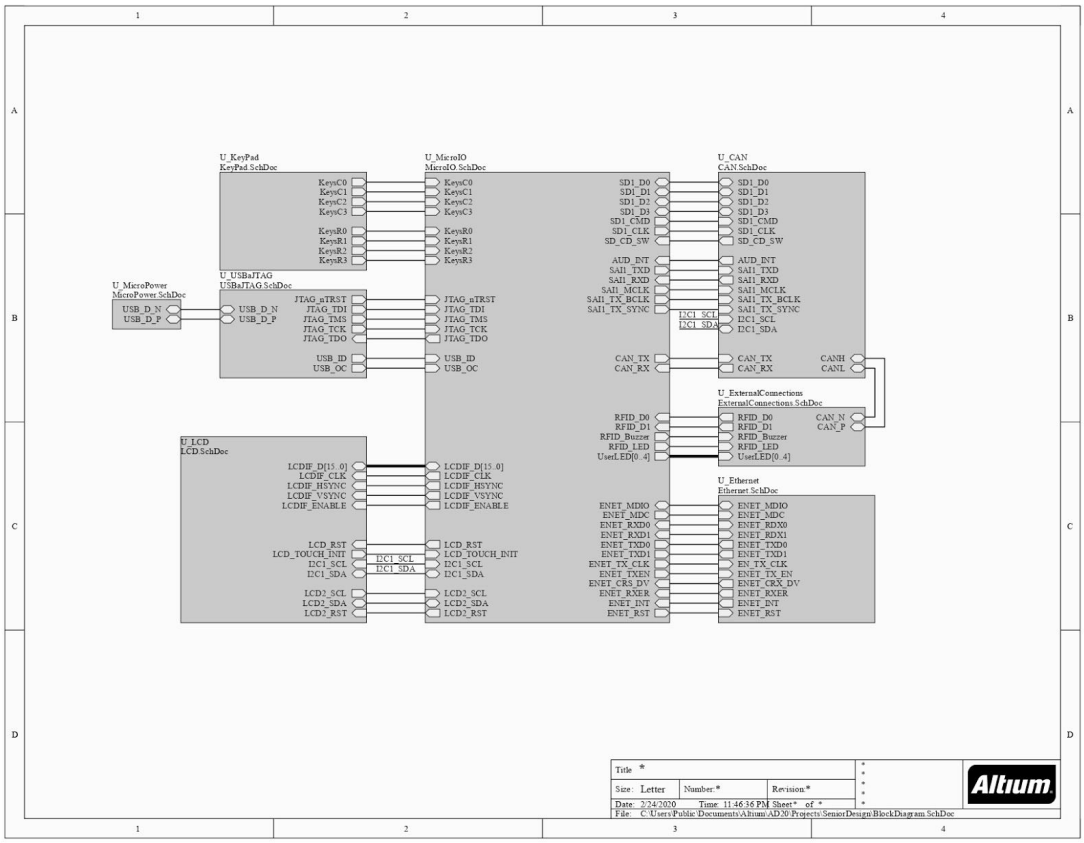
UART Breakout

Locker Closure Detection

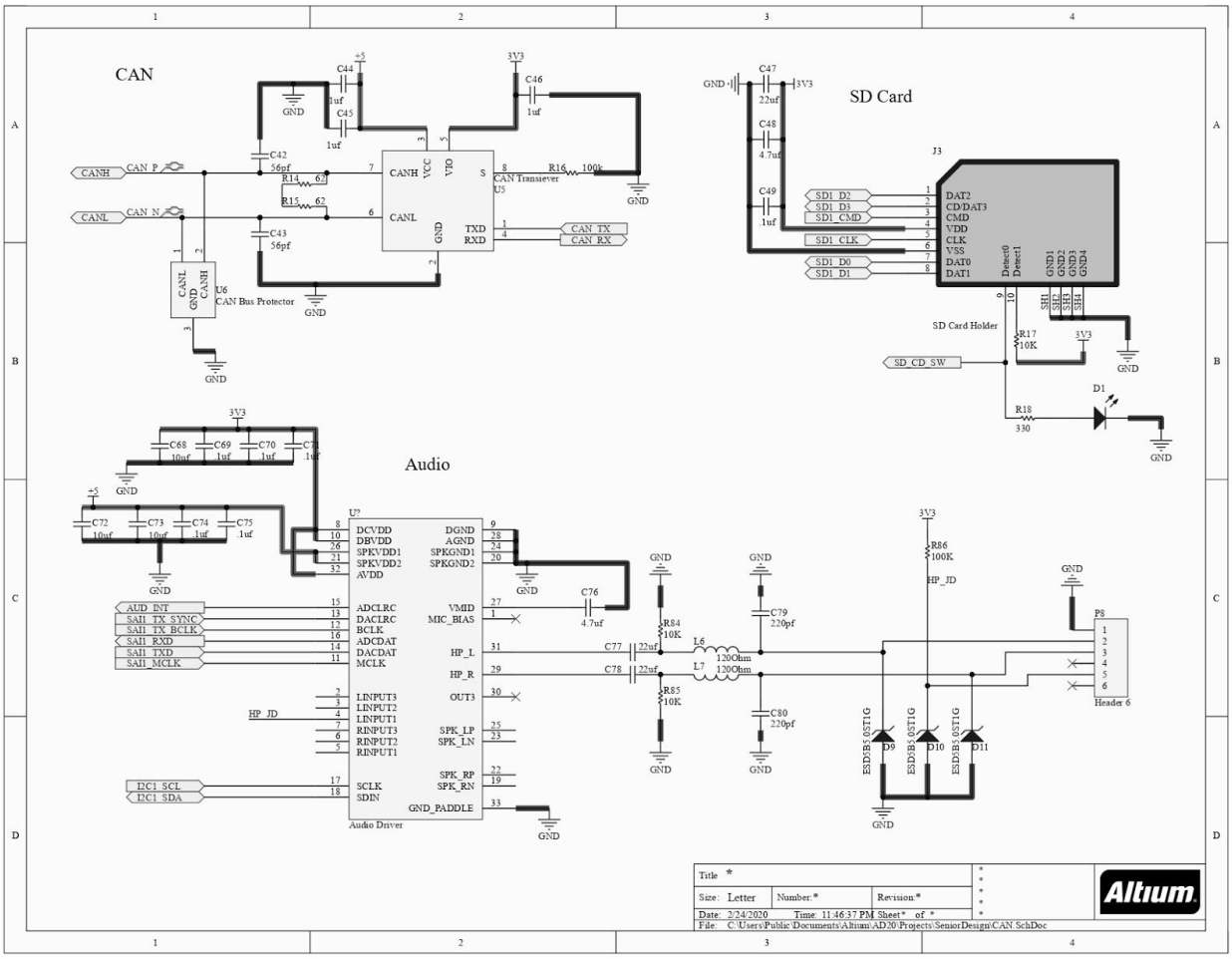


2.6.2 User Interface Board

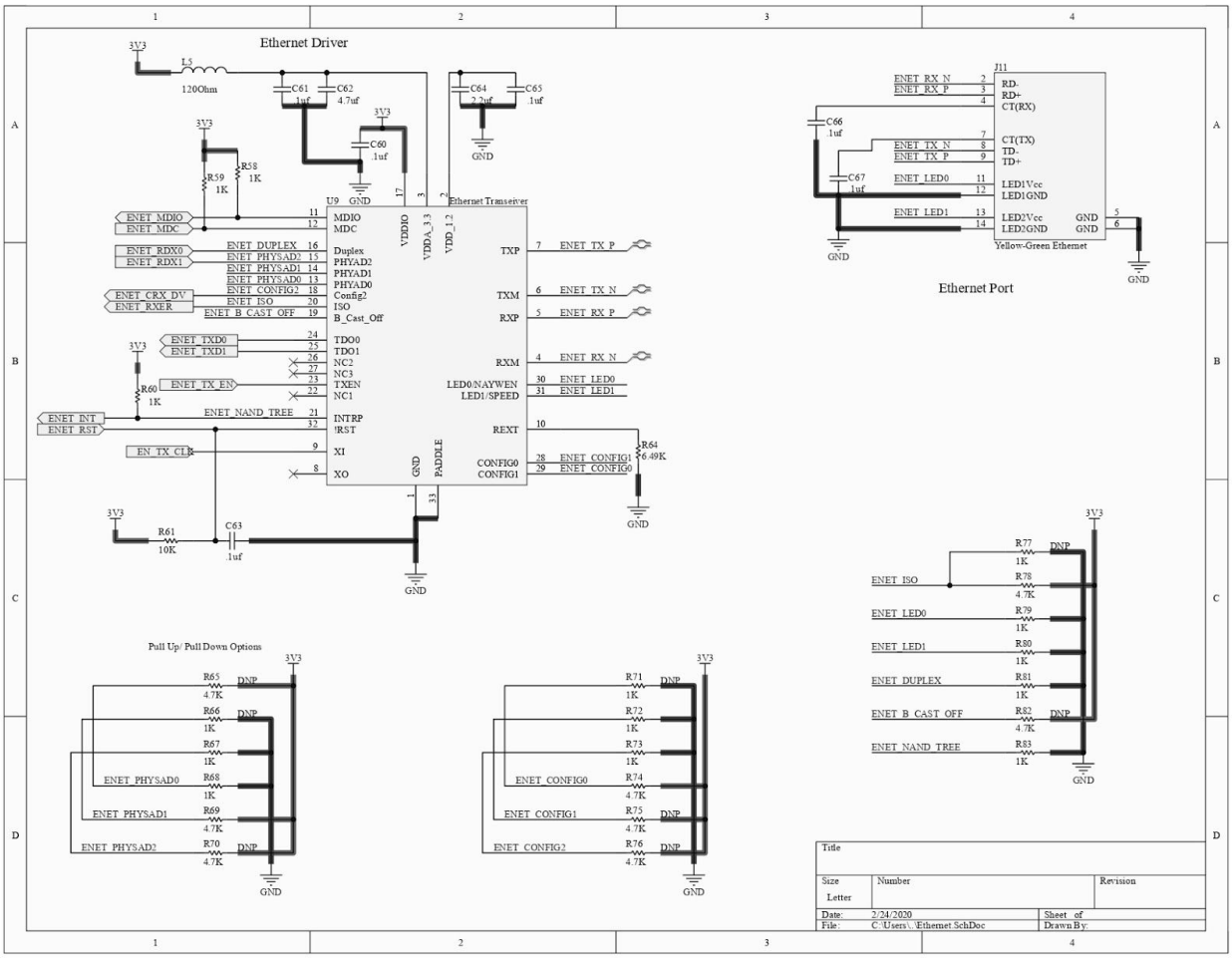
Block Diagram:



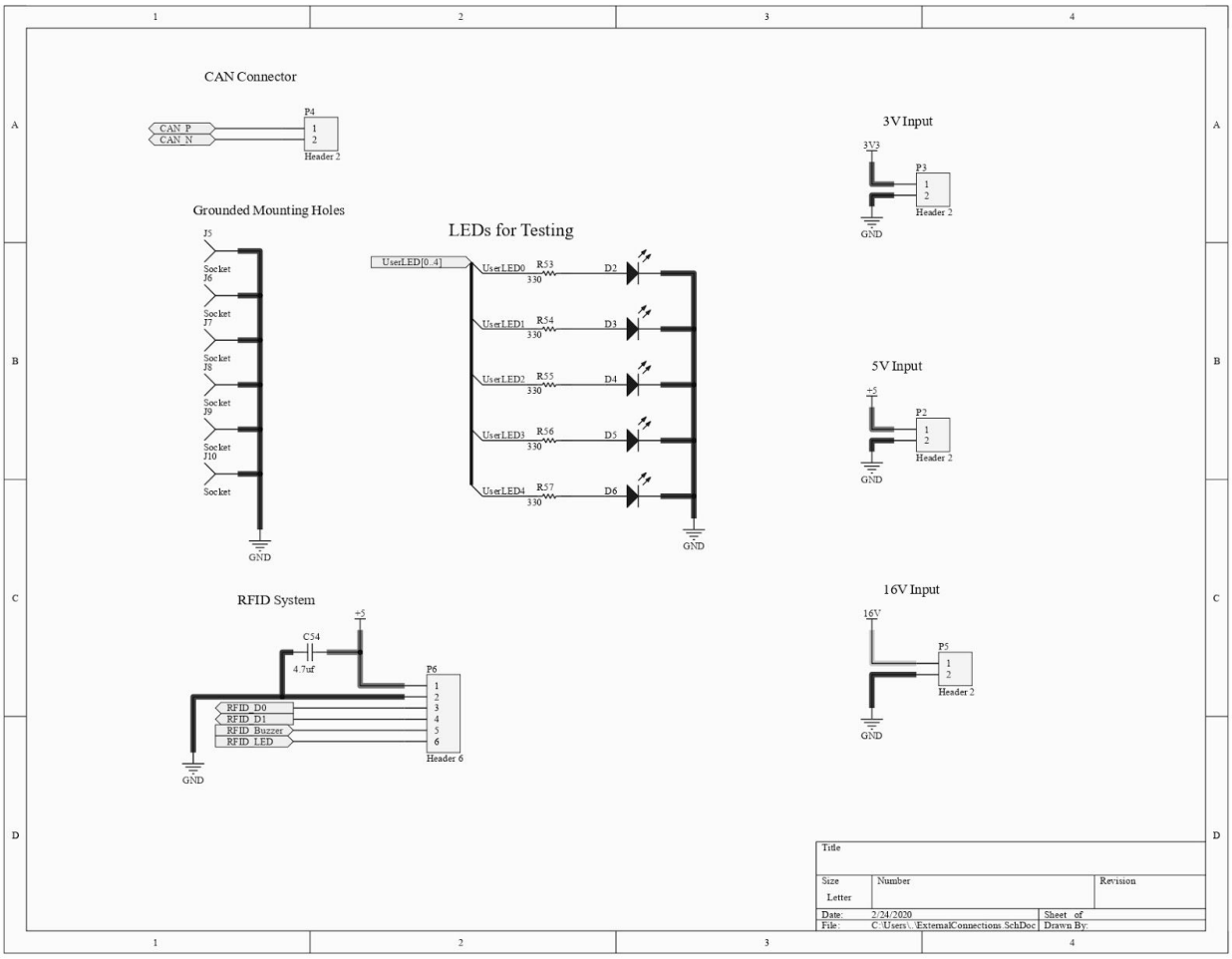
CAN/SD/Audio:


CAN
SD Card
Audio
CAN_P
CANH
CAN_N
CANL
C42
56pf
C43
56pf
R14
60
R15
62
U5
CAN Transiever
R16
100k
U6
CAN Bus Protector
CAN_TX
CAN_RX
C44
1uf
C45
1uf
C46
1uf
C47
22uf
C48
4.7uf
C49
.1uf
J3
SD1_D2
SD1_D3
SD1_CMD
SD1_CLK
SD1_D0
SD1_D1
DAT2
CD/DAT3
CMD
VDD
CLK
VSS
DAT0
DAT1
SD Card Holder
SD_CD_SW
R17
10K
R18
330
D1
C68
10uf
C69
1uf
C70
1uf
C71
1uf
C72
10uf
C73
10uf
C74
.1uf
C75
.1uf
U?
Audio Driver
AUD_INT
SAI1_TX_SYNC
SAI1_TX_BCLK
SAI1_RXD
SAI1_TXD
SAI1_MCLK
I2C1_SCL
I2C1_SDA
HP_JD
C76
4.7uf
C77
22uf
C78
22uf
L6
1200hm
L7
1200hm
R84
10K
R85
10K
C79
220pf
C80
220pf
R86
100K
P8
Header 6
D9
D10
D11
ESD3B5.0ST1G
Title *
Size: Letter
Number:*
Revision:*
Date: 2/24/2020
Time: 11:46:37 PM
Sheet* of *
File: C:\Users\Public\Documents\Altium\AD20\Projects\SeniorDesign\CAN.SchDoc
Altium

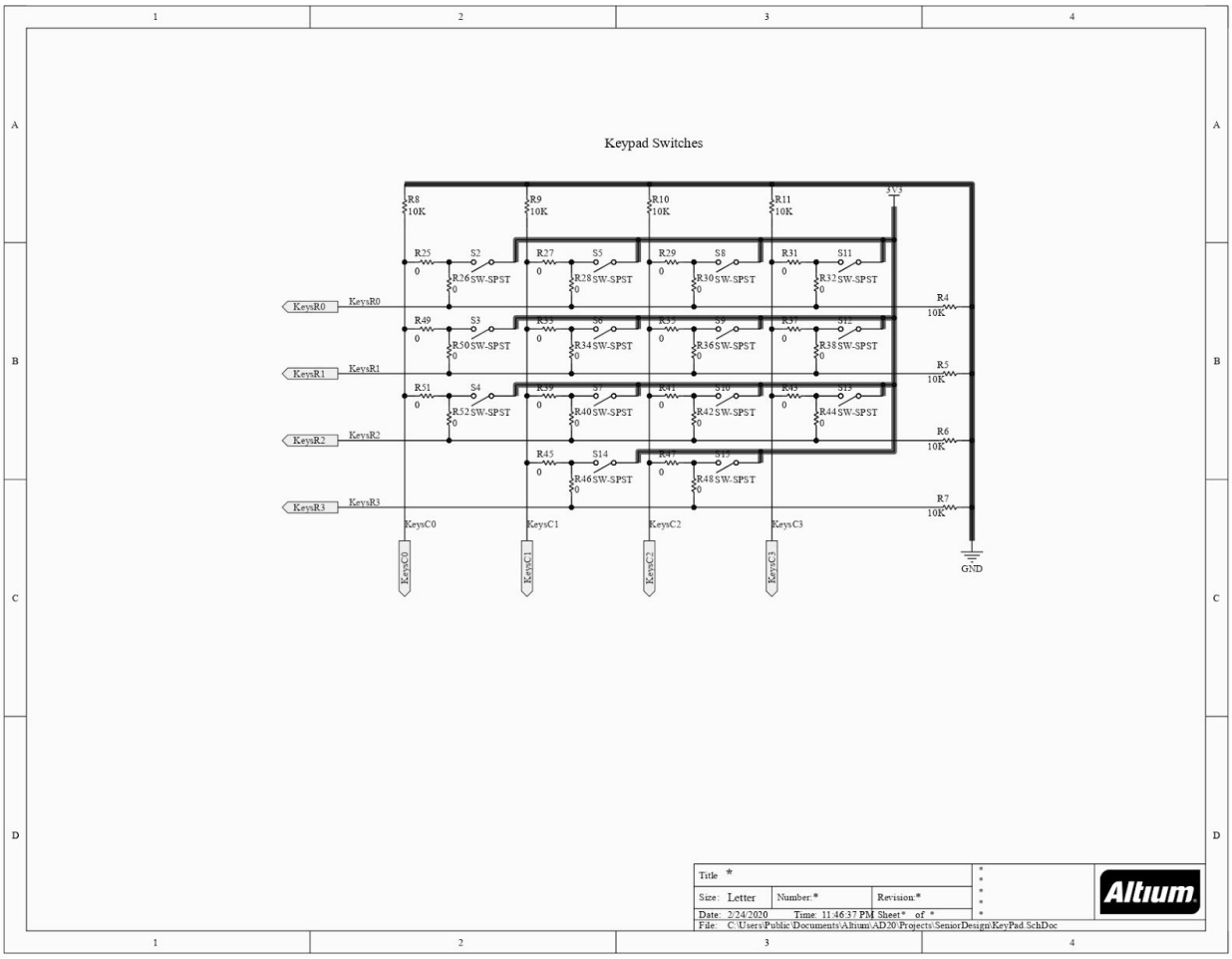
Ethernet:


Ethernet Driver
Ethernet Port
Pull Up/ Pull Down Options
Ethernet Transeiver
Yellow-Green Ethernet
Title
Size
Letter
Number
Revision
Date: 2/24/2020
File: C:\Users\..\Ethernet.SchDoc
Sheet of
Drawn By:

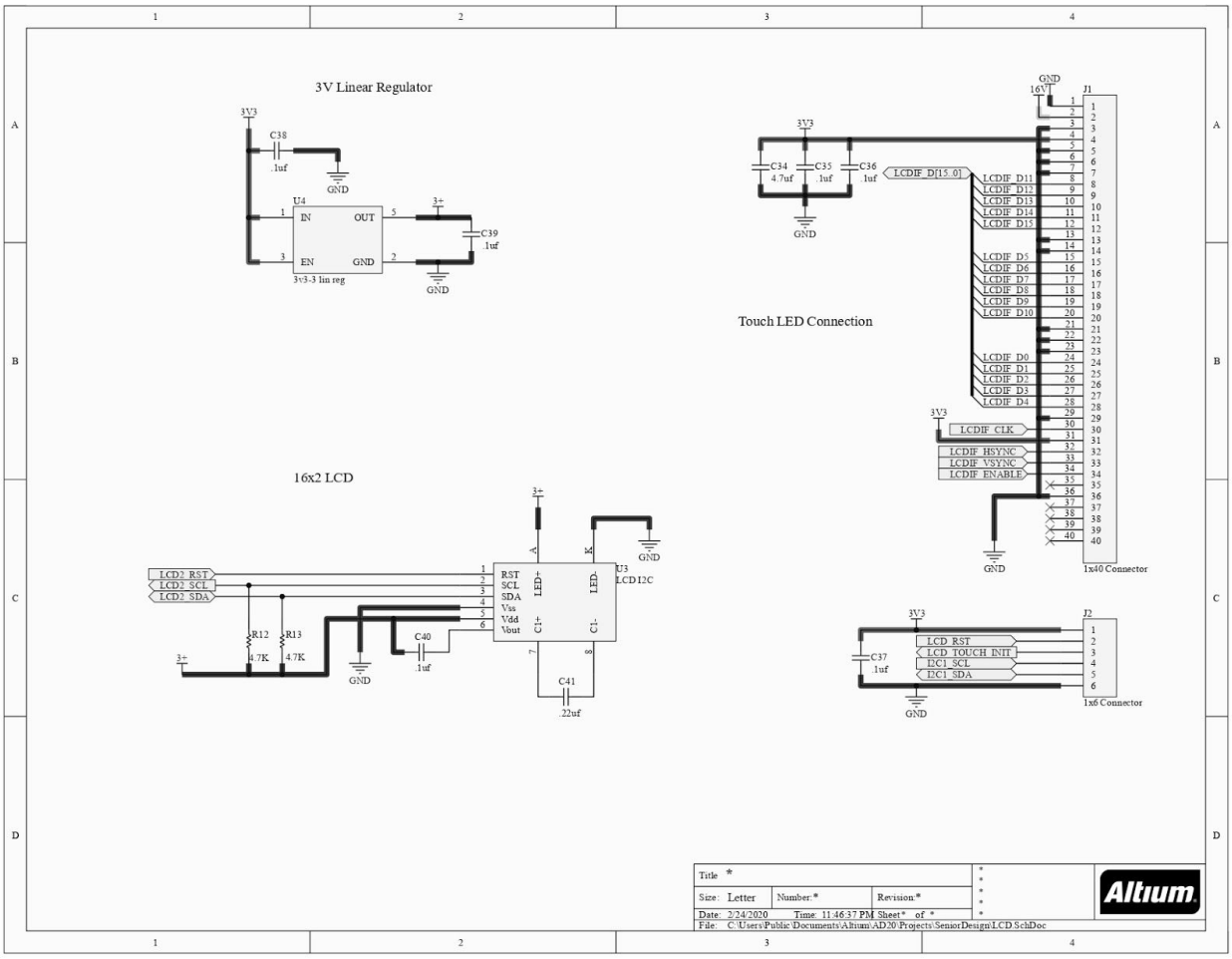
External Connections:



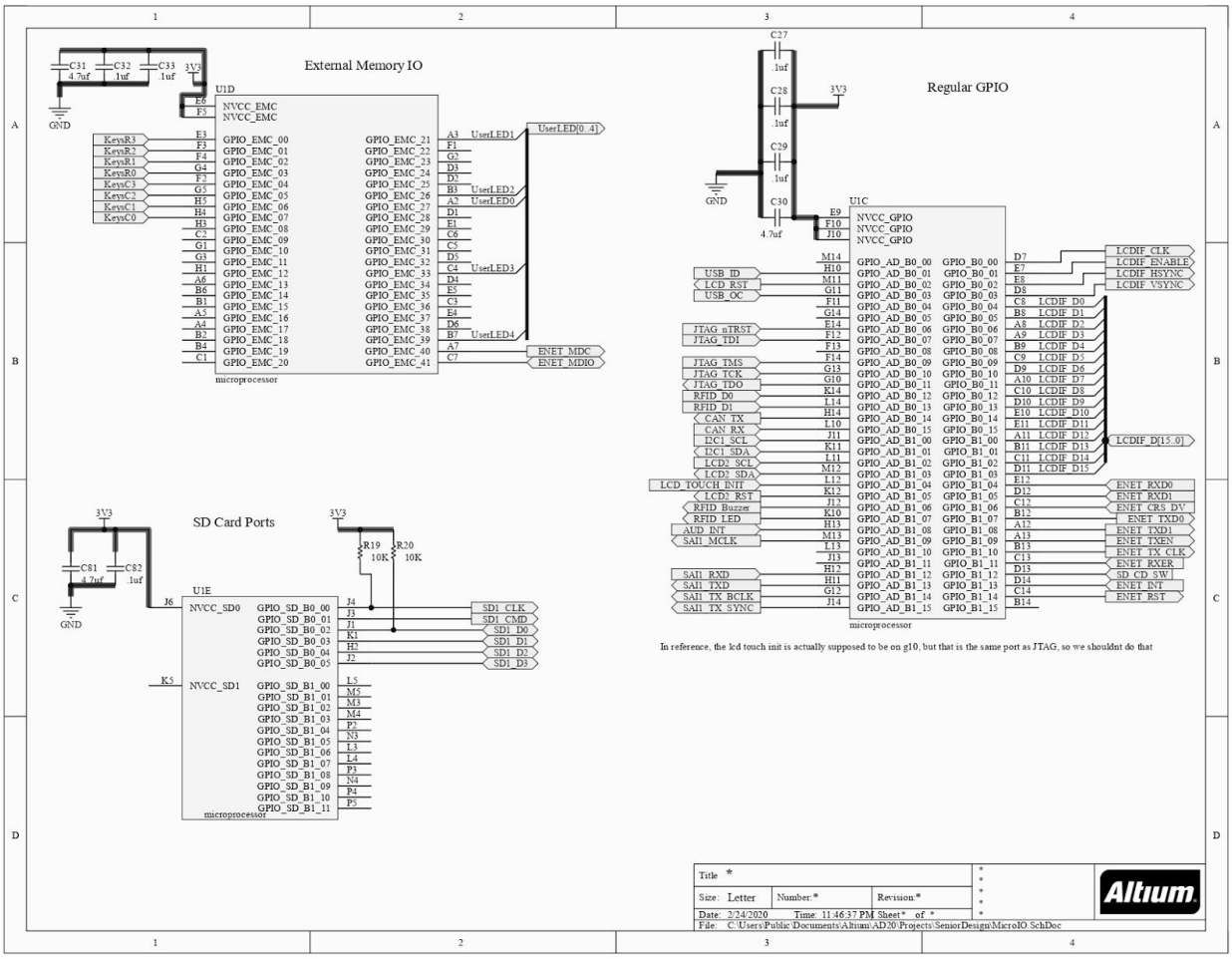
Keypad Switches



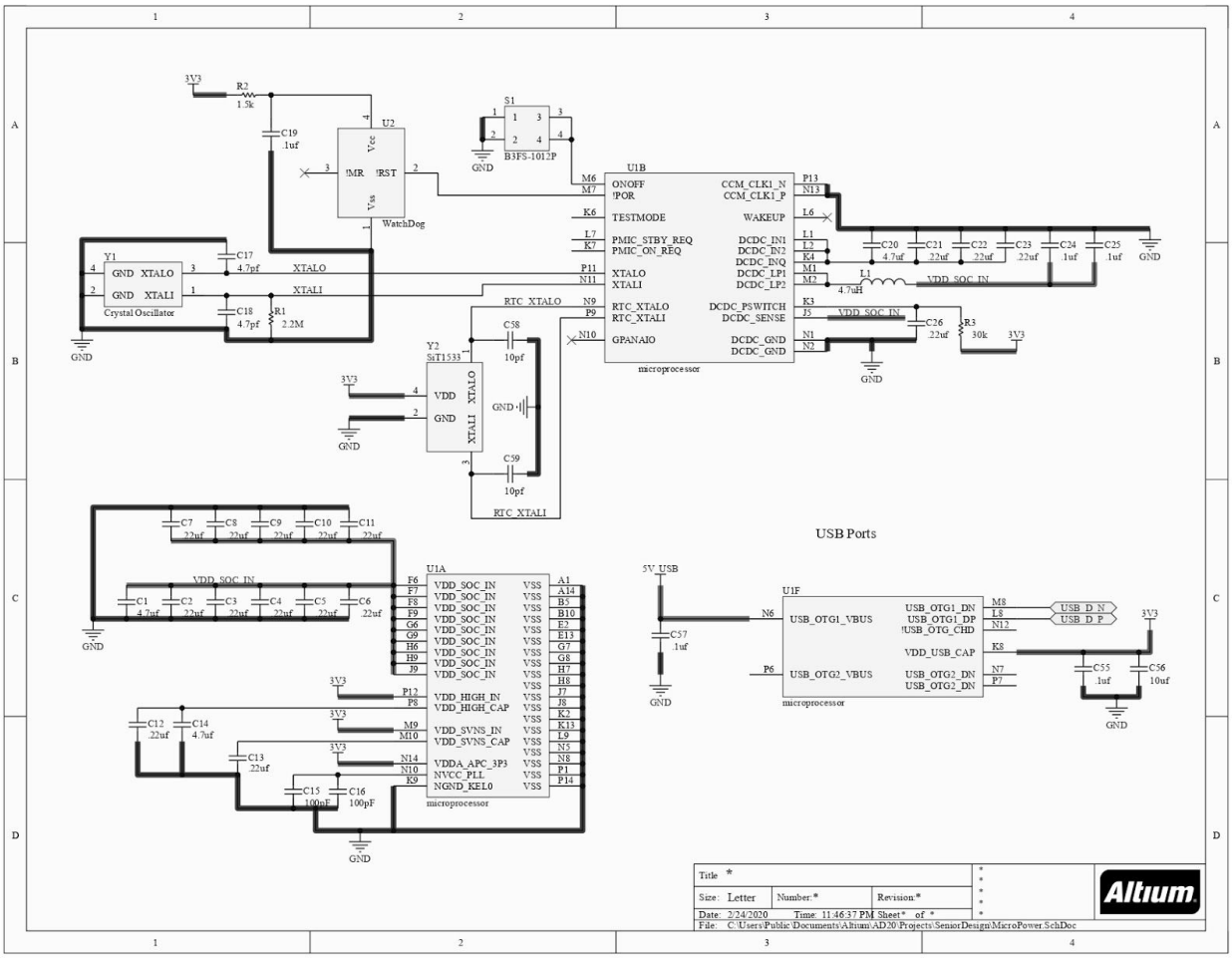
LCD Connections



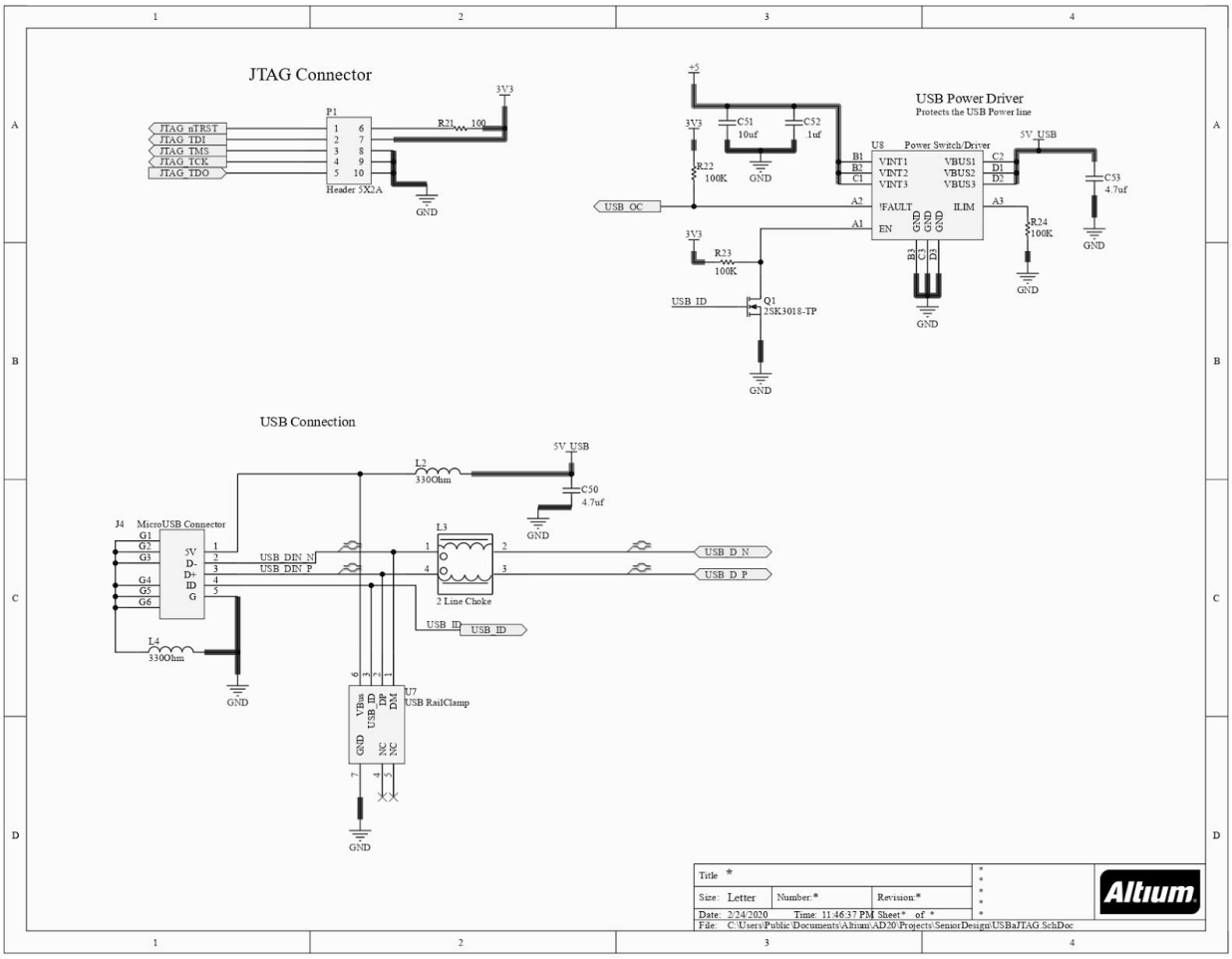
Main Micro GPIO:



Main Micro Power

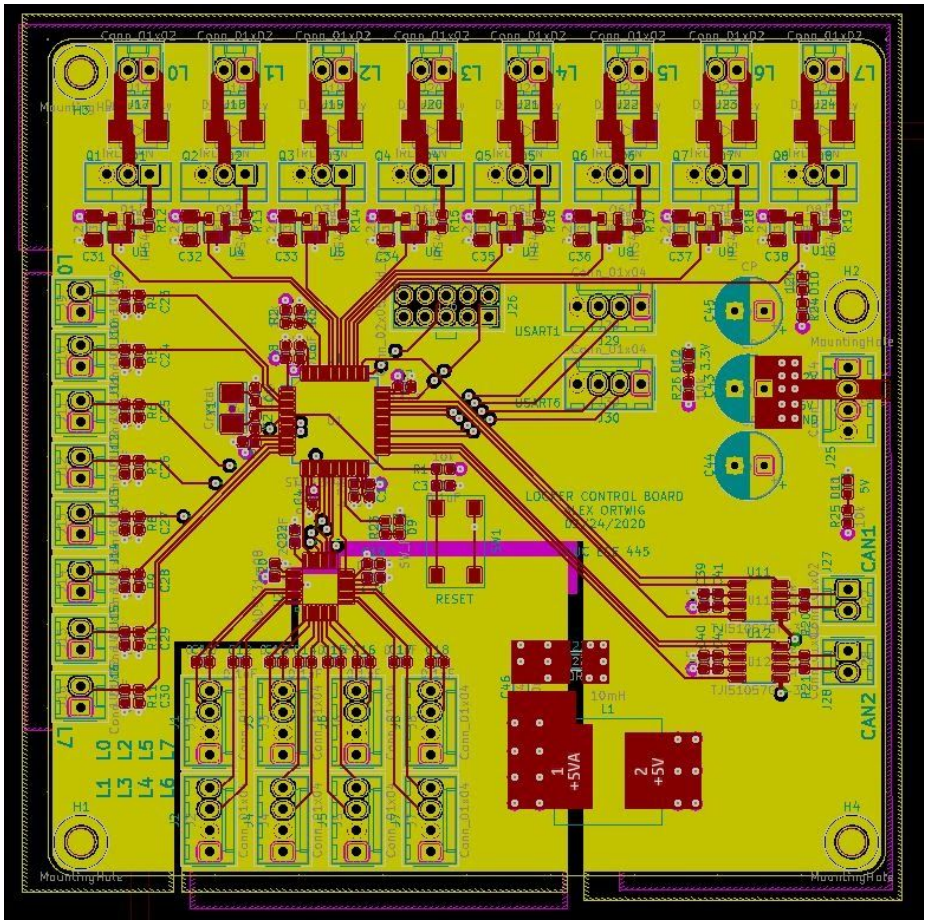


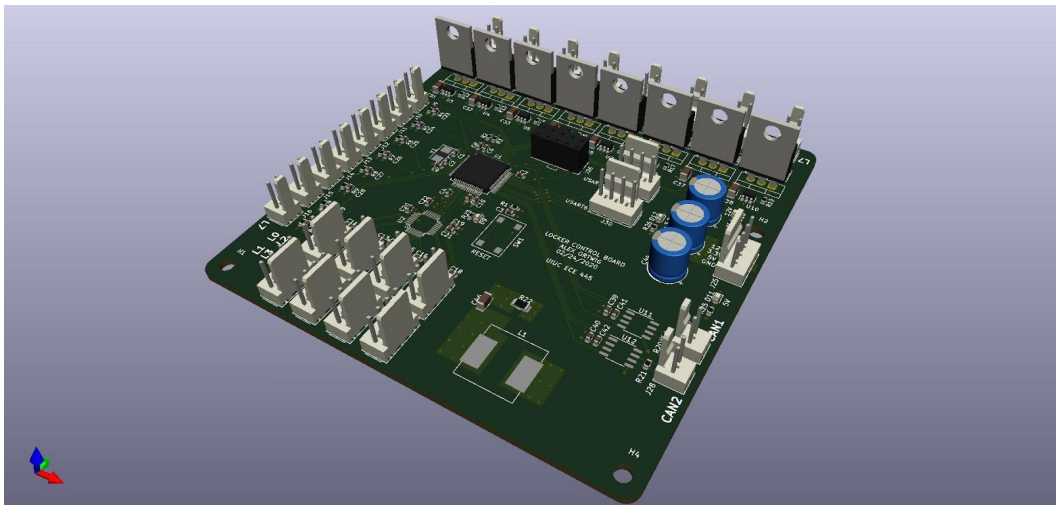
USB and JTAG Connections



2.7 PCB Design

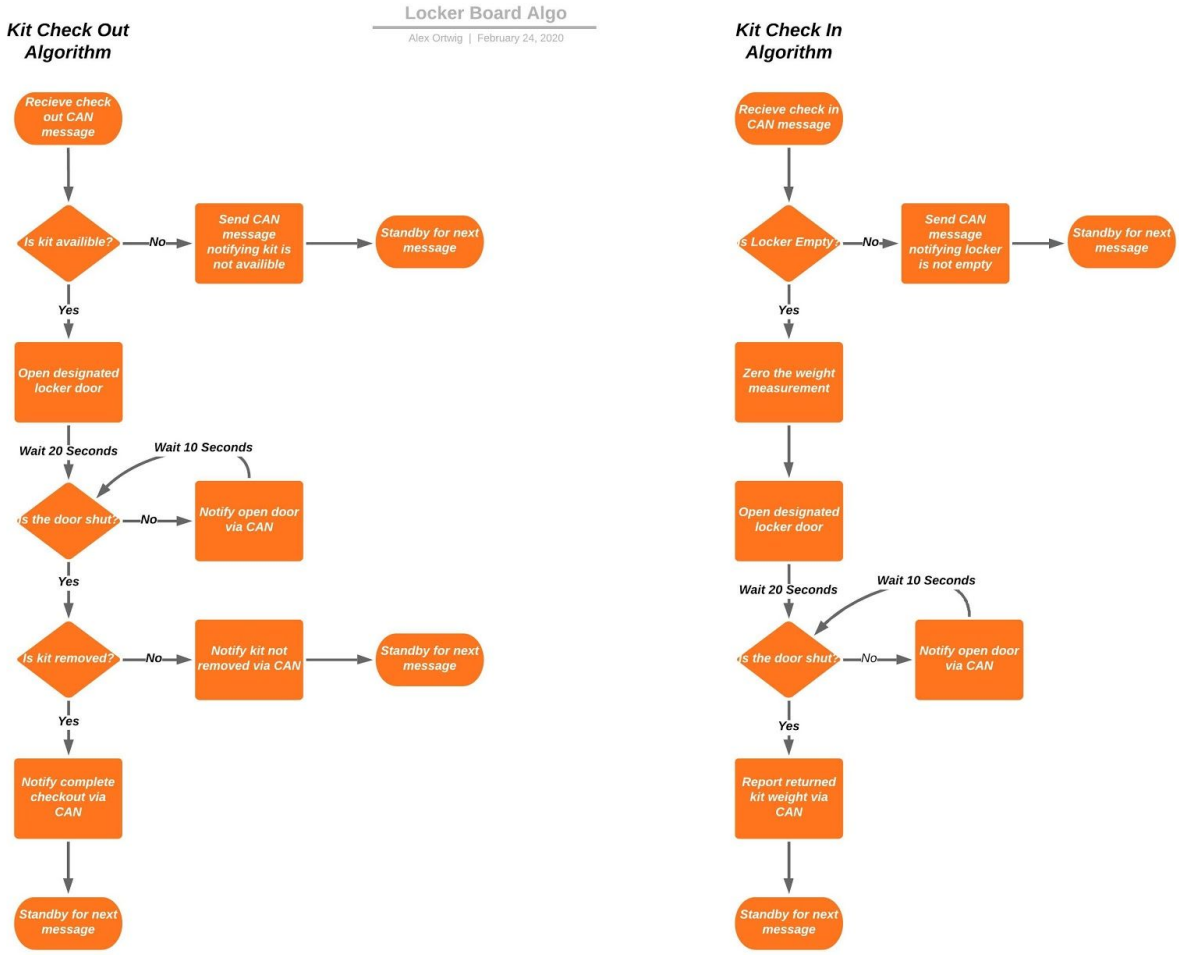
2.6.1 Locker Control Board



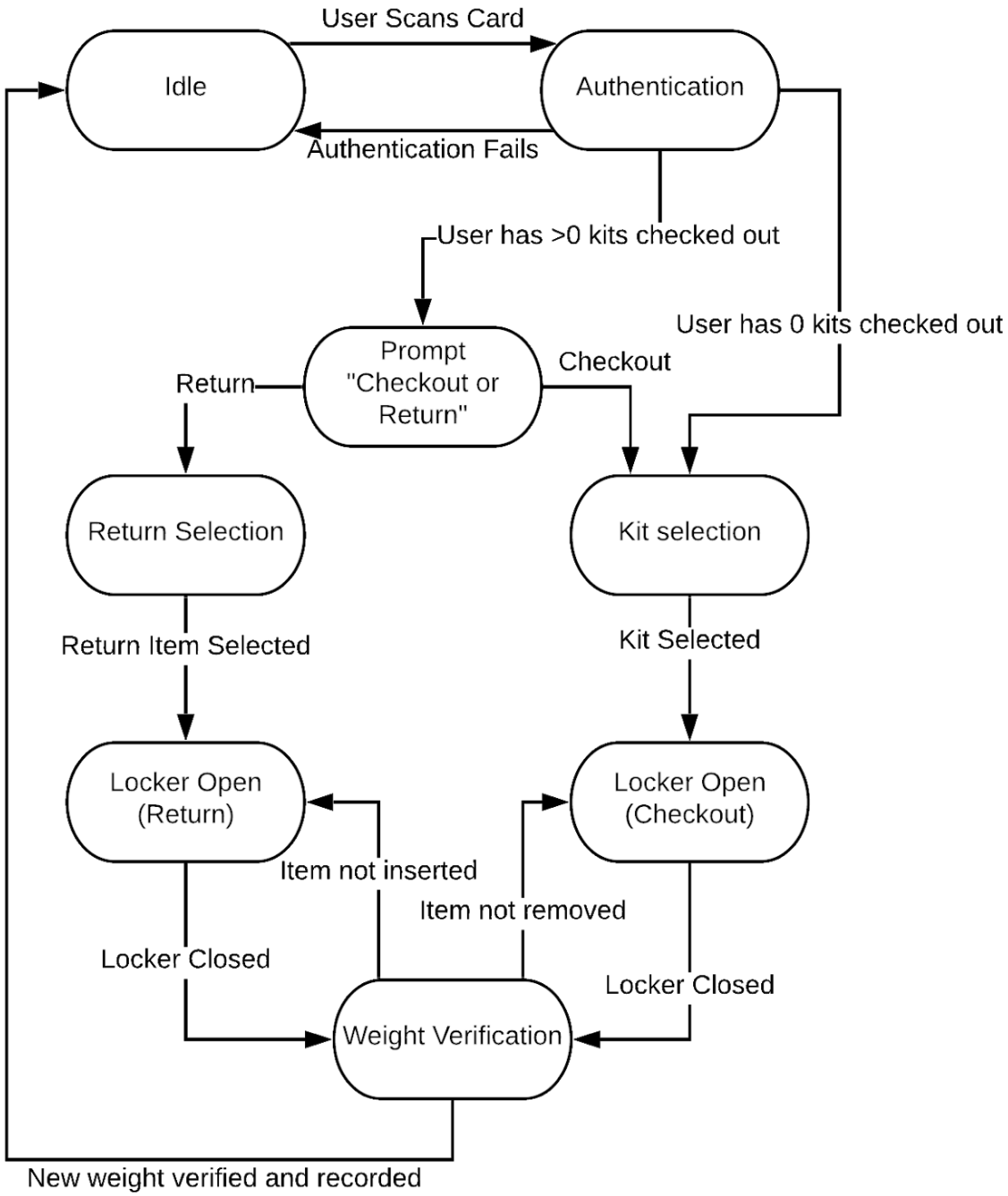


2.8 Software

2.8.1 Locker Control Board



2.8.2 User Display



2.9 Tolerance Analysis

The most important area of concern for tolerance analysis in our design is going to be the tolerance of the load cells and their measurements. The load cell we are utilizing has a rated output of “1.0 +- 0.15mV/V” meaning that there is a +/- 15% tolerance on the gain of the load cell []. This means that each individual load cell will need to be calibrated to determine the gain of the cell.

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.