Smart Bike Lock

By

James Arnold

Justin Meyer

Nate Post

Final Report for ECE 445, Senior Design, Spring 2020

TA: Ruomu Hao

8 May 2020

Based on Project No. 26 Spring 2019

Abstract

Bike thieves are very hard to stop if they bring proper cutting tools. The original solution, the Enkidu Bike Lock, used a sturdier design with a loud alarm and phone notification to discourage those thieves from targeting that specific bike with a phone app unlocking system. The Smart Bike Lock uses a conventional chain lock with a phone notification and GPS tracking to recover the bike and identify the thief. The biggest difference between the projects is that the old solution focused on prevention while the new solution focuses on the retrieval and identification of the thieves.

1 Second Project Motivation

1.1 Updated Problem Statement

According to Project 529, the world's largest bike registry, around 2 million bikes are stolen annually in North America which is a bike stolen every 30 seconds [10]. Bike locks provide a good first line of defense versus any opportunistic thieves that see unattended bikes. It is not uncommon though for those thieves to be equipped with cutting tools to remove those locks. Changing the material of the lock to not be cut is expensive and a lot of time just makes the lock too bulky or expensive and sometimes does not even work if they brought more heavy duty cutting tools. The idea of this project is to create a bike lock that lets the owner of the bike react to their bike being stolen if they're in the area or to retrieve it after if the owner is not. This GPS alternative would be cheaper than and easier to handle than alternatives. The lock will also be electronically unlocked to stop any thieves trying to pick the lock rather than using brute force. Since it is electronically controlled it is also more convenient to unlock with an app rather than a loose key

1.2 Updated Solution

Locks have been getting more advanced with cutting resistant materials like the Tex-lock or electronic unlocks like the Bitlock [1]. There are also GPS trackers for bikes such as the Sherlock Bike Tracker, this however is not a lock The past project that this is based off of used a wheel locking mechanism if the bike is moved without being unlocked properly. We see the front-locking mechanism as a weakness because if the thieves have cutting tools then the locking mechanism can be removed like any other normal lock. Our bike lock will incorporate multiple of these features like the GPS tracking, the app for unlocking, plus a lock that is difficult to remove improperly. Unlike the last attempt at this project, we are more focused on detection and recovery as our primary defense mechanism, as opposed to deterrence from the last project, since determined bike thieves will be able to bypass just about any lock.

1.3 Updated High-Level Requirements

I. The lithium polymer battery must be able to power the device continuously for 48 hours of operation and be weather-proof.
II. The lock must be able to transmit a "cut-chain" notification signaling the owner that the lock has been cut with 100% accuracy, as long as the bike has a network connection the distance between the owner and the lock is irrelevant.
III. The device must be able to track GPS location continuously to the app while operating, giving updated location every minute with a location accuracy of at least 10 feet.

1.4 Updated Visual Aid

Fig. 1 shows an example of what a user would see when tracking their device. The red pin points to where the device is located overlayed on a map, so if the user is looking for their bike they can easily locate it in the real world. Map providers like Google maps can make this functionality easy to create and make it reliable for the user.

Additionally, there will be a screen on the app to allow the user to easily see what the status of their lock is and quickly unlock it. The most important statuses will appear near the top so that the user can quickly determine if action needs to be taken to prevent their bike from being stolen.

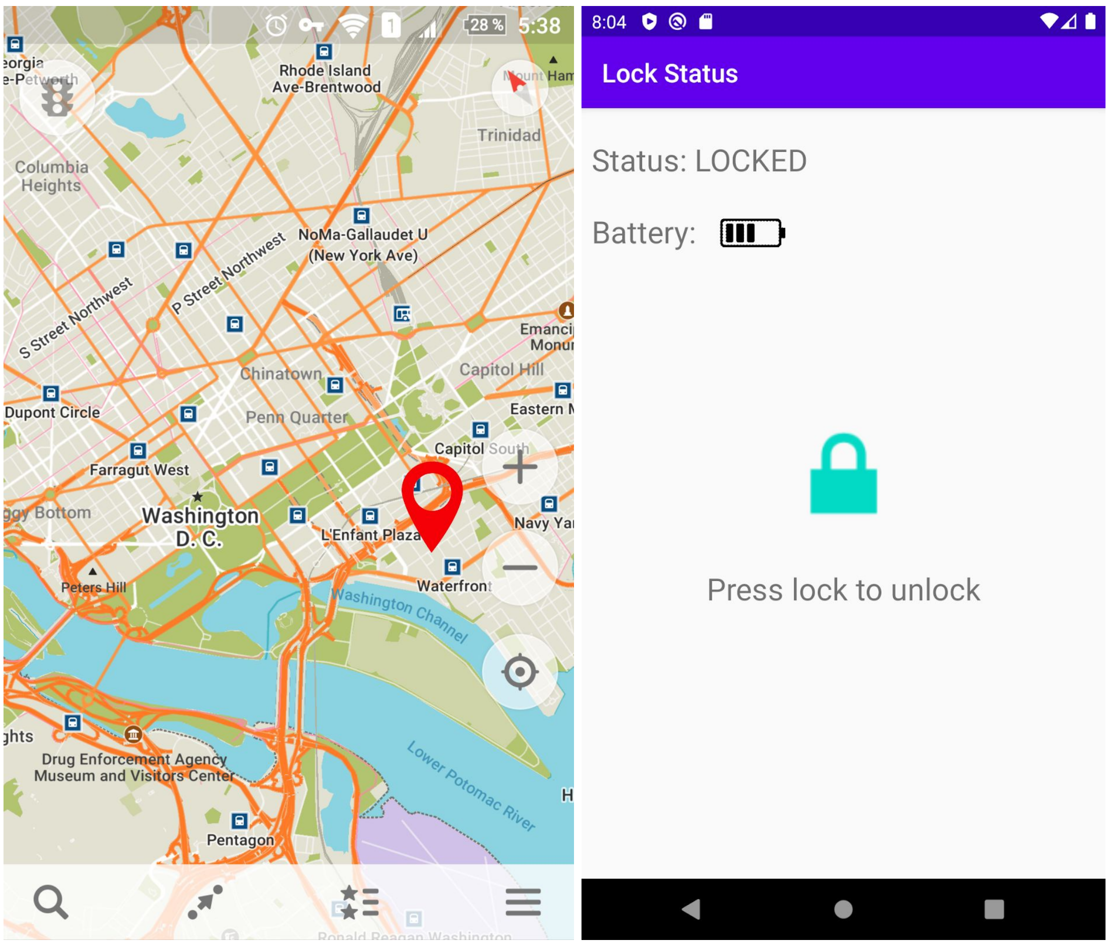


Fig. 1 A mockup of the location tracking screen (left) and lock status screen (right) for the app

1.5 Updated Block Diagram

The design overview can best be understood via the block diagram in figure 2. This figure is arranged such that all submodules receive the same voltage I.E. all components of the control module run off of the same 5V rail. Communication between the microprocessor and the individual components are performed as a serial data transfer. Communication to a phone and from the GPS satellite will use appropriate data transfer standards for those applications. Components in green are not a module in our design, but are important external components that our system interacts with.

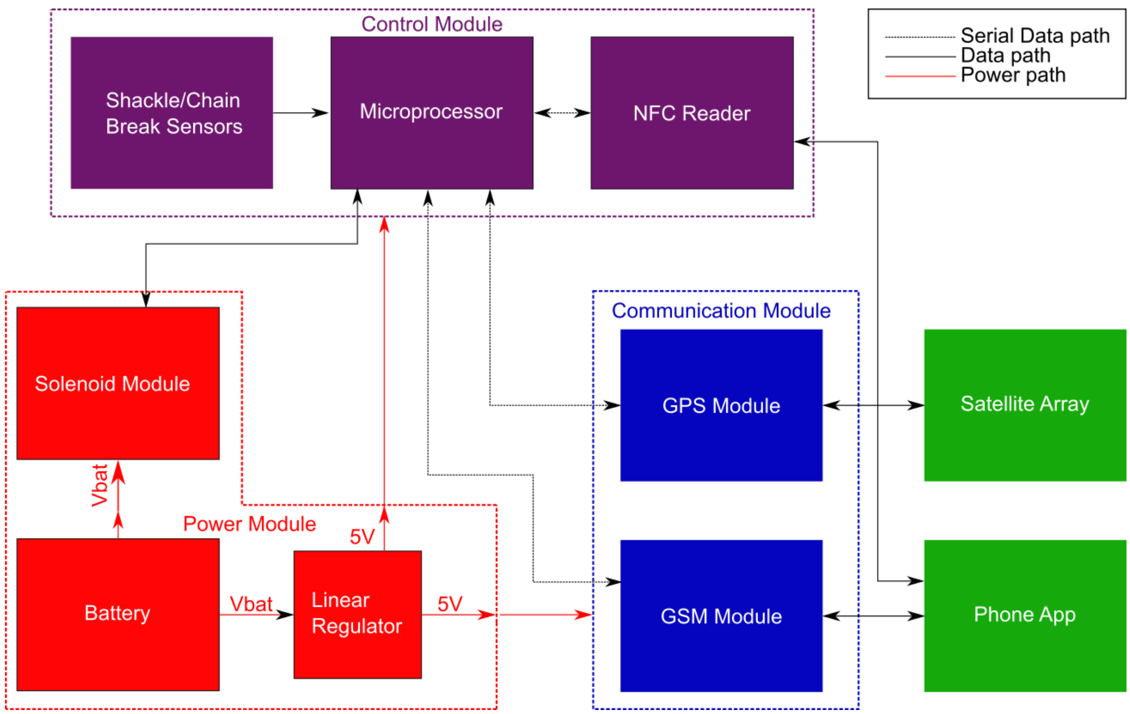


Fig. 2 Block Diagram of proposed smart lock solution

2 Second Project Implementation

2.1 Physical Design

The physical design of the lock consists of several components. Firstly, there is the lock body which provides the bulk of the mechanical stability for the whole system and houses the electronic components. The lock body concept can be seen in figure 3, with an etched indicator of where a user would place their phone to perform an NFC handshake as well as the slots for the shackles. Figure 4 depicts the rear side of the lock body with the mounting mechanism attached. The mount is designed to close around the main portion of a bike frame, to be secured and tightened by a pair of proprietary screws which are incompatible with standard driver heads. In addition these screws will be hidden with small rubber or plastic caps. These features seek to deter a thief from removing the lock itself which would prevent us from tracking the stolen bike. The shackles, as seen in figure 5, hold a chain in place. One shackle will be attached permanently to the lock body along with one end of the chain. This is to allow a seamless and secure connection of the short-detection wire. The other shackle will be held in place by our solenoid bar and can be removed. The wire connection on this side will be placed somewhere discrete, close to the hole for the shackle. An image of the full assembly can be seen in the appendix section 1.7.

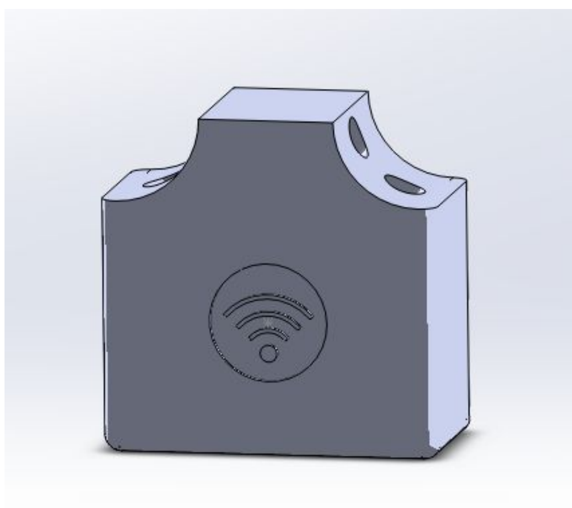


Fig. 3 Front side of the lock body with shackle holes and NFC etching displayed

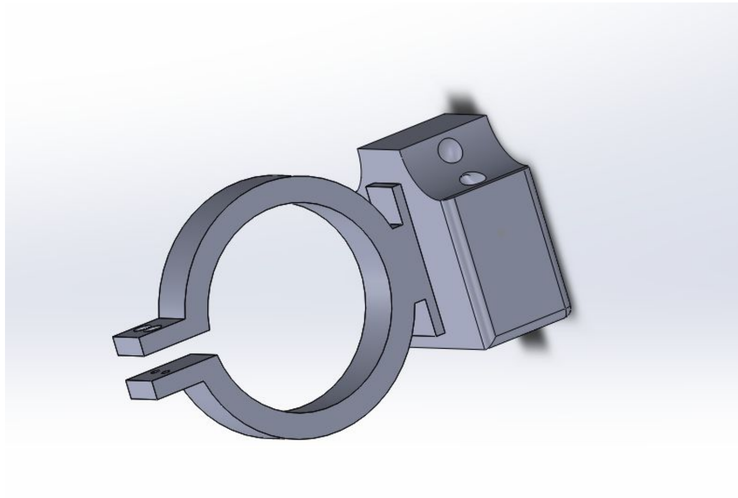


Fig. 4 Rear side of lock body demonstrating frame mount mechanism

Fig. 5 Concept for a removable shackle

2.2 Battery Charger

To implement that battery charger for our pack, we need just a single main IC and some small passive components. Texas Instruments makes an excellent single-cell charging IC called the BQ24040, pictured in figure 6. The IC is a mere 2mmX2mm and is able to provide all of the functionality we need for charging with just a 5V rail. This rail is supplied via a micro USB connection.

Fig. 6 TI BQ24040 LiPo charging IC [2]

To charge, each battery will in turn run through a simple charge curve consisting of a constant current portion followed by a constant voltage portion. The finer details are best understood via figure 7. The BQ24040 enacts such a curve with its built-in control loop which uses user-determined components to observe the system and control it properly. These components include resistors to program the current levels, LEDs to give charging indicators to the end-user, filtering capacitors, and a thermistor to monitor temperature.

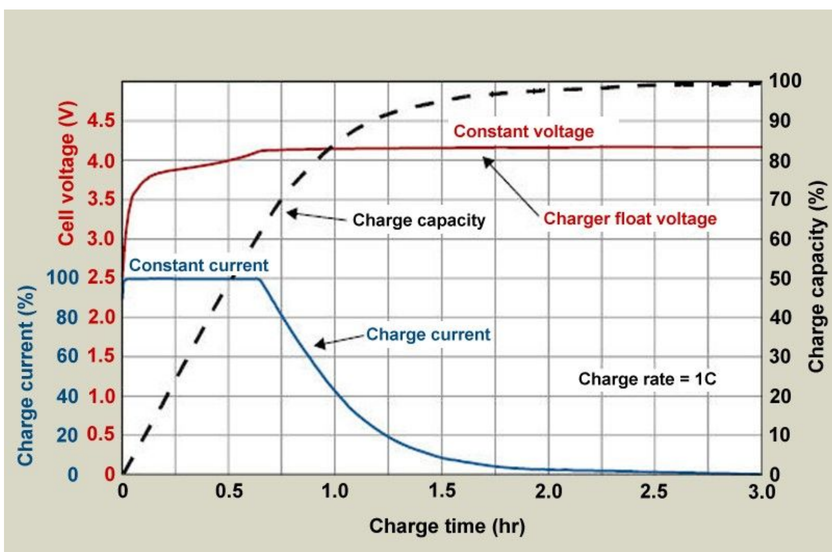


Fig. 7 Standard LiPo charging curve [3]

A model of our specific implementation is displayed in figure 8. The resistor connected to ISET is 8.7k Ohms which corresponds to a maximum charge current of 240mA. The 1k resistor connecting to PRE-TERM designates that charging should terminate when the current draw is 1/20th of the maximum current as per the battery's specifications. ISET2 going to +5V indicates that we will allow up to 500mA to be drawn from the input source. This is practical for essentially any USB power supply one might own. TS must connect to a thermistor with the specifications that it is a 10k NTC (Negative temperature coefficient) thermistor with a Beta value of 3370 for a range of 25C-85C. A suitable selection would be the NTCLE101E3C90173 from Vishay Semiconductors[4]. EP is a representation of the large thermal dissipation ground pin on the IC. This pin is internally connected to VSS but should be given its own connection to ground. PG is a “power good” indicator which is not something we wish to concern our end-users with. The CHG pin is connected to the drain of a FET which the control loop turns on and off. If the FET is on, current will conduct through the LED and indicate to the user that charging is occurring. The input and output each have a bypass capacitor of 1 uF with the purpose of directing high frequency noise to ground. All components would be size 0201 SMD excluding the thermistor which will use THT leads and the LED which is size 0603 SMD.

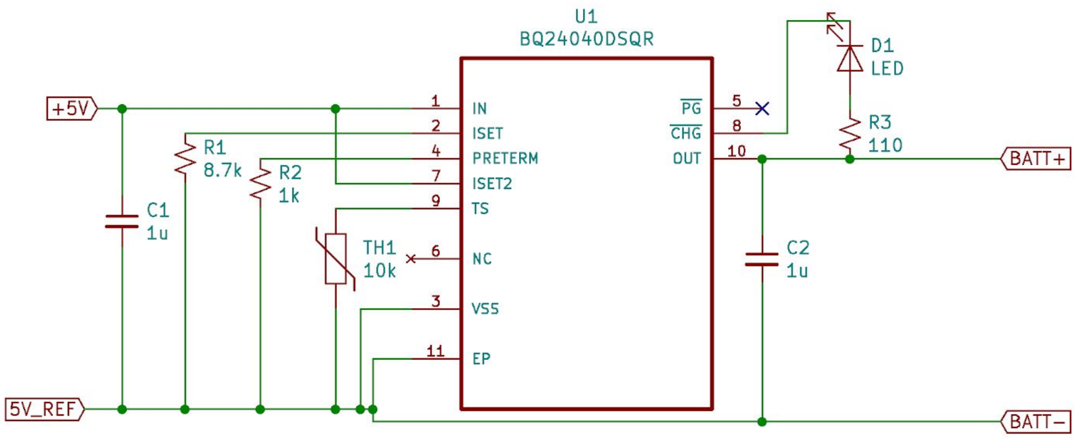


Fig. 8 Model Implementation of charging IC

In order to implement this for both batteries, we would construct a control loop such that one battery will charge first and when we detect that one charge cycle has completed we switch which battery is charging. We can know if charging has completed for the first cell by checking when IN receives +5V, then polling the node between the LED and its resistor which will be Vf of the LED when charging is occurring and OUT when it is done. The switching could be implemented by several small FETs as displayed in figure 8. Placing the FETs in series with the cells in this manner is not problematic. For instance, a good candidate for these FETs is the SI2342DS-T1-GE3, which has an “on” resistance of 17mOhms. At our 240mA, this results in an extra drop of about 5mV which is negligible given the scale of the battery voltage. In Mode I, we charge BT1 by turning on Q2 and Q3. In Mode II, we charge BT2 by turning Q1 on only. Q3 is necessary in this circuit as protection for BT1. Without Q3, Mode II would cause BT1 to short itself and when charging is over charge could leak from BT2 to BT1 through the body diode of Q1. A more elegant solution would have been to use a relay of some sort which would require fewer I/O connections to the microcontroller, but this would have almost certainly required more physical space.

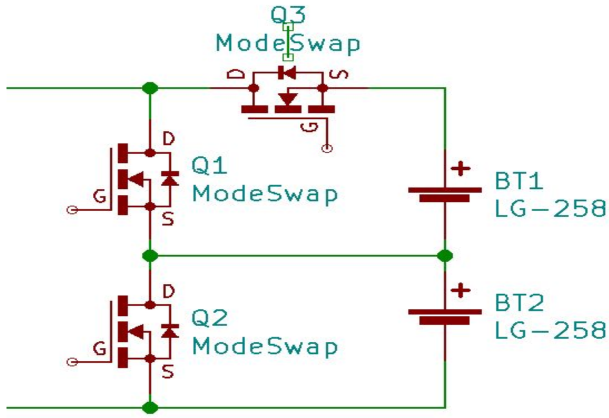


Fig. 9 MOSFET circuit for charging the two batteries independently

2.3 Control Module

2.3.1 Microprocessor

A small microprocessor is needed to control the lock, as well as communicate the status of the device to the owner. A simple controller like an ATmega 328 (an arduino) can perform this function. [11] However, both the GPS and Wireless modules require a serial connection, so the microprocessor must be able to support connections to each. Due to the 328's popularity, robust software serial libraries already exist, so it is simple to use the digital pins already present as additional serial connections.

Since the ATmega 328 is a very popular processor, schematics for connecting it into external circuits are widely available. In particular, the Arduino Pro Mini's design will be suitable for our project, with unused I/O leads removed to save space. Fig. 10 Below shows this reference design. By removing accessory components, such as the power LED, we can achieve significant power saving, around 5 mA when the device is in active mode.[12] Additionally, we can remove the voltage regulator used in the schematics since we will be using a separate 5v regulator from our power module.

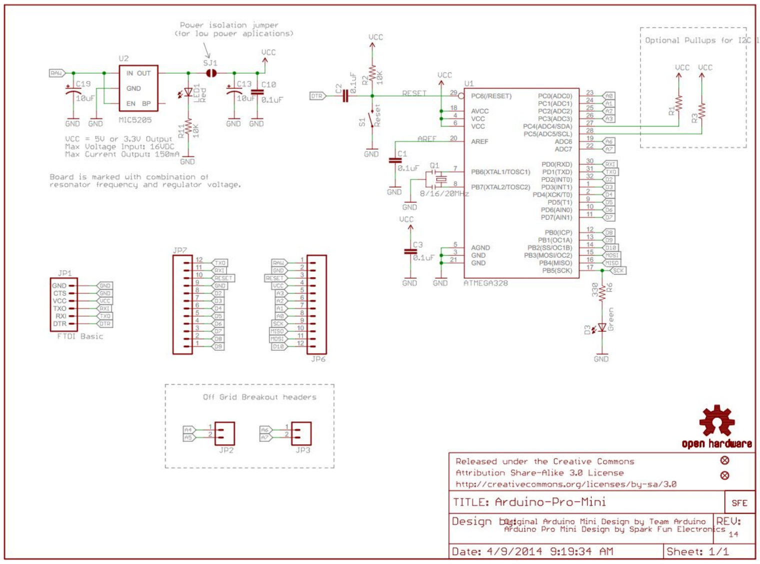


Fig. 10 A reference design for the ATmega 328 to use in our design. Includes all components necessary for full functionality.[11]

2.3.2 NFC Reader

The lock must be able to acknowledge when the user wants to open it, so an NFC reader will be built so that the user can hold their phone while using the application to be able to unlock the lock. NFC is better than other communication methods because it does not require sending data over an internet connection, potentially providing more attack vectors.

2.3.3 Lock Status Sensors

To detect if the lock shackle were broken, an infrared emitter/sensor pair can be included to detect if the components were separated. A single mA or less would be sufficiently powerful to detect a separation, since the sensor will not be exposed to sunlight or other forms of infrared light.

For detecting the status of the chain, we would conceal a small 25 AWG wire running around the length of the chain and run current through it sourced by the microcontrollers internal pull-up resistors. If the chain were cut, the wire would be as well and we would detect an open circuit. The pullup resistors connected to the digital pins on the ATmega 328 are 50KΩ, and with a 5v supply, will apply 10μA of current across this wire. The low voltage and current make it so that cutting the chain is not dangerous, consumes little power, and will still be able to detect the cut chain easily.

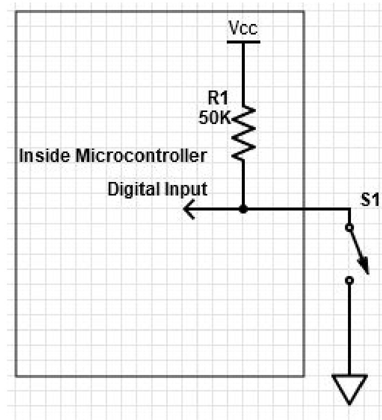


Fig. 11 A demonstration of the chain break sensor. Power is provided by the microcontroller.

2.4 Communication Module

2.4.1 GPS Module

A GPS module will be used to track the location of the lock and the bike attached to it, so that the owner can find their bike in the event that it is stolen or lost. This module will communicate with the microprocessor via a digital serial interface to send data over cellular to the owner's smartphone.

2.4.2 GSM Module

The lock will send location and security information to the users phone via a network connection across the internet. The device should be able to communicate in as many places as possible, so a GSM radio will achieve this while using infrastructure already built in place. It will also communicate via a digital serial interface, using a separate port from the GPS module.

2.5 Software

2.5.1 Mobile application

The user of the lock can interact with the software system to learn what the status of the lock is and where the device is located. It would allow the user to unlock the lock using NFC and see its location using the GPS coordinates generated by the device. The mobile application should also be able to provide the user with battery charge information so the user can know when the lock needs charging. Additional information about the layout can be found in section 1.4.

2.5.2 System Control Loop

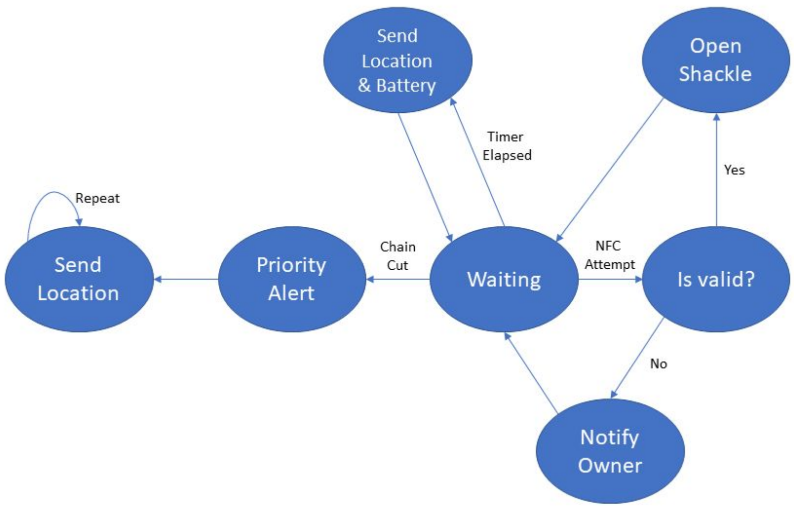


Fig. 12 Flowchart showing the high-level functionality of the lock. Includes security measures and low power mode.

The microcontroller on board the lock will be responsible for running the control loop on the device, where it will verify security and periodically send information to the owner about the status. Fig. 12 shows an overview of this functionality, where the device sits in a low power waiting state until it receives an input. If there is an NFC attempt or a timer wake up, then the device will return back to a sleep state until a new input is received. However, if the chain is cut it will not return to low power, since it will be constantly updating to send the position to the owner.

3 Second Project Conclusions

3.1 Implementation Summary

For this project, all active electronic components, like the microprocessor, solenoid shackle, battery, battery charge, GSM, and NFC module needed have been picked out by all team members with a list of passive components required to use them properly. Also an initial mechanical chassis has been designed by James. This means the electronics can be tested to see if they work based on the high level requirements and verification techniques that were listed in our design document. So the control loops can be tested for the “cut-chain” notification, and the GPS could be tested for the expected accuracy. Once those subsystems are confirmed to be working, the battery life of the system as whole can be observed. There is also a CAD design that could be shown to the machine shop for improvement and machining.

3.2 Unknowns, uncertainties, testing needed

The largest unknown for this project is the mechanical lock part of the project. There is no access to the machine shop and we have none of the machines available. This leaves a lot of uncertainty on the integrity and security of the lock. This includes the solenoid shackle strength, as in, can the shackle just be moved out of the way by some thin piece of metal. There is also no way of knowing if the GPS tracking chassis is as hard to remove as we believe it is, if the lock is too easy to remove then the lock can not track the thief as intended. A uncertainty with the whole project is the server on which the app will be hosted on. The server though is outside the scope of the class so it is not discussed in depth. Without the server we also can not test the GPS accuracy or the reliability of the notifications from the lock being opened improperly.

3.3 Ethics and Safety

In the case of ethics, designing a smart lock for a bike is congruent with both the IEEE code of ethics and the ACM code of ethics. Most requirements of these codes are not strictly applicable to this project. Beyond non-applicable codes, the concept of a smart lock for a bike serves to integrate technology into society in a manner which provides individuals with greater security and comfort which is a concept represented in both codes. This concept is reflected most accurately by code 1.1 of the ACM code of ethics [9] and code 5 of the IEEE code of ethics [8]. In the design of such a commercial product with competitors, it is also imperative that we respect patent and copyright law. In designing our product, we will research competing products which will allow us to understand various industry standard design features whilst allowing us to differentiate our design from others both for the purpose of innovation and to respect the intellectual property of competing designs.

To stay safe, the current through the wire has to be sufficiently small as not to heat up and damage itself but also keep anyone from shocking and hurting themselves. The wire is just there to notify of a cut chain, not to hurt anyone. The heat issue also applies to the battery so we need to make sure we can sink that heat and keep it from burning up. Heat concerns for the internals can be handled by a thermistor and external thermals would be calculated based on wire specifications. This lock design does not have any inherently dangerous components that would reasonably be expected to cause damage to any person or property in the vicinity. In the case of a malicious attempt to break the lock, some amount of shrapnel could be produced or a battery failure could be caused, however the responsibility for the possible damages in this scenario are assumed to lie with the person destroying the lock i.e. due to gross misuse. As for regulations, we would primarily expect to need to comply with FCC standards and standards for rechargeable batteries. In the case of batteries, most responsibility seems to fall with the battery manufacturer and the end user. This includes strict regulations on the transport, manufacturing, and testing of such batteries [13]. It is difficult to find any material pertaining to regulations that the designer of a given product is burdened with. Because we are performing Radio Frequency (RF) communications, our device needs to be authorized by the FCC for use [14].

3.4 Project Improvements

The most obvious improvement is the shackle holding the GPS tracker to the bike frame. We will be hiding the proprietary screws but it is not too hard to find them. As of this iteration we are still relying on the assumption that the lock will stay on just long enough for us to report the bike as stolen and having the police go to the location to retrieve the bike. With more time to complete this project we could pick more efficient or even make custom parts that consume less power but still perform the same function. This would improve our battery life without increasing the amount of batteries needed. This would also optimize the cost as well because presumably the lower power components would be cheaper as well. Optimizing the control loop would also be able to reduce power consumption by reducing the amount of cycles we have to compute or shortening the cycles which keeps the microprocessor in standby mode for longer.

4 Progress made on First Project

Our first project was a multi-phase maximum power point tracker for use with the solar panels on the roof of the ECE building. Overall, the project goal was to build a switching power supply that could extract the maximum power available from a partially shaded solar panel, output this power as a regulated DC rail, and transmit information about the power generation over Wi-Fi. A basic block diagram of how the solar panel was split up to allow for multiple maximum power point tracking devices can be seen in figure 13. The most time-intensive contribution to the project was that of selecting all of the components for use including the specifications for passive components. Appendix section 1.1 includes a table detailing all of these components. All members contributed to the formation of this table. James specifically created two very in-depth tolerance analysis sections for two different topologies of a necessary part of the circuit called the snubber. These write-ups can be found in appendix section 1.2 and 1.3. James also created a CAD model of a possible enclosure design for the system which can be viewed in appendix section 1.4. Justin performed a great deal of calculations for the specifying of individual passive components. The descriptions for how these design decision were made are under appendix section 1.5. Lastly, Nate performed extensive work in designing verification methods for the networking portion of the project. These verifications are very specific and are exceptionally suited to giving us a quantifiable understanding of the networking performance for the system. Information pertaining to these methods is contained in appendix section 1.6.

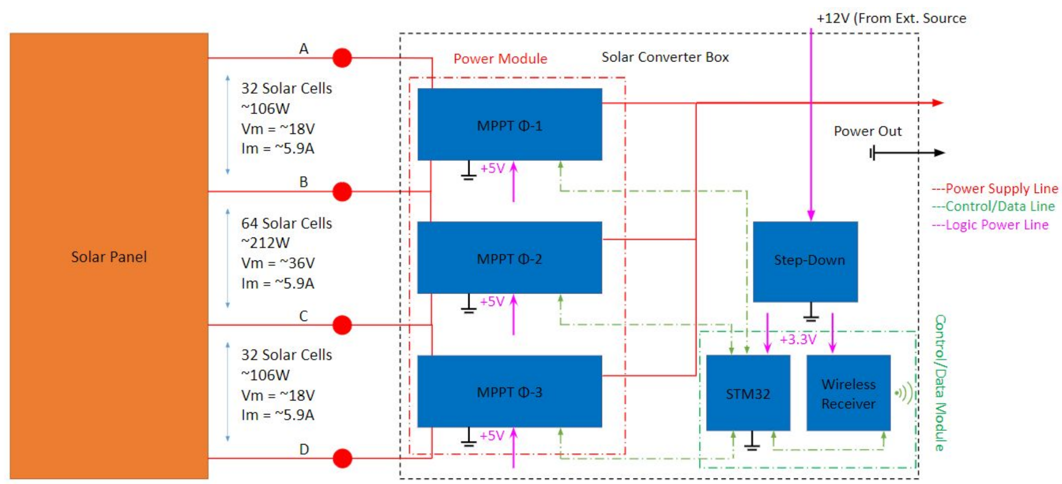


Fig. 13 A basic block diagram for the Multiple Maximum Power Point Tracker project.

5 References

[1] “These 7 smart bike locks combine technology and functionality”, bikecitizens.net, 2017. [Online] Available: https://www.bikecitizens.net/10-smart-bike-locks/ (accessed 31 March 2020).
[2] “Best GPS Bike Trackers and Smart Locks”, postscapes.com. [Online] Available: https://www.postscapes.com/gps-bike-tracker/ (accessed 31 March 2020).
[3] “Dual 4-Line to 1-Line Data Selectors/Multiplexers” Texas Instruments. [Online] Available: http://www.ti.com/lit/ds/symlink/sn74ls153.pdf (Accessed 2 April 2020).
[4] “Datasheet - ST25R95 - Near Field Communication Transceiver” ST.com [Online] Available: https://www.st.com/resource/en/datasheet/st25r95.pdf (Accessed 2 April 2020)
[5]”Delta Electronics DSOS-0416-24D” DSOS-0416-24D Digikey [Online] Available: https://www.digikey.com/product-detail/en/delta-electronics/DSOS-0416-24D/1144-1401-ND/6599949 (Accessed 2 April 2020)
[6] “NEO-6 u-blox 6 GPS Modules” [Online] Available: https://www.u-blox.com/sites/default/files/products/documents/NEO-6_DataSheet_%28GPS.G6-HW-09005%29.pdf (Accessed 2 April 2020)
[7]”Adafruit Industries LLC 258” 258 Digikey [Online] Available: https://www.digikey.com/product-detail/en/adafruit-industries-llc/258/1528-1838-ND/5054544 (Accessed 2 April 2020)
[8] “7.8 IEEE Code of Ethics” ieee.org, 2020. [Online] Available: https://www.ieee.org/about/corporate/governance/p7-8.html (Accessed 2 April 2020)
[9]"ACM Code Of Ethics", *Acm.org*, 2020. [Online]. Available: https://www.acm.org/code-of-ethics. (Accessed 2 April 2020).
[10] “Every 30 Seconds, One Bike Is Stolen. Here’s How to FIght Back” bicycling.com, 2019. [Online] Available: https://www.bicycling.com/news/a28846575/project-529-bike-theft-data/ (Accessed 14 April 2020)
[11] “Arduino Pro Mini.” Arduino, 2020. [Online] Available: https://store.arduino.cc/usa/arduino-pro-mini (Accessed 15 April 2020)
[12] Jeff Barber. “GPS Accuracy Test: GPS vs. Smartphone vs. Cyclocomputer (Round 2).” SingleTracks, 25 January 2017. [Online]. Available: https://www.singletracks.com/mtb-gear/gps-accuracy-gps-vs-smartphone-vs-cyclocomputer/ (Accessed 15 April 2020)
[13] Legal Information Institute“49 CFR § 173.185 - Lithium cells and batteries“ Cornell Law School [Onlion] Available: https://www.law.cornell.edu/cfr/text/49/173.185 (Accessed 17 April 2020)
[14] FCC “Equipment Authorization Approval Guide” FCC. [Online] Available: https://www.fcc.gov/engineering-technology/laboratory-division/general/equipment-authorization (Accessed 17 April 2020)
[15] 258 Lithium Ion Battery. Digikey. [Online] Available: https://www.digikey.com/product-detail/en/adafruit-industries-llc/258/1528-1838-ND/5054544 (Accessed 17 April 2020)

[16] 1-cell 1-A linear battery charger with 4.2-V VBAT and Temperature Sensing. Texas Instruments. [Online] Available: https://www.ti.com/product/BQ24040
[17] BQ24040DSQR IC Battery Charger. Digikey. [Online] Available: https://www.digikey.com/product-detail/en/texas-instruments/BQ24040DSQR/296-37142-1-ND/4505899
[18] "BU-409: Charging Lithium-ion." Battery University. [Online] Available: https://batteryuniversity.com/learn/article/charging_lithium_ion_batteries
[19] NTCLE101E3C90173 Transducer. Digikey. [Online] Available: https://www.digikey.com/short/p19m2h?_ga=2.216010710.138636762.1588638539-1533161776.1582587792&_gac=1.90520936.1588638539.Cj0KCQjw-r71BRDuARIsAB7i_QNm7gtdTjtOolBGbwOWk0IhRuHNAB-WHYI31oINloxUaNbTS1zYxDgaAmFaEALw_wcB
[20] SML-LX0603GW-TR Green LED. Digikey. [Online] Available: https://www.digikey.com/product-detail/en/lumex-opto-components-inc/SML-LX0603GW-TR/67-1549-1-ND/304360
[21] SI2342DS-T1-GE3 N-MOSFET. Digikey. [Online] Available: https://www.digikey.com/product-detail/en/vishay-siliconix/SI2342DS-T1-GE3/SI2342DS-T1-GE3CT-ND/5805424
[22] Igor. "Arduino Power Consumption Normal & Sleep." Gadget Makers' Blog. [Online] Available: https://www.gadgetmakersblog.com/arduino-power-consumption/

Appendix

1 Work on Previous Project

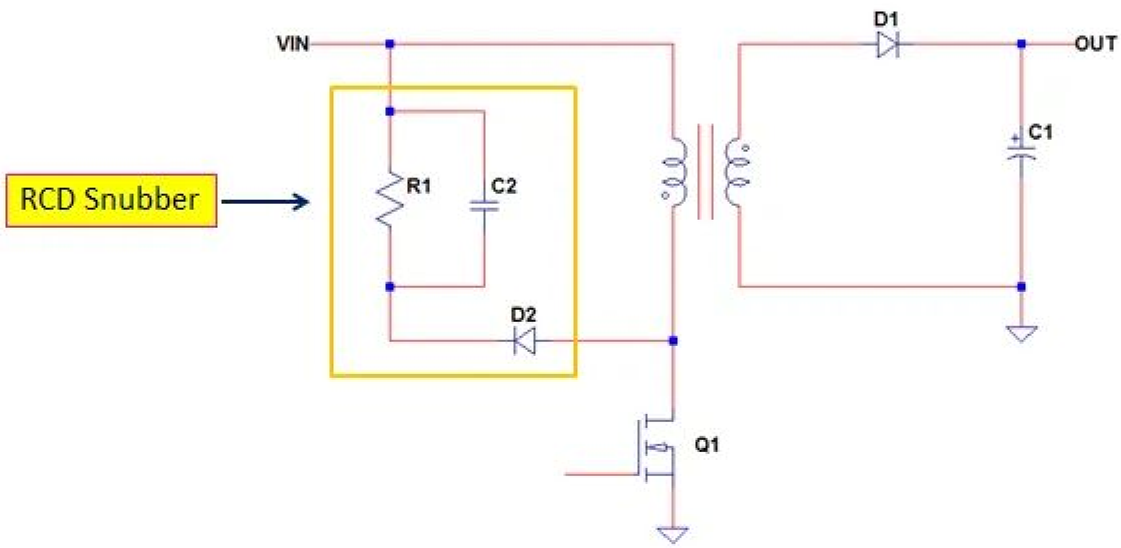
1.1 List of specced parts and components from original project

Description	Manufacturer/Part No.	Quantity	Cost	Total
STM32F103 Daughterboard	Various	1	$5.00	$5.00
ESP-01 Wifi board	MakerFocus #SE154	4	$3.50	$13.98
ST-Link v2	DAOKI #BG-US-973898	1	$6.29	$6.29
Schottky Diode	VBT1045BP-E3/8W	12	$0.88	$10.56
Output Capacitor	EEU-FM1H471	4	$0.24	$0.96
Output Inductor	157D	4	$17.34	$69.36
Transformer	753013441	4	$3.88	$19.52
MOSFET	TK7S10N1Z,LQ	4	$1.33	$5.32
Snubber Resistor	30k SMD 1210 RES	8	$.12	$.96
Snubber Capacitor	1uF ALUM ELEC CAP	4	$.25	$1.00
Total				$132.95

1.2 Write-up describing process for speccing an RCD snubber in a switching power supply

In a forward converter, we use a transformer to achieve isolation and/or a specific desired step-up from the turns ratio. In this case, we don't seek to utilize the inductance of the transformer for any purpose unlike other converter topologies which utilize the stored energy in the transformer. So, we select a transformer that has very low inductance with the caveat that we still need to decide what to do with the excess energy stored in the transformer. In certain situations, like when a battery powers the circuit, it is appropriate to inject the excess energy back into the source as a form of regeneration. However, it is not useful to do so to a solar panel so we must dissipate the energy which is ideally quite minimal.

There are multiple angles from which to approach this task, but we have opted for an RCD snubber or resistor-capacitor-diode snubber. In this case, the diode prevents us from having constant dissipation, the resistor dissipates the energy, and the capacitor provides voltage regulation. The full calculations and design process for the snubber can be found in section 2.9 Tolerance Analysis.

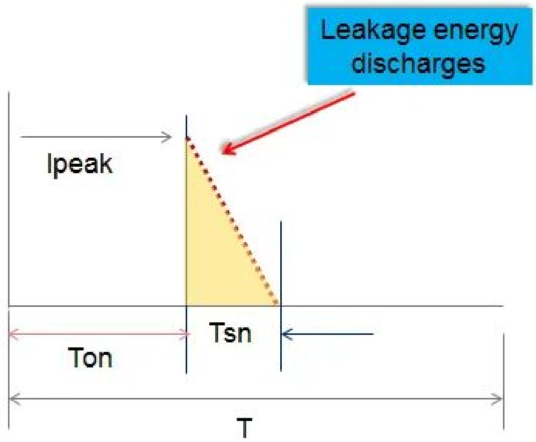


Requirement	*Verification*
The snubber should have a clamp voltage such that the maximum ringing across our MOSFET is no larger than 80V	We will use an oscilloscope probe to measure the voltages across the FETs in each converter to determine what the ringing voltage is.

Our evaluations have revealed that the most complex and difficult to implement component is the switching converter. Especially with continued use, many parts are prone to heating up. Proper thermal management and device choices need to be made to account for this constant use. The part most likely to fail in the converter is the switching MOSFET, this is due to the high ringing of the voltage across the drain and source of the MOSFET during switching times which might go over the rated blocking voltage of the MOSFET. We have opted to use an RCD clamp, covered in section 2.4.1.3. The algorithm for designing an RCD clamp is as follows

- Acquire from the manufacturer or in a lab the leakage inductance of the transformer
  - For the 750313441 transformer, this is typically 600nH
- Determine the power which the inductance stores
  - E = .5*L*I^2 is the energy per cycle
  - P = .5*L*I^2*fsw is the power
  - P = .5*600nH*(5.9)^2 * 15000 =156.65mW

    - We select 5.9A as this is the theoretical maximum current through the inductor
- Determine the theoretical power dissipated in our clamp resistor
  - Figure 9 shows how over time we should see a linear decrease in current through the clamp resistor which is based on the inductor equation V = L*dI/dt
  - We take the integral of this dissipation and multiply by the switching frequency in order to find the power-- P = .5*fsw*I*Tsn*Vclamp
  - Convert the time term into a function of constants and other design parameters such as Vclamp-- Tdis = I*L/(Vclamp - Vsec *n) where Vclamp is the clamp voltage (i.e. what do we clamp the ringing to) and Vsec is the voltage across the secondary terminal of the transformer.
  - We make this substitution and then also substitute the power through the resistor with the expression P = Vclamp^2/R
  - The resulting equation allowing us to solve for R based upon design parameters is R = (2*Vclamp*(Vclamp - n*Vsec)/(fsw*Ipeak^2*L)
- Select a clamp voltage
  - The clamp voltage affects the FET, which will see a maximum of Vin + Vclamp at its terminals during ringing. The maximum Vin per phase is only 16V, which allows us to select a relatively high Vclamp. A high clamp voltage reduces the time required to dissipate the additional energy but we will see later that this increases the required capacitance. Thus, we can select a middling value like 50V for the clamp. This way, we can select a FET with a 100V rating that will operate very comfortably and be incredibly unlikely to fail.
    - From here, we check Rcalc which comes out to be (2*50*(50-16*.5)/(15000*5.9^2*600e-9) where we have picked 16V as the secondary voltage, i.e. the maximum secondary voltage. N = .5 because we intend to step up our input voltage with the 2:1 transformer. Rcalc = 13.4k Ohm
    - The power dissipated in the resistor is just 186.5mW based on the calculation from earlier
    - The time to discharge is 84.286nsec according to the equation for Tdis which fits very comfortably within our switching period of 66.67usec
- Calculate the necessary capacitance
  - The capacitance mostly depends upon the ripple that we would like to see in our clamp network. Using the standard decay equation for a charged capacitor, we get Vmin = Vclamp* exp(-Tsw/(R*C)) which converts to be C = -Tsw/(R*ln(Vmin/Vclamp)) where Vmin is the minimum voltage we would like to charge the capacitor to. We would like our ripple to be very small and Tsw is very small so we can select a 200mv ripple and use a capacitor of .6194uF and achieve our desired effect.
- Select a diode-- All of the diodes in our system need approximately the same current and fast switching ratings, so we can opt to use the same schottky diode we use elsewhere.



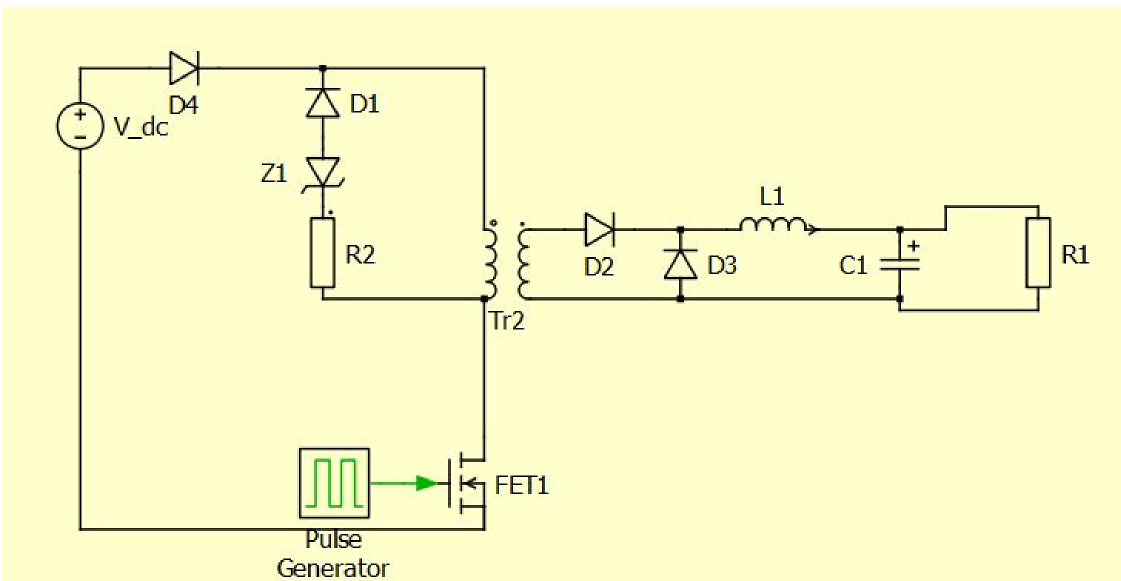
1.3 Write-up describing process for speccing a zener diode snubber in a switching power supply

In a forward converter, we use a transformer to achieve isolation and/or a specific desired step-up from the turns ratio. In this case, we don't seek to utilize the inductance of the transformer for any purpose unlike other converter topologies which utilize the stored energy in the transformer. So, we select a transformer that has very low inductance with the caveat that we still need to decide what to do with the excess energy stored in the transformer. In certain situations, like when a battery powers the circuit, it is appropriate to inject the excess energy back into the source as a form of regeneration. However, it is not useful to do so to a solar panel so we must dissipate the energy which is ideally quite minimal.

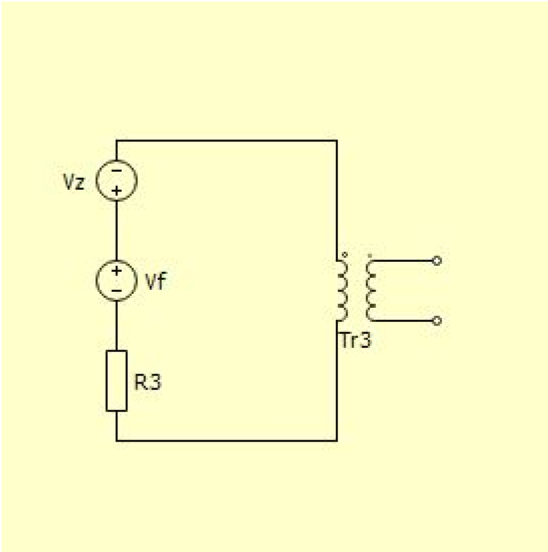
There are multiple angles from which to approach this task, but we have opted for a zener diode snubber/clamp. In this case, we use a zener diode to aggressively clamp the ringing voltage from the inductor whilst providing a means for the power to dissipate through a resistor. The full calculations and design process for the snubber can be found in section 2.9 Tolerance Analysis.

Our evaluations have revealed that the most complex and difficult to implement component is the switching converter. Especially with continued use, many parts are prone to heating up. Proper thermal management and device choices need to be made to account for this constant use. The part most likely to fail in the converter is the switching MOSFET, which is due to the high ringing of the voltage across the drain and source of the MOSFET during switching times which might go over the rated blocking voltage of the MOSFET. We have opted to use a zener clamp. Our algorithm for designing a zener clamp is as follows

- We generalize all of the components such that their relevant qualities such as the breakdown voltage of the zener diode are generic and named Vbrk, etc.
- Acquire from the manufacturer or in a lab the leakage inductance of the transformer
  - For the 750313441 transformer, this is typically 600nH
- Determine the power which the inductance stores
  - E = .5*L*I^2 is the energy per cycle
  - P = .5*L*I^2*fsw is the power
  - P = .5*600nH*(5.9)^2 * 15000 =156.65mW
    - We select 5.9A as this is the theoretical maximum current through the inductor
- Analyze and transform the circuit for the time interval where the inductor must dissipate and create a generalized model. For this purpose, we will assume that the zener diode becomes a voltage source with a value Vz that is equivalent to the zener breakdown voltage. The other diode can also be modeled as a voltage source with a value Vf which is the forward voltage of that diode.



- Ultimately, we would like to solve for the maximum voltage drop across the FET, however we will start with the KVL loop below
  - KVL loop pic
  - We transform this loop as specified above



- Solving this KVL results in the equation VL = Vz - Vf + Vr where VL is the voltage across the inductor and Vr is the voltage across the resistor.

● Next, we look at the KVL loop that includes the FET using the same transformation as before
  - This results in the equation Vds = Vin - Vz - Vr + Vf.
  - Vr expands into i(t)*R where i(t) is the time dependent current flowing through the resistor.

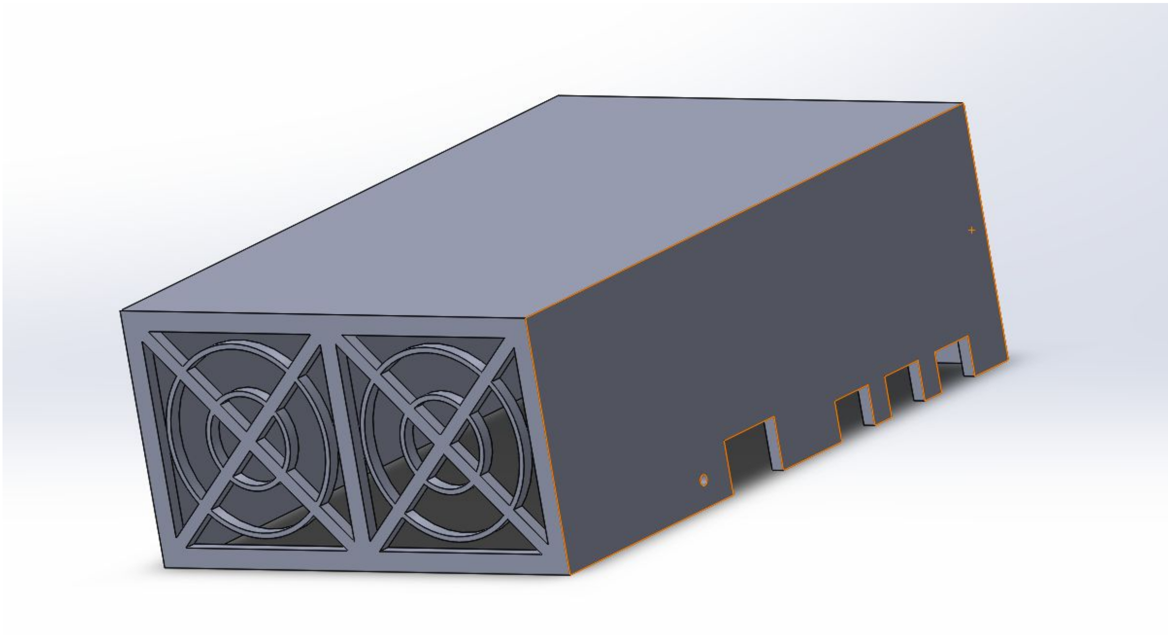
● Finally, we must use the differential equation for the diode, VL = L*dI/dt. Since this circuit ultimately amounts to an RL circuit with a single source, we know that the change in VL linear and thus can say that VL = L*ΔI/Δt.

● Substitution both the first KVL and this differential equation into the second KVL equation, we get that Vds = Vin - Vz - (L*ΔI/Δt*(1-e^-(R*t/L)) + Vf.

● In this situation, our design parameters are the time it takes for the inductor to discharge, the zener breakdown voltage,

● Select a diode-- All of the diodes in our system need approximately the same current and fast switching ratings, so we can opt to use the same schottky diode we use elsewhere.

1.4 CAD model for enclosure of previous project



1.5 Calculations for passives of previous project

Capacitors

The output capacitor was chosen such that the ripple voltage at the output stayed at 1.25% of the maximum average output voltage of 25V. This maximum voltage plus the voltage ripple of .3125V is equal to 25.3125V. To achieve this ripple, a minimum of 56uF are needed, the capacitor also needs to have a ripple current rating of 2.125A at 15kHz. The capacitor chosen has a capacitance of 470uF and a voltage rating of 50V.

Output Inductors

To stay within reasonable size and cost, the ripple current experienced at the output will be 2% of the maximum possible average current of 8.5A which gives a ripple current of 2.125A, so the maximum current at the peak will be 9.56A. At this ripple current, at minimum voltage output and maximum voltage input, a minimum inductance of .76mH is required. The inductor chosen has an inductance of 1mH and a current rating of 10A.

Diodes

The diode for the forward converter should have multiple qualities. It should be able to take the rated reverse voltage, and be able to conduct the desired current continuously. To be safe, the voltage ratings of the diode are set at least twice as high as expected, the continuous current through the diode should be at least 1.5 times higher. Because of this the **VBT1045BP-E3/8W** schottky diode is picked. Other desirable aspects of this diode are a fast recovery time, slightly lower forward voltage and low leakage current.

1.6 Detailed networking verification methods for previous project

Wireless Access Point

A compatible wireless access point with a matching protocol is necessary for the devices to communicate with the server.

<table>
<tr><td>Requirement</td><td>Verification</td></tr>
<tr><td>Communicate at a rate of at least 1kbits/sec to the MPPT device at least 30 feet away while outdoors</td><td>1. Connect the device to a private wireless network while outdoors and at least 30 feet away
2. Connect a laptop to the router using a wired connecting
3. Sample laptop-router network latency using `ping <router IP>`. mark average latency down
4. Now use `ping <device IP>`. Take that average latency and subtract laptop-router latency to find device-router latency.
5. Network speed can be taken from 256bits/(ping speed). Verify that this ping is at least 1kbits/sec (latency is less than .25 seconds)</td></tr>
</table>

Digital Signal Processing

Like any power application, the output of the forward converters is subject to noise, particularly ringing from switching. A finite impulse response low pass filter will be applied before the control loop performs calculations on the data. This can be accomplished by using a “rolling average” with optional weighting so that the data has less “inertia”, meaning it will respond more quickly to change in voltage outputs.

Noise is short, undesirable output changes based on surrounding environment or physical properties of electronic devices. A high spike in voltage due to switching would be considered noise, but a person accidentally covering a portion of the solar panel for more than a brief moment would not be, as it changes the steady state output of the system. The radiance on the solar panel may change quickly due to obstructions, so the device must both account for noise and changes in maximum power

Requirement	Verification
Low amplitude noise (<1V deviations from mean) are reduced by at least 90%	1. Set up a waveform generator to produce a sine wave of magnitude 1V (offset 1.5v) with a frequency of 10 kHz (high-Z mode) Attach this to an ADC input on the microcontroller 2. Run ADC code on microcontroller, connect serial interface to laptop for debugging 3. Serially print the voltage level read on the ADC, and the new output voltage to a debug console to save as file 4. Plot these points (Volts vs. Time), verifying that the change in output is never more than ±.05V
High amplitude noise (>1V deviations from mean) are reduced by at least 75%	Same procedure, except the experimental input will be a sine wave of magnitude 2V (offset 1.5v) with a frequency of 1 kHz (high-Z mode)
Large voltage level changes (a rate of more than 0.5V/sec) are accounted for at DSP output within 0.25 seconds	Same procedure, except the experimental input will be a square wave of magnitude 3V (offset 1.5v) with a frequency of .5 Hz (high-Z mode). DSP output should reach 3V within .25 seconds of rising edge, and 0V within .25 seconds of falling edge

Note: A sharp voltage increase of over 100 V/sec is extremely unlikely at the ADC input. Using a square wave make it easier to verify that the DSP is working as intended

Wireless communication

The ESP-01 communicates with the STM32 over UART, allowing for serial data to be converted to a wireless transmission to be sent over the Wi-Fi 802.11 transmission protocol. Once assigned an IP, the converter can communicate over Wi-Fi by hosting an HTTP server that another device can access through a variety of means, including a web browser or more complex data collection program. The converter will respond to HTTP GET requests and return the current power output of the device, and possibly additional debug information.

Requirement	Verification
The HTTP server on the converter responds to GET requests	1. Set up an HTTP endpoint, `<Device IP>:80/hello`, as a GET request that returns “Hello, World!” 2. Connect the device to a private

	wireless network 3. Connect any device with a web browser to the same network 4. Visit the website <Device IP>:80/hello and verify that the message “Hello, World! Has been successfully returned (will be displayed in the browsers content window)

1.7 Full Lock Assembly