E-Bike Theft Detection System

ECE 445 Senior Design Final Report

Group 71

Kacper Bakun, John Hanley, Paul Harris

Department of Electrical and Computer Engineering
University of Illinois Urbana-Champaign

TA: Yulei Shen

May 2026

Abstract

This report details the design, implementation, and verification of a real time E-Bike Theft Detection System. Traditional mechanical locks act merely as physical barriers that delay theft. They fail to provide the real time deterrence necessary to stop an attempt once it begins. To address this, our system utilizes a custom embedded printed circuit board (PCB) featuring an ESP32 microcontroller and a LIS3DHTR Inertial Measurement Unit (IMU). By employing digital low pass filtering and Root Mean Square (RMS) energy calculations, the system successfully distinguishes between ambient environmental noise and sustained tampering. Upon detecting a confirmed theft attempt, the system activates a 75 dB siren to deter thieves and alert bystanders. Verification testing confirms the system achieves a 100% accuracy rate on tamper trials and a 95% accuracy rate on non tamper trials with an average detection latency of 2.09 seconds. This project demonstrates a reliable, intelligent layer of active security tailored for micromobility fleets.

Contents

1. Introduction

1.1 Problem Statement

Bicycle and e-bike theft remains a widespread issue in both urban and suburban environments, resulting in significant financial losses and reduced accessibility to sustainable transportation. Many ride sharing companies, such as Lyft with their divvy bike products frequently experience persistent brute force attacks on their docked bicycles. Even when these theft attempts are unsuccessful, the resulting damage to locking mechanisms and docking infrastructure drives up maintenance costs and reduces fleet availability.

Current theft prevention methods primarily rely on mechanical locks, which act as passive barriers but do not actively respond once tampering begins. As a result, determined attackers can exploit these systems through repeated shaking, pulling, or force application until the lock or docking mechanism fails. This forces companies to divert resources away from service expansion to cover replacement costs, ultimately stalling the growth of sustainable green transportation.

1.2 Proposed Solution

The goal of our project is to develop a real time theft detection system capable of identifying sustained tampering and responding immediately. The system is designed as a compact embedded solution that can be mounted directly onto an e-bike frame. It continuously monitors motion using an inertial measurement unit (IMU) and processes sensor data using an ESP32 microcontroller. By applying signal filtering and evaluating motion over time, the system distinguishes between normal environmental disturbances and motion patterns characteristic of theft attempts.

The system architecture consists of four primary subsystems: power, sensing, control, and alarm. The power subsystem provides a regulated 3.3 V supply to ensure stable operation. The sensing subsystem uses an IMU to measure acceleration of the bike frame. The control subsystem processes sensor data and implements a finite state machine (FSM) to classify system behavior into idle, warning, and alarm states. When sustained tampering is detected, the alarm subsystem activates a high decibel siren to deter the thief and alert nearby individuals.

The performance of the system is evaluated based on several key requirements, including detection accuracy, response latency, and alarm effectiveness. The final design achieves greater than 90% detection accuracy, responds within 2 seconds of sustained tampering, and produces an alarm exceeding 75 dB at 1 meter. These results demonstrate the feasibility of using embedded sensing and real time processing as an effective enhancement to traditional theft prevention methods.

2. Design Methodology

2.1 Introduction

The hardware and software architectures used were designed to balance low power consumption with rapid, real time signal processing. Our system is divided into four main subsystems: Power, Sensing, Control, and Alarm.

2.2 Power Subsystem

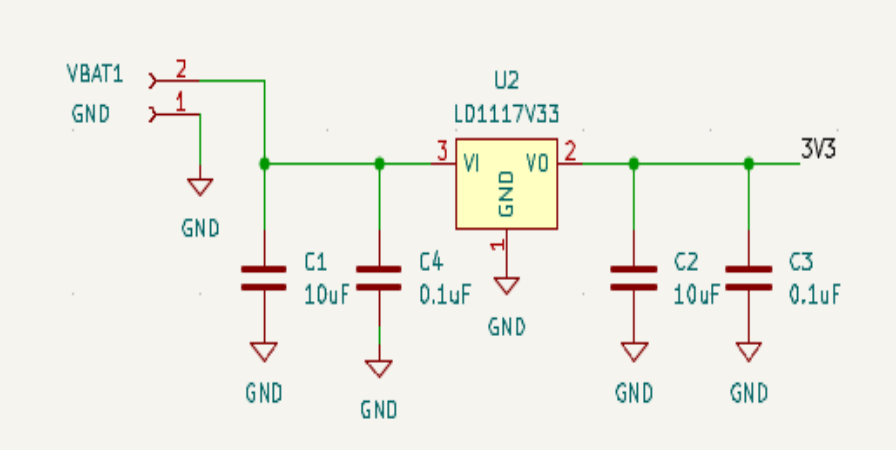

Figure 1. Power Subsystem PCB Schematic

The power subsystem is responsible for providing stable and reliable voltage to all system components under both steady state and transient conditions. The system is powered by a 7.4 V lithium polymer battery which supports the piezo siren output required to achieve 75dB. Because the ESP32 microcontroller and the LIS3DHTR IMU require a 3.3 V operating voltage, an LD1117-3.3 linear voltage regulator was selected to step the battery voltage down to a regulated 3.3 V rail. We chose this approach over switching regulation due to its simplicity and low noise characteristics. These aspects were important for maintaining accurate sensor readings and having a stable microcontroller during operation and testing. We added several decoupling capacitors to reduce voltage ripple and stabilize the supply during transient events such as alarm activation.

The alarm subsystem is powered directly from our 7.4 V battery rather than the regulated 3.3 V rail. This process isolates high current switching from sensitive digital components and prevents voltage drops that could disrupt system operation. We wanted to make a system which could effectively stay within the 3.3 V range without shifting more than .1 V in either direction to protect all other components of our system.

2.2.1 Power Subsystem Verification

Requirements	Verification
• The power subsystem shall supply 3.3 V ± 0.1 V at up to 200 mA continuous load	• Record voltage values and verify they remain within tolerance with meter
• The 3.3 V rail shall not dip below 3.2 V during siren switching events	• Probe 3.3 V with an oscilloscope while triggering alarm bursts; verify minimum voltage ≥ 3.2 V

Figure 2. Power Subsystem R&V Table

Figure 3. Power Subsystem Voltage Measurements(Battery Power Supplied, Voltage Regulator Output, Voltage Regulator Output During Siren Activation)

Stable power delivery is a critical part of our design to prevent the ESP32 from entering a brownout state during siren activation. We recorded voltage measurements shown above in figure 3 above using a digital multimeter in order to verify the conditions outlined in our R&V table. These measurements confirmed that our regulated voltage measured 3.290 V, which lines up correctly with our first power requirement. Similarly, during siren activation we recorded the regulated voltage measured 3.288 V, remaining well within the 3.3 V ± 0.1 V requirement and never dipping below the critical 3.2V threshold.

2.3 Sensing Subsystem

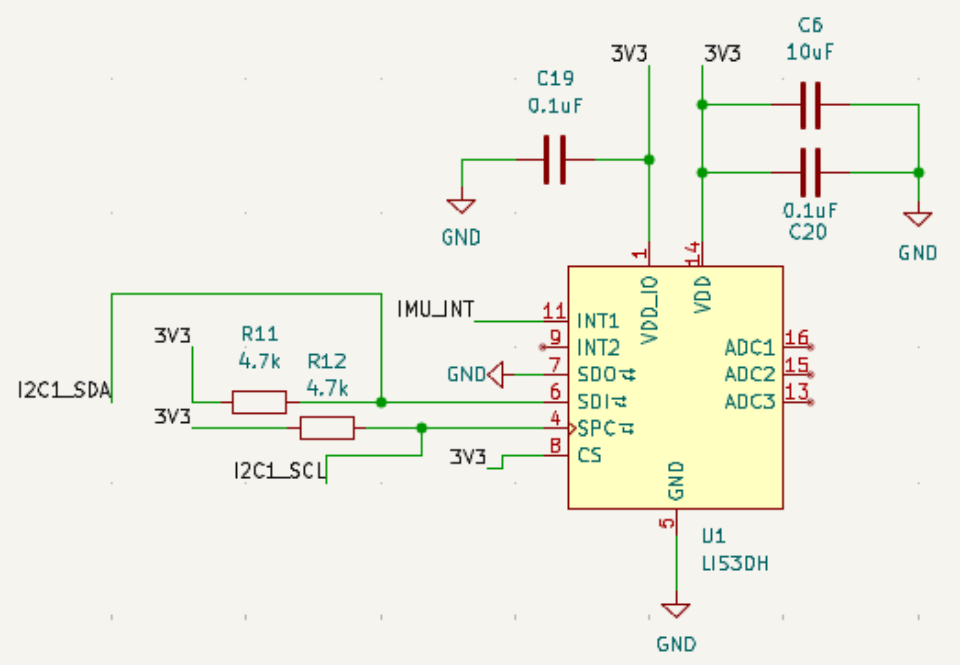

Figure 4. Sensing Subsystem PCB Schematic

The sensing subsystem is responsible for detecting motion of the e-bike frame and providing real time data for theft detection. We implemented this using an inertial measurement unit (IMU) that measures acceleration along three axes. Several IMUs were evaluated during our design process. The initial design used an MPU series sensor, followed by an ICM series IMU. Through testing we found that the ICM device's VDDIO pin was not compatible with the system's 3.3 V logic level as it was rated for a maximum of 1.8 V. This resulted in a component failure and a redesign. Our final design uses a LIS3 series IMU, which is fully compatible with 3.3 V operation and provides reliable performance.

In our final design, our IMU is mounted directly onto the PCB to ensure accurate measurement of frame vibrations and communicates with the ESP32 WROOM via the I2C protocol with pull-up resistors for signal integrity.

Instead of outputting acceleration directly in standard gravity units (g), the LIS3DHTR outputs raw digital values measured in least significant bits (LSB). Based on our configured sensitivity range the sensor operates with a scale factor of 1024 LSB/g. Before our control subsystem can evaluate the motion for tampering, we have to normalize these raw 16-bit integer values into standard float values representing g forces. Our firmware parses the high and low data registers then shifts the bits appropriately and lastly divides the result by 1024.0.

To quantify the motion sensed our system computes the magnitude of acceleration from the three axis outputs which represents the total acceleration experienced by the system.

$$a_{mag} = \sqrt{a_x^2 + a_y^2 + a_z^2}$$

We apply filtering to reduce high-frequency noise, and motion is evaluated over time rather than instantaneously to distinguish between environmental disturbances and sustained tampering. Our system is designed to detect acceleration changes on the order of 0.1 g while minimizing false positives.

2.3.1 Sensing Subsystem Verification

Requirements	Verification
• The sensing subsystem shall detect sustained vibration above the acceleration threshold.	• Apply controlled vibration with a message gun to the assembled system and verify the measured acceleration exceeds the threshold. Average g force over 10 seconds is 0.43 g from the message gun.
• The sensing subsystem shall detect acceleration changes of at least 0.1 g after filtering	• Apply controlled vibration or step acceleration, and verify measured acceleration ≥ 0.1 g

Figure 5. Sensing Subsystem R&V Table

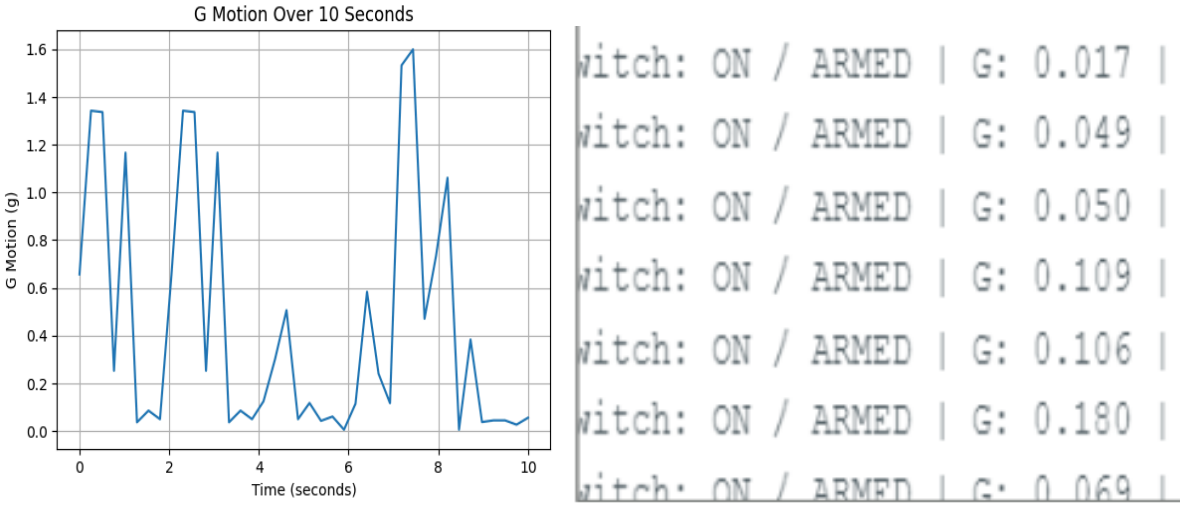

Figure 6. Sensing Subsystem Constant Applied Acceleration & System detection of g values of approximately .1 g

It was essential that our sensing subsystem should reliably sense high energy tampering signatures and minor environmental fluctuations so that accurate signals could be sent to our control subsystem, where within our control subsystem this logic will be used to make accurate decisions within our finite state machine. The data presented above in Figure 6 verifies that our LIS3-series IMU successfully meets both design requirements.

- **Sustained Vibration Detection:** We needed to verify that our system could accurately detect an active theft attempt. To test this we applied a massage gun to our bike frame with our enclosure mounted on to simulate sustained mechanical stress. As seen above in Figure 6, our sensor captured continuous high amplitude oscillations. Our system recorded an average acceleration of 0.43 g over this 10-second window. This value of .43 g exceeds our established 0.25 g tampering threshold. This effectively confirms that the sensor easily senses the sustained energy required to trigger the alarm.
- **Granular Acceleration Filtering:** To verify the sensor's sensitivity and the effectiveness of our filtering we monitored the system during normal environmental conditions. We saw that the serial output log in Figure 6 showed the system registering minor acceleration changes, such as 0.049 g, 0.106 g, and 0.180 g. This confirms the system successfully detects acceleration shifts well below the 0.1 g requirement. Because these readings remain strictly under the 0.25 g threshold it proves that our system can accurately capture very small and precise movements while making sure our device stays within the ARMED/IDLE states. This helps us in the case of how it will limit the number of false positives occurring on non tamper trail tests.

2.4 Control Subsystem

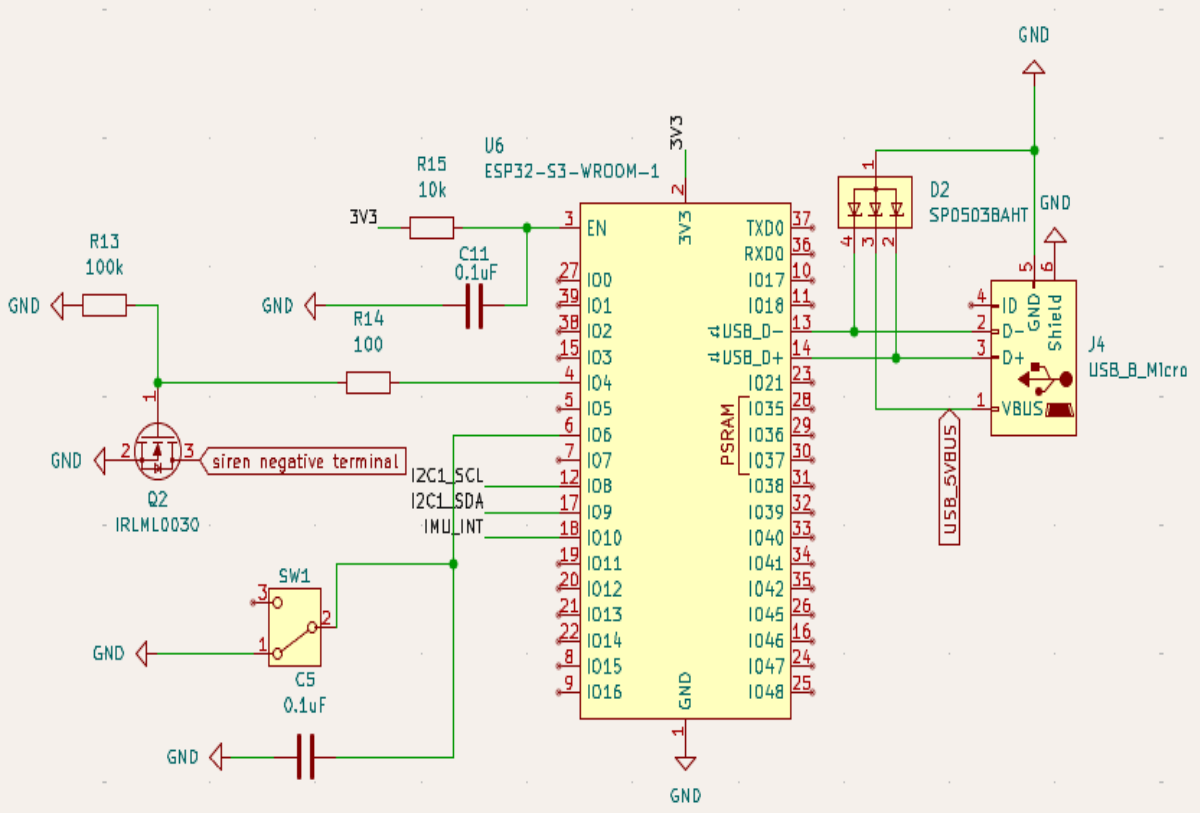

Figure 7. Control Subsystem PCB Schematic

The Control subsystem is the main processing unit of our E-Bike Theft Detection System. It is responsible for communicating with our sensing and alarm subsystems, while receiving 3.3 Volts from our power subsystem. As seen above in figure 7, the microcontroller is centered around our ESP32-S3-WROOM-1 chip. This ESP32 chip is responsible for monitoring sensor inputs, processing motion data, and controlling all outputs. As shown below in figure 8, the control subsystem acts as the “brain” of the project through how it executes our finite state machine(FSM) where we can be within states such as our reset, idle, warning or alert. These are all determined based on acceleration motion which is sent from our IMU to determine if an actual theft attempt is occurring.

The most important part of the control subsystem is its ability to control communication between all the different hardware components connected to the system. Through an I2C communication interface the ESP32 microcontroller is able to receive acceleration and motion data from our IMU. From this the control subsystem processes this information using RMS-based calculations and compares the results against programmed thresholds to distinguish between normal movement and potential theft activity.

The Microcontroller is also essential to the design through how it communicates with our alarm output subsystem. The ESP32 microcontroller receives signals from our IMU and classifies them in windows of .1 seconds, from this the microcontroller keeps track of the past 20 windows(2 seconds). If any 12 out of the last 20 windows have a 3 axis normalized acceleration of above .25 g then our microcontroller will send a signal to our alarm subsystem through a MOSFET to set off our piezo siren.

2.4.1 Finite State Machine

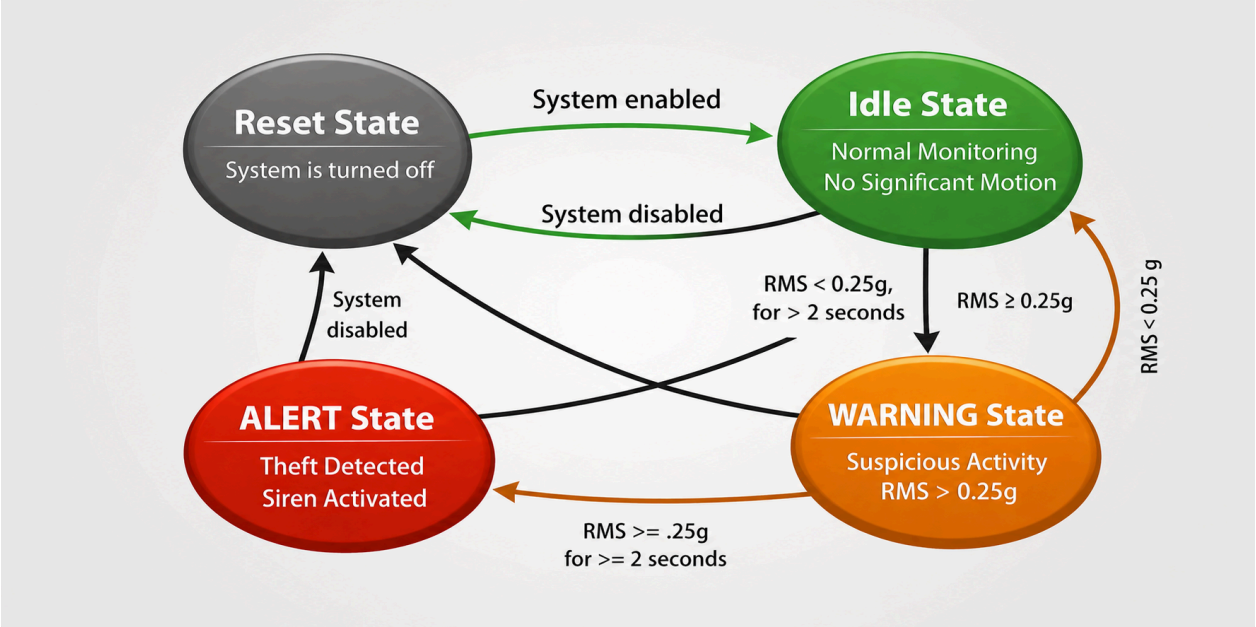

Figure 8. Finite State Machine(FSM)

The E-Bike Theft Detection System uses a Finite State Machine (FSM) to classify motion behavior and determine when to activate the alarm. The FSM consists of four states: reset, idle, warning, and alert. State transitions are determined by the magnitude and persistence of filtered motion, this is quantified through RMS acceleration energy computed over fixed time windows.

Reset State

The Reset state represents the unarmed condition of the system when the bike is unlocked or actively in use. In this state, the alarm subsystem remains disabled and can be enabled through a switch located on our printed circuit board(PCB). Once the bike is locked, the system automatically transitions to the Idle state and begins active monitoring. This ensures that the theft detection system only operates when the bike is locked.

Idle State

We made the Idle state represent normal operation where the bike is stationary or experiencing minor environmental disturbances. In this state, the ESP32 continuously polls the IMU at a 100 Hz sampling rate to compute the E_{RMS} for each window. The system remains in Idle as long as the E_{RMS} remains below the predefined tamper threshold of 0.25g. If at any point the user decides to switch the system off the FSM will return to the reset state.

Warning State

The FSM transitions from Idle to Warning when a single 100 ms window records an E_{RMS} of above 0.25g, indicating suspicious activity. This state acts as a digital debounce and false-alarm prevention stage. While in Warning, an internal software timer accumulates the duration of sustained motion. If any subsequent 100 ms window falls below the 0.25g threshold, the timer is immediately cleared, and the system returns to the Idle state. This ensures that momentary shocks, such as a heavy door closing or wind gusts do not trigger the alarm. If at any point the user decides to switch the system off the FSM will return to the reset state.

Alert State

The FSM transitions from Warning to Alert only when the accumulated duration of suspicious activity reaches or exceeds 2.0 seconds for 12 out of 20 of the past 100 ms windows. This persistence requirement ensures that only sustained tampering, such as rattling or lifting, initiates a response. When entering the alert state the ESP32 asserts a logic HIGH on the GPIO pin connected to the MOSFET gate, completing the circuit for the 7.4V battery to power the sirens. The system remains in the Alert state for a minimum of two seconds and can stay for longer if the threshold is constantly still being met, from here it will return to the idle state and continue monitoring motion. If at any point the user decides to switch the system off the FSM will return to the reset state.

2.4.2 Control Subsystem Verification

Requirements	Verification
• The FSM shall transition to Alarm within 2.0 s ± 0.2 s of sustained tamper motion	• Apply a repeatable shaking stimulus to the mounted system, which maintains an average of over .25 g. • Use a GPIO pin to indicate FSM Alarm state. • Repeat tests across multiple trials, and compute the average.
• The system shall achieve ≥ 90% tamper detection accuracy over 10 trials tamper trials and 10 non tamper trials	• A tamper trial is defined as sustained shaking motion of over .25 g back and forth for over 2 seconds • A non-tamper trail consists of either a rapid spike of over .25 g for less than a second or any amount of shaking with a force of .25 g or less for any period of time.
• The firmware shall boot into a safe non-alarm state (Idle)	• Verify alarm remains inactive until valid detection occurs.

Figure 9. Control Subsystem Requirements & Verification

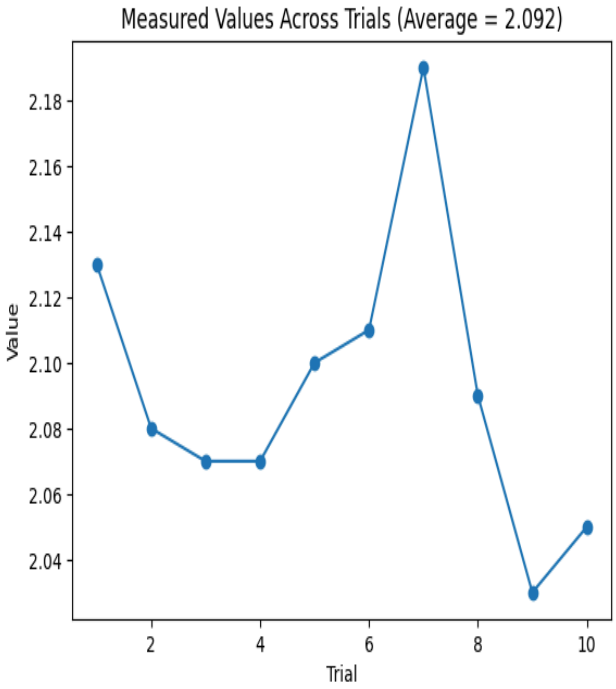

Figure 10. Alarm Transition Time Trials

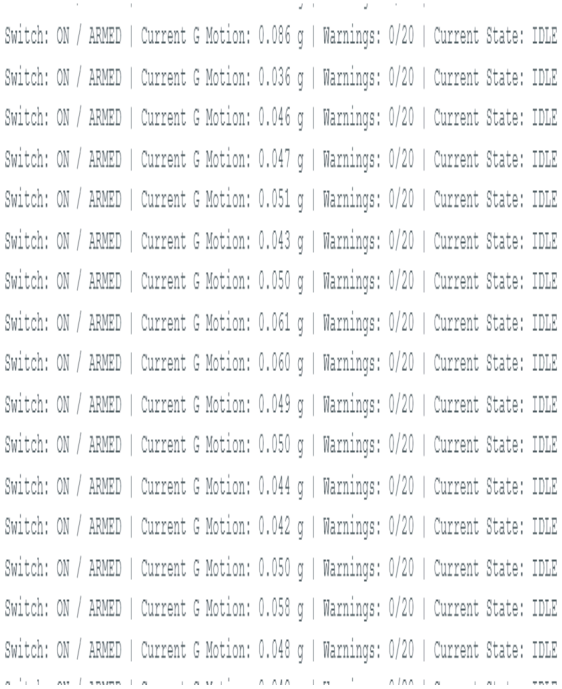

Figure 11. Firmware Bootup State

To ensure that the theft detection device could prevent theft almost immediately while still being sure that a theft attempt was occurring, it was a necessary requirement that the alarm had to activate within 2 seconds +/- .2 seconds following consistent shaking with an average acceleration of above .25 g. To test this requirement, a force of above .25 g was applied to the enclosed theft detection system. As seen above in figure 10, over 10 trials we saw a high of 2.19 seconds and a low of 2.03 seconds for the alarm to activate. Every single case within the 10 trials fit within the requirement of the alarm activating within 2 +/- .2 seconds of sustained theft motion. An average of 2.092 seconds for the alarm subsystem to activate was obtained, supporting how theft can be prevented quickly once a theft is confirmed.

Another important requirement is that the system must boot into an idle state to start, this is important because users of our theft detection system should never turn their system on and immediately hear an alarm which could disturb them and possibly annoy others around them. As seen above in figure 11, our firmware on booting up starts in our idle state when switched on and starts monitoring for motion above the .25 g threshold to go into the warning state.

It is an essential requirement that the theft detection system should achieve an accuracy of above 90% accuracy on tamper trials and non tamper trials. Across 20 tamper trails of sustained motion of above .25 g for 2 seconds, 100% accuracy was recorded. Across 20 non tamper trails, where motion could either be above .25 g for less than 2 seconds or motion was sustained at a level below .25 g for any period of time, 95% accuracy was recorded. Out of 40 total trials there

was only one case of a false positive and 39 cases of true positive and true negatives. These tests showed a high accuracy rate and showcased our systems ability to correctly predict theft attempts from non theft events such as wind or bumps into the bike.

2.5 Alarm Subsystem

The Alarm Subsystem produces the physical deterrent in our design. An IRLML0030 N-Channel MOSFET is used as a low side switch. The ESP32's 3.3 V GPIO pin drives the MOSFET gate, which connects the negative terminal of the 75 dB piezo siren to ground. The siren is powered directly from the 7.4 V battery rail, allowing it to achieve maximum volume without loading the sensitive 3.3 V logic rail.

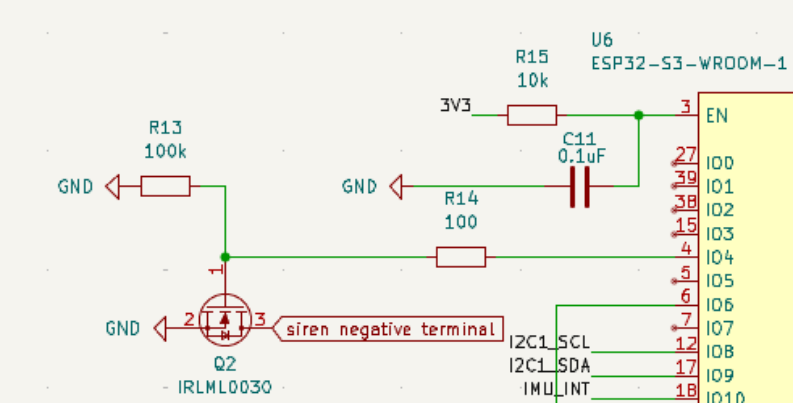

Figure 12. Alarm Subsystem PCB Schematic

2.5.1 Alarm Subsystem Verification

Requirements	Verification
• The piezo siren must produce a minimum sound pressure level of 75 ± 5 dB measured at a distance of 1.0m from the source	• Place the siren on a flat surface and measure exactly 1.0m away. • Activate the alarm and use a digital sound level meter to record the peak dB level.
• The MOSFET must fully saturate with a gate voltage of 3.3 ± 0.1V, ensuring the voltage across the siren is at least 7.1V (assuming a 7.4V battery)	• Trigger the alarm from the ESP32.

Figure 13. Alarm Subsystem R&V Table

Figure 14. Alarm Subsystem Sound and Voltage Measurements

The sound pressure level (SPL) of the piezo siren was measured using a digital decimal meter. The image in the top left displays the testing done on the siren; over our three and a half minute test, we observed an average SPL of 76 dB, which is within our limit of greater than 75 dB. On the right, we see the voltage across the gate pin of our mosfet while the siren is active. This measurement ensures that the mosfet does in fact saturate with the output from our 3.3 V regulator.

2.6 Physical Design

Figure 15. Physical Design and Application

A very important part of the design throughout our project was the size and space of our enclosure. We had to make sure our enclosure was able to fit a piezo siren, battery and the printed circuit board. For our design we chose to do a snap on case for convenience and duct tape the enclosure with our system to our bike. In a situation where we had more time we would

choose a more protective case and would weld the device to the bike to prevent tampering from thieves. The main design choice we decided on was to position the piezo siren as close to the edge of the box as possible, this would make sure the box would not have too much interference with the sound coming out of the alarm, effectively keeping our alarm above our 75 dB range.

3. Costs

The economic feasibility of the project was analyzed based on both component costs and engineering labor. Using the standard formula for labor estimates (Hourly Rate × 2.5 × Total Hours), we calculated the development costs assuming an ideal salary of $40/hour and approximately 100 hours of work per partner.

Category	Description	Estimated Cost ($)
Labor	3 Engineers × 100 hours × $40/hr × 2.5 multiplier	$30,000.00
Parts	ESP32, LIS3DHTR, PCB Fabrication, Passives, Siren, Battery	~$35.00
Total	**Estimated Prototype Cost**	**$30,035.00**

Figure 15. Cost Analysis Table

4. Conclusion and Future Work

The E-Bike Theft Detection System successfully proves that active and intelligent monitoring can bridge the security gap left by traditional mechanical locks. By carefully processing RMS energy over time windows, our system was able to accurately dismiss environmental noise while reliably reacting to theft attempts within two seconds.

4.1 Ethical Considerations

Throughout the entire design process we as a team strictly adhered to the IEEE Code of Ethics, ensuring the system protects the public without introducing physical hazards. One primary concern we had to address was the risk of creating a public disturbance due to false alarms. Our implementation of digital low pass filtering and debouncing FSM logic was able to eliminate the majority of accidental triggers. In accordance with the ACM Code of Ethics regarding the

avoidance of harm, the siren's output is physically capped near 80 dB to prevent hearing damage to bystanders while remaining loud enough to serve as an effective deterrent.

4.2 Future Work

In the future we would look to turn this prototype into a commercially viable product. The main areas of improvement we would plan to focus on include environmental resilience, power improvements and docking integration.

- **Upgraded Enclosure:** Transitioning from a generic metal box to a custom 3D printed, weather sealed enclosure to protect the PCB from rain and physical impact. We would also try and weld this enclosure onto our bike rather than using tape to attach our box onto the bike.
- **Smart Docking Integration:** We would replace the manual arm/disarm switch with a magnetic sensor that automatically arms the system when the bike is secured in a designated docking station. For any other type of bikes we would likely decide to make an app which could switch our system on and off for when the user would want to use their bike.
- **Power Management:** If given more time we would introduce a battery management system with a charging circuit. This allows our system to continuously recharge from the e-bike's main motor battery. This would be a feature which would have to be added into the divvy bikes docking station.

References

[1] C. Farr, "Divvy Responds to Video Showing Bike Methodically Dislodged From Docking Station," NBC Chicago, Jul. 24, 2018. [Online]. Available: https://www.nbcchicago.com/news/local/divvy-bike-theft-video/176532/

[2] "IEEE Code of Ethics," IEEE, 2020. [Online]. Available: https://www.ieee.org/about/corporate/governance/p7-8

[3] "ACM Code of Ethics and Professional Conduct," Association for Computing Machinery, 2018.[Online]. Available: https://www.acm.org/code-of-ethics

[4] STMicroelectronics, “LIS3DH MEMS digital output motion sensor: ultra-low-power high-performance 3-axis accelerometer,” Datasheet, 2017. [Online]. Available: https://www.st.com/resource/en/datasheet/lis3dh.pdf

[5] Espressif Systems, “ESP32-WROOM-32 Datasheet,” 2020. [Online]. Available: https://www.espressif.com/sites/default/files/documentation/esp32-wroom-32_datasheet_en.pdf

[6] STMicroelectronics, “LD1117 Voltage Regulator Datasheet,” 2016. [Online]. Available: https://www.st.com/resource/en/datasheet/ld1117.pdf

[7] Infineon Technologies, “IRLML0030TRPBF HEXFET Power MOSFET Datasheet,” [Online]. Available: https://www.infineon.com/dgdl/irlml0030pbf.pdf