E-Bike Theft Detection System

ECE 445 - Design Document - Spring 2026

Project #71

Kacper Bakun, John Hanley, Paul Harris

Professor: Craig Shultz

TA: Yulei Shen

Contents

1. Introduction

1.1 Problem

Bicycle theft is a widespread issue in both urban areas and suburban neighborhoods, resulting in significant financial losses for individuals and companies alike. Large ride-sharing companies, such as Lyft, have frequently reported persistent rattling, shaking, or even brute force attacks on their Divvy bike fleets. While traditional mechanical locks serve as a physical barrier to theft, they lack any real-time deterrence necessary to stop a thief once an attempt begins. As a result, these systems only delay theft rather than actively preventing it. Bikes are also most often stolen late at night when most people are asleep, making detection even more difficult. This lack of visibility allows thieves to exploit mechanical weaknesses over extended periods of time without interruption. Even when theft attempts are unsuccessful, damage to locking mechanisms and docking infrastructure leads to additional maintenance and operational costs. This loss of a bike results in more than just property damage. From a global and environmental perspective, high theft rates act as a barrier to sustainable green transportation. Shared micromobility systems play an important role in reducing congestion, lowering emissions, and promoting accessible transportation. However, the high replacement and repair costs associated with theft force companies to divert resources away from expanding service areas, improving reliability, and investing in cleaner transportation solutions. These costs are often passed on to users in the form of increased rental prices or reduced availability. Furthermore, current theft prevention strategies primarily focus on improving mechanical security. While stronger locks and docking mechanisms can delay theft, they do not address the fundamental issue: the lack of intelligent, real-time monitoring. As new lock designs are introduced, thieves continuously adapt their methods. Without active sensing and deterrence, the cycle of lock improvement and exploitation will continue.

The attached article below demonstrates a real-world example in which excessive shaking and repeated attempts were used to dislodge a Divvy bike from its docking station. This highlights the need for a complementary electronic solution capable of detecting and responding to tampering as it occurs. An intelligent monitoring system could not only deter theft in real time but also provide data insights to improve fleet management and infrastructure design.

[Divvy Responds to Video Showing Bike Methodically Dislodged From Docking Station – NBC Chicago]

1.2 Solution

The proposed E-Bike Theft Detection System is an embedded, low-power solution designed to provide the real-time deterrence that mechanical locks lack. The system consists of a custom printed circuit board (PCB) that integrates a microcontroller and an inertial measurement unit (IMU) to monitor vibration, motion, and rotation of the bike. By placing these sensors directly onto the bike frame, the system can detect motion patterns that are characteristic of theft attempts rather than relying solely on physical locking mechanisms. This approach enables continuous monitoring and immediate response when abnormal activity is detected. The system processes sensor data in real time using a Finite State Machine (FSM) that classifies activity into three operating states: Idle, Warning, and Alarm. To minimize false positives caused by environmental factors such as wind, minor bumps, or pedestrian interaction, the system applies a Digital Low-Pass Filter (DLPF) and evaluates motion over time using Root Mean Square (RMS) energy calculations. This filtering ensures that only sustained and abnormal motion patterns trigger a response. When tampering activity persists for more than two seconds, the system transitions from the Warning state to the Alarm state. Once a confirmed theft attempt is detected, the microcontroller activates a high-power alarm through a MOSFET driver, producing a sound level of at least 75 dB. This audible alert is designed to deter the thief and notify nearby pedestrians, increasing the likelihood of intervention or abandonment of the theft attempt. By combining intelligent sensing, real-time processing, and active deterrence, this solution addresses the limitations of traditional locks and provides a practical approach to reducing e-bike theft and supporting sustainable transportation.

1.3 Visual Aid

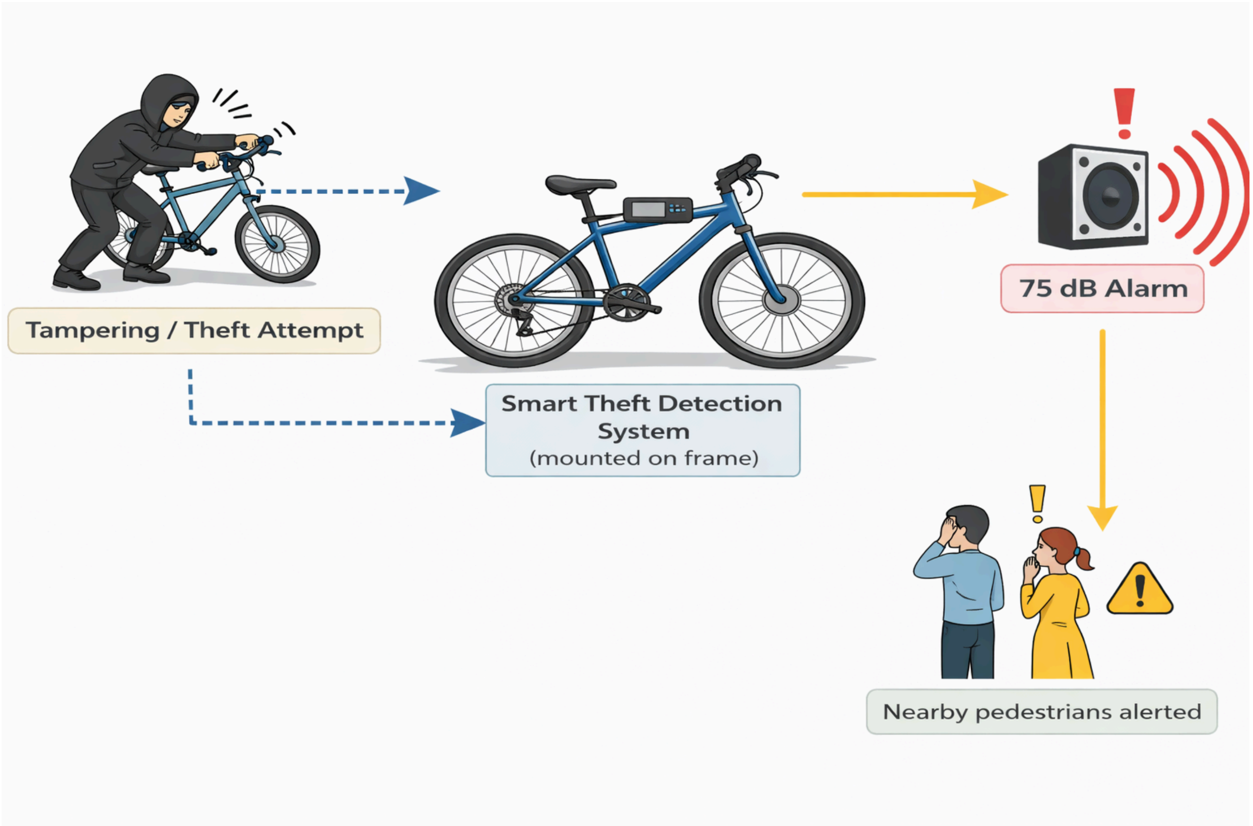

Figure #1: Visual Aid & Functional Operation of the E-Bike Theft Detection System

The following diagram illustrates the deployment of the system on a standard e-bike frame. It depicts the interaction between the physical tampering attempt, the processing by the "Smart Theft Detection System" mounted to the bike, and the resulting high-decibel siren that alerts nearby pedestrians to intervene. Although not directly depicted in the visual aid, we expect to place sirens in multiple places on the bike's frame so as to prevent easy destruction or identification of the siren.

1.4 High Level Requirements

To consider our project successful, our safety suite must fulfill the following:

1. **Tamper Detection Accuracy:** The system must correctly differentiate between normal environmental motion and tampering with at least 90% accuracy over 40 test trials, ensuring that the system reliably detects theft attempts without being triggered by common environmental movements like wind or minor bumps.
2. **Detection Latency:** The system must transition from the armed state to the alarm state within 2 seconds of detecting sustained tampering activity, ensuring a rapid response to theft attempts.
3. **Alarm Effectiveness:** When a confirmed theft attempt is detected, the system must trigger an alarm with a sound pressure level of at least 75dB measured at 1 meter from the bike, ensuring that nearby pedestrians are alerted and the thief is deterred.

2 Design

2.1 Physical Diagram

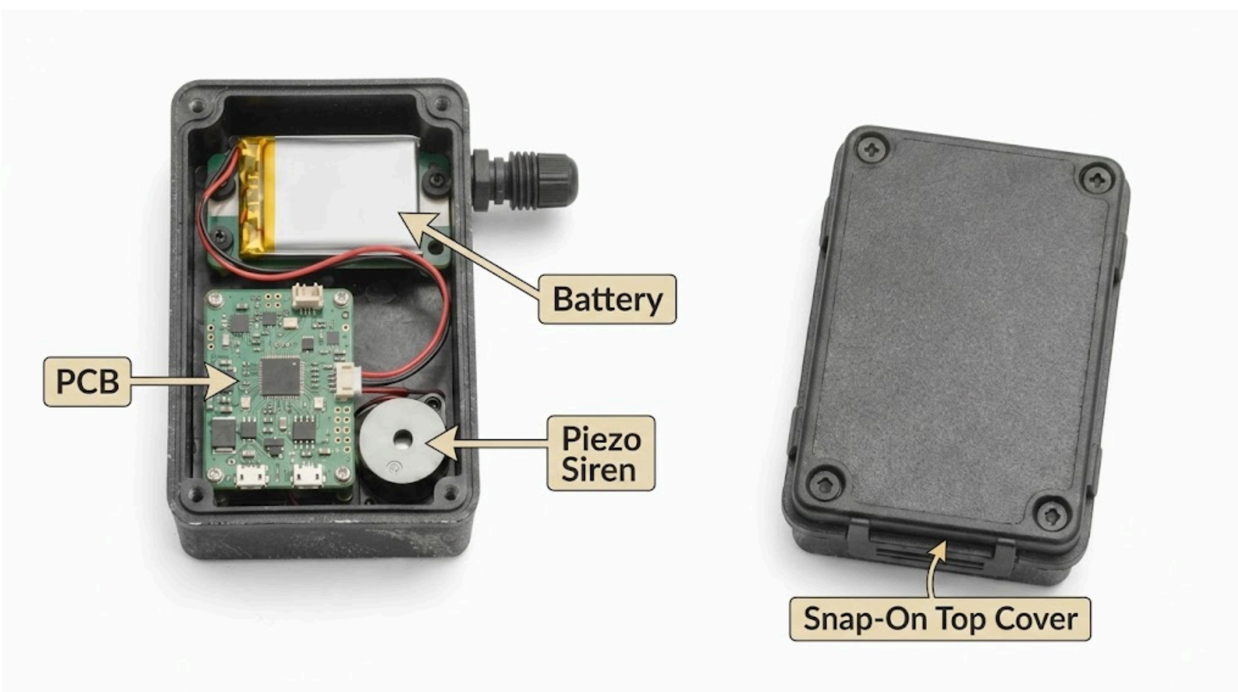

Figure #2: Physical Diagram, Internal Component Layout and Enclosure Design

The physical design of the E-Bike Theft Detection System uses the enclosure assembly shown in Figure X. The system consists of four main components: the weather-resistant enclosure, the custom PCB, the lithium-polymer battery, and the piezo siren. The custom PCB, which includes the microcontroller, IMU, and supporting circuitry, is rigidly mounted inside the enclosure to ensure accurate vibration and motion sensing from the bike frame. The battery is secured within the enclosure using foam padding to prevent movement and mechanical damage during operation. The piezo siren is positioned within the enclosure to allow sufficient sound propagation while maintaining environmental protection. The snap-on top cover provides a secure and tamper-resistant seal while allowing easy access for charging, maintenance, and debugging during development and testing.

Figure #3: Open PCB container mounted onto E-Bike

This figure illustrates the proposed mounting location of the theft detection system on the top tube of the e-bike frame. The sensing module is housed in a compact, weather-resistant enclosure and secured to the frame using mounting straps. Allowing it to remain stable while the bike is in motion. Placing the system on the top tube provides a central and rigid mounting point, which improves vibration and motion detection accuracy by capturing movement from the entire bike structure. This location is a position which causes no interference at all with the rider.

2.2 Block Diagram

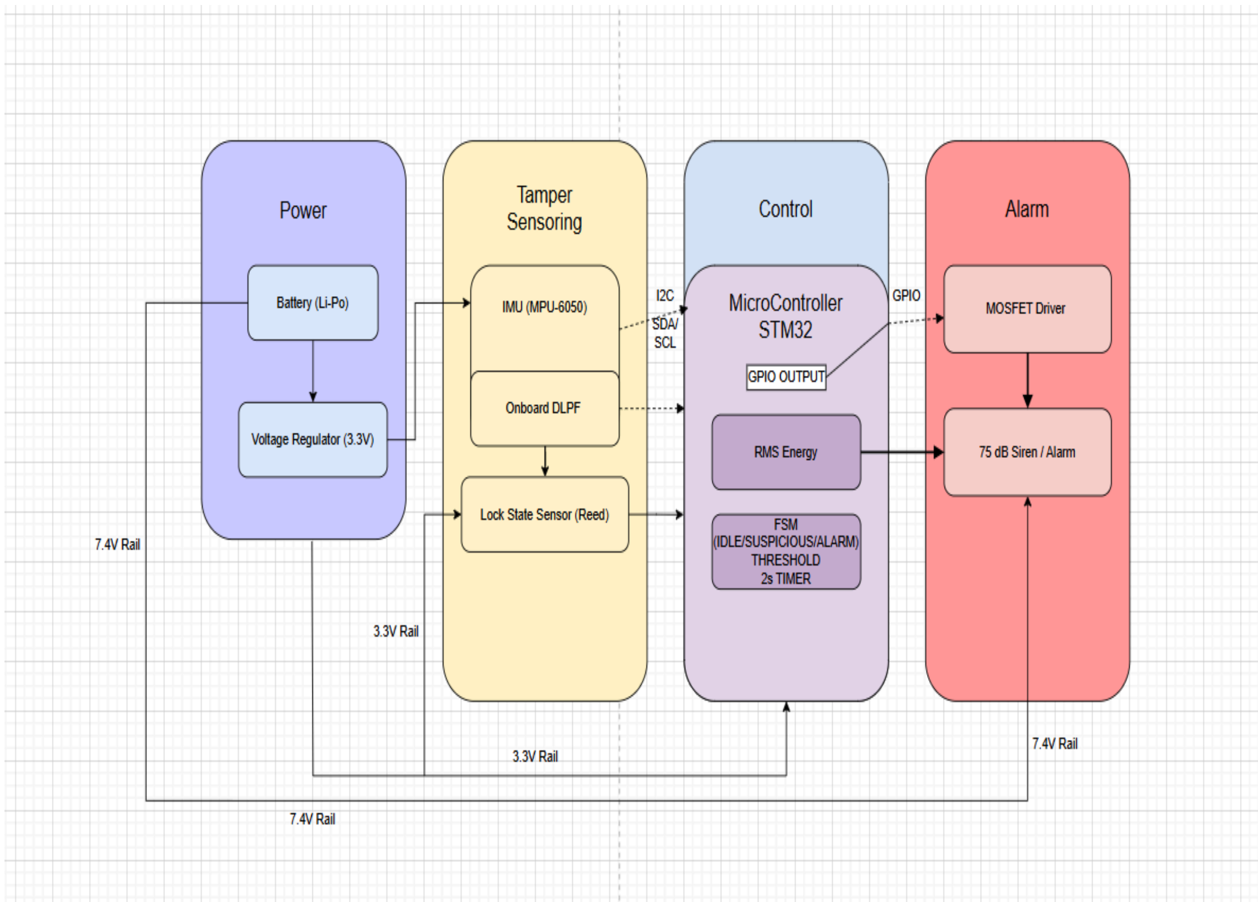

Figure #4: Block Diagram

2.3 Functional/Subsystem Overview and Block Diagram Requirements

2.3.1 Power Subsystem

This subsystem provides stable energy to the electronics. It takes the variable voltage from a Lithium-Polymer battery and regulates it down to a steady 3.3V. It connects to all other subsystems via power rails to ensure the sensors and MCU do not lose power during an alarm event. The battery is connected directly to the Piezo Sirens to provide it enough voltage for peak performance, while it provides the rest of the system parts with a steady 3.3V. The Power Subsystem supplies regulated power to all electronic components. A 7.4 V (2S) Lithium-Polymer battery provides the primary energy source. A linear voltage regulator (LD1117-3.3) steps the battery voltage down to a stable 3.3 V rail for the MCU and IMU. Bulk and decoupling capacitors ensure voltage stability during transient loads caused by alarm activation. This subsystem enables continuous monitoring even during alarm events, satisfying the low-latency and reliability requirements.

High Level Requirement: Must supply 3.3V ± 0.1V at a continuous current of at least 200mA. Stable power delivery ensures uninterrupted sensing and fast alarm activation, directly supporting the detection latency and alarm effectiveness requirements.

Requirements	Verification
• The power subsystem shall supply 3.3 V ± 0.1 V at up to 200 mA continuous load	• Connect a programmable electronic load to the 3.3 V rail. Measure voltage with a DMM at loads of 50 mA, 100 mA, and 200 mA • Record voltage values and verify they remain within tolerance. • Repeat measurements after 2 minutes of continuous operation to confirm thermal stability.
• Voltage ripple shall not exceed 50 mVpp during alarm activation	• Connect an oscilloscope probe directly across the 3.3 V rail and ground. • Configure the oscilloscope for AC coupling and high bandwidth. • Trigger the alarm repeatedly to create worst-case transient load conditions. • Measure peak-to-peak voltage ripple

	during siren activation. ● Verify ripple remains below 50 mVpp.
● 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
● The siren shall be powered from the battery rail and not from the 3.3 V rail	● Measure siren supply node during alarm; confirm near battery voltage while 3.3 V remains regulated

2.3.2 Sensing Subsystem

This is the "eyes" of the system. It uses an IMU to monitor 3-axis acceleration and rotation. It is constantly powered and communicates with the Control Subsystem via the I2C protocol, sending raw motion data for analysis. The Sensing Subsystem consists of the MPU-6050 inertial measurement unit (IMU), which provides 3-axis acceleration and 3-axis angular rate data. The IMU is mounted rigidly to the PCB so that measured vibrations and rotations accurately represent frame motion. The MPU-6050 communicates with the STM32 via I^2C (Fast Mode, 400 kHz). To suppress high-frequency noise and reduce false triggers from brief impacts, the MPU-6050's internal Digital Low-Pass Filter (DLPF) is enabled and configured through its register settings. This ensures the sensor outputs delivered to the Control Subsystem are bandwidth-limited before any higher-level processing is performed.

High Level Requirement: Must support I2C communication and detect acceleration changes as small as 0.1g. Reliable motion sensing with hardware filtering reduces false alarms while preserving detection of sustained tampering signatures, supporting the ≥90% detection accuracy requirement.

Requirements	**Verification**
• The sensing subsystem shall provide filtered 3-axis acceleration data to the STM32 over I^2C at 400 kHz	• Probe SDA and SCL lines with an oscilloscope. • Verify clock frequency is 400 kHz ± 10%. • Stream IMU data continuously for at least 60 seconds.
• The MPU-6050 DLPF shall be enabled and configured to a cutoff frequency of Fc ± 10% (chosen in firmware, e.g., 20 Hz or 42 Hz)	• Read MPU-6050 configuration registers over I^2C. • Decode DLPF configuration bits per datasheet. • Log register values to confirm correct cutoff frequency selection. • Power-cycle the system and re-read registers to verify persistence.
• The sensing subsystem shall detect acceleration changes of at least 0.1 g after filtering	• Apply controlled vibration or step acceleration. • Compute peak-to-peak acceleration change. • Verify measured acceleration ≥ 0.1 g.
• The sensing subsystem shall provide data at a minimum update rate of 100 Hz	• Timestamp successive acceleration samples in firmware. • Log timestamps over serial output. • Compute effective sample rate over a 60s interval. • Verify average rate ≥ 100 Hz with minimal jitter.

The MPU-6050 DLPF is configured to a cutoff frequency of:

$$F_c = 20\text{-}42 \text{ Hz}$$

This choice ensures:

- Preservation of all relevant theft motion content (≤10 Hz)
- Attenuation of impulsive noise and sensor-level vibration
- Minimal phase delay relative to the 2-second detection latency requirement

Because the RMS energy computation integrates motion over a 100 ms window, any small phase delay introduced by the DLPF does not affect detection accuracy or system responsiveness.

2.3.3 Control Subsystem

This is the "brain" of the device. It ingests data from the IMU, applies a digital low-pass filter to remove noise, and runs a Finite State Machine (FSM). The Control Subsystem is implemented on the STM32F103 microcontroller. The STM32 periodically reads filtered IMU outputs from the Sensing Subsystem via I²C and computes tamper metrics in real time. The core detection algorithm includes:

1. Computing acceleration magnitude Amag from the 3-axis data
2. Computing windowed RMS energy Erms over a 100 ms window
3. Applying an FSM with states Idle → Warning → Alarm, where Alarm is asserted only after sustained windows above a threshold of 0.25g(≥2 seconds total)

The STM32 outputs a digital control signal to the Alarm Subsystem (MOSFET gate driver path) when entering the Alarm state.

High Level Requirement: This subsystem is responsible for meeting the 2-second detection latency requirement and enforcing the decision logic that achieves ≥90% detection accuracy across trials.

Requirements	**Verification**
• The STM32 shall execute the detection loop at 100 Hz ± 5%	• Toggle a dedicated GPIO pin once per loop iteration. • Measure GPIO frequency using an oscilloscope or logic analyzer. • Record frequency over a 60 s interval.
• 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 causes at least 2 cm of displacement for the bike on each shake forward or backward. • Use a GPIO pin to indicate FSM Alarm state. • Measure time between motion onset and GPIO transition. • Repeat tests across multiple trials, and compute the average.
• The system shall achieve ≥ 90% tamper detection accuracy over 40 trials	• Define 20 tamper trials and 20 non-tamper trials. • Apply consistent motion profiles for each trial type. • Log FSM state outcomes for each trial.

	• Compute true positives, true negatives, and overall accuracy. • Present results in a summarized table.
• The STM32 shall assert the alarm control output within 50 ms of entering Alarm state	• Monitor FSM state variable via UART logging. • Probe MOSFET gate signal with an oscilloscope. • Measure time between FSM Alarm state and gate assertion. • Repeat for multiple alarm events. • Verify timing requirements are consistently met.
• The firmware shall boot into a safe non-alarm state (Idle)	• Power-cycle the system at least 10 times. • Monitor FSM state on boot via serial output. • Verify alarm remains inactive until valid detection occurs.

2.3.4 Alarm Subsystem

The Alarm Subsystem is the "voice" of the device, responsible for producing a high-decibel deterrent when a theft is confirmed. While the rest of the system operates at **3.3V** to protect sensitive logic, the alarm utilizes the full **7.4V** from the battery to ensure the siren reaches its maximum volume.

Design Justification: MOSFET and Siren

The **IRLML0030TRPBF** MOSFET was selected for its "Logic-Level" performance, which is essential for operation with a 3.3V microcontroller.

- **Gate Threshold Voltage (V_{GS}(th)):** The datasheet specifies a maximum threshold voltage of 2.3 V; however, this value only indicates when the MOSFET begins to conduct a small current and does not represent full enhancement. Therefore, VGS(th) alone cannot guarantee low-resistance switching. Instead, the RDS(on) versus VGS characteristics were evaluated, which show that at the STM32 logic HIGH level of 3.3 V, the MOSFET achieves sufficiently low on-resistance to efficiently drive the piezo siren with minimal conduction loss. [4]
- **Drain Current Capacity (I_D):** While our siren draws approximately **100–150mA**, this MOSFET supports a continuous drain current of up to **5.3A** at 25℃. This provides a massive safety factor, preventing the component from overheating during sustained 60-second alarm cycles. [4]
- **On-Resistance (R_{DS}(on)):** At a gate voltage of 4.5V, the resistance is only **40mΩ**. Even at our 3.3V drive level, the resistance remains low enough to ensure that nearly the entire 7.4V battery rail is delivered to the siren for maximum sound pressure. [4]

Gate Resistor (100Ω-150Ω): Placed between the MCU and the MOSFET to limit instantaneous current and protect the MCU pin from damage during switching.

High-Level Requirements: This subsystem directly satisfies alarm effectiveness by ensuring the siren achieves ≥ 75 dB at 1 m and is driven robustly from the battery without loading the 3.3 V logic rail.

Requirements	Verification
• Sound Pressure Level: 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 using a yardstick. • Activate the alarm and use a digital sound level meter to record the peak dB level. • Present the result as a single numerical value in the lab notebook.
• Switching Efficiency: The MOSFET must fully saturate with a gate voltage of 3.3 ± 0.1V, ensuring the voltage across the siren is at least 7.0V (assuming a 7.4V battery)	• Connect an oscilloscope probe to the drain of the MOSFET and the other to the source. • Trigger the alarm from the STM32. • Verify the voltage drop (V_{DS}) is < 0.4V, ensuring most power reaches the siren.

• The MOSFET shall remain OFF during reset/boot (no unintended siren activation)	• Power-cycle system 10 times. • Observe siren output and gate voltage with oscilloscope • Verify no alarm output before firmware asserts Alarm.

2.4 FINITE STATE MACHINE(FSM)

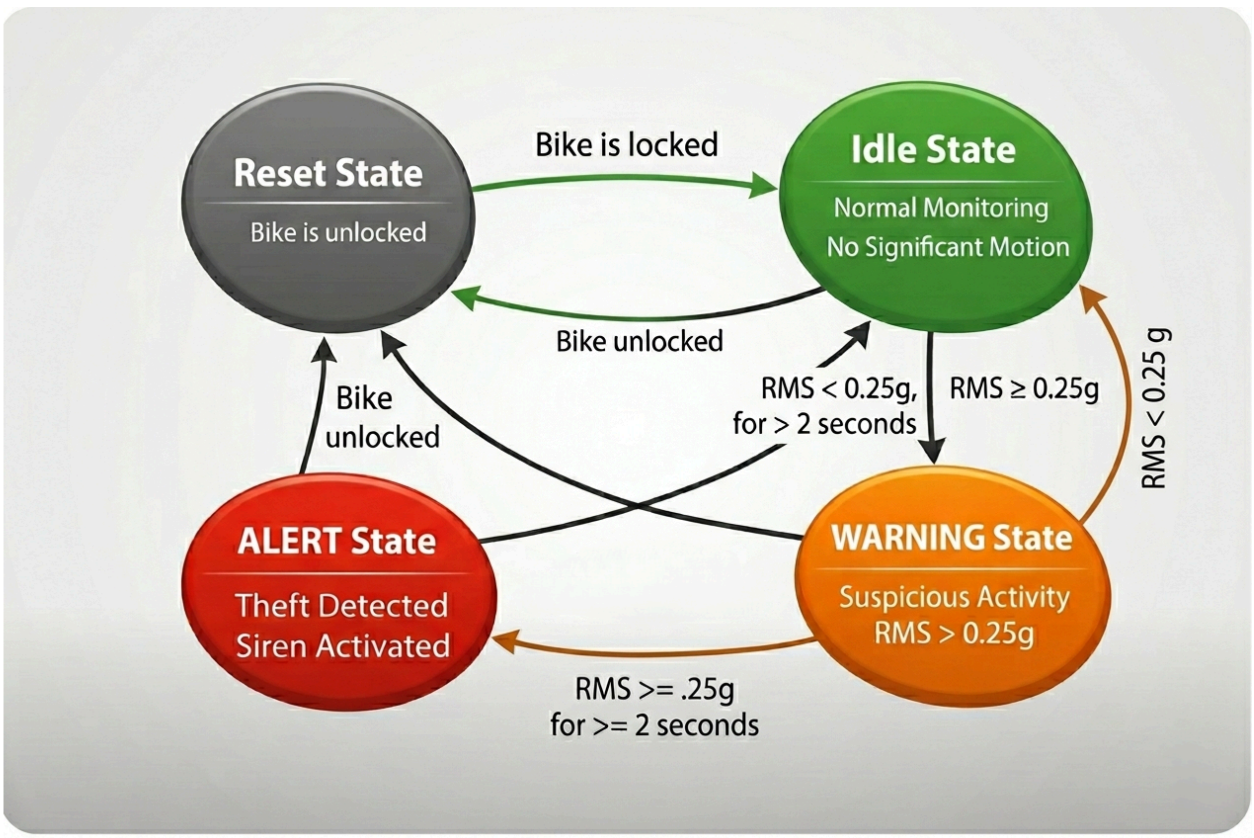

Figure #5: Finite State Machine

The E-Bike Theft Detection System employs a Finite State Machine (FSM) to classify motion behavior and determine when to activate the alarm. The FSM consists of three states: Idle, Warning, and Alert. State transitions are governed by the magnitude and persistence of filtered motion, quantified using 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 The STM32 continuously monitors the reed switch to detect the lock status of the bike. 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 secured.

Idle State

The Idle state represents normal operation where the bike is stationary or experiencing minor environmental disturbances. In this state, the STM32 continuously polls the MPU-6050 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 the Reed switch (Lock State Sensor) detects a magnet (indicating the bike is unlocked), the FSM will switch to the Reset state.

Warning State

The FSM transitions from Idle to Warning when a single 100 ms window records an E_{RMS} exceeding 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 the Reed switch (Lock State Sensor) detects a magnet (indicating the bike is unlocked), the FSM will switch 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. This persistence requirement ensures that only sustained tampering, such as rattling or lifting, initiates a response. Upon entry, the STM32 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 until over a two second period the RMS value falls below the 0.25g threshold, the timer is immediately cleared, and the system returns to the Reset state. We can also switch out of the alert state if the Reed switch detects a "Unlocked" state change or the system is manually reset, returning the FSM to the Reset state.

2.5 Tolerance Analysis

The most critical risk to this project is the system's ability to distinguish between environmental noise (e.g., wind or a light bump) and theft (e.g., shaking or lifting). If the system is too sensitive, it will initiate false alarms; if it is not sensitive enough, it will fail its core function of theft detection and deterrence.

Signal Processing Methodology

The system utilizes an IMU to monitor 3-axis acceleration. To normalize this motion, the microcontroller first calculates the magnitude of the acceleration vector A_{mag}:

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

To prevent false triggers from momentary acceleration spikes, the system evaluates the Root Mean Square (RMS) energy over a short time window rather than triggering on a single data point. A Digital Low-Pass Filter (DLPF) is also applied to block background noise.

Quantitative Verification

The RMS energy E_{RMS} is calculated over a 100ms window (n samples) to isolate dynamic motion from gravity:

$$E_{RMS} = \sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(A_{mag,i} - 1g\right)^2}$$

Step-by-Step Calculation: Sampling and Processing Feasibility

To meet the 2-second latency requirement, we must ensure our sampling rate (f_s) provides enough data points for a statistically valid RMS calculation within our 100ms window.

1. **Window Size (T_w):** 100ms.
2. **Required Samples (n):** To accurately capture a theft signature (sustained oscillations up to 10Hz), we aim for a sampling rate of 100Hz (f_s = 100 samples/sec).
3. **Samples per Window:** $n = f_s \times T_w = 100 \times 0.1 = 10\ samples/evaluation.$
4. **Processing Time:** The **STM32F103** runs at 72MHz. Calculating one square root and several additions/multiplications for 10 samples takes approximately 50µs.
5. **I2C Latency:** Reading 6 bytes of data from the MPU-6050 at 400kHz takes approximately 150µs.
6. **Total Loop Time:** ≅ 200µs, which is significantly less than our 10ms inter-sample period ($1/f_s$), proving the MCU is not overburdened.

Scenario Analysis:

- **Environmental Noise Floor:** Typical urban vibrations or wind movement produce small A_{mag} deviations (0.1g to 0.2g). In a 100ms window, these yield an E_{RMS} of approximately 0.13g.

- **Theft Signature:** Brute-force shaking or rattling typically produces sustained oscillations between 0.5g and 1.5g. This results in an E_{RMS} of 0.56g.

- **Safety Margin:** By setting the Warning State threshold at 0.25g, we can effectively filter out any background noise while ensuring that the system still correctly detects theft attempts.

Latency Confirmation

To meet the 2-second latency requirement, the Finite State Machine (FSM) requires sustained E_{RMS} readings above the threshold for a set number of consecutive windows. With a 100ms window, the system can perform 20 full evaluations within the 2-second limit. This would allow for more than enough data to detect a theft attempt.

2.6 Cost Analysis

The total cost for parts as seen below before shipping is \$50.63. A 5% shipping cost adds another \$2.53 and 10% sales tax adds another \$5.06. We can expect a salary of \$40.00/hr×2.5×60hrs = \$6,000.00 per team member. We need to multiply this amount with the number of team members, \$6,000.00× 3 = \$18,000.00 in labor cost. This comes out to be a total cost of \$18,058.22.

2.6.1 Part Costs

Description	Manufacturer	Quantity	Extended Price	Link
Microcontroller - STM32F103C8 (48LQFP)	STMicroelectronics	1	\$6.08	Link
Voltage Regulator - LD1117-3.3 (SOT-223-3L)	UMW	1	\$0.30	Link
MOSFET - IRLML0030TRPBF (SOT23)	Infineon Technologies	1	\$0.50	Link
Capacitor - 0.1µF 10% / 16V (0603)	KEMET	7	\$0.10	Link
Capacitor - 4.7µF / 25V (0805)	KEMET	2	\$0.66	Link
Capacitor - 10µF / 20% / 10V (0603)	TAIYO YUDEN	2	\$0.49	Link
Resistor - 4.7kΩ (0603)	YAGEO	2	\$0.10	Link
Resistor - 150Ω (0603)	Stackpole Electronics Inc	1	\$0.10	Link
Resistor - 100kΩ 5%(1/8W) (0805)	YAGEO	3	\$0.10	Link
Capacitor - 0.01µF / 16V (0603)	YAGEO	1	\$0.08	Link
Resistor - 0Ω (0603)	YAGEO	1	\$0.10	Link
CPI-4233C-120 MINI PIEZO SIREN	Same Sky	2	\$11.06	Link
Resistor - 10kΩ (0603)	YAGEO	3	\$0.10	Link

Capacitor - 10µF / 50V (0805)	Murata Electronics	1	$0.37	Link
Gy-521 MPU-6050 MPU6050 Module 3 Axis Analog Gyro Sensors+ 3 Axis Accelerometer Module	InvenSense	1	$6.99	Link
FTSH-105-01-L-DV	Samtec Inc.	1	$1.36	Link
RI-02GP1520	Comus International	1	$0.75	Link
N52P250125	Magnet Applications	1	$0.62	Link
Turnigy 1000mAh 2S (7.4V) 40C Lipo Battery Pack w/JST	Turnigy	1	$7.19	link
Total Part Costs			$50.63	

Figure #6: Itemized List of Components and Costs

2.7 Schedule

Week	Task	Person
February 23rd – March 2nd	• Order breadboard, 7.4V battery, LD1117V33 regulators, and TH,0603 and 0805 components for prototyping. • Establish basic I2C communication between STM32 and MPU-6050 on a breadboard. • Research mounting solutions for a weather-resistant bike frame enclosure. • Test the 7.4V to 3.3V regulation circuit and measure current draw with a multimeter.	Paul Kacper JP Everyone
March 2nd – March 9th	• Finalize the FSM logic (Idle, Warning, Alarm states) in firmware. • Breadboard test the MOSFET switching circuit with the 7.4V rail and the 75dB siren. • Characterize environmental noise vs. theft signatures to set RMS energy thresholds.	Kacper Paul JP

March 9th - March 16th	• **PCB Design Week:** Begin schematic capture using TH,0805 and 0603 footprints for easy soldering. • Implement Digital Low-Pass Filtering (DLPF) in the STM32 control loop. • Conduct 40 test trials on the breadboard to verify the 90% detection accuracy requirement.	Everyone Kacper Everyone
March 16th - March 23rd	• **Spring Break:** Finalize and order the custom PCB.	JP
March 23rd- March 30th	• Solder the 3.3V regulator and MCU support circuitry to the PCB first; verify power rails. • Assemble the siren and battery connectors into the physical bike enclosure.	Paul JP
March 30th - April 6th	• Complete hand-soldering of sensors (MPU-6050, SW-420) to the PCB. • Integrate all firmware modules and perform initial system-wide tests. • Verify the 75dB sound pressure level at 1 meter using a decibel meter.	Paul Kacper Everyone
April 6th - April 13th	• **Integration Testing:** Mount the system on a test bike and refine RMS thresholds for real-world use.	Everyone
April 13th - April 20th	• Fix any remaining firmware bugs or mechanical mounting issues.	Everyone
April 20th - April 31st	• Final Mock-up and Senior Design Demo.	Everyone

Figure #7: Schedule for Project Progression

3. Discussion of Societal Impact, Engineering Standards, Ethics, and Safety Considerations

3.1 Societal and Environmental Impact

This project directly supports public welfare by protecting personal property and fostering a secure environment for eco-friendly transportation. By reducing theft-related losses for individual owners and ride-sharing companies like Lyft or Lime, economic resources can be redirected toward service expansion and infrastructure maintenance. Furthermore, a reliable security system encourages the adoption of e-bikes, contributing to a reduction in carbon emissions from traditional vehicle traffic and supporting global sustainability goals.

3.2 Engineering Standards

Our design adheres to several critical engineering and communication standards:

- **I2C Communication (Inter-Integrated Circuit):** Used for standardized data transfer between the MPU-6050 IMU and the STM32 microcontroller.
- **IPC-2221:** Standards followed for the design and clearance of the custom PCB to ensure electrical reliability. [5]
- **IEEE 802.15.4:** Relevant if the system is expanded to include low-power wireless alerts. [2]
- **OSHA Standards & Urban Ordinances:** The alarm is capped at 90dB to remain effective as a deterrent while complying with common noise pollution regulations and avoiding hearing damage to the public. [3]

3.3 Ethical Considerations

We prioritize the **IEEE Code of Ethics Section 1.1**, which mandates holding "paramount the safety, health, and welfare of the public" [2]. A primary ethical concern is the risk of "public nuisance" caused by frequent false alarms. To address this, we have implemented rigorous signal processing, including DLPF and RMS energy calculations, to ensure the alarm only triggers during legitimate theft signatures. Additionally, in accordance with **ACM Code of Ethics Section 1.2**, we prioritize "avoiding harm" by ensuring the alarm volume does not exceed levels that could cause physical distress to bystanders.

3.4 Safety Concerns and Procedures

Electrical Safety:

- **Regulation:** The power subsystem must strictly regulate voltage to 3.3 ± 0.1V to prevent component damage or fire hazards.
- **Protection:** Decoupling capacitors (0.1µF) and bulk capacitors (4.7-10µF) are used to stabilize the power rail and prevent MCU resets during the high-current draw of an alarm event.

Battery Safety (Li-Po):

- **Charging/Discharging:** We will follow a strict lab safety protocol for Lithium-Polymer batteries, ensuring they are only charged using dedicated balanced chargers to prevent thermal runaway or swelling.
- **Handling:** Li-Po batteries will be stored in fire-resistant bags when not in use.

Mechanical Safety:

- **Enclosure:** The final PCB and battery will be housed in a weather-resistant, impact-proof enclosure securely mounted to the bike to prevent it from becoming a mechanical hazard or causing an electrical short due to environmental exposure.

Mitigation Procedures:

1. **Lab Safety:** Always use a current-limited power supply during initial PCB testing before connecting the Li-Po battery.
2. **Emergency Stop:** The firmware includes a "disarm" button to immediately silence the alarm if it is triggered accidentally.

4. References:

[1] C. Farr, “Divvy Responds to Video Showing Bike Methodically Dislodged From Docking Station,” *NBC Chicago*, Jul. 24, 2018.

https://www.nbcchicago.com/news/local/divvy-bike-theft-video/176532/ (accessed Feb. 13, 2026).

[2] IEEE, “IEEE Code of Ethics | IEEE,” *Ieee.org*, 2020. https://www.ieee.org/about/corporate/governance/p7-8 (accessed Feb. 13, 2026).

[3] OSHA, “Occupational Noise Exposure - Overview | Occupational Safety and Health Administration, 2023. https://www.osha.gov/noise

[4] “IRLML0030TRPbF HEXFET ® Power MOSFET Application(s) Micro3 TM (SOT-23) IRLML0030TRPbF,” Feb. 2012. Accessed: Feb. 26, 2026. [Online]. Available: IRLML0030TRPbF

[5] “Generic Standard on Printed Board Design,” Nov. 2012. Accessed: Feb. 26, 2026. [Online]. Available: IPC-2221B Generic Standard on Printed Board Design - Table of Contents