Helix Vault

Embedded Systems Final Project — ESE 5190 (Fall 2025)

A three layer secure safe integrating biometric authentication, analog combination input, and PIN verification. Powered by two ATmega328PB microcontrollers and an ESP32 fingerprint module, Helix Vault blends embedded security logic, mechanical actuation, and a guided LCD user interface.

Team: Byte This (Team 16)

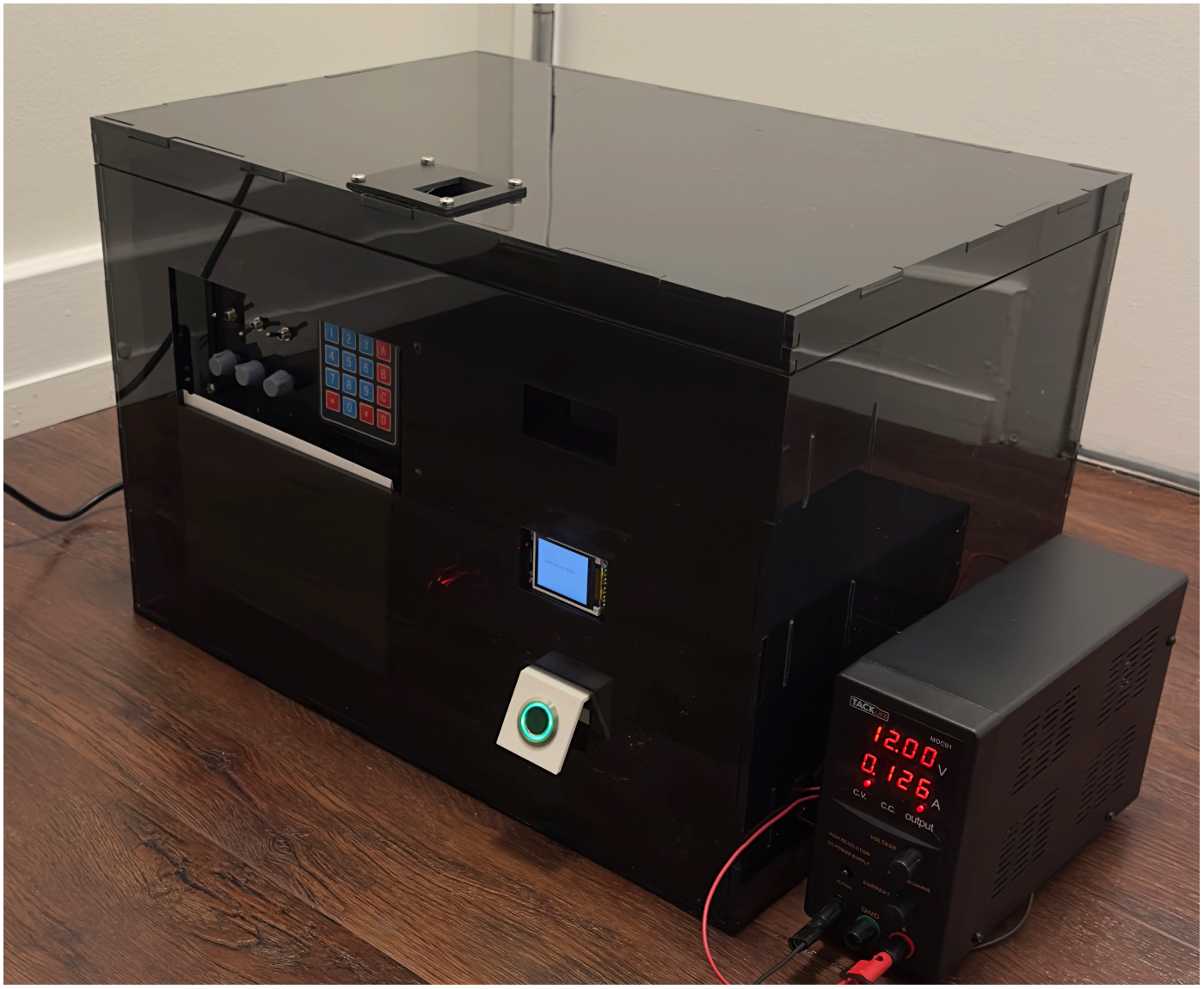
Members: Yongwoo Park, Jeevan Karandikar, Tomas Ascoli

Demo Video

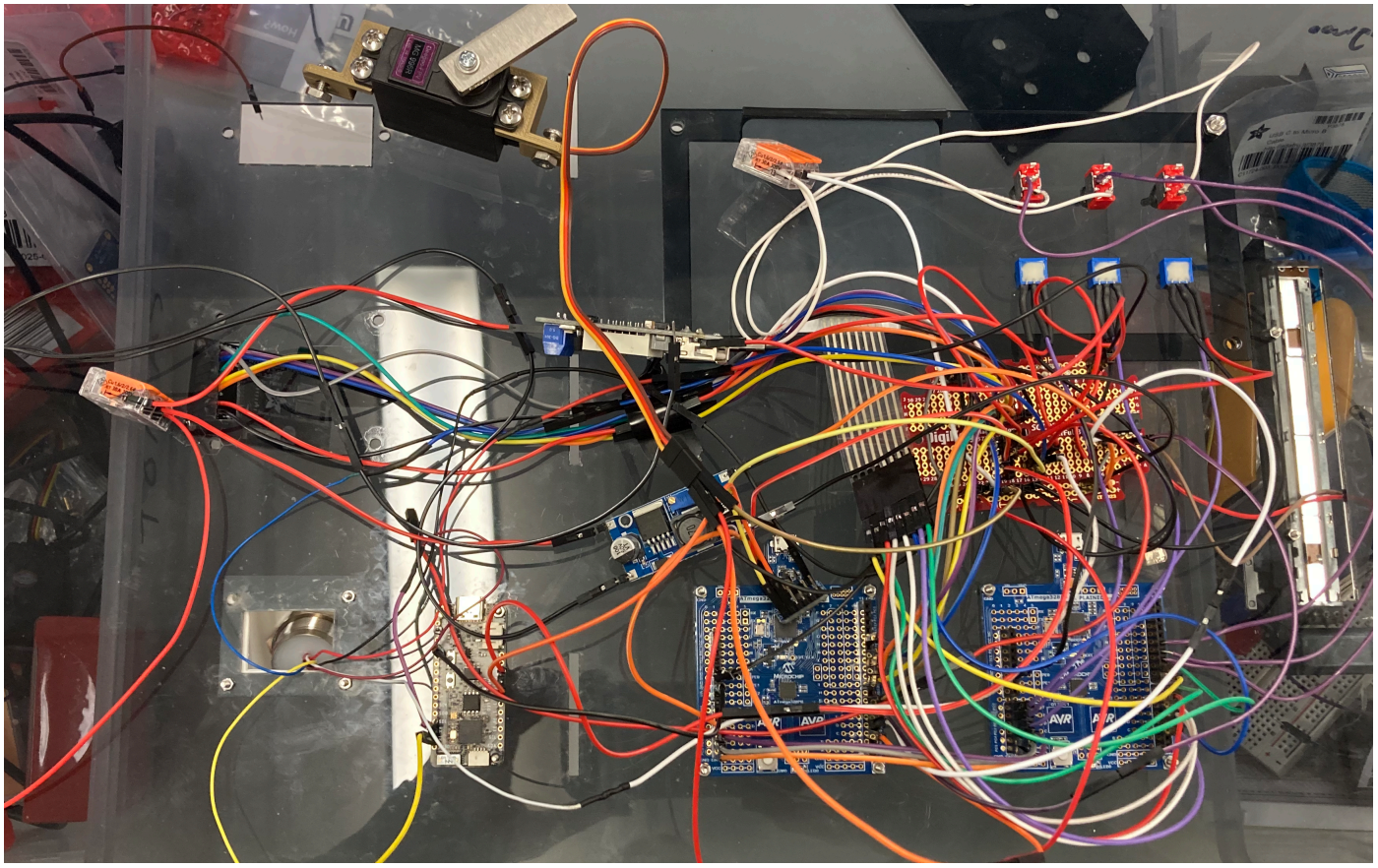
https://youtu.be/f8Z03Lm1yS4

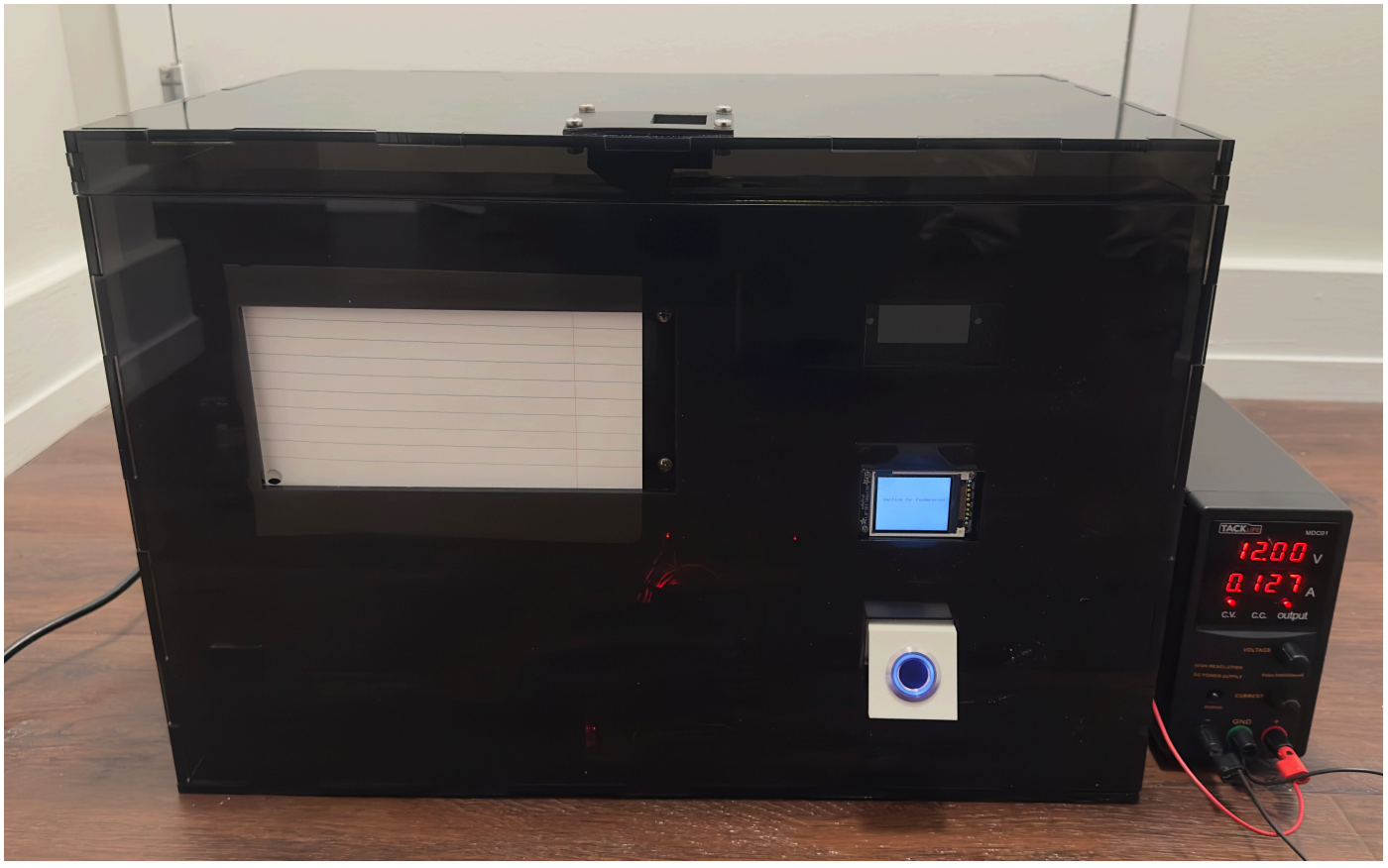
Final Product Images

Device Overview

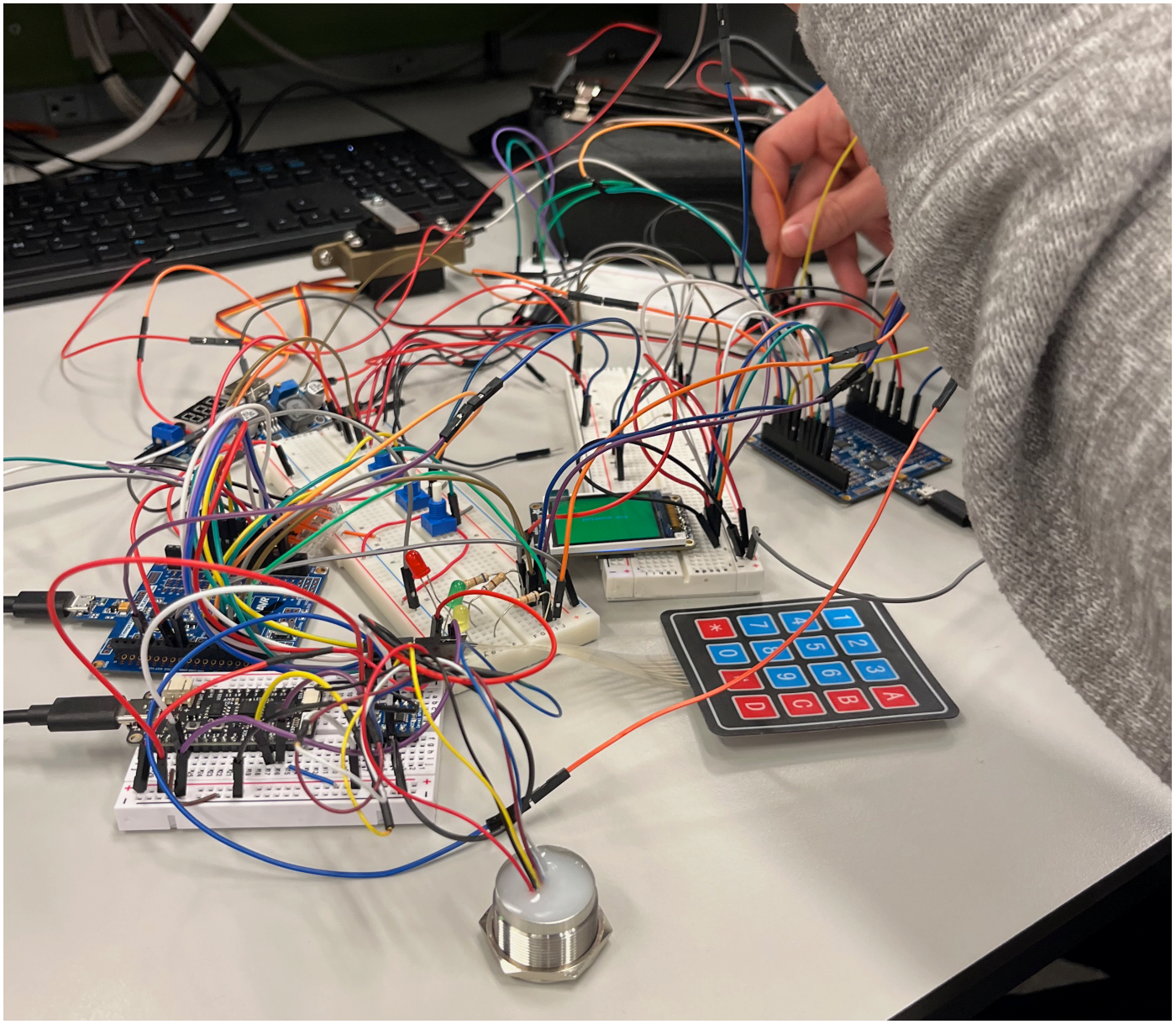

12.00
V
0.126
A
C.V.
C.C.
output

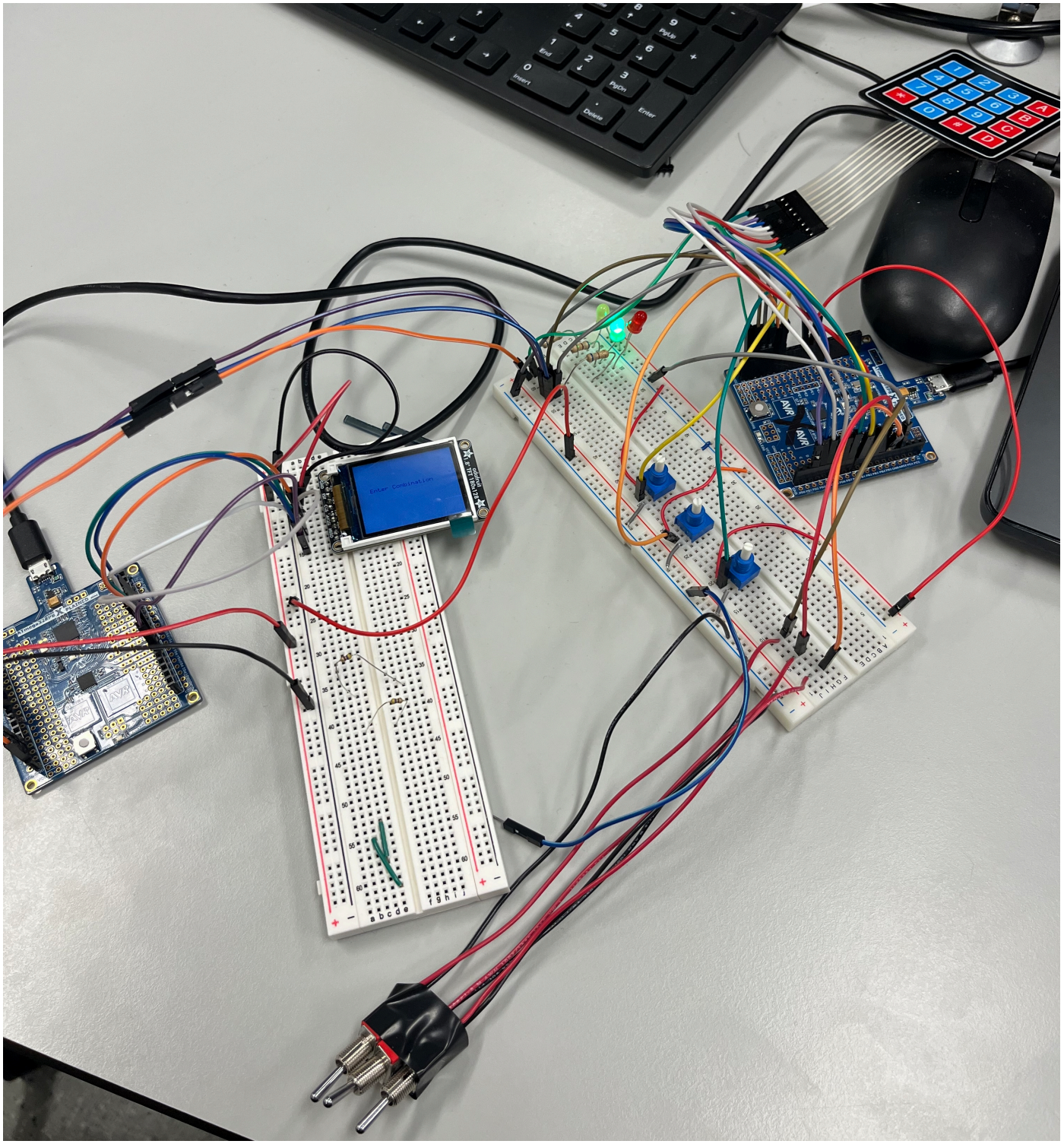

12.00
0.125
V
A
C.V.
C.C.
output



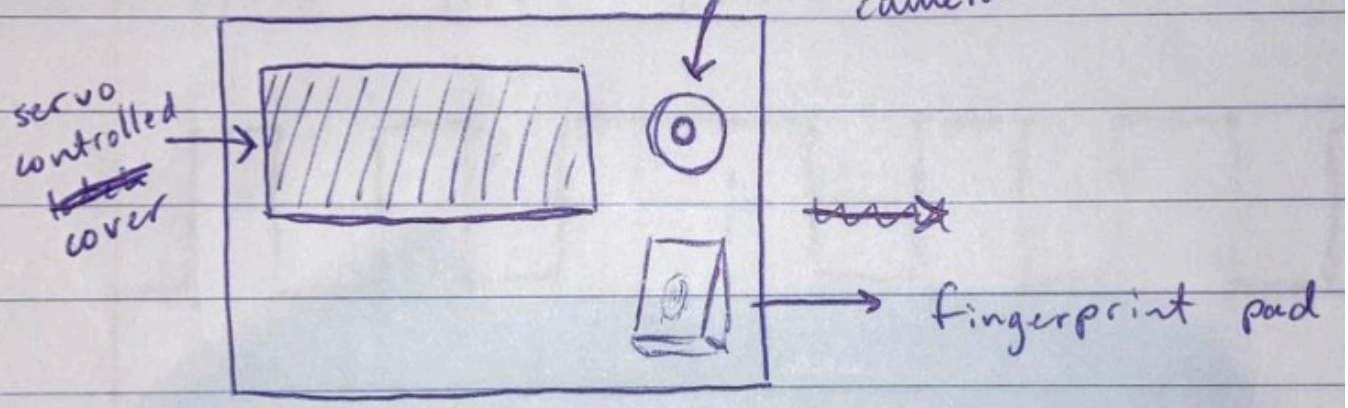


Prototype & Sketches

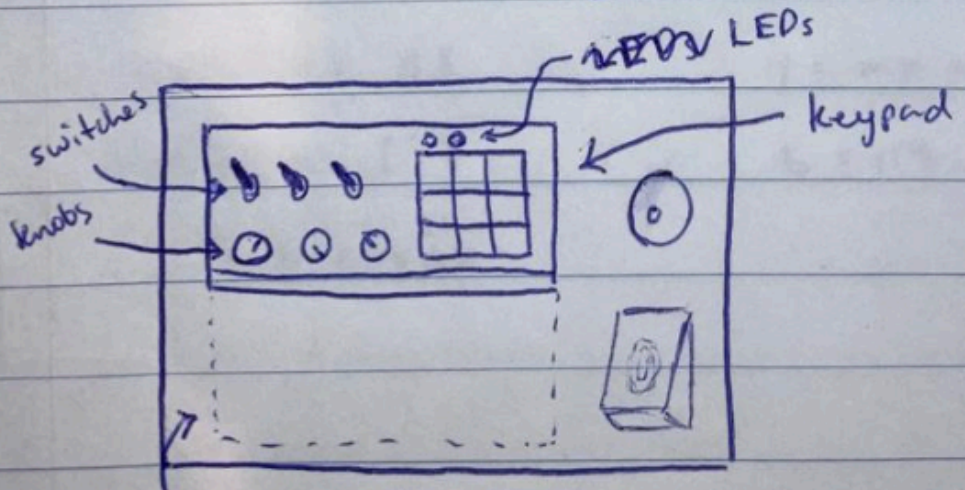

1 2 3 A
4 5 6 B
7 8 9 C
* 0 # D


Enter Combination

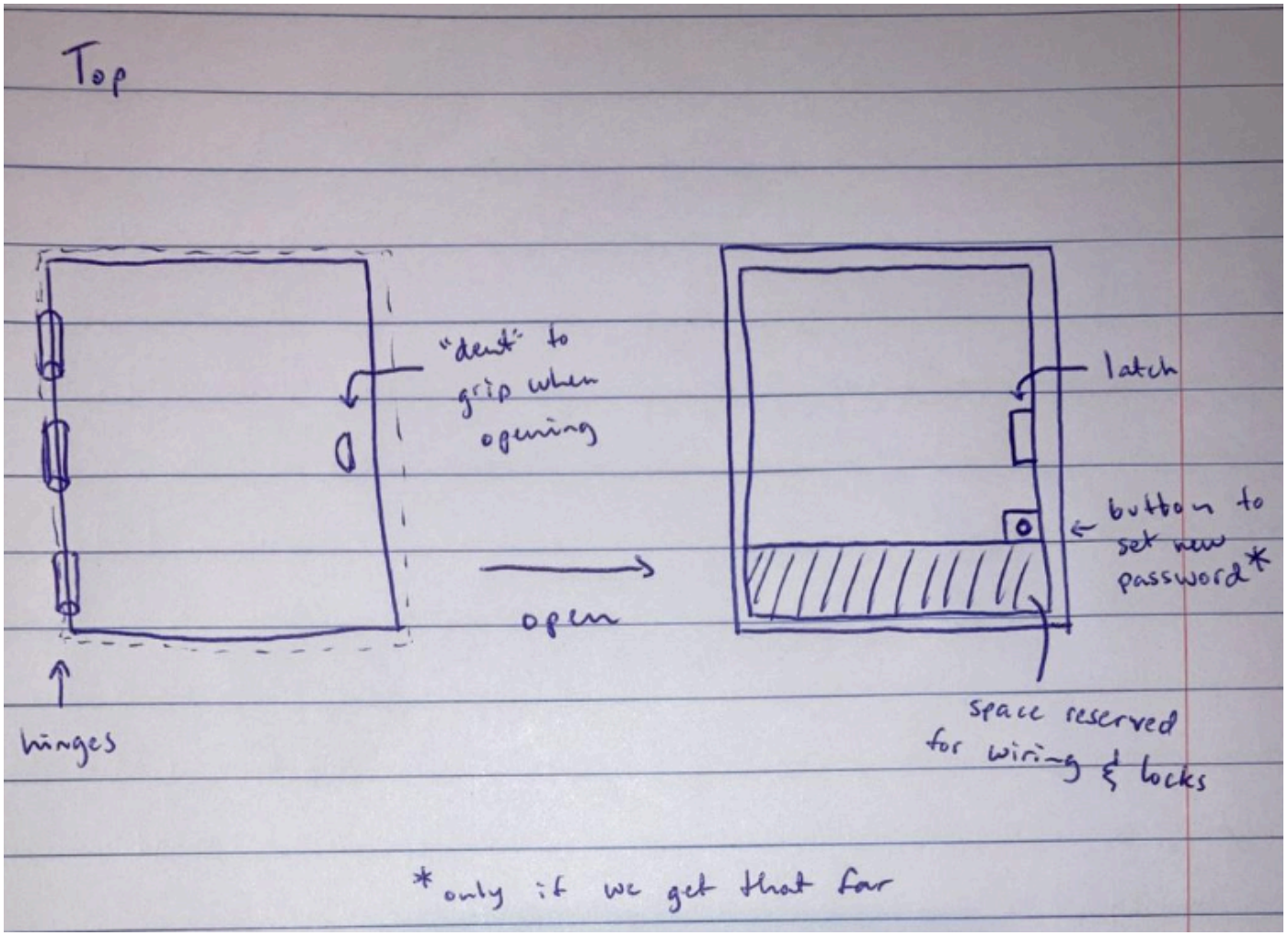
Front Panel



after face & finger print are recognized



cover slides down using servo + rack & pinion



System Overview

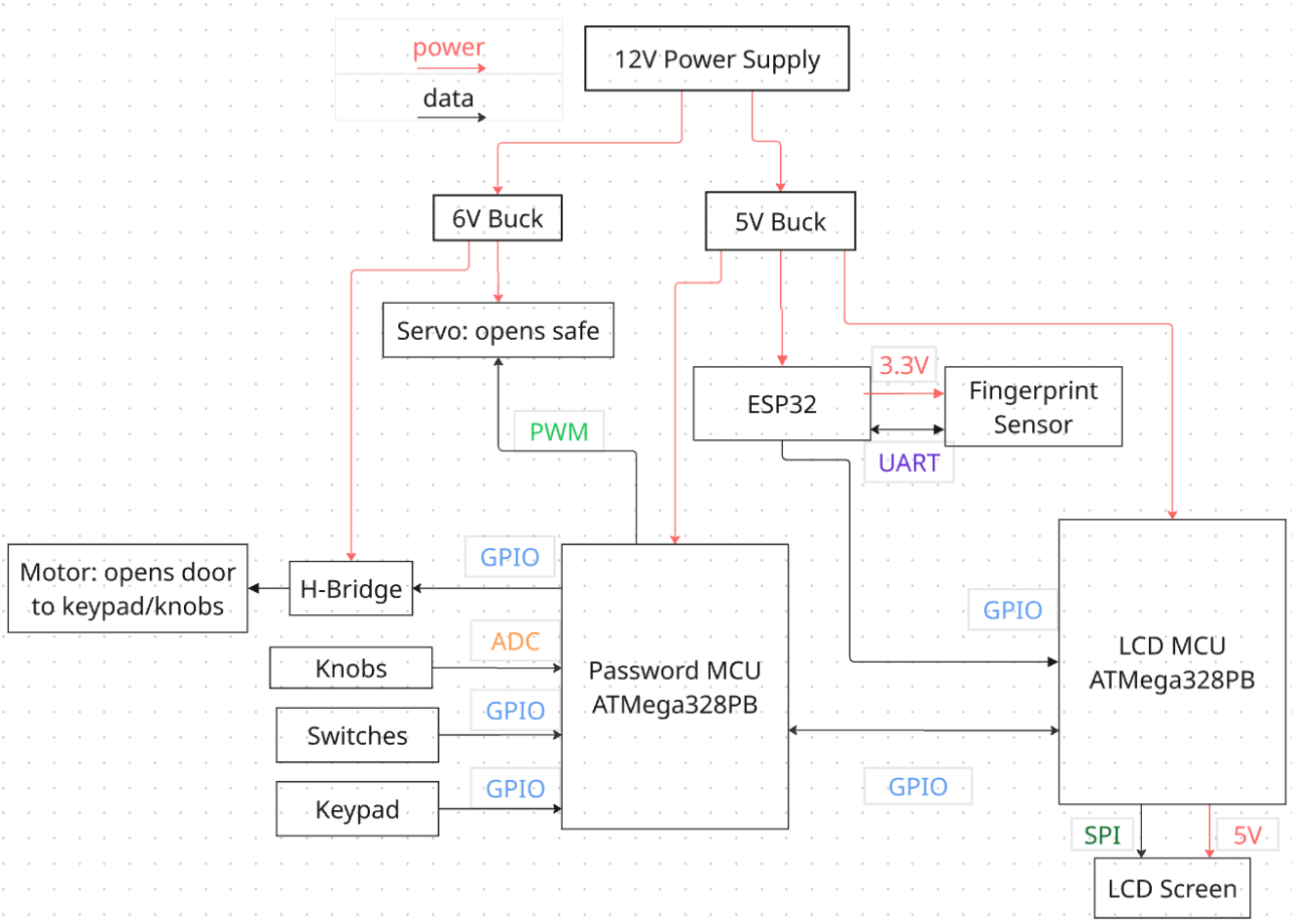
Helix Vault uses a three stage unlock sequence:

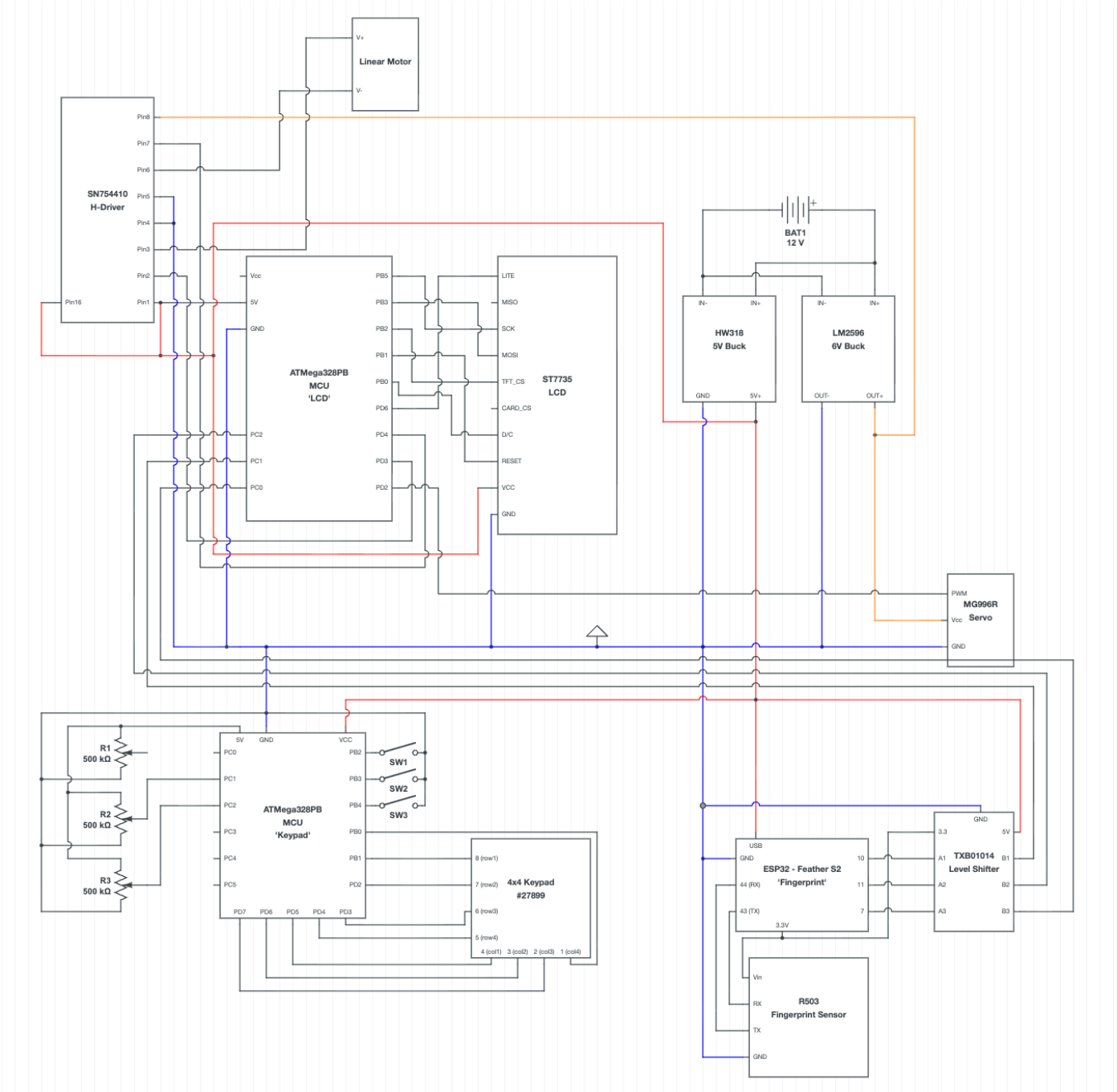
1. **Fingerprint verification** handled by an ESP32 and R503 optical fingerprint sensor
2. **Analog combination** read via ADC knobs and switches
3. **PIN entry** using a matrix keypad

Only when all three layers succeed, in order, does the servo release the final latch.

A DC motor opens the internal sliding door immediately after the fingerprint stage, revealing the analog combination panel and the keypad.

System Block Diagram


power
data
12V Power Supply
6V Buck
5V Buck
Servo: opens safe
3.3V
ESP32
Fingerprint Sensor
PWM
UART
Motor: opens door to keypad/knobs
H-Bridge
GPIO
GPIO
LCD MCU ATMega328PB
ADC
Knobs
Password MCU ATMega328PB
GPIO
Switches
GPIO
GPIO
Keypad
SPI
5V
LCD Screen



Software Requirements Specification (SRS)

Definitions

- **MCU** : Microcontroller Unit
- **LCD** : Liquid Crystal Display
- **ADC** : Analog-to-digital converter
- **PIN** : Personal Identification Number
- **Unlock Sequence** : Fingerprint → Combination → PIN

- **R503** : Fingerprint sensor module

SRS-01 - Low Power Management

Requirement: The system shall enter low power mode when idle for more than 5 minutes. If the battery dies, the system shall be rechargeable without unlocking or compromising the safe.

Result: We did not add a low-power mode, but powering up the system never compromises safety—on startup, it always verifies that all locks are closed. If the box is powered off, it does not lock itself, so users should ensure it is closed and latched before disconnecting power. The box can also be easily locked by pressing "*", and any power loss during unlocking resets it to the first security layer.

SRS-02 - Correct Password Recognition

Requirement: The safe shall only open when all three security layers are successfully completed in sequence: (1) a registered fingerprint is recognized, (2) the correct analog combination (potentiometer positions and switch states) is entered, and (3) the correct 4-digit PIN associated with the recognized fingerprint is entered. The system shall reject any incorrect input at any stage and shall not proceed to subsequent stages.

Result: Requirement fully met. The fingerprint sensor reliably accepts only saved fingerprints, each linked to a unique combination and PIN. The keypad is disabled until the analog combination is correctly entered, and only the exact 4-digit PIN associated with the authenticated fingerprint will open the box.

SRS-03 - Servo + Motor Control

Requirement: The DC motor shall open the sliding door only when a registered fingerprint is successfully recognized. The servo shall actuate the latch only after all three security layers (fingerprint, analog combination, and PIN) are successfully completed in sequence. The door shall close when the user presses the "*" key on the keypad.

Result: We updated this requirement to servo + DC motor control. The DC motor opens the first door only after a valid fingerprint match, and extensive testing with all of our unregistered fingers and other classmates confirmed that incorrect fingerprints never trigger it. The combination and PIN panel is physically inaccessible until this door opens, and the servo latch actuates only after the correct fingerprint, correct combination, and

correct PIN are entered in sequence. All incorrect fingerprints and PINs tested showed a 100% success rate in blocking access.

SRS-04 - System Lockdown

Requirement: The system shall lock down for 5 minutes if the user types in an incorrect PIN 3 times in a row during a single unlock attempt session.

Result: The system does not lock down after 3 incorrect tries, but does lock down if the user manually triggers it by pressing "*" on the keypad when the box is open.

SRS-05 - Storage Management

Requirement: There shall be an interface for creating new passwords and deleting old ones. The system shall support storage for at least 3 user profiles, each with a unique fingerprint, analog combination, and PIN. The system shall reject an attempt to add a new password when storage capacity (3 profiles) is reached.

Result: We modified this requirement, instead of having a built in interface that allows the user to change passwords and add fingerprints, this can be done using a computer and connecting to the ATMega's when the box is open and the lid protecting the electronics is taken off.

Hardware Requirements Specification (HRS)

Definitions

- **DC Motor** : Linear actuator for sliding door
- **Servo** : Rotary actuator for latch
- **H-Bridge** : Motor driver IC
- **Sliding Door** : Inner door covering combination + keypad

---

HRS-01 - Microcontroller

Requirement: The overall system control shall be provided by at least one ATmega328PB microcontroller.

Result: Requirement fulfilled. The system uses two ATmega328PB microcontrollers for system control.

HRS-02 - Biometric Lock 1

Requirement: A fingerprint scanner (R503 module) shall be used as the first biometric lock. The fingerprint scanner shall be able to scan and recognize fingerprints from at least 3 different users (Yongwoo, Jeevan, and Tomas), and shall differentiate between them with at least 95% accuracy.

Result: Requirement fulfilled. The fingerprint scanner successfully scans and recognizes fingerprints from all three team members and differentiates between them with 100% accuracy in testing.

HRS-03 - Biometric Lock 2

Requirement: A facial recognition camera shall be used as the second biometric scanner. This camera shall be able to scan and recognize faces, and shall differentiate between them with at least 90% accuracy.

Result: Unfortunately due to shipping issues we never received the facial recognition module. Requirement not met.

HRS-04 - Keypad

Requirement: A matrix keypad shall be used as the last lock, where the user has to type a 4-digit PIN to open the box. The keypad shall have visual feedback: a red LED that turns on when the keypad is active but the box is closed, and a green LED that turns on when the correct password is typed in.

Result: The keypad is used to enter a 4-digit PIN. Instead of LEDs, an LCD screen was used instead for prompting the user and showing progress, providing better visual feedback.

HRS-05 - Servo

Requirement: A servo motor shall be used to open the door that allows the user to access the knobs and keypad. This door shall only open if a registered fingerprint is successfully recognized. The servo shall have a torque of at least 2.5 kg-cm to reliably open the door mechanism.

Result: The door revealing the knobs and keypad is actuated by a DC motor driving a linear slider instead of a servo. This door only opens once the fingerprint is verified. The DC motor provides sufficient force to reliably open the sliding door mechanism.

HRS-06 - Relay

Requirement: A relay shall be used to turn on the keypad power only when the correct combination of switches and knobs is inputted.

Result: The keypad does not need a separate power source - instead GPIO pins are used to scan for keypad inputs. The GPIOs do not scan the keypad unless the correct switch and knob combination is detected, achieving the same functional requirement without a relay.

Conclusion

Helix Vault brought together firmware design, inter-MCU communication, mechanical actuation, and user interface development into a cohesive embedded system.

What went well

- Reliable multi-MCU communication using simple GPIO encoding
- Smooth integration of actuators with LCD-guided user experience
- Robust fingerprint performance
- Effective power management with simple 12V power supply to power all circuitry
- Mechanical design and hardware installation was seamless
- Efficiently split up tasks to create hardware and software parts that could come together for the final product

Lessons learned

- Designing modular firmware significantly simplifies integration
- UART debugging with mis-matched voltage domains requires careful inspection
- Mechanical choices (servo torque, motor force) matter as much as code

Proudest Accomplishments

- Homemade Multi MCU communication was seamless and effective
- No broken/fried electronic components
- Extremely smooth operation and unlock process
- Final result looks very close to a final prototype

Approach changes

- Original facial recognition stage was removed because the module never arrived
- Two servos were replaced with a DC motor + servo approach for reliability
- LEDs were replaced with a full LCD UI to satisfy SPI and improve UX

Obstacles

- Laser cutter downtime
- Hardware shipping delays
- Limited budget ($150 total)
- Low torque DC motor actuating sliding door
- Couldn't get a bare-metal C UART driver working with the fingerprint sensor

Next steps

- Add facial recognition
- Add increased security layers
    - Biometric, for example iris scanner
    - More unique combination lock inputs
- Create a custom PCB to shrink the electronics footprint
- Secure override key for power failures
- Implement onboard user management
- Unlock attempt history
    - With facial recognition camera pictures can be taken of the user/intruder

References

- R503 Fingerprint Sensor Library: https://github.com/mpagnoulle/R503-Fingerprint-Sensor-Library
    - Used on ESP32

Repository Links

- **GitHub Repo:** https://github.com/upenn-embedded/helix-vault

---

Team Information

Team 16 — Byte This

- Jeevan Karandikar — jeev@seas.upenn.edu
- Yongwoo Park — yongwoo@seas.upenn.edu
- Tomas Ascoli — tascoli@seas.upenn.edu