ECE 445: SENIOR DESIGN LABORATORY
DESIGN DOCUMENT

Intelligent Shared Item Cabinet

Team #23

Team Members:
Nihaoxuan Ruan (ruan14)
Yihong Yang (yihongy3)
Xiaotong Cui (xcui15)
Yanxin Lu (yanxinl4)

Sponsor: Piao Chen

TA: Luozhen Wang

Date: April 14, 2025

1 Introduction

1.1 Problem and Solution 0verview

In modern campus environments, students frequently need to borrow small tools (e.g., screwdrivers, wrenches) outside standard front-desk hours, leading to significant inconvenience and wasted time.

Our intelligent shared item cabinet addresses the critical gap in 24/7 access to shared tools on campuses by integrating campus card authentication, automated item recognition, and a user-friendly interface, which are optimized specifically for the university setting. Another alternative to bypass the issues of the manual check-out systems and general lockers is having a system that is scalable, real-time tracking, and seamless integration with campus infrastructure. Achieving an ECE-centric setup is critical to connect the hardware reliability (sensor design, cabinet durability) with the software intelligence (real-time database synchronization, fault-tolerant operations), giving pedagogical effectiveness and sustainability respectively. Our approach differs by offering a proof of concept model that is based on investigating campus card APIs and modular approach to emphasize security, accessibility, and scalability.

Our key success criteria include reliable item detection, user-friendly operation, and seamless integration with existing campus infrastructure, ultimately creating a secure and efficient platform that enhances the overall student experience.

1.2 Visual Aid

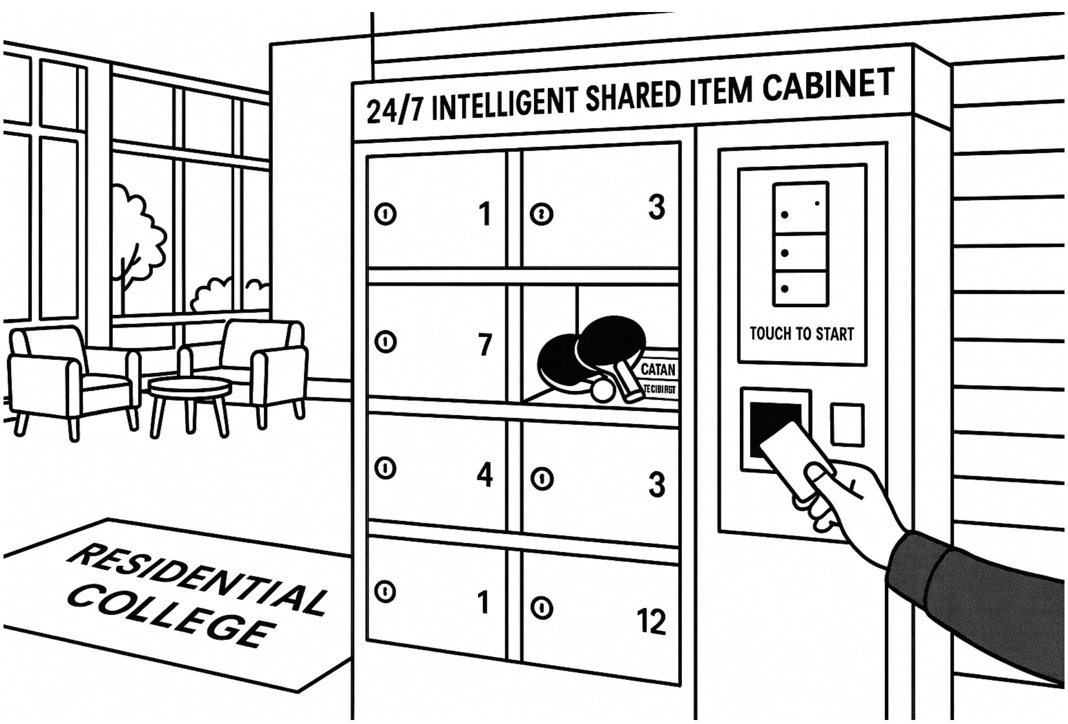

Figure 1: **Visual Aid.** Generated by GPT-4o[1].

1.3 High-Level Requirements List

- The cabinet must unlock a compartment within 2 seconds after scanning a valid campus card.
- The Item Detection Subsystem must correctly identify returned items at least 95% of the time.
- The system must log every borrow and return event in the database with 100% reliability.

2 Design

2.1 Block Diagram

The block diagram in Figure 2 provides an overview of the system architecture, illustrating the interconnection among the Cabinet Subsystem, Power Subsystem, Control Subsystem, Item Detection Subsystem, and User Interface Subsystem. The Cabinet Subsystem includes an electromagnetic lock for securing items, while the Item Detection Subsystem integrates load cells and cameras to detect stored objects. A centralized Control Subsystem, including the microprocessor and SD card, coordinates data exchange with all subsystems. The Power Subsystem ensures stable energy delivery through its Li-Ion battery and voltage regulator, and the User Interface Subsystem offers real-time feedback and user authentication via a card reader and touch screen. This diagram shows how power and data signals are routed between subsystems to enable reliable, cohesive operation.

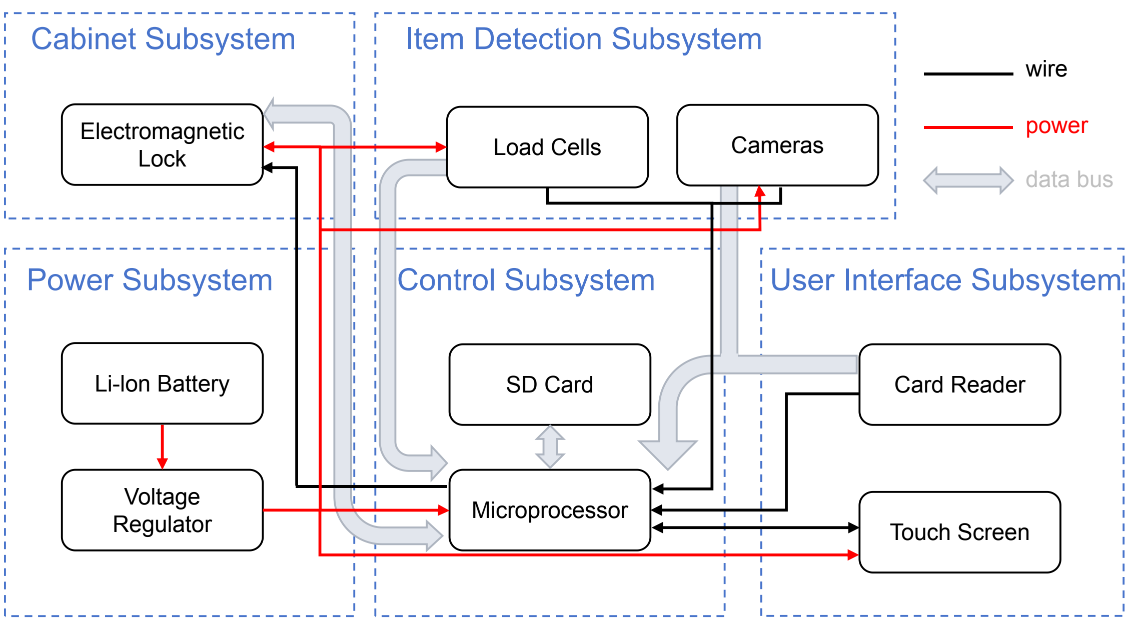

Figure 2: **Block Diagram.** High-level system overview showing the interconnections among the Cabinet, Power, Control, Item Detection, and User Interface Subsystems.

2.2 Physical Design

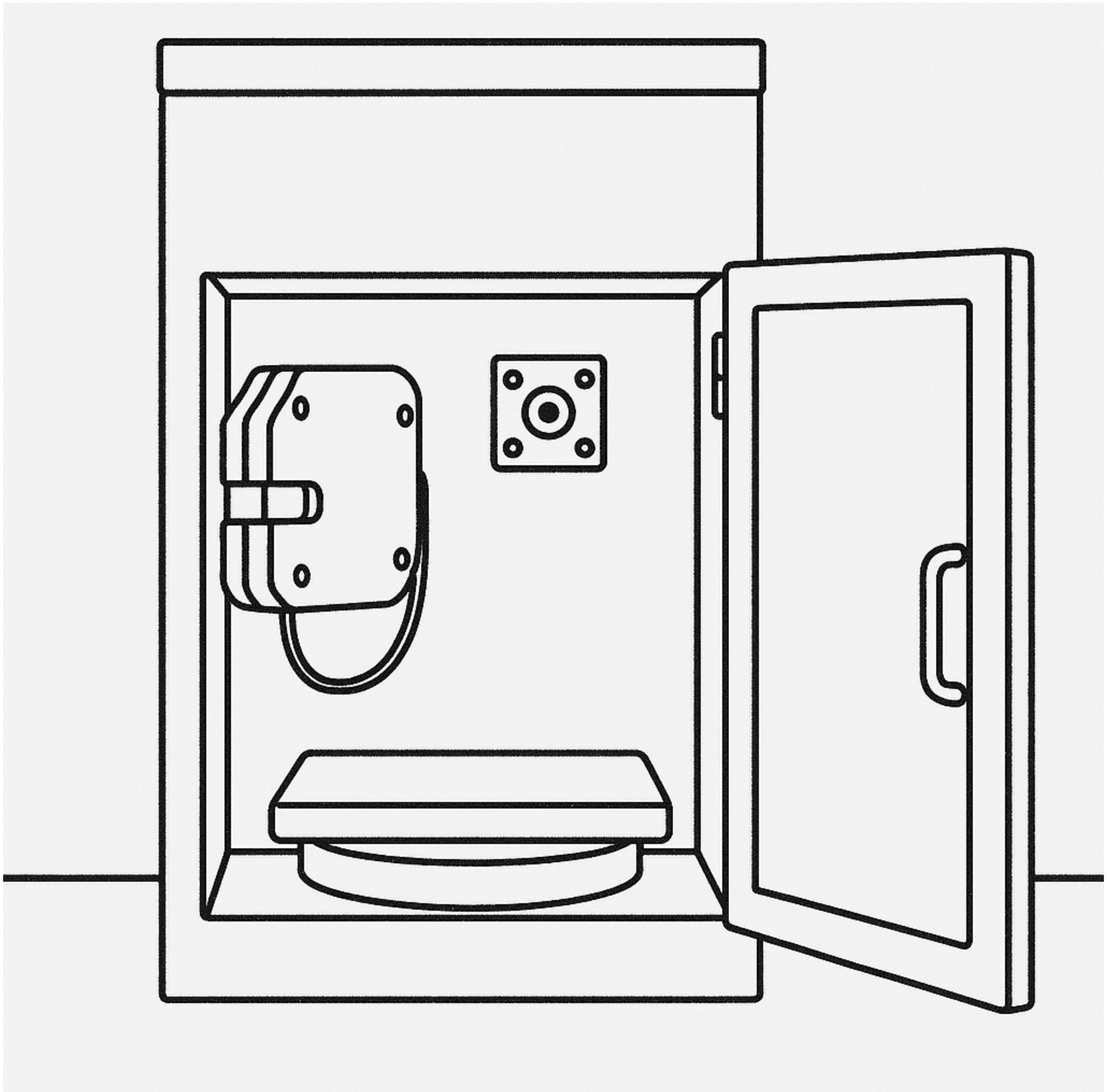

Figure 3: **Physical Design.** Generated by GPT-4o[1].

The cabinet has several key parts. On the left side, a black electromagnetic lock replaces the traditional mechanical lock. It works with the door latch to open automatically. Below, a black pressure sensor is installed. It detects weight changes on the board to help check if the returned item is the same one that was borrowed. Inside the cabinet, a camera is used for simple image recognition to further confirm the item's identity. Finally, an NFC reader is mounted on the wooden board, and each item has an NFC chip. This setup helps ensure that the item returned is the correct one.

2.3 Cabinet Subsystem

The cabinet subsystem is responsible for the safe storage of items in individual compartments. It continuously monitors the status of the door in real time and incorporates a manual release mechanism for emergency access.

2.3.1 Electromagnetic Lock

The electromagnetic lock operates at 12V and is designed for high reliability with a service life exceeding 300,000 cycles. It features an internal detection switch that provides real-time door status feedback and includes a manual release mechanism to allow emergency access when needed.

Table 1: Requirements & Verification for Electromagnetic Lock

Requirement	**Verification**	**Verification Status**
The electromagnetic lock must operate at DC 12V/2.4A and fully lock or unlock within 2 seconds after receiving the control signal. In addition, the lock should include a manual release lever for emergency situations	(a) Measure the voltage and current supplied to the lock with a multimeter to ensure it receives DC 12V/2.4A; (b) Verify that the cabinet door can be opened manually; (c) Use a stopwatch or timer to record the time from the control signal to complete unlocking; (d) Verify that unlocking completes within 2 seconds; (e) 100% of tests meet the timing requirement.	Y

2.4 Power Subsystem

The power subsystem provides a stable and continuous electrical supply to all system electronics. It ensures reliable operation during supply fluctuations or outages and supports independent voltage requirements for different subsystems.

2.4.1 Li-Ion Battery

A rechargeable Li-Ion battery pack with a nominal voltage of 7.4V and a capacity of 2200 mAh supplies backup power to the system. It ensures uninterrupted operation for at least 8 hours under a typical load of 300–500 mA. The battery is equipped with sophisticated protection circuitry against over-voltage, under-voltage, over-current, and over-temperature conditions.

Table 2: Requirements & Verification for Li-Ion Battery

Requirement	**Verification**	**Verification Status**
The Li-Ion battery shall power the entire system for a minimum of 8 hours under a load of 300–500 mA.	(a) Connect the battery to a test rig emulating a load of 300–500 mA; (b) Log the operational duration with a data logger; (c) Confirm continuous operation for at least 8 hours; (d) Battery operation meets or exceeds the 8-hour requirement.	Y
The battery shall incorporate protection circuitry against over-voltage, under-voltage, over-current, and over-temperature conditions.	(a) Subject the battery to simulated fault conditions (over/under voltage, excessive current, high temperature); (b) Monitor the response using appropriate sensors; (c) Verify that the protection circuits trigger appropriately; (d) All protection features activate within the design thresholds.	Y

2.4.2 Voltage Regulator

A DC-DC buck converter is used to step down the battery voltage to stable rails (5 V or 3.3 V) required by different subsystems. This regulator is designed to supply clean and regulated power with an output voltage tolerance within ±5% and a ripple of less than 50 mV. It is capable of delivering up to 2 A and must support multiple voltage outputs to accommodate components that are independently powered or supplied via the Raspberry Pi.

Table 3: Requirements & Verification for Voltage Regulator

Requirement	Verification	Verification Status
The voltage regulator shall maintain an output voltage within ±5% of the target value with a ripple of less than 50 mV over the full load range.	(a) Apply a variable load while supplying power from the regulator; (b) Measure the output voltage and ripple using an oscilloscope; (c) Confirm that the voltage and ripple remain within the specified limits; (d) All tests yield values within ±5% and ripple less than 50 mV.	Y
The voltage regulator shall deliver a maximum current of up to 2 A with an efficiency of at least 80%.	(a) Connect an electronic load to the regulator; (b) Measure current output and power consumption; (c) Calculate efficiency from input and output power; (d) Efficiency is $\geq$ 80% at full load.	Y
The voltage regulator shall supply distinct voltage rails to support different subsystem requirements.	(a) Interface multiple subsystems requiring different voltage levels; (b) Measure each rail's voltage under load with a digital multimeter; (c) Verify each rail maintains its design voltage within tolerance; (d) All voltage rails operate within specified limits under test.	Y

2.5 Control Subsystem

The control subsystem manages system data processing and coordination, handling communication with storage, sensors, and user interface components.

2.5.1 Microprocessor

Raspberry Pi 5 with 4 GB of memory is used as the primary processing unit. Based on a quad-core ARM architecture, this board delivers enhanced processing speed and efficiency for executing real-time control tasks and complex computations. It also integrates a dedicated GPU for handling graphical processing and hardware-accelerated routines. The extensive connectivity options—including a 40-pin GPIO header, USB ports, Ethernet, and wireless interfaces—allow for versatile interfacing with various sensors, displays, and storage devices, supporting rapid software development and robust peripheral integration.

Table 4: Requirements & Verification for Microprocessor (Raspberry Pi 5 4 GB)

Requirement	**Verification**	**Verification Status**
The microprocessor shall support simultaneous communications on SPI, I2C, and UART interfaces with a minimum data rate of 2 Mbps per interface.	(a) Connect test peripherals to each interface; (b) Use protocol analyzers to capture data rates; (c) Verify that each interface meets or exceeds 2 Mbps; (d) 100% of interfaces achieve the data rate requirement.	Y
The GPIO pins shall consistently provide 3.3 V logic levels with a drive capability of at least 10 mA ($\pm 5\%$ tolerance).	(a) Attach a digital multimeter to each GPIO pin under load; (b) Measure voltage levels and current drive; (c) Verify measurements against design specifications; (d) All GPIO outputs perform within the stated tolerances.	Y
The microprocessor shall execute real-time data processing with minimal latency while supporting multitasking in a resource-constrained environment.	(a) Run standardized benchmarks simulating real-time tasks; (b) Profile response times and system load; (c) Verify that latency remains within acceptable limits; (d) Latency and multitasking performance meet design requirements.	Y

2.5.2 SD Card

A dedicated SD card is used for local data storage and caching. It interfaces with the Raspberry Pi via the SPI bus, ensuring fast and reliable read/write operations that support the system's data management requirements.

Table 5: Requirements & Verification for SD Card Interface

Requirement	Verification	Verification Status
The SD card interface shall support SPI clock speeds up to 10 MHz for fast read/write operations.	(a) Connect the SD card to the Raspberry Pi via SPI; (b) Use an oscilloscope to measure the SPI clock speed during continuous data transfer; (c) Verify that the clock speed reaches or approximates 10 MHz; (d) The interface operates at or near the specified clock speed.	Y
The SD card interface shall implement robust error-checking mechanisms to ensure data integrity.	(a) Conduct multiple read/write cycles; (b) Use checksum or hash functions to validate data integrity; (c) Compare input and output data for consistency; (d) No data errors occur, confirming error-checking functionality.	Y

2.6 Item Detection Subsystem

The item detection subsystem identifies items placed within the cabinet by combining weight measurements and visual analysis. It integrates sensor data to produce accurate and reliable item identification.

2.6.1 Load Cells

High-precision load cells, in conjunction with an HX711 24-bit analog-to-digital converter, measure the weight of items. The HX711 amplifies and converts the analog signal from the load cell into digital data with a resolution sufficient to detect variations of ± 0.1 gram. The system's response time is maintained at 0.5 seconds or less for timely feedback.

Table 6: Requirements & Verification for Load Cell with HX711

Requirement	**Verification**	**Verification Status**
The load cell system shall measure item weight with an accuracy of ± 1 gram.	(a) Calibrate the load cells using certified calibration weights; (b) Compare measured values with the standard weights; (c) Confirm deviation is within ± 1 gram; (d) Accuracy meets the specification for all test samples.	Y
The load cell system shall provide weight feedback within 0.5 seconds to support near real-time detection.	(a) Simulate rapid weight changes on the load cell; (b) Record the response time using data acquisition equipment; (c) Verify that the response time does not exceed 0.5 seconds; (d) Response time is consistently ≤ 0.5 seconds.	Y
The load cell system shall reliably transmit digital weight data to the control subsystem.	(a) Interface the HX711 with the Raspberry Pi; (b) Monitor continuous data output during simulated loading; (c) Compare transmitted data with expected values; (d) Data transmission is error-free throughout extended tests.	Y

2.6.2 Cameras

5-megapixel cameras are used for capturing and transmitting video data to the Raspberry Pi. The camera provides 1080p video at 30 frames per second and operates on a stable 3.3V supply. The captured video feed is then processed by computer vision algorithms deployed on the Raspberry Pi for tasks such as image recognition and anomaly detection. This separation ensures that the camera's function is limited to high-quality image acquisition and reliable data transmission.

Table 7: Requirements & Verification for Cameras

Requirement	Verification	Verification Status
The camera shall capture and transmit video at 1080p resolution and 30 frames per second.	(a) Connect the camera to the Raspberry Pi; (b) Use video analysis software to assess the resolution and frame rate; (c) Verify that the output is 1080p at 30 fps; (d) Video output meets the specification in all trials.	Y
The camera shall operate reliably at a stable 3.3 V power supply.	(a) Measure the supply voltage using a digital multimeter during operation; (b) Confirm that the voltage remains stable at 3.3 V; (c) Verify continuous operation at the specified voltage; (d) Voltage remains within tolerance with no performance issues.	Y
The camera shall transmit video data with minimal end-to-end latency to support real-time processing.	(a) Perform an integrated test between the camera and the Raspberry Pi; (b) Measure the latency from capture to processing; (c) Verify that the latency falls within the acceptable design limits; (d) End-to-end latency is consistently within specification.	Y

2.7 User Interface Subsystem

The user interface subsystem provides a direct interaction channel between the user and the system, supporting authentication and visual display functions.

2.7.1 NFC Card Reader

An NFC card reader based on a Raspberry Pi NFC expansion board (integrated with a 40-pin GPIO interface) utilizes a PN532 chip. It supports I2C, SPI, and UART communication interfaces and is capable of both reading and writing NFC cards for user authentication.

Table 8: Requirements & Verification for NFC Card Reader

Requirement	Verification	Verification Status
The NFC card reader shall complete reading and writing operations within 2 seconds upon card contact.	(a) Execute multiple read/write cycles with test NFC cards; (b) Use a stopwatch to measure transaction times; (c) Verify that each operation completes within 2 seconds;	Y
The NFC card reader shall support multiple communication interfaces (I2C, SPI, UART) selectable via software.	(a) Configure the reader for each interface mode; (b) Conduct standard data exchange tests; (c) Verify successful operation in every mode; (d) All interfaces perform reliably as configured.	Y
The NFC card reader shall operate reliably when interfaced with the Raspberry Pi's 40-pin GPIO header.	(a) Connect the NFC reader via the 40-pin header; (b) Monitor signal stability and voltage levels during prolonged testing; (c) Verify continuous and stable operation; (d) No interruption or deviation in performance is observed.	Y

2.7.2 Touch Screen

A 3.5-inch TFT LCD resistive touchscreen serves as the visual output and user input device. It offers a smooth display with a refresh rate of 50 frames per second and communicates with the system via an SPI interface, ensuring clear visuals and responsive touch interaction.

Table 9: Requirements & Verification for TFT LCD Resistive Touchscreen

Requirement	Verification	Verification Status
The touchscreen shall correctly display dynamic system messages (e.g., “Please swipe card”, “Borrow successful”, “Enter cabinet ID”) during relevant operations.	(a) Simulate system states for borrowing and returning operations; (b) Capture the displayed output using screen recording software; (c) Compare the captured messages with the expected instructions; (d) 100% match between displayed and expected messages.	Y
The touchscreen shall register touch inputs on function keys (e.g., “borrow” and “return”) with a response latency below 150 ms.	(a) Measure the delay between the touch event and the system’s visual response; (b) Average latency under 150 ms over 10 trials.	Y
The touchscreen shall accurately process cabinet number inputs and command selections to ensure proper system operation.	(a) Manually input a series of cabinet numbers and function commands via the touchscreen; (b) Verify that the system logs or on-screen confirmations correctly register each input; (c) 100% correct input registration across multiple tests.	Y

2.8 Tolerance Analysis

The system faces potential performance risks due to parameter variations in critical subsystems, necessitating rigorous tolerance analysis to ensure compliance with design specifications. The power module must maintain stable voltage outputs and reliable battery runtime under fluctuating loads, requiring precise regulation and protection against over/under-voltage, overcurrent, and thermal extremes to safeguard both functionality and safety. The control module handles high-speed SPI and UART communication channels (e.g., SD card operations at 10 MHz SPI and microcontroller UART at 2 Mbps), demanding strict timing tolerances and signal integrity to avoid data corruption or delays. The item detection module, relying on weight sensors, must achieve ± 1 gram accuracy and sub-second response times despite environmental factors like temperature drift and mechanical stress. Finally, the user interface module imposes real-time constraints—such as NFC card authentication within 2 seconds and LCD display updates under 100 ms—where even minor timing deviations could degrade user experience. These interconnected challenges underscore the need for comprehensive tolerance analysis to balance performance, reliability, and safety across all subsystems.

$$\Gamma = \frac{Z_L - Z_0}{Z_L + Z_0}, \quad \text{VSWR} = \frac{1 + |\Gamma|}{1 - |\Gamma|}$$

2.8.1 Greatest Risk Justification

The power module faces significant risks due to potential degradation of the lithium-ion battery. Although the nominal capacity is 2200 mAh, factors such as aging and low-temperature conditions can reduce the effective capacity to approximately 2000 mAh, potentially compromising the required 8-hour operational duration. Additionally, input voltage fluctuations of $\pm 10\%$ around the nominal 7.4V can affect the stability of the buck converter's output.

In the control module, the external crystal oscillator's accuracy of ± 50 ppm may lead to timing deviations in SPI/UART communications, risking data integrity. Variations in GPIO output impedance, influenced by PCB trace mismatches, can further degrade signal quality.

The user interface module's NFC reader is susceptible to antenna impedance mismatches. Deviations from the target 50Ω $\pm 5\%$ impedance can result in a reflection coefficient (Γ) exceeding 0.1, leading to a Voltage Standing Wave Ratio (VSWR) above 2:1, which diminishes read efficiency. Environmental electromagnetic interference (EMI), such as from WiFi sources, poses additional challenges to reliable NFC operation.

2.8.2 Acceptable tolerances

The buck converter in the power module is designed to maintain an output voltage within $\pm 5\%$ of the 5V target, with ripple voltage kept below 50 mV. This stability is achieved using feedback resistors with $\pm 1\%$ tolerance.

For the control module, SPI and UART communication rates are expected to meet or exceed 2 Mbps, with GPIO pins capable of sourcing or sinking 10 mA $\pm 5\%$. The external crystal oscillator's ± 50 ppm accuracy is deemed sufficient to maintain protocol timing requirements.

In the user interface module, the LCD display is required to have an update delay of no more than 100 ms, operating with an SPI clock frequency up to 10 MHz. The NFC reader should complete read operations within 2 seconds, maintaining a communication rate of at least 1 Mbps.

2.8.3 Alignment with High-Level Requirements

To ensure the power module meets the 8-hour operational requirement, discharge tests should be conducted under worst-case conditions, considering a reduced battery capacity of 2000 mAh. The buck converter's performance must be validated across a 0–2A load range, verifying output voltage stability and ripple compliance.

The control module's SPI and UART interfaces should be assessed using oscilloscope eye diagrams to confirm signal timing within protocol limits. Stress tests involving simultaneous SD card access and display updates will help verify microcontroller stability under concurrent tasks.

For the user interface module, SPI signal integrity must be measured to ensure compliance with LCD display specifications. The performance of the NFC card reader should be evaluated through 100 read trials, measuring success rates and average response times to confirm adherence to the requirements of 2 second read time and 1 Mbps communication rate.

To ensure the system operates reliably under all conditions, a Worst-Case Circuit Analysis is recommended. WCCA involves a comprehensive evaluation of circuit performance, accounting for manufacturing tolerances, environmental factors, and component aging.[8] This analysis helps verify that the design meets performance specifications throughout its lifecycle, reducing the risk of failures and enhancing overall reliability.

3 Cost and Schedule

3.1 Cost Analysis

3.1.1 Total Labor for All Partners

According to UIUC ECE department, the average starting salaries of Electrical Engineering and Computer Engineering graduate are 87769 and 109176 dollars [7]. So the total labor for all partners is:

$$\begin{aligned}\text{Labor} &= 4 \cdot \frac{(87\,769 + 109\,176) dollars}{2} \cdot \frac{1\,\text{year}}{2080\,\text{hours}} \cdot (10\,\text{hours/week}) \cdot (12\,\text{weeks}) \\ &\approx 22\,724.4 \text{ dollars.}\end{aligned}$$

3.1.2 Bill of Materials

Part #	Mft	Price (¥)	Qty	Total (¥)
Small Storage Cabinet Lock	Guangzhou Sai Rui Factory	15.5	4	62
4-door, lockable storage cabinet	Xuzhou Seven-Colored Fox Furniture Co., Ltd.	130	1	130
HX711 Load Cell	Unknown	14.25	1	14.25
External Keyboard Expansion	Unknown	3.77	1	3.77
Raspberry Pi 3B+/4B N	Raspberry Pi Ltd.	115.69	1	115.69
Raspberry Pi 5 (5B) 3.5-inch 50fps Display	Raspberry Pi Ltd.	58.69	1	58.69
Raspberry Pi 5th 5B/4B Development Board with Camera	Raspberry Pi Ltd.	598.6	1	598.6
			Total	**983**

Table 10: Bill of Materials

3.2 Schedule

Our team has made the following progress in the past weeks:

- Constructed the body of the cabinet Item,

- Tested the use of electromagnetic locks,
- Purchased most of the required hardware components for the project,
- Complete the basic logic and structure of the image capture and preprocessing on Rasberry Pi,
- Deployed our computer vision model locally.

The future schedule is shown in the table below:

Week	**Niahoaxuan Ruan**	**Yihong Yang**	**Xiaotong Cui**	**Yanxin Lu**
4/13	Begin drafting design modifications for the lock mechanism and plan how to integrate additional sensors and the camera into the cabinet's body	Start designing the PCB layout and control circuit that will integrate pressure sensors, SD card data, and for robust data transfer	Research potential computer vision models that run efficiently on the Raspberry Pi, and identify methods for inference acceleration	Start interfacing the display with the Raspberry Pi, ensuring that the display hardware is correctly connected and can provide basic output
4/20	Work on physically modifying the lock and cabinet, incorporating sensor mounts and securing the camera in the optimal location	Finalize the PCB schematic and construct a prototype control circuit on a breadboard, testing the communication channels between the sensors, camera, and Raspberry Pi	Refine the selection of a vision model and begin initial coding for accelerating model inference on the Raspberry Pi to meet performance targets	Develop the logic for storage and retrieval functions, integrating this functionality with the display to indicate, for example, which cabinet is in use for storing or retrieving an item

4/27	Perform integrated testing on the modified lock alongside the newly added sensors and camera, adjusting the physical setup as necessary based on test results	Shift focus to building a physical PCB prototype, thoroughly testing the control circuit to validate that pressure sensor data, SD card operations, and overall communication between components are reliable and robust	Optimize the computer vision model, conducting real-world tests on the Raspberry Pi to ensure that the model's inference speed and accuracy meet the set criteria	Refine and debug the display interface, ensuring that dynamic status updates (e.g., storage and retrieval, cabinet numbers) are accurately rendered and responsive to user commands
5/4	Make any last mechanical adjustments to the lock and cabinet modifications, ensuring all sensor and camera integrations are secure and functioning as intended	Integrate the PCB circuit with the overall system, executing full system tests to verify reliable data transfer through the Raspberry Pi, then onto the remote computer for item recognition, and finally back to trigger the lock mechanism	Finalize tuning and performance validation of the integrated computer vision system on the Raspberry Pi, confirming that recognition and inference operate seamlessly in real-time	Complete final debugging on the display and the storage/retrieval logic, ensuring that the user interface clearly reflects system status during operation
5/11	**Final testing and preparation for the demo!**			

4 Ethics and Safety

4.1 Ethics

Our project, the *Intelligent Shared Item Cabinet*, is designed with strong consideration for ethical standards as outlined by the IEEE Code of Ethics. We aim to ensure that the system upholds user rights, respects privacy, promotes transparency, and avoids introducing harm or discrimination.

Firstly, we prioritize **user privacy**. The system utilizes campus cards for user authentication, allowing students to access the cabinet without revealing personal information unnecessarily. All usage data—including borrowing and returning records—is stored securely in a restricted-access database. Only authorized personnel will be able to view this data for maintenance and audit purposes. Personally identifiable information (PII) is minimized to reduce risk in the event of data breach.

Secondly, we embrace **transparency and accountability**. Users can view their transaction history through a user interface, which increases trust and allows them to identify potential anomalies. The system will notify users of any detected inconsistencies, such as mismatched returns or sensor errors, in real-time. These design choices aim to build a responsible borrowing environment.

We also commit to **non-discrimination and equitable access**. The cabinet is intended for all students within the residential college community, and no group will be excluded based on gender, background, or ability. Furthermore, we ensure that the design and interaction methods are simple and inclusive, including readable displays and accessible interfaces.

Finally, the system includes a comprehensive **error logging and feedback mechanism** to support continuous improvement. By systematically tracking operational issues, we can improve system reliability and avoid repeated failures. Our team is committed to ethical problem-solving and responsible innovation throughout the project's development and deployment lifecycle.

4.2 Safety

Safety is a core priority for both the development phase and the final deployment of our system. All work conducted in the laboratory strictly follows the ECE 445 safety guidelines, which mandate that no student works alone and all team members complete mandatory online safety training before using lab equipment.

Our system includes multiple electrical and mechanical components such as:

- A rechargeable battery with built-in protection circuitry,
- A SD Card to local data storage and caching,
- A Raspberry Pi for control and communication,
- Electromagnetic locks for physical security.

To ensure **electrical safety**, all components will operate within their rated voltage and current limits. Protective measures such as over-voltage, over-current, and thermal cut-off mechanisms are implemented to prevent potential accidents. All wiring will be insulated and routed securely to reduce risks of short circuits, arcing, or contact with conductive surfaces.

Mechanical safety is also addressed. The cabinet structure is securely mounted and includes enclosed compartments to prevent access to moving parts during operation. The locking mechanism is designed to engage only when all sensors confirm safe conditions, thus avoiding pinch or entrapment hazards.

A complete **lab safety manual** will be developed to support safe handling, including emergency procedures and a checklist for working with batteries and power modules. Furthermore, the physical design minimizes sharp edges and unsafe protrusions, enhancing safety for end users.

Enclosure Robustness and Physical Safety is an essential part of our design as well. The cabinet enclosure is built for robustness and safety to protect both the electronics inside and anyone interacting with the cabinet. Our enclosure design follows established guidelines for electrical housings: it shields the internal components from environmental factors and simultaneously protects users from internal hazards. The enclosure is also designed to keep out dust or debris that could cause electrical shorts and guards the electronics from minor drips or humidity. To prevent electrical shocks, any metal parts of the cabinet that a user might touch are either grounded or double-insulated from the circuitry. There are no exposed wires; all high-current connections are securely covered and taped down. The removal of external buttons in the updated design further improves the enclosure integrity – without cutouts for buttons, there are fewer entry points for dust or moisture and less risk of a user inadvertently contacting any circuit. Physically, the cabinet is constructed to be stable and durable. It has a low center of gravity and can be affixed to a wall or floor, ensuring it cannot tip over if bumped. Importantly, the enclosure includes safety signage and labels warning that it contains electrical components and should only be serviced by authorized personnel.

By integrating these safety considerations into every stage of development and testing, we aim to deliver a robust and secure system that ensures the well-being of both team members and users.

References

[1] OpenAI, "Introducing 4o Image Generation," *OpenAI*, Mar. 25, 2025. [Online]. Available: `https://openai.com/index/introducing-4o-image-generation/`

[2] SARY, "XG-07 Series Electromagnetic Lock Parameters," [Online]. Available: `http://www.16868.com/page88?product_id=73`, Accessed: 2025.

[3] EEWorld, "MP1584 Switching Regulator Parameters," [Online]. Available: `https://www.eeworld.com.cn/RDesigns_detail/57920`, Accessed: 2025.

[4] IEEE, "IEEE Code of Ethics," [Online]. Available: `https://www.ieee.org/about/corporate/governance/p7-8.html`, 2016.

[5] The Grainger College of Engineering, University of Illinois at Urbana–Champaign, "Safety – ECE 445: Senior Design Laboratory," [Online]. Available: `https://courses.grainger.illinois.edu/ece445zjui/guidelines/safety.asp`, Accessed: 2025.

[6] KDM Steel, "Electrical Enclosure Safety," *KDM Steel*. [Online]. Available: `https://www.kdmsteel.com/electrical-enclosure-safety/`, Accessed: 2025.

[7] University of Illinois Electrical & Computer Engineering, "Salary Averages," *UIUC ECE*. [Online]. Available: `https://ece.illinois.edu/admissions/why-ece/salary-averages`, Accessed: 2025.

[8] Maplesoft worst-case circuit anslysis[EB/OL]. (2024-11-07). [Online]. Available: `https://blog.csdn.net/maplesoft/article/details/141645450`, Accessed: 2025.