

ECE 445
Senior Design Laboratory
Fall 2026
Project Proposal

SECURE CHAIN-OF-CUSTODY CONTAINER

Team No. 4

Team Members:

Sena Tiryaki (stiry2)
Serdar Alp Oğuz (soguz2)
Selim Mamak (smamak2)

TA: Alex Lee

Professor: Arne Fliflet

September 17, 2026

1. Introduction

1.1 Problem

Confidential engineering prototypes may need to move between laboratories, offices, and authorized employees before a product is publicly released. A conventional locked case can restrict physical access, but it does not automatically identify who opened the case, when access occurred, or whether someone attempted to bypass the lock or damage the enclosure. For intellectual property and prototype-development workflows, this missing history can make it difficult to distinguish normal handling from suspicious access after the fact.

Existing approaches address only portions of this problem. Paper custody logs depend on users recording every interaction correctly and can be altered later. Shipping data loggers may record shock, temperature, or other transport conditions, but they normally do not control access to the protected contents. Electronic lockboxes can authenticate users, but access control alone does not provide a combined record of lid opening, enclosure tampering, impacts, and long-term custody history. The project therefore focuses on integrating these functions into one reusable device rather than replacing any single commercial product category.

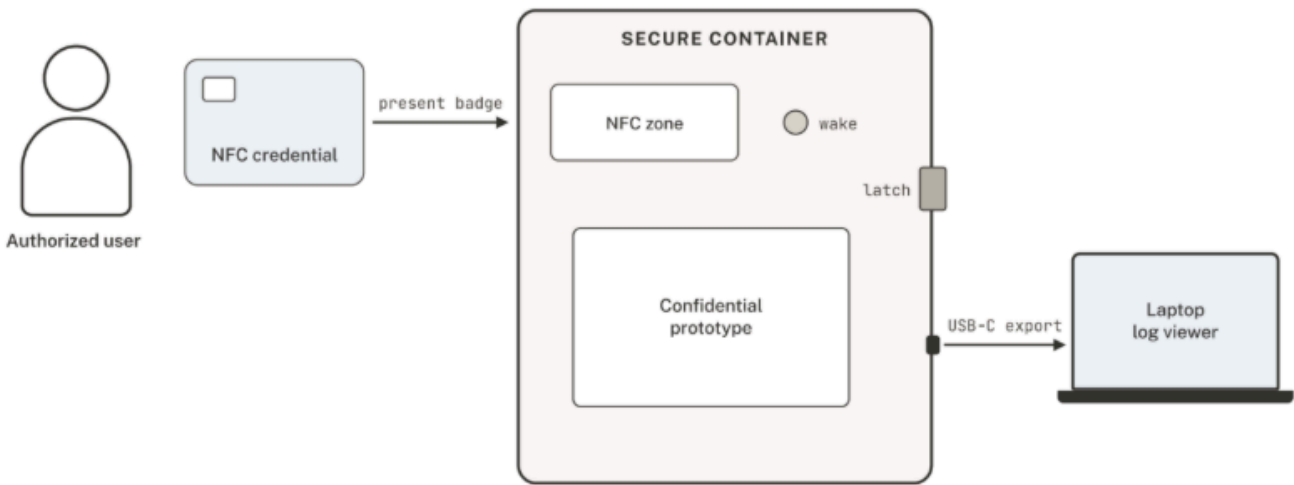
Reliable handling records also have an ethical dimension. A log entry may influence how an organization investigates a missing or damaged prototype, so the system must report only what its sensors can actually establish. NIST guidance on evidence preservation discusses the importance of preserving information associated with handled evidence; although this prototype is not intended to establish legal evidentiary sufficiency, the same general need for traceable handling motivates a persistent, reviewable history [1].

1.2 Solution

The proposed system is a battery-powered secure container that grants access only after an enrolled NFC credential is successfully authenticated. A pushbutton provides a simple low-power wake mechanism; once awake, the microcontroller enables the NFC reader, verifies the credential using an authentication method stronger than UID comparison, and commands an electronic latch only after authorization succeeds. A Hall-effect lid sensor, conductive tamper loop, and low-power accelerometer monitor unauthorized opening, enclosure penetration, and significant impact events.

A low-power microcontroller coordinates the system and spends most of its time in a sleep state while the sensing circuitry remains armed. Completed access and tamper events are timestamped by a battery-backed real-time clock and stored in nonvolatile FRAM. Records are linked with a SHA-256 hash chain so that the desktop verification program can detect modification of stored history. NFC and latch power are switched off during standby. A USB-C connection allows an authorized user to export the event history to a simple Python desktop utility that displays the custody record and reports whether the integrity check passes. The final design will be implemented on a custom PCB containing the microcontroller, power-management circuitry, sensor interfaces, storage, NFC interface, and latch driver.

1.3 Visual Aid



During normal use the laptop is not required. Lid, tamper-loop, and impact events are logged automatically.

Typical flow: wake system → authenticate credential → release latch → record access/tamper history → verify history on laptop.

Figure 1. Intended use of the secure chain-of-custody container. The laptop is used only for log export and verification; ordinary access is handled locally by the container.

1.4 High-Level Requirements

- HLR1 – Authenticated access and reliable locking: The assembled container shall release the latch only after successful authentication of an enrolled NFC credential and shall complete at least 20 consecutive authorized lock/unlock cycles without an MCU reset, lost log record, or unintended release; ten presentations of unenrolled credentials shall produce zero latch releases.
- HLR2 – Tamper detection and persistent custody history: The system shall detect and timestamp unauthorized lid opening, conductive-loop interruption, and the defined significant-impact event in at least three consecutive trials per event type; previously completed records shall remain available after at least 10 minutes of complete main-battery removal and restoration, and the desktop verifier shall report an integrity failure when any stored record is deliberately modified.
- HLR3 – Low-power autonomous operation and time retention: With the NFC reader and latch circuitry inactive, the fully assembled system shall draw less than 100 μA average current in armed standby, and the battery-backed RTC shall remain within ± 2 s of a reference clock after 10 minutes with the main battery disconnected.

2. Design

2.1 System Architecture and Block Diagram

The design is intentionally divided into the same three functional areas described in the approved RFA: (1) power management, (2) access control and tamper sensing, and (3) control, logging, and readout. This keeps the project modular while avoiding an unnecessary split between a separately powered always-on controller and a main controller. The MCU remains on the low-power 3.3 V rail and uses a deep-sleep mode; only the NFC reader and latch power path are switched on when required.

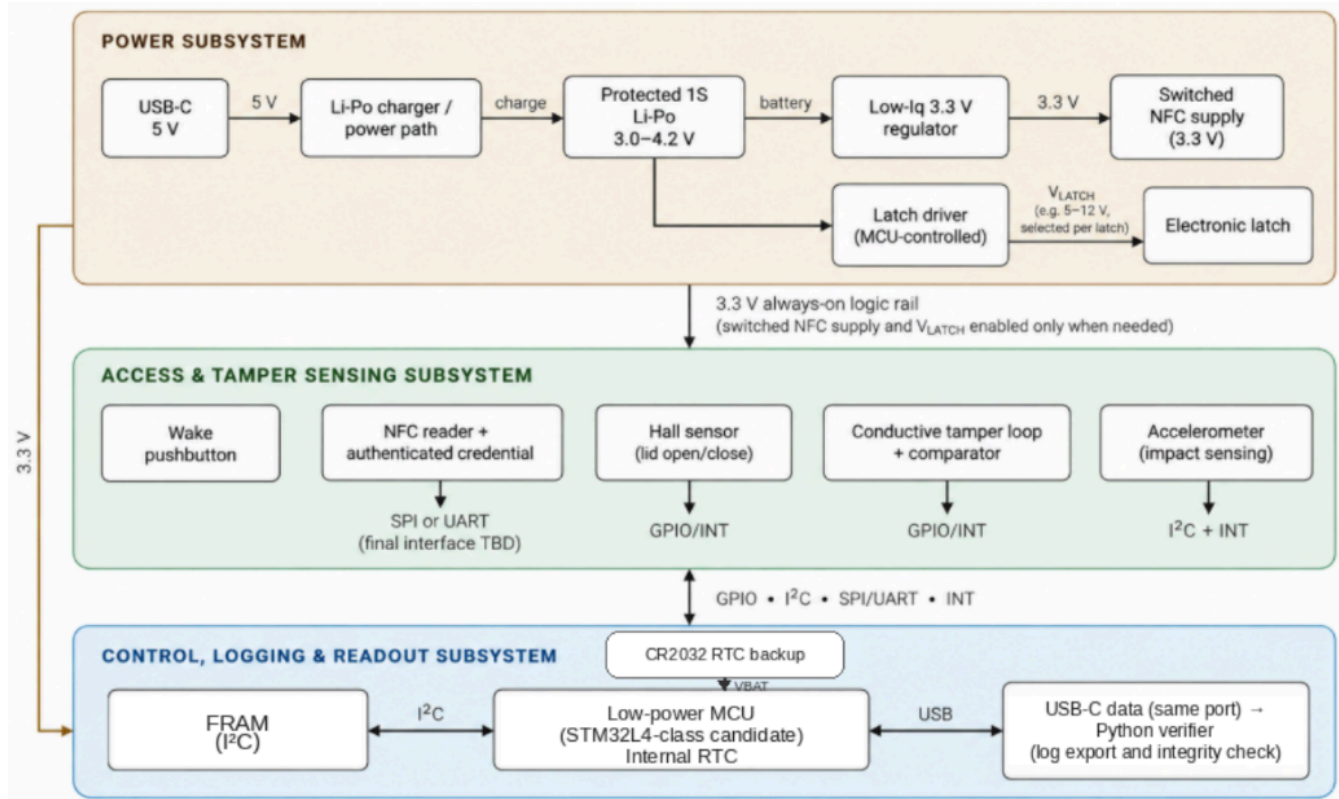


Figure 2. Proposed block diagram. Major data interfaces and nominal supply voltages are labeled; NFC and latch power are switched only when needed.

2.2 Preliminary Mechanical Concept

The enclosure is a physical part of the sensing system, so a preliminary layout is included even though final fabrication dimensions will depend on the selected latch, battery, antenna clearance, and PCB size. The current planning envelope is approximately 240 × 160 × 100 mm. Electronics and the battery are separated from the protected item and moving latch components. The conductive loop is routed around selected enclosure seams and the service bay so that normal lid motion does not break the loop.

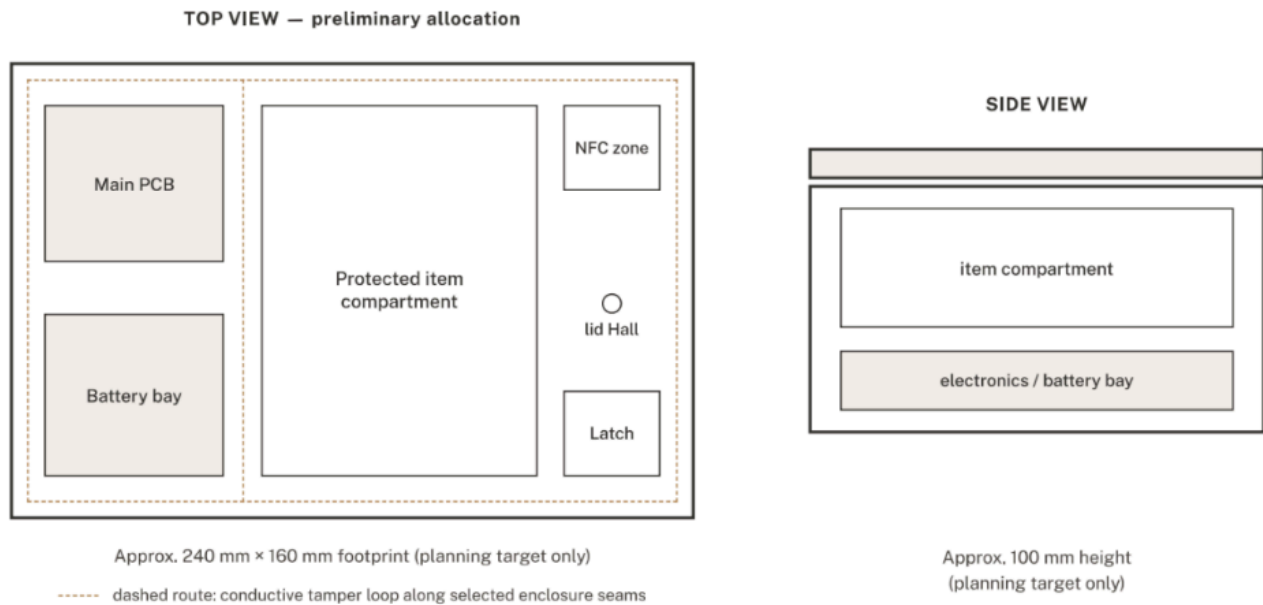


Figure 3. Preliminary enclosure allocation. Dimensions are planning targets rather than final fabrication dimensions.

2.3 Power Subsystem

The power subsystem supports all three HLRs. A protected single-cell Li-Po battery supplies the device, and USB-C provides the charging input. A charger/power-path circuit prevents the USB input from directly bypassing battery-management limits. A low-quiescent-current 3.3 V regulator powers the MCU, FRAM, and low-power sensing circuitry continuously. The MCU's internal RTC uses a 32.768 kHz crystal and a CR2032-backed VBAT domain so timekeeping can continue during main-battery removal. The NFC reader is supplied through a load switch so it can be fully disabled in standby. The latch driver uses a separately enabled boost or direct-drive stage selected after the actual latch pull-in current and voltage are measured. A hardware default-off gate condition prevents latch activation during reset.

Table 1. Initial standby-current design budget (targets, not measured values).

Load group	Design allocation	Purpose
MCU sleep + internal RTC	15 μ A	Controller remains wake-capable; RTC retains time
Hall sensor + tamper-loop circuit	10 μ A	Lid and enclosure monitoring
Accelerometer	15 μ A	Impact interrupt in low-power mode
FRAM, regulator, charger, load switches, pullups/leakage	25 μ A	Board-level overhead
Total target / margin to 100 μ A	65 μ A / 35 μ A	Allows measured component variation

The current budget is a design allocation only. The completed PCB must be measured because breakout boards, pullups, charger leakage, and regulator quiescent current can dominate a microamp-level system. The team will use bench power during initial bring-up and connect the Li-Po only after the charger and protection circuitry have been reviewed and validated according to ECE 445 battery procedures [10].

ID	Required behavior / verification
PW-1	The 3.3 V rail shall remain within $\pm 5\%$ over the protected battery operating range while supplying the MCU, storage, and sensing loads.
PW-2	In armed standby, the NFC reader and latch power paths shall be off, and the complete assembled device shall average less than 100 μ A from the main battery.

ID	Required behavior / verification
PW-3	The latch power stage shall supply the measured pull-in current and voltage of the selected latch with at least 25% current margin, while the 3.3 V rail remains above the MCU brownout threshold and no reset occurs.
PW-4	The USB-C charging path shall limit charge current according to the selected protected Li-Po cell, prevent reverse current into the USB source, and prevent the latch load from bypassing the battery/power-path limits.

2.4 Access Control and Tamper Sensing Subsystem

This subsystem primarily supports HLR1 and HLR2 through authenticated access and physical tamper detection. A pushbutton wakes the MCU for a user-requested access attempt. The MCU then enables the NFC reader and authenticates an enrolled credential. The exact reader/credential pair will be finalized through early compatibility testing; a PN532-class reader [4] and a cryptographically authenticated ISO/IEC 14443 credential are current candidates. Authorization will not be based only on a UID. A fail-secure electronic latch remains mechanically locked when unpowered and is driven only for a bounded release pulse.

Three sensors monitor the enclosure. A low-power Hall-effect sensor reports lid state, a continuity loop routed through protected seams is evaluated by a nanowatt comparator, and a low-power three-axis accelerometer [5] generates an interrupt when an experimentally selected impact threshold is exceeded. The threshold will be tuned using controlled tests with an empty enclosure so that normal handling does not produce excessive false events.

ID	Required behavior / verification
AT-1	After a wake request, an enrolled credential shall permit one latch-release command; an unenrolled credential shall not produce a latch command in any of ten negative test presentations.
AT-2	The latch shall remain engaged when the container is securely closed and unpowered, and it shall complete 20 consecutive authorized release/re-engagement cycles without mechanical binding or controller reset.
AT-3	The lid sensor shall distinguish the closed and open positions across the final magnet/sensor mounting tolerance and shall generate a digital interrupt when the lid is opened.
AT-4	The conductive loop shall distinguish an intact loop of up to 10 k Ω from an open circuit with at least 0.5 V worst-case decision margin at the comparator input.
AT-5	The accelerometer shall generate a latched interrupt for the project-defined significant-impact test in three consecutive trials while producing no false impact event during ten normal open/close handling cycles.

2.5 Control, Logging, and Readout Subsystem

This subsystem supports all three high-level requirements by coordinating access decisions, preserving event history and timestamps, and managing low-power system operation. A low-power MCU coordinates wakeup, sensing, NFC authentication, latch control, logging, and USB service. An STM32L4-class device is the current MCU candidate because it combines low-power sleep modes with SPI/I²C, USB, and an internal RTC with a backup-power domain [8]. The MCU sleeps between events and wakes on the user pushbutton or a sensor interrupt. Firmware gives tamper events priority over a new access request so that an unresolved lid or loop fault prevents ordinary latch release.

Event history is stored in I²C FRAM so previously written records remain available with the main battery removed [7]. Each record contains a sequence number, event type, timestamp, credential slot when applicable, and the previous hash. The firmware computes a SHA-256 hash chain so the desktop utility can detect modification of previously stored records while keeping the logging implementation appropriate for the scope of the prototype. If power is lost during the newest write, the verifier may mark that final record incomplete, but previously completed records must remain readable and valid.

Table 2. Proposed event-record contents.

Field	Purpose	Example
Sequence number	Ordering independent of timestamp	154
Timestamp	RTC time of event	2026-09-14 16:35:22
Event type	Access, lid, loop, impact, power fault	LID_OPEN
Credential slot	Identity link for authorized access only	User 2 / 0xFF if N/A
Previous hash	Links record to prior completed record	32-byte SHA-256 value
Current hash	Integrity check for this record + chain	32-byte SHA-256 value

Let D_i denote the non-hash event fields of record i , including the sequence number, timestamp, event type, and credential slot. The chain is computed as $H_i = \text{SHA-256}(D_i \parallel H_{i-1})$. Each stored record contains the previous hash H_{i-1} and the resulting current hash H_i . This software mechanism detects modification of stored records during export; the prototype does not claim protection against an attacker who can replace the entire log and recompute every hash.

ID	Required behavior / verification
CL-1	For every completed authorized access, unauthorized lid opening, loop interruption, or significant-impact event, the MCU shall write a timestamped event record to FRAM before returning to armed standby.
CL-2	Previously completed FRAM records shall remain readable after at least 10 minutes of complete main-battery removal and restoration.
CL-3	With the main battery removed for 10 minutes, the backup-powered RTC shall remain within ± 2 s of a reference clock when read immediately after power is restored.
CL-4	The USB-C desktop utility shall export the stored history in order and shall report an integrity failure after any one stored event record is deliberately modified before verification.
CL-5	The firmware shall never issue a latch-release command while an unresolved lid-open or broken-loop tamper condition is active.

2.6 Tolerance Analysis: Conductive Tamper Loop

The conductive loop is a critical function because it must remain active while the MCU is sleeping and must reliably distinguish an intact routed conductor from a cut/open condition despite resistor tolerance, leakage, noise, and supply variation. The proposed circuit uses a 1 M Ω pull-up on the sense node and a 1 M Ω /1 M Ω reference divider. A nanowatt comparator compares V_{SENSE} against approximately $V_{\text{AON}}/2$. The analysis below treats the selected limits as design bounds to be verified on the completed PCB.

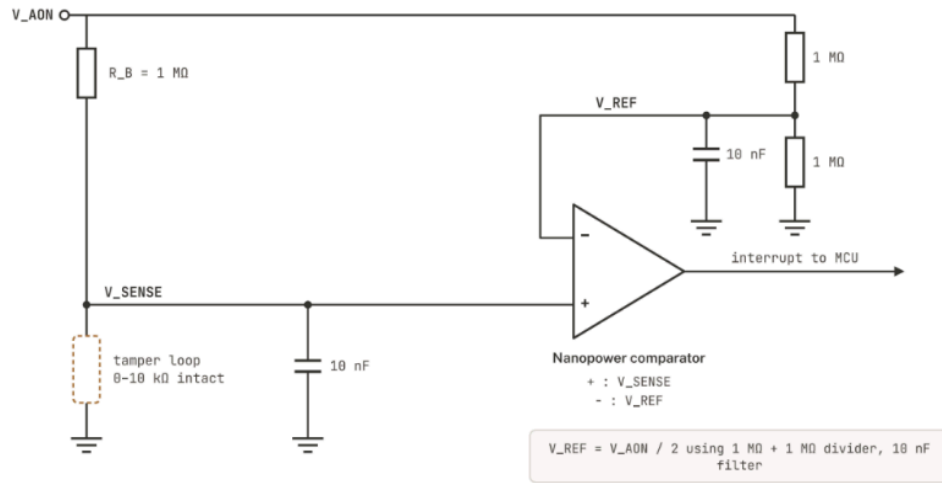


Figure 4. Proposed conductive-loop detector used for the tolerance analysis.

Analysis bounds: V_{AON} is the always-on 3.3 V logic/sensing rail, so $V_{AON} = 3.135\text{--}3.465\text{ V}$ ($3.3\text{ V} \pm 5\%$); all 1 MΩ resistors $\pm 1\%$; intact loop resistance 0–10 kΩ; node leakage allowance $\pm 50\text{ nA}$; comparator/noise decision uncertainty $\pm 50\text{ mV}$; 10 nF capacitors $\pm 10\%$.

Worst-case intact-loop voltage: $V_{\text{closed,max}} = 3.465 \times 10\text{ k}\Omega / (990\text{ k}\Omega + 10\text{ k}\Omega) + 50\text{ nA} \times (990\text{ k}\Omega \parallel 10\text{ k}\Omega) = 0.0351\text{ V}$ (1)

The reference-divider ratio ranges from approximately 0.495 to 0.505. Including the $\pm 50\text{ nA}$ leakage allowance, $V_{\text{REF,min}} \approx 1.527\text{ V}$ and $V_{\text{REF,max}} \approx 1.775\text{ V}$. Applying the $\pm 50\text{ mV}$ decision uncertainty gives a threshold envelope of 1.477–1.825 V.

Closed-loop margin: $M_{\text{closed}} = 1.477 - 0.0351 = 1.441\text{ V}$ (2)

Worst-case open-loop voltage: $V_{\text{open,min}} = 3.135 - (50\text{ nA})(1.01\text{ M}\Omega) = 3.085\text{ V}$ (3)

Open-loop margin: $M_{\text{open}} = 3.085 - 1.825 = 1.259\text{ V}$ (4)

Both worst-case margins exceed the 0.5 V subsystem requirement. The maximum open-loop RC time constant is approximately $(1.01\text{ M}\Omega)(11\text{ nF}) = 11.11\text{ ms}$. Using the highest threshold and lowest open-state final voltage gives an approximate threshold-crossing time of 9.95 ms, leaving substantial time for comparator propagation, MCU wakeup, timestamping, and FRAM logging. If measured board leakage or switching noise exceeds the assumed bounds, the resistor values and qualification delay will be revised rather than accepting a smaller undocumented margin. The comparator itself is a practical low-power choice because devices such as TI's TLV3691 operate from sub-3.3 V supplies with nanoamp-scale quiescent current [6].

2.7 Verification and Traceability Plan

Table 3. High-level requirement verification plan.

Requirement	Primary test	Pass criterion
HLR1	Authorized/unauthorized NFC trials and repeated latch cycling	20/20 authorized cycles complete with no reset or lost log; 0/10 unintended releases for unenrolled credentials.
HLR2	Three trials each of lid opening, loop break, and defined impact; battery removal; deliberate record modification	All 9 tamper events logged with timestamps; prior records survive battery removal; verifier flags modified record.
HLR3	Measure assembled standby current; disconnect main battery for RTC retention test	Average armed-standby current $< 100\text{ }\mu\text{A}$; RTC error $\leq 2\text{ s}$ after 10 min without main battery.

3. Ethics, Safety, and Societal Impact

3.1 Ethics and Responsible Use

The system records access attempts and physical events that could be used when investigating a sensitive prototype. The ethical risk is therefore not only unauthorized access, but also over-interpreting the log. A broken loop, impact, or badge use indicates a sensor or credential event; it does not by itself prove malicious intent or identify the person physically holding the credential. Consistent with the ACM principles of avoiding harm, being honest about system limitations, protecting privacy, and designing robust systems [9], the desktop interface will label events neutrally and will not describe sensor events as proof of misconduct.

The device will minimize personal data by recording a credential slot or project identifier rather than a person's full name. Log export will be limited to authorized service use, and NFC authentication secrets will not be included in ordinary exports or debug messages. Demonstration data will use harmless sample objects rather than confidential, regulated, medical, or legal-evidence contents. The project will explicitly state that it is a prototype custody aid and not a certified legal-evidence system.

3.2 Safety and Applicable Standards

The main development hazards are the rechargeable Li-Po battery, moving latch hardware, soldering, and controlled impact testing. ECE 445 requires laboratory safety training, prohibits working alone in the lab, and requires additional precautions for projects using certain battery chemistries [3]. The course battery procedure requires review of the battery circuit, validation before attaching the battery, and lithium-battery handling precautions [10]. Initial bring-up will therefore use a current-limited bench supply. A protected cell will be restrained away from the latch, sharp edges, and coil heat, and any swollen or damaged cell will be removed from service.

The latch driver will default off during reset and will enforce a bounded pulse so a firmware fault cannot continuously energize the coil. Repeated latch tests will check switch, connector, wiring, and coil heating. Mechanical testing will use an empty enclosure, keep hands clear of pinch points, and use a repeatable drop/impact fixture rather than uncontrolled drops. Eye protection and fume extraction will be used during soldering and enclosure fabrication.

The selected Li-Po cell/pack will be sourced with appropriate manufacturer safety documentation; IEC 62133-2 provides a relevant portable lithium-cell/battery safety framework [11]. The 13.56 MHz NFC interface also makes FCC Part 15 radio-emission requirements relevant to any deployment beyond the classroom prototype [12]. The project will not claim regulatory certification of the completed device.

3.3 Societal, Economic, Environmental, and Global Impact

A reusable custody container could improve accountability for high-value engineering prototypes without requiring continuous network connectivity or a cloud subscription. Local event storage also reduces dependence on network availability, which can be useful in laboratories or organizations with restricted networks. Economically, the system has a higher initial hardware cost than a paper log or disposable tamper seal, but a reusable and serviceable design may reduce recurring material and replacement costs. The design may reduce reliance on disposable tamper seals and paper logs, but it introduces a rechargeable battery and electronic waste. The enclosure will therefore be designed so the battery, PCB, latch, and tamper wire can be serviced separately, and the battery will be disposed of through approved collection channels. The system is not intended to replace organizational access policies or legal chain-of-custody procedures; deployment in another organization or country would require review of its privacy, security, radio, battery, and handling requirements.

References

- [1] B. Guttman, D. R. White, S. Williams, and T. Walraven, Digital Evidence Preservation: Considerations for Evidence Handlers, NISTIR 8387, National Institute of Standards and Technology, Sep. 2022. doi: 10.6028/NIST.IR.8387.
- [2] University of Illinois Urbana-Champaign, “Project Proposal,” ECE 445 Senior Design Laboratory, 2026. [Online]. Available: <https://courses.grainger.illinois.edu/ece445/guidelines/proposal.asp>. Accessed: Sep. 14, 2026.
- [3] University of Illinois Urbana-Champaign, “Safety,” ECE 445 Senior Design Laboratory, 2026. [Online]. Available: <https://courses.grainger.illinois.edu/ece445/guidelines/safety.asp>. Accessed: Sep. 14, 2026.
- [4] NXP Semiconductors, PN532 User Manual, UM0701-02. [Online]. Available: <https://www.nxp.com/docs/en/user-guide/141520.pdf>.
- [5] STMicroelectronics, LIS2DW12: MEMS Digital Output Motion Sensor, product documentation. [Online]. Available: <https://www.st.com/en/mems-and-sensors/lis2dw12.html>.
- [6] Texas Instruments, TLV3691 0.9-V to 6.5-V Nanopower Comparator, Rev. A. [Online]. Available: <https://www.ti.com/product/TLV3691>.
- [7] RAMXEED, MB85RC256V I²C FeRAM, product documentation. [Online]. Available: <https://www.ramxeed.com/products/feram/i3.html>.
- [8] STMicroelectronics, STM32L433xx Ultra-Low-Power Arm Cortex-M4 MCU, DS11449 Rev. 8, Jul. 2024. [Online]. Available: <https://www.st.com/resource/en/datasheet/stm32l433cc.pdf>.
- [9] Association for Computing Machinery, ACM Code of Ethics and Professional Conduct, 2018. [Online]. Available: <https://www.acm.org/about-acm/code-of-ethics>.
- [10] University of Illinois Urbana-Champaign, “Safe Practice for Lead Acid and Lithium Batteries,” ECE 445 Senior Design Laboratory. [Online]. Available: <https://courses.grainger.illinois.edu/ece445/documents/GeneralBatterySafety.pdf>. Accessed: Sep. 14, 2026.
- [11] International Electrotechnical Commission, IEC 62133-2:2017+AMD1:2021, Safety requirements for portable sealed secondary lithium cells and batteries for use in portable applications, 2021.
- [12] Federal Communications Commission, “Radio Frequency Devices,” 47 C.F.R. Part 15, including § 15.225.