

Secure Chain-of-Custody Container

Design Document

ECE 445 Senior Design Laboratory
Fall 2026 • Team 4

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

TA: Alex Lee
Professor: Arne Fliflet

Contents

1. Introduction	2
2. Design and interfaces	3
Physical design and latch	4
Control and timekeeping	5
Authentication and USB	6
Tamper sensing	7
Logging and persistence	8
Power and charging	9
Switched power and actuator tests	10
Interface and actuator verification	11
Integrated system requirements	12
Standby feasibility and release decision	13
Tolerance analysis	14
3. Bill of materials and cost	15
Schedule	19
4. Impact, ethics and standards	20
Safety and release gates	21
5. References	22
Appendix A. Complete circuit schematics	24

1. Introduction

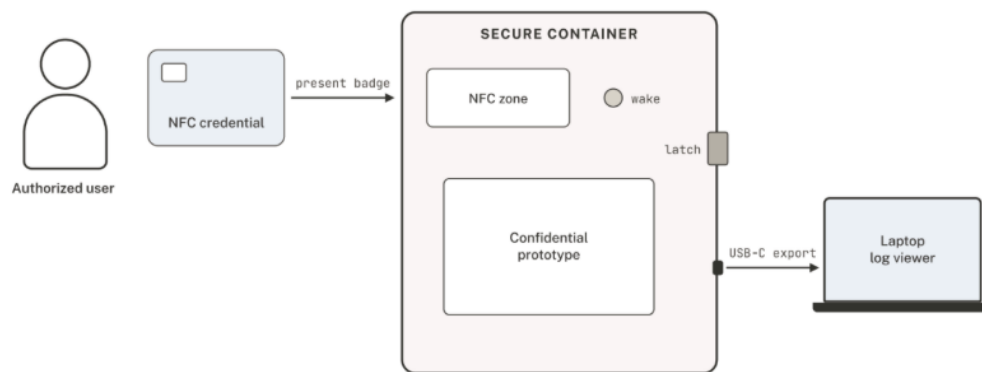
1.1 Problem and solution

Confidential engineering prototypes and other sensitive items move between laboratories, offices and authorized handlers. A lock limits access but does not by itself provide a reviewable handling history. Paper logs depend on manual entries. NIST guidance explains preservation concerns for digital evidence; the analogous need for traceable handling motivates this project, without claiming legal evidentiary sufficiency. [43]

This design integrates functions that can otherwise be separate: a lock restricts access, a transport logger records handling conditions, and a custody log preserves a history. Combining authenticated access, lid/loop sensing, impact detection and persistent local records is the proposed improvement. This is an integration benefit, not a claim that every commercial product lacks these functions.

An enrolled DESFire EV3 card must pass AES authentication before latch release. Hall, conductive-loop and impact sensors generate RTC-stamped FRAM records; authenticated USB export feeds a desktop integrity verifier. The engaged bolt remains locked without power. Credential slots identify cards, not people. [16]

1.2 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. Wake, authenticate, open and reclose, then authorize USB export. Section 2.5 defines the history's power, capacity and integrity limits.

1.3 High-level requirements

- **HLR1: Authenticated access.** The container shall release only after cryptographic authentication and enrollment. It shall complete 20 consecutive authorized lock/unlock cycles without reset, lost record or unintended release; ten unenrolled presentations shall produce zero releases.
- **HLR2: Tamper detection and history.** The container shall detect and timestamp unauthorized lid opening, loop interruption and the defined impact in at least three consecutive trials each. Committed records shall survive 10 minutes without main power, and deliberate record modification shall cause verifier failure.
- **HLR3: Autonomous operation.** Armed standby shall average below 100 μ A at the cell, including pack protection. RTC error shall be ≤ 2 s after 10 minutes without main power.

1.4 Development and evidence

Simulation proceeds directly to PCB fabrication, assembly and verification. Nucleo/module harnesses support firmware work. Acceptance tests remain planned unless identified as reported simulation; component ratings and calculations do not establish assembled-system compliance.

2. Design and interfaces

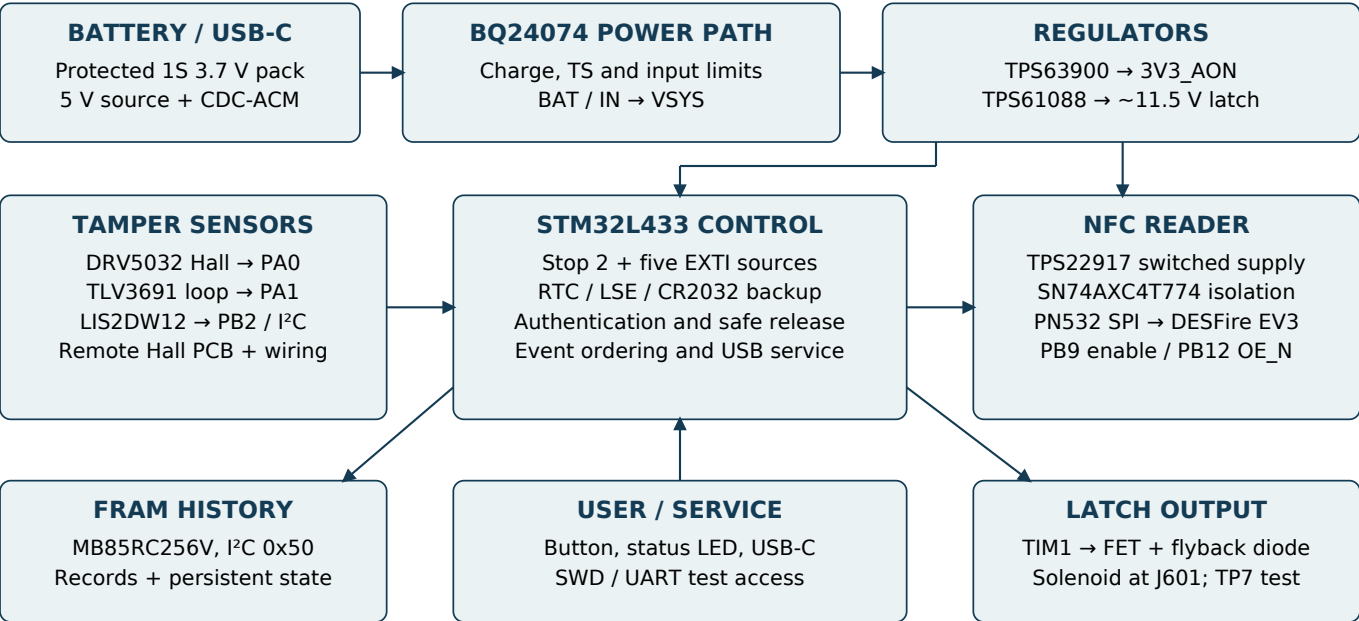


Figure 2. Functional architecture. The main PCB is 100 × 80 mm, four layers; the remote Hall PCB is 18 × 24 mm, two layers. Full circuit connections appear in Appendix A.

AON powers control, sensing, RTC and FRAM. TPS22917 switches NFC; the translator isolates SPI when off. The boost draws VSYS through removable R601. USB provides charging and gated service. I²C uses 4.7 kΩ pull-ups at 100 kHz. [17], [20], [23]-[27]

Function (Table 1)	Pin (pad) / mode
Button	PB11 (22), EXTI11 falling
Hall / loop / impact	PA0 (10) / PA1 (11) / PB2 (20), EXTI0/1/2
Charger PGOOD	PB14 (27), active-low, EXTI14 both edges
SPI1 SCK/MISO/MOSI	PA5/6/7 (15/16/17), AF5
NFC CS / enable / OE_N	PB6/9/12 (42/46/25); OE_N high isolates
I ² C1 SDA/SCL	PB7/8 (43/45), AF4; 100 kHz
ADC / divider enable	PB1/0 (19/18), ADC1_IN16/GPIO
Latch / boost	PA8 (29), TIM1_CH1 AF1 / PB10 (21)
Charger EN1/EN2	PA4 (14) / PB15 (28)
LED / test marker	PB13 (26), J204 pin 1; separate instrumented builds
USB D−/D+	PA11/12 (32/33), AF10
UART TX/RX	PA2/3 (12/13), USART2 AF7
SWDIO/SWCLK	PA13/14 (34/37), J101
LSE / reset / boot	PC14/15 (3/4); NRST (7); PH3/BOOT0 (44)

LQFP48 allocation. PA9 is unconnected. PB13 uses separate LED/instrumentation builds. Check native schematic, footprint and netlist consistency before fabrication.

2.1 Physical design and latch

The enclosure/latch support HLR1 retention and HLR2 sensing. A spring-return solenoid needs no holding current; the divider separates battery/electronics from payload.

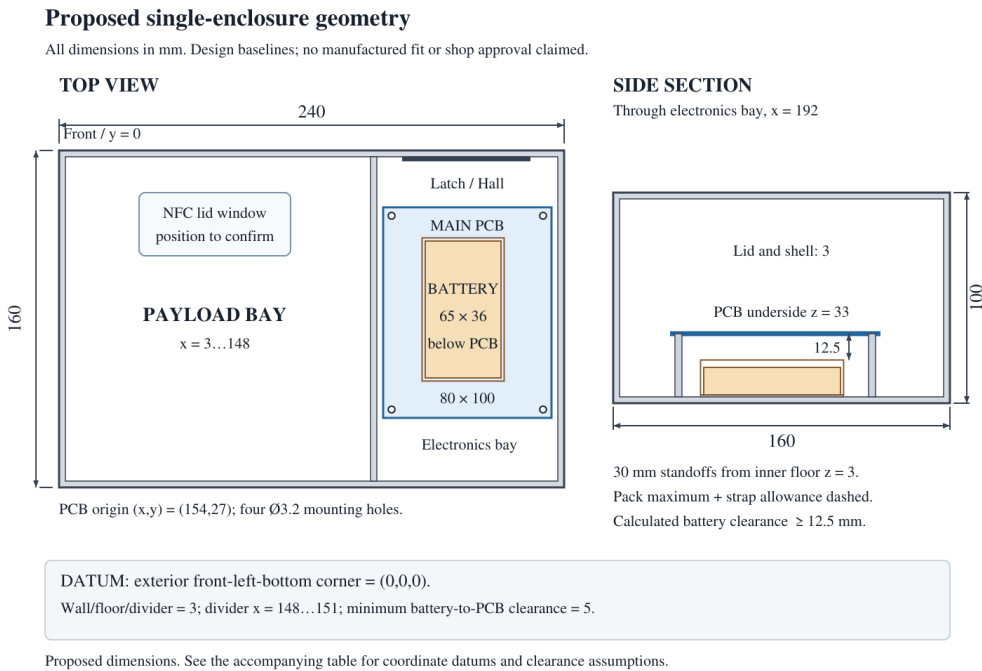


Figure 3. Proposed single-enclosure geometry, in millimetres. Dimensions are design baselines; manufactured fit and shop approval remain pending.

A hinged 240 × 160 × 100 mm enclosure uses nominal 3 mm walls, floor, lid and divider. From the exterior front-left-bottom datum, payload x=3...148 mm, divider x=148...151 mm and electronics x=151...237 mm; both bays span y=3...157 mm. The rotated PCB maps local (u,v) to (154+v,27+u) mm. Its Ø3.2 mm NPTH holes are (4,4), (96,4), (4,76), (96,76) locally, with insulated M3 hardware and copper keepouts. Thirty-millimetre standoffs place the underside at z=33 mm.

The battery lies nominally at x=174...210, y=43...108 mm. A 1 mm liner, 14.5 mm maximum pack height and 2 mm strap allowance leave 12.5 mm to bare PCB; require ≥5 mm to underside features. Confirm the 3 mm side clearances, wiring bends, connector access and latch sweep before shop release. Retain the D22 magnet, mount PN532 behind a nonconductive lid window and strain-relieve the hinge loop.

Adafruit 1512 is the candidate solenoid. TPS61088 provides approximately 11.5 V through an IRLML6344 low-side switch and SS34 flyback diode. The unpowered bolt holds only when mechanically engaged. The 200 ms commissioning pulse remains provisional until LA-2. [27], [29], [31]

Requirement (Table 2)	Verification procedure and pass criterion
LA-1 Unpowered bolt retraction shall be ≤0.5 mm under 50 N for 5 s.	Remove driver MOSFET; engage bolt. Apply calibrated 50 N at the handle, perpendicular to lid, for 5 s, ten times. Dial indicator resolution 0.01 mm: bolt retraction ≤0.5 mm in 10/10. Record fixture compliance and separately check lid lift. This is mechanism acceptance, not a forced-entry rating.
LA-2 Pulse width shall equal twice the worst pull-in minimum, within vendor limits and ≤1 s, with reliable release.	Sweep 500→50 ms, ten trials/width, two runs, at {V_DRIVE,V_MIN_LOAD} × {0,20 N preload}. Run minima agree within 10%. Set T_PULSE=2×largest minimum; require 40/40 releases, vendor envelope and ≤1 s. Revise design if margin exceeds limits; never clip it.

Shop drawing/scope review and measured fit remain release gates. These are project acceptance tests, not a forced-entry rating.

2.2 Control and timekeeping

Control supports HLR1 safe actuation, HLR2 ordering/time and HLR3 sleep/RTC backup. STM32L433 integrates the required peripherals; hardware pulse timing survives a CPU stall.

STM32L433 coordinates all subsystems. Stop 2 uses five external EXTI sources plus a 60 s RTC health wake. Active HCLK/APB run at 16 MHz. IWDG_STOP=0 freezes the watchdog in Stop 2; feed on wake and within 20 s during active sessions. Stop-mode supervision therefore depends on the EXTI/RTC path. Limit housekeeping to 240 μ C per wake at 3.3 V, equivalent to 4 μ A. [17]-[19]

TIM1 upcounting PWM2, one-pulse mode uses PSC=1599, a 10 kHz counter, CNT=0, CCR1=1 and RCR=0. ARR=2000/10000 produces the 200 ms commissioning pulse/1 s hard cap. Stop entry is blocked during a pulse. This avoids the 16-bit range failure at a 1 MHz tick.

PB1 is ADC1_IN16. Use 12-bit acquisition, 640.5-cycle sampling for the approximately 20.8 k Ω source, VREFINT-derived VDDA, ≥ 2 ms settling and discard the first sample after enabling PB0. Release requires 3.6 V with 50 mV hysteresis; invalid conversion denies release. RTC uses ABS07 32.768 kHz/7 pF, initial 10 pF COG loads and CR2032 backup. Disable coin-cell charging and keep PC13 quiet. [17], [19], [21]

Requirement (Table 3)	Verification procedure and pass criterion
CM-1 Stop 2 MCU current shall be $\leq 5 \mu$ A at 3.3 V with RTC active and debugger disconnected.	At 3.3 V/20-30°C, debugger disconnected: three 60 s MCU-domain averages $\leq 5 \mu$ A. Measure its branch or apply measured conversion efficiency and uncertainty; raw battery microamps are insufficient.
CM-2 All five sources shall wake and be identified, including paired assertions within 1 ms.	Ten wakes per external source: 50/50 correct; five dual-source trials within 1 ms: both identified; held-active source must not hide another edge.
CM-3 Reset/power controls shall remain ≤ 0.30 V, without ≥ 100 ns excursions; ROM recovery shall comply or be isolated.	Links removed; scope reader/boost/latch controls during held reset, first 100 ms after release, IWDG reset and power-up: ≤ 0.30 V, no ≥ 100 ns excursion. ROM recovery must pass or be disabled/isolated.
CM-4 Each TIM1 pulse shall meet $\pm 1\%$ and the 1 s cap, returning low despite CPU hang.	Ten scoped pulses within $\pm 1\%$; CPU-hang trial returns low and stays low 10 s without retrigger. Disable timer debug-freeze.
CL-3/RT-1 RTC error shall be ≤ 2 s after 10 min without main power; LSE startup shall be ≤ 2 s.	Remove main battery, USB and debugger for 10 min: restored RTC error ≤ 2 s in three trials, uncertainty < 0.2 s. Five true backup-domain cold starts: LSE ready ≤ 2 s with advancing calendar.
RT-2/3 VBAT current shall be $\leq 3 \mu$ A with main power absent; bound any charging current by instrument uncertainty. At 20-30°C, 24 h drift ≤ 5 s; record temperature/reference error and requalify changed load capacitors.	

2.3 Authentication and USB service

NFC supports HLR1 through authentication/enrollment; USB supports HLR2 export. DESFire AES strengthens UID-only checks; PN532 provides the RF interface without a custom radio design.

PN532 uses SPI mode 0, LSB first, initially 1 MHz and no more than 4 MHz. DESFire EV3 AuthenticateAES selects application 0x534343 (wire bytes 43 43 53), key 0. A provisioned AES-128 project key and current stable 7-byte UID enrollment are both required. Trusted physical SWD provisioning initializes keys and enrollment; blank or corrupt metadata never creates administrative access. [4], [20], [22], [32]

Range-1/HSI48 hardware RNG supplies 16 fresh challenge bytes within one shared 10 ms readiness/acquisition deadline. Clock, seed, data-ready or zero-value faults deny release; never reuse a challenge or substitute a fallback PRNG. The reader turns off within 5.0 s of NFC_EN rising. Stop transactions by 4.9 s, isolate OE, set SCK/MOSI/CS LOW and MISO analog, then lower PB9. Cleanup precedes boost, latch or lid waiting. Enforce ≥ 1 s off dwell; early requests return BUSY.

The six privileged commands, including EXPORT, require an enrolled-card authenticated 30 s monotonic window, ending on reset or USB disconnection. Only explicitly authorized empty-table SWD provisioning is an exception. SET_TIME must not extend the window. USB uses a 90 Ω differential pair, 22 Ω series resistors, USBLC6 protection, HSI48/CRS and CDC-ACM. Restore clocks after Stop 2; re-enumeration is expected. APB must remain ≥ 10 MHz while USB is active. [6], [7], [19], [33]

Requirement (Table 4)	Verification procedure and pass criterion
NF-1 PN532 initialization shall be byte-correct within 100 ms after qualified cold-start and settling intervals.	Ten cold starts; ≥ 2 s off, confirming ≥ 1 s below 0.1 V. After ≥ 20 ms settling, firmware/version and SAM exchanges must be byte-correct within 100 ms.
NF-2/AT-1 Only authenticated, enrolled credentials shall release; RNG faults shall deny within 10 ms without a pulse.	Authentication: 20/20 valid, 10/10 wrong-key failures; reader remains responsive. Access: 10/10 authorized single pulses, 0/10 negative-credential pulses. Inject clock-ready/DRDY/clock-error/seed-error/zero faults $\times 3$: deny within 10 ms, no pulse, then recover on clean wake.
NF-3 Reader power shall end within 5 s for every outcome; no-card shall end in 4.9-5.0 s.	Five trials each at 0/10/20 mm, plus three each unenrolled/wrong-key/no-card/communication-fault: all 27 powered intervals ≤ 5 s; 15 valid authenticate; failures never pulse. No-card ends in 4.9-5.0 s. Hold one lid open: reader stays off.
NF-4/5 Firmware shall expose no key; privileged authority shall expire after 30 s or reset/disconnect, except authorized SWD provisioning.	Capture release UART/USB/FRAM: no key in raw, hex, Base64 and reversed forms; inspect logging. Six privileged commands $\times$ seven authorization cases; reject unauthorized/expired sessions. SET_TIME, reset and USB-disconnect expiry tests preserve the monotonic boundary.

2.4 Tamper sensing

Sensing supports HLR2 and HLR3. Hall avoids a moving electrical contact, the comparator monitors during sleep, and latched impact interrupts persist until serviced.

DRV5032FB samples at 5 Hz (maximum period 286 ms); PA0 is LOW closed and HIGH open. The D22 N42 magnet is $\varnothing 3.18 \times 3.18$ mm. Calculated closed field is approximately 56 mT on-axis and 41 mT at the lateral corner using $B_r = 1.32$ T maximum, so it is not a guaranteed minimum. At 30 mm, the modeled field is about 0.18 mT against the 0.25 mT release target; qualify actual hinge geometry. [24], [29]

An insulated 30 AWG conductor follows body, lid, divider and cable passage. A 1 M Ω sense pull-up, 1 M Ω /1 M Ω reference and two 10 nF filters feed TLV3691; PA1 is LOW intact and HIGH cut. LIS2DW12 at I²C 0x19 uses low-power mode 1, 25 Hz, ± 8 g and latched INT1 to PB2. Per-axis high-pass threshold steps are FS/64. Sampling rate alone does not guarantee short-shock detection. [23], [25]

Requirement (Table 5)	Verification procedure and pass criterion
AT-3 Hall output shall be LOW throughout specified closed geometries and HIGH at ≥ 30 mm separation.	D22: gaps 1.5/2.0/3.0 mm $\times$ offsets 0/-1.5/+1.5 mm, all nine LOW. Measure pole-face-to-sensing-location gap; dwell ≥ 0.5 s. Actual hinge-open separation ≥ 30 mm and 30 mm jig must be HIGH, ten repeats; record transition gap and hinge angle. Jig 25 mm is characterization only.
HL-1/HL-2 Lid timestamps shall be within ± 1 s with sticky tamper; Hall current shall be ≤ 2.0 μ A.	Hold bolt back with removable pin; three unauthorized open/wait ≥ 2 s/close cycles from Stop 2. Require three open/close pairs, timestamps ± 1 s, valid chain and persistent tamper. Measure Hall branch contribution for 60 s in each state: both ≤ 2.0 μ A.
AT-4/TL-1 Loop sensing shall distinguish 0-10 k Ω from open with ≥ 0.5 V margin and ≤ 20 ms cut detection.	At 3.135/3.300/3.465 V test short, 10 k Ω and open. Use ≥ 1 G Ω instrument or correct 10 M Ω loading. Require LOW/LOW/HIGH; intact margin= $V_{REF} - 0.050 - V_{SENSE}$, open= $V_{SENSE} - V_{REF} - 0.050$, each ≥ 0.5 V. Scope ten cuts at each extreme rail: 20/20 ≤ 20 ms.
TL-2/TL-3/TL-4 Loop sensing shall reject defined disturbances, draw ≤ 6 μ A and timestamp cuts within ± 1 s with sticky tamper.	Require no transitions during ten taps/flexes, ten make-before-break 10 k Ω insertions and 10 s of ≥ 50 mVpp at V_{SENSE} with the 10 k Ω fixture installed: 1 kHz square, 50 Ω source through 1 nF; generator ≤ 1 Vpp. Measure total feed 60 s at 3.465 V: ≤ 6 μ A including uncertainty. Three cuts must log timestamps within ± 1 s and set sticky tamper.
AC-1/AC-2 Accelerometer current shall be ≤ 3 μ A; INT1 shall persist ≥ 500 ms and clear only after WAKE_UP_SRC read.	Read back configuration; 60 s branch current ≤ 3 μ A. Ten taps with servicing disabled: INT1 stays HIGH for 500 ms, clearing only after WAKE_UP_SRC read.
AT-5 Impact sensing shall detect every defined drop within 100 ms of contact and reject all ten handling cycles.	Tune with five impacts/ten handling cycles: threshold midway between maximum handling and minimum impact-at-contact values if separable; otherwise revise ODR/FS/filter and repeat. Freeze THS/DUR before acceptance. Empty payload, battery/electronics installed: guided base-down 100 ± 2 mm drop within $\pm 5^\circ$ onto 6 mm ~ 60 Shore A mat. Three drops ≥ 30 s apart: INT1 at contact, not release; contact-strip/INT1 delay ≤ 100 ms, three IMPACT records. Ten handling cycles: lift, carry 3 m in 3 ± 1 s, set down from 50 mm within 1 s, open/close, slide 100 mm; zero events. Record mass, mat, THS/DUR codes/mg, ODR/FS, peaks and contact timing.

2.5 Logging and persistence

FRAM supports HLR2 with writes requiring no flash erase; dual metadata/readback preserve transaction boundaries. Section 2.10 addresses its standby-current risk.

MB85RC256V, 32 KiB at I²C 0x50, provides 380 immutable 80-byte records: 364 general and 16 tamper-reserved. Alternating copies hold 24-byte headers, 128-byte configuration and 64-byte fault snapshots. A record contains sequence (4 B), UTC (4 B), event (1 B), slot (1 B), flags (2 B), previous hash (32 B), current hash (32 B) and CRC32 (4 B). Use the selected narrow SOP MB85RC256VPNF package. [5], [26]

Write/read back the record before the alternate header. Boot selects generation before sequence, verifies the whole committed prefix and recovers at most one next complete append. Never hide corruption by selecting an older prefix. Sequence spans both partitions; genesis binds the generation. Configuration/fault transactions recover to a complete old or new state. Reserve four general records before ACCESS_GRANTED; other events cannot consume them. Without room, deny release. CLEAR_LOG needs a verified current export in the same authorized session, atomically starts a new generation and preserves enrollment, time and unresolved lockouts.

Queue depth is eight. A ninth arrival replaces entry eight with a marker counting two losses and event-eight time; later losses accumulate without changing an in-flight snapshot. Every committed/replayed overflow marker conservatively sets lid and loop lockout. This records lost coverage, not proof both sensors fired. Idle commits finish ≤ 50 ms from interrupt; queued commits finish ≤ 50 ms from their turn after rail qualification. Writes pause during the pulse and resume only after AON ≥ 3.135 V for 5 ms. Eight turns drain within 400 ms. After 500 ms without qualified power, inhibit release and declare a fault; volatile observations may be lost.

Requirement (Table 6)	Verification procedure and pass criterion
CL-1 Events shall appear once, in order, with timestamp error ≤ 1 s; grant precedes pulse and completion follows closure.	Manifest five completed accesses, three unauthorized opens, three loop cuts and three impacts, plus authorized clears. Export: every expected event appears once, in sequence, timestamp error ≤ 1 s; grant precedes pulse and completion follows reclosure.
LG-1 Commits shall meet 50 ms deadlines and eight shall drain ≤ 400 ms; overflow shall record loss.	Scope interrupt/gate/PB13 at J204, LED disabled. Test 10 idle, 11 queued and nine arrivals during one pulse: verify 29 records (10+11+7+marker), hashes/CRCs, ≤ 50 ms applicable deadlines and ≤ 400 ms drain. Marker counts two losses. Repeat arrivals during recovery/drain; cut after marker before checkpoint and require lockout.
LG-2/CL-2 Committed history shall survive interruptions/10 min power loss; transactions recover old/new states with ≤ 1 next append.	Five cuts each during body, between body/header, during header and after header: all 20 preserve prior records; at most one append recovers. Also interrupt prepared/final configuration, CLEAR_LOG and full-log metadata stages, five trials per stage: only old/new states allowed. Remove battery/USB/debugger 10 minutes; prior committed exports remain identical.
CL-4 The verifier shall accept the original image and reject all 18 specified mutations, including the tail.	Save a valid 20-record image. Restore before each one-byte mutation in six fields: timestamp, sequence, event, slot, previous/current hash; target records 1, 10, 20. Require all 18 failures, including the tail; original passes.
LG-4 Full storage shall preserve history, reserve four slots per access and persist loss/tamper state.	Test five/four/three free general slots; four allows the reserved access despite interleaved tamper, three denies. Exhaust reserve, inject tamper: record bytes unchanged, fault count/sticky state updated. Authorized export/clear preserves enrollment and unresolved lockouts.

2.6 Power and charging

Power supports all HLRs. Buck-boost conversion spans battery voltage above/below 3.3 V; the charger shares USB/battery loads, and a separate boost supplies latch pulses.

Protected CU-JAS427, 1S/3000 mAh/5 A, feeds BQ24074 BAT; OUT supplies VSYS, TPS63900 and TPS61088 through R601. TPS63900 uses SEL/CFG2 grounded, CFG1=36.5 k Ω and CFG3=16.2 k Ω for 3.3 V. Its $\pm 1.5\%$ DC accuracy leaves margin within the system $\pm 5\%$ requirement. PW-1 reaches 3.0 V on a bench source; armed use stops at 3.3 V. [27], [30]

At loaded battery ≤ 3.3 V, persist LOW_BATTERY and disable reader, boost and latch. Recovery needs valid PGOOD and ten valid readings ≥ 3.65 V at 100 ms spacing; low/invalid readings restart qualification. Persist recovery before clearing lockout. Reset/USB insertion alone cannot clear it. TPS63900 remains enabled, so firmware cannot enforce a permanent 3.0 V floor or guarantee depleted-pack storage. Promptly recharge under supervision or disconnect J501. The published 2.75 V pack endpoint is not a verified protector trip.

R501=1.78 k $\Omega \pm 1\%$ programs 500 mA nominal, 443-553 mA before limiting. R502=3.65 k $\Omega \pm 1\%$ gives about 418 mA typical/476 mA maximum input in EN2/EN1=10, allowed only with permission for ≥ 500 mA. Use 00 before configuration and 11 for suspend; CE_N is grounded. R503=68 k $\Omega \pm 1\%$ gives 9.07 h nominal, 6.73-11.45 h initial timer bounds with datasheet dynamic behavior. R509 is fed by VSYS. Separate CC pull-downs are 5.1 k Ω ; attachment alone grants no 500 mA permission. [27]

USB-only uses IN $\rightarrow$ OUT $\rightarrow$ AON and prohibits latch release; defer NFC until source permission. Battery-only uses BAT $\rightarrow$ OUT $\rightarrow$ AON/boost. Combined power shares input with charging and draws battery supplement when needed. Measure signed battery current and system current at VSYS. Qualify the 4.5 A BQ battery path, 5 A pack and interconnects. Use exactly one verified, insulated 103AT-2 attached to the pack; insulate the unused pack NTC lead. [15], [27], [30]

Requirement (Table 7) Verification procedure and pass criterion

PW-1 AON shall remain 3.135-3.465 V across 3.0-4.2 V battery input under the specified operating loads.	Sweep J501 4.2 $\rightarrow$ 3.0 V in 0.1 V steps, MCU awake/FRAM writing, NFC/latch off: every AON reading 3.135-3.465 V.
PW-4a Unrestricted fast charge shall be 443-553 mA; production 3.65 k Ω ILIM shall be restored before USB-host use.	No PC: 5 V bench source ≥ 1.5 A capability, 1 A limit; temporarily fit 1.62 k Ω ILIM, mode10, battery ≈ 3.7 V, VSYS load ≤ 100 mA. Outside input/thermal/taper limiting, charge=443-553 mA. Restore 3.65 k Ω unpowered.
PW-4b USB input shall be $\leq 100/500$ mA before/after permission; reverse current ≤ 10 μ A; USB-only release prohibited.	Test USB-only, battery-only and combined paths. Connector current ≤ 100 mA before configuration/ ≤ 500 mA after permission; removed-source reverse current ≤ 10 μ A. Confirm battery supplement during latch pulses and prohibit USB-only release.

2.7 Switched power and actuator qualification

Switched power supports HLR1 startup/release and HLR3 standby. Controlled slew limits inrush, SPI isolation limits off-state current, and timer actuation bounds coil energy.

TPS22917 CT=2.2 nF connects to VIN; QOD connects through R402=1 k Ω . Board 10.1 μ F plus assumed reader 100 μ F yields 110.1 μ F. With approximately 150 Ω typical internal QOD, decay 3.3 $\rightarrow$ 0.1 V is 443 ms; no guaranteed worst case follows. At 0.86 V/ms typical slew, capacitive inrush is 94.7 mA before boot demand. Translator off leakage is finite and included in the budget. [27]

TP7 is a bench test point, not an MCU ADC. The latch uses a qualified fixed boost delay, initially 50 ms with gate LOW. Require ≥ 11 V by 25 ms; otherwise use at least twice the observed startup time and requalify the ≤ 2 s eligible AUTH_OK $\rightarrow$ gate deadline. Reader power must already be off. At battery 3.6 V, total resistance 0.15 Ω and 85% efficiency, the model predicts 3.82 A and 3.027 V boost input for 11.49 V $\times$ 0.8125 A plus 3.3 V $\times$ 0.15 A. This does not prove switching stability. [27]

Requirement (Table 8)	Verification procedure and pass criterion
NP-1 Reader rail shall reach ≤ 0.1 V within 750 ms and remain low; re-enable shall wait ≥ 1 s.	Actual reader: reach ≤ 0.1 V within 750 ms and remain there during application-off, reset, power-up and USB-present/absent cases across the qualified envelope. Enforce ≥ 1 s ordinary off dwell; cold-start tests use ≥ 2 s off, confirming ≥ 1 s below 0.1 V.
NP-2 The R411 reader branch shall draw ≤ 5 μ A while off, with translator/GPIO feed accounted separately.	Measure R411 upstream current for 60 s in these states: ≤ 5 μ A. Account separately for translator/GPIO paths; low rail voltage alone cannot prove zero backfeed.
NP-3 Reader rail shall reach ≥ 3.0 V within 20 ms and initialize successfully; premature requests shall return BUSY.	Twenty power cycles: rail ≥ 3.0 V within 20 ms and first GetFirmwareVersion after settling succeeds 20/20. Requests inside off dwell return BUSY.
PR-1/NP-4 Reader startup shall keep AON ≥ 3.135 V and combined capacitive, boot and RF peak current ≤ 200 mA.	At 3.0 V with 0.25 Ω series, capture 20 reader enables: AON ≥ 3.135 V throughout; capture combined capacitive/boot and RF peaks on ≥ 10 enables, each ≤ 200 mA. Use differential/current probing.
PR-4 Pulse-time AON shall stay ≥ 2.85 V; FRAM shall wait until pulse completion and ≥ 3.135 V for 5 ms.	During 20 latch pulses, AON ≥ 2.85 V continuously; no FRAM transaction during pulses or until ≥ 3.135 V for 5 ms afterward. Inject ten lid events and verify queued timestamps.
PW-3/lockout Release shall inhibit below 3.6 V; ≤ 3.3 V shall latch lockout until ten qualified ≥ 3.65 V charging readings.	Sweep through 3.6/3.3 V: inhibit release/enter persistent lockout respectively. Reset must retain lockout; only the ten-reading charging qualification clears it.

2.8 Interface and actuator verification

These tests complete NFC/USB support for HLR1 and HLR2 and qualify the power/latch interaction for HLR1 and HLR3. They use the same hardware and firmware contracts as Sections 2.1, 2.3, 2.6 and 2.7.

Requirement (Table 9)	Verification procedure and pass criterion
UC-3 CDC shall enumerate within 3 s; verified 20-record export shall finish within 5 s, excluding authentication.	Range 1; valid VDDUSB before setting USV; attach only with VBUS. On Windows 10 22H2, Windows 11 23H2 and Ubuntu 24.04 LTS, five trials per host: CDC appears ≤ 3 s after insertion; authorized 20-record export and verifier PASS ≤ 5 s, excluding authentication. Require 15/15 for both.
PW-3/startup For a 50 ms delay, boost shall reach ≥ 11 V by 25 ms; eligible AUTH_OK-to-gate shall be ≤ 2 s.	Scope TP7 across qualified source/load conditions: ≥ 11 V by 25 ms for the 50 ms delay. Record 20 eligible AUTH_OK→gate intervals ≤ 2 s; verify no BQ path interruption or exceeded current rating.
UC-1/2 Sources shall supply 4.75-5.25 V; PGOOD shall meet 0.4/2.9 V logic, 100 ms response and ≤ 3.6 V unpowered.	PC USB, A-to-C 5 V charger and C-to-C source must deliver 4.75-5.25 V. At both AON limits, PGOOD ≤ 0.4 V present/ ≥ 2.9 V absent within 100 ms, wakes on both edges, and stays ≤ 3.6 V with MCU unpowered.
AT-2/LA-4 Cycling shall avoid binding/resets; normal duty shall be $\leq 5\%$, coil rise $\leq 20^\circ\text{C}$ and component temperatures $\leq 60^\circ\text{C}$.	Require 20/20 releases/re-engagements without binding or NRST pulses. Normal period = $\max(5 \text{ s}, 20\text{T})$; cool, then twenty supervised abuse pulses at $\max(1 \text{ s}, 4\text{T})$, bypassing the normal $\leq 5\%$ duty interlock only for the $\leq 25\%$ abuse run. Thermocouple/IR: coil rise $\leq 20^\circ\text{C}$; coil/FET/diode $\leq 60^\circ\text{C}$. Stop at 60°C or excessive rise. Record ambient, temperatures immediately/30 s afterward; temperatures must fall. At 200 ms, abuse off-time is 800 ms.
LA-3 Flyback shall keep drain $\leq V_{\text{LATCH}} + 1$ V and $\leq 0.5 \times \text{rated } V_{\text{DS}}$; current shall fall below 10% peak within 5L/R.	With diode fitted, scope drain tip to circuit-ground reference only; use clamp probe or differential shunt inside the recirculation loop for current, not the source shunt. Trigger gate falling at 2 $\mu\text{s}/\text{div}$ and 2 ms/div; five pulses each at $V_{\text{rated}}/V_{\text{DRIVE}}$. All ten: drain $\leq V_{\text{LATCH}} + 1$ V and $\leq 0.5 V_{\text{DS}}$ rating; current $< 10\%$ peak within 5L/R.

AT-1 negative set: three presentations with a project-key but unenrolled EV3, three revoked, two factory-key EV3, one Classic and one NTAG. NF-5 commands: ENROLL, REVOKE, SET_TIME, CLEAR_TAMPER, CLEAR_LOG, EXPORT. Test each from restored fixtures P (two enrolled) / E (valid empty): P/no auth, P/auth at 5/29/31 s, P/failed auth, P/SWD without auth, E/SWD. Command-specific preconditions still apply. Validate AES against FIPS 197 vectors before integration.

2.9 Integrated system requirements

System tests join HLR1 access, HLR2 history and HLR3 standby/time retention, checking interactions beyond isolated subsystem tests.

Eligible access follows: reserve four records → commit ACCESS_GRANTED → turn reader off → enable boost and wait qualified delay → one hardware pulse → recover rail and drain queue → lid open/close or 60 s timeout → final record. Tamper or unresolved lockout, invalid state, low battery, failed authentication or insufficient log space inhibits release. Committed sticky state OR current sensor levels after the 50 ms startup mask restores lockout.

Requirement (Table 10)	Verification procedure and pass criterion
CL-5 Tamper shall inhibit every pulse and persist across reset until valid, authorized, durably logged clearance.	For each lid/loop channel: active fault + five enrolled attempts; physically restored without clear + five; re-create, reject/log authenticated CLEAR_TAMPER while active + one; restore, remove battery/USB one minute, then three attempts. Require 0/14 pulses and denial records. Restore + authorized logged clear then permits 1/1.
LG-3 I ² C rise time shall be ≤1000 ns at 100 kHz; 400 kHz shall require measured rise ≤300 ns.	Scope SDA/SCL during FRAM reads with ≤10 pF probes and 4.7 kΩ pull-ups. At 100 kHz, 30-70% rise time ≤1000 ns. Compute TIMINGR from actual kernel clock; 400 kHz is permitted only after ≤300 ns measurement.
PW-3 / PR-3 Stage capacity shall be ≥1.25×I_PULLIN; BOR falling maximum ≤0.8×minimum rail; transients shall cause zero resets with AON ≥2.85 V.	Measure pull-in current at armature knee and peak current at V_DRIVE using source shunt. Stage capability from fitted FET/diode/BQ/pack/interconnect ratings and source resistance must be ≥1.25×I_PULLIN. Select highest BOR0-4 with falling-threshold maximum ≤0.8×minimum modeled/measured pulse rail; read back option bytes. Scope 20 final-source latch pulses + 20 NFC steps: 0/40 resets, pulse rail ≥2.85 V and above selected BOR; 3.135 V is the design goal.
HLR1-3 / IS-1 HLR1-3 shall pass; five integrated cycles shall need no manual recovery, with <100 μA standby and ±2 s RTC retention.	Complete HLR1's 20 valid cycles and ten unenrolled denials; verify all expected records. For HLR2, three each lid/loop/impact, timestamps ±1 s; remove battery, USB and debugger 10 min, restore, require identical valid committed prefix; record mutation fails verification. HLR3 passes PW-2 and three CL-3 trials. IS-1: five complete button→card→release→open→close→ACCESS_COMPLETE→authorized export→verifier PASS runs, no reset/reflash/power-cycle/manual recovery.
PW-2/PR-2 Standby shall be <100 μA including pack drain; each 60 s health wake shall add ≤240 μC.	At 20-30°C, USB absent, average ≥5 min at 4.2/3.7/just-above-3.3 V. Require I_J501+confirmed I_pack<100 μA; a 10 μA bound requires J501<90 μA. Integrate wake charge and reconcile isolated shares by power, including converter loss.

Common verification conditions

Use the assembled PCB or complete container as specified. Record firmware/build, instrument IDs, temperature, traces and uncertainty. Default analog corners are 3.135/3.300/3.465 V; current tests are at 20-30°C. Current-meter accuracy is ≤1% + 0.1 μA, with burden recorded. Scope clips connect only to circuit ground. State reset, power and credential preconditions before each trial. Record each requirement/trial, stimulus, measured value, limit, uncertainty, pass/fail and trace/export filename. Pass/fail applies to every repetition.

2.10 Standby feasibility and release decision

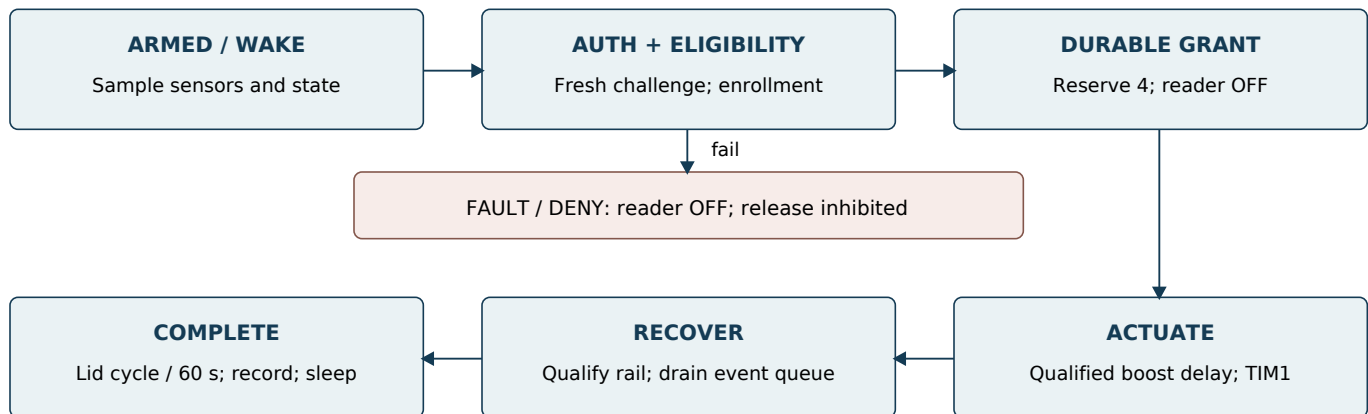


Figure 4. Access-request flow. Other wakes service sensors/health/history and return to standby. Failed eligibility or commit inhibits release; tamper updates lockouts at any state. Logging follows Section 2.5.

Power budget and acceptance

Planning allocations on 3.3 V total 66.35 μA : MCU 5, Hall 1.8, loop 5.45, impact 3, FRAM 27 typical, translator 10, disabled switch 0.1, housekeeping 4 and leakage 10. Direct battery allowances total 19.5 μA : charger 6.5, boost shutdown 3 and provisional pack protection 10. Include settled boost-divider current. Converter efficiency η already includes its losses; do not add IQ twice. [17], [24]-[27], [30]

$$I_{\text{cell}} [\mu\text{A}] = 3.3 \times 66.35 / (V_{\text{BAT}} \times \eta) + 19.5 + 10^6 \times V_{\text{BAT}} / (0.99 \times 531000)$$

At $\eta=90\%$, 4.2/3.7/3.3 V produce 85.41/92.29/99.50 μA . At 3.3 V/85%, the estimate is 103.84 μA ; FRAM's 56 μA maximum also exceeds the nominal budget. Thus these assumptions do not prove compliance. PW-2/PR-2: USB absent, average ≥ 5 min at 4.2, 3.7 and just above 3.3 V; require I_{J501} + confirmed internal pack drain $< 100 \mu\text{A}$. A confirmed 10 μA pack bound requires J501 $< 90 \mu\text{A}$. Do not open the pack. Integrate wake charge and reconcile branch powers, efficiency and uncertainty.

Contingency and release gate

Retain HLR3 below 100 μA . Before fabrication, reconcile an upper-bound cell-current budget across the declared standby envelope and obtain team/TA disposition; use 90 μA as an engineering target, not a relaxed acceptance limit. Converter efficiency, housekeeping, interface leakage and internal pack drain need supported bounds. The present baseline does not clear this gate.

A specific candidate is replacing FRAM U302 with Infineon CY15B256J-SXA, 32 KiB I²C, and implementing explicit sleep/wake. It specifies 8 μA maximum sleep current and $\leq 400 \mu\text{s}$ wake at 2.0-3.6 V; ordinary standby can be 150 μA and is unsuitable. This is a proposed contingency, not an implemented or approved substitution. [44]

Allocate $\leq 10 \mu\text{A}$ to the complete FRAM contribution including wake overhead. With all other allocations unchanged, the model gives 83.84 μA at 3.3 V battery/rail and 85% efficiency, or 86.74 μA at the 3.465 V rail corner. These results remain conditional on the other allowances. Before selection, verify every pin and package dimension, update native CAD/BOM/cost, qualify sleep entry and wake retries on the shared bus, and repeat latency, interrupted-write and full-log tests. Confirm all budget bounds; final PW-2 must still pass on the assembled unit.

Decision record before order release: chosen FRAM and firmware protocol; worst-case budget with sources/uncertainty; native CAD revision and checks; revised purchasing cost; team/TA disposition. Until recorded, retain the baseline BOM and mark fabrication release pending.

2.11 Critical tolerance analysis

The tamper-loop comparator is critical because false detection can implicate a handler, while a missed cut defeats the intended evidence. AT-4 requires intact resistance 0-10 kΩ versus an open loop with ≥ 0.5 V decision margin. The following establishes modeled feasibility under stated allowances; hardware must confirm them. [23]

Parameter (Table 11)	Bound and rationale
Supply / resistors	3.135-3.465 V; all three 1 MΩ resistors $\pm 1\%$.
Leakage / decision	± 50 nA per node is a board-leakage allowance. The executed grid uses ± 70 nA including 20 nA comparator bias. Decision allowance ± 50 mV = 22 mV offset + 8.5 mV half typical hysteresis + 19.5 mV noise allowance.
Capacitors	10 nF $\pm 10\%$ initial tolerance; timing uses 11 nF. X7R voltage/temperature effects are outside this model.

Closed-node maximum: $3.465 \times 10 \text{ k}\Omega / (990 \text{ k}\Omega + 10 \text{ k}\Omega) + 50 \text{ nA} \times (990 \text{ k}\Omega \parallel 10 \text{ k}\Omega) = 35.1 \text{ mV}$. The reference spans 0.495...0.505 of the rail, with $\pm 25 \text{ mV}$ leakage shift: 1.527...1.775 V. Including decision uncertainty gives 1.477...1.825 V thresholds. Open-node minimum is $3.135 - 50 \text{ nA} \times 1.01 \text{ M}\Omega = 3.085 \text{ V}$. Conservative closed/open margins are therefore 1.442/1.260 V. These combine different supply extrema and are deliberately conservative.

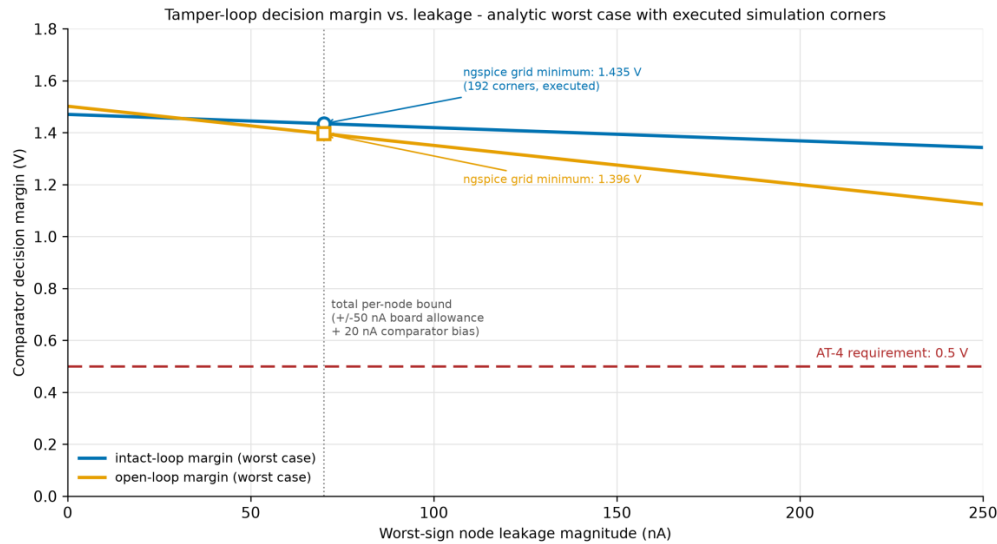


Figure 5: Both decision margins stay above the 0.5 V requirement across the plotted sweep (to 250 nA, $\sim 3.6\times$ the ± 70 nA total per-node bound); the requirement line is reached only near $\pm 0.66 \mu\text{A}$ per node. Curves: closed-form worst case. Points: executed 192-corner ngspice DC grid minima at ± 70 nA.

Figure 5. Reported leakage sweep and ngspice corner results from the project analysis. These simulations were not rerun for this shortened report.

Shared-supply analytical minima are 1.445/1.426 V; the reported 192-corner DC grid at ± 70 nA yields 1.435/1.396 V. Its closed endpoints are 0.1 Ω and 10 kΩ, and cut is ideal open; a 1 GΩ path is approximately 3 mV lower. The ≥ 0.5 V target is approached around $\pm 0.66 \mu\text{A}$ per node, about $13\times$ the 50 nA board allowance. This is conditional headroom, not an environmental guarantee.

After a cut, $\tau \leq 1.01 \text{ M}\Omega \times 11 \text{ nF} = 11.1 \text{ ms}$; conservative threshold time $-\tau \ln(1 - 1.825/3.085) = 9.95 \text{ ms}$. The reported 256-corner transient grid reaches 8.74 ms; the comparator's approximately 24 μs delay is typical, not a slow-ramp maximum. The modeled 100 mV/1 ms burst does not assert intact-loop output. TL-1 still requires measured $\leq 20 \text{ ms}$, TL-2 checks injected noise and TL-3 total feed $\leq 6 \mu\text{A}$. Idle wake/timestamp/ $\leq 50 \text{ ms}$ commit targets 100 ms end-to-end; pulse-time events use queue/recovery deadlines. Mask startup 50 ms, then sample standing state.

3. Bill of materials: main PCB, part 1

Table 12 / ref.	Description / package	Manufacturer; linked part number	Unit	Buy	USD ea.	USD total
U101	STM32L433CCT6 (LQFP-48)	STMicro: STM32L433CCT6	1	3	7.50	22.50
BT101	CR2032 holder (CR2032 hldr)	Keystone: 1060	1	3	1.60	4.80
J101	SWD 1.27mm (2x5 1.27 mm)	Samtec: FTSH-105-01-L-D	1	3	3.60	10.80
J102	UART 3.3V (XH-3)	JST: B3B-XH-A(LF)(SN)	1	4	0.24	0.96
Y101	32.768kHz CL=7pF (3215)	Abracon: ABS07-32.768KHZ-7-T	1	4	0.32	1.28
R101, R102	10k (0603)	Yageo: RC0603FR-0710KL	2	6	0.10	0.60
C101-104, C107, C108, C203, C204, C301, C303, C304, C404-406, C603, C605	100n (0603)	Murata: GRM188R71C104KA01D	16	48	0.10	4.80
C105, C401, C501	1u (0603)	Murata: GRM188R71C105KA12D	3	9	0.10	0.90
C106, C502, C604	4.7u (0603)	Murata: GRM188R61A475KAAJD	3	9	0.10	0.90
C109, C110	10p (0603)	Murata: GRM1885C1H100JA01D	2	6	0.10	0.60
U201	TLV3691IDCKR (SC-70-5)	TI: TLV3691IDCKR	1	3	1.10	3.30
R201-203	1M (0603)	Yageo: RC0603FR-071ML	3	9	0.10	0.90
C201, C202, C701	10n (0603)	Murata: GRM188R71H103KA01D	3	9	0.10	0.90
J201	TAMPER LOOP (XH-2)	JST: B2B-XH-A(LF)(SN)	1	4	0.20	0.80
J202	REMOTE HALL (XH-3)	JST: B3B-XH-A(LF)(SN)	1	4	0.24	0.96
J203	WAKE BUTTON (XH-2)	JST: B2B-XH-A(LF)(SN)	1	4	0.20	0.80
J204	STATUS LED (XH-2)	JST: B2B-XH-A(LF)(SN)	1	4	0.20	0.80
R204, R401, R403, R504-506, R703	100k (0603)	Yageo: RC0603FR-07100KL	7	21	0.10	2.10
R205, R402	1k (0603)	Yageo: RC0603FR-071KL	2	6	0.10	0.60
U301	LIS2DW12TR (LGA-12)	STMicro: LIS2DW12TR	1	3	2.60	7.80
U302	MB85RC256VPNF-G-AMERE2 (SOIC-8)	RAMXEED: MB85RC256VPNF-G-AMERE2	1	3	4.80	14.40
C302, C402	10u (0603)	Murata: GRM188R61A106KE69D	2	6	0.10	0.60
R301, R302	4.7k (0603)	Yageo: RC0603FR-074K7L	2	6	0.10	0.60
U401	TPS22917DBVR (SOT-23-6)	TI: TPS22917DBVR	1	4	0.62	2.48
U402	SN74AXC4T774PWR (TSSOP-16)	TI: SN74AXC4T774PWR	1	4	0.85	3.40
J401	PN532 3.3V SPI (XH-6)	JST: B6B-XH-A(LF)(SN)	1	4	0.38	1.52
R404-406	33 (0603)	Yageo: RC0603FR-0733RL	3	9	0.10	0.90
C403	2.2n (0603)	Murata: GRM188R71H222KA01D	1	4	0.10	0.40
R411	0 (0603)	Yageo: RC0603JR-070RL	1	4	0.10	0.40
J402	USB-C / USB2.0 sink (USB-C 16p)	Korean HRO: TYPE-C-31-M-12	1	4	0.55	2.20
U403	USBLC6-2SC6 (SOT-23-6)	STMicro: USBLC6-2SC6	1	4	0.55	2.20
R407, R408	22 (0603)	Yageo: RC0603FR-0722RL	2	6	0.10	0.60
R409, R410	5.1k (0603)	Yageo: RC0603FR-075K1L	2	6	0.10	0.60
U501	BQ24074RGTR (VQFN-16)	TI: BQ24074RGTR	1	3	1.85	5.55
U502	TPS63900DSKR (WSON-10)	TI: TPS63900DSKR	1	3	2.90	8.70

3.1 Main PCB, part 2, and remote Hall board

Table 13 / ref.	Description / package	Manufacturer; linked part number	Unit	Buy	USD ea.	USD total
J501	PROTECTED 1S PACK (VH-3)	JST: B3P-VH(LF)(SN)	1	4	0.45	1.80
L501	2.2uH 3.3A (2520)	Murata: DFE252012F-2R2M=P2	1	4	0.38	1.52
R501	1.78k (0603)	Yageo: RC0603FR-071K78L	1	4	0.10	0.40
R502	3.65k (0603)	Yageo: RC0603FR-073K65L	1	4	0.10	0.40
R503	68k (0603)	Yageo: RC0603FR-0768KL	1	4	0.10	0.40
R507	36.5k (0603)	Yageo: RC0603FR-0736K5L	1	4	0.10	0.40
R508	16.2k (0603)	Yageo: RC0603FR-0716K2L	1	4	0.10	0.40
R509	2.2k (0603)	Yageo: RC0603FR-072K2L	1	4	0.10	0.40
C503, C505, C506	22u (0805)	Murata: GRM21BR61C226ME44L	3	9	0.25	2.25
C504	10u (0805)	Murata: GRM21BR61C106KE15L	1	4	0.15	0.60
D501	CHARGE LED (0603)	Lite-On: LTST-C190KFKT	1	4	0.35	1.40
U601	TPS61088RHLR (VQFN-20)	TI: TPS61088RHLR	1	3	2.90	8.70
L601	1.2uH 12A (XAL6030)	Coilcraft: XAL6030-122MEC	1	3	1.95	5.85
Q601	IRLML6344TRPBF (SOT-23)	Infineon: IRLML6344TRPBF	1	4	0.45	1.80
D601	SS34 (SMC)	Vishay: SS34-E3/57T	1	4	0.45	1.80
J601	9-12V SOLENOID (VH-2)	JST: B2P-VH(LF)(SN)	1	4	0.38	1.52
R601	0 (2512)	Vishay: CRCW25120000Z0EG	1	4	0.55	2.20
R602, R609	100k (0603)	Yageo: RC0603FR-07100KL	2	6	0.10	0.60
R603	255k (0603)	Yageo: RC0603FR-07255KL	1	4	0.10	0.40
R604	475k (0603)	Yageo: RC0603FR-07475KL	1	4	0.10	0.40
R605	56k (0603)	Yageo: RC0603FR-0756KL	1	4	0.10	0.40
R606	169k (0603)	Yageo: RC0603FR-07169KL	1	4	0.10	0.40
R607	17.4k (0603)	Yageo: RC0603FR-0717K4L	1	4	0.10	0.40
R608	100 (0603)	Yageo: RC0603FR-07100RL	1	4	0.10	0.40
C601, C602	22u (1206)	Murata: GRM31CR61C226KE15L	2	6	0.35	2.10
C606	47n (0603)	Murata: GRM188R71H473KA61D	1	4	0.10	0.40
C607	4.7n (0603)	Murata: GRM188R71H472KA01D	1	4	0.10	0.40
C608-611	22u (1210)	Murata: GRM32ER71E226KE15L	4	12	0.55	6.60
C612	22u (1206)	Murata: GRM31CR61C226KE15L	1	4	0.35	1.40
Q701	AO3401A (SOT-23)	AOS: AO3401A	1	4	0.30	1.20
Q702	2N7002 (SOT-23)	Nexperia: 2N7002,215	1	4	0.20	0.80
R701	100k (0603)	Yageo: RC0603FR-07100KL	1	4	0.10	0.40
R702	100 (0603)	Yageo: RC0603FR-07100RL	1	4	0.10	0.40
R704	30k (0603)	Yageo: RC0603FR-0730KL	1	4	0.10	0.40
R705	68k (0603)	Yageo: RC0603FR-0768KL	1	4	0.10	0.40
HALL U1	DRV5032FBDBZR	TI: DRV5032FBDBZR	1	4	0.95	3.80
HALL C1	100n (0603)	Murata: GRM188R71C104KA01D	1	4	0.10	0.40
HALL J1	TO MAIN J202 (XH-3)	JST: B3B-XH-A(LF)(SN)	1	4	0.24	0.96

3.2 Off-board hardware and development equipment

Table 14 / ref.	Description / package	Manufacturer; linked part number	Unit	Buy	USD ea.	USD total
OB01	NFC reader breakout, SPI 3.3 V	Adafruit: 364 (PN532 v1.6)	;	1	39.95	39.95
OB02	MIFARE DESFire EV3 2K credentials	NXP / CardLogix: SKU 3900147	;	5	4.00	20.00
OB03	Lock-style solenoid latch 12 V	Adafruit: 1512	;	1	14.95	14.95
OB04	Protected 1S Li-Po, 3.7 V, 3000 mAh, 5 A	BatterySpace: CU-JAS427	;	1	39.68	39.68
OB05	NTC thermistor 10 kΩ, battery TS	Semitec: 103AT-2	;	2	2.50	5.00
OB06	CR2032 primary cell	Panasonic: CR2032	;	2	0.80	1.60
OB07	Momentary pushbutton, NO, panel mount	E-Switch (typ.): RP3502ABLK	;	2	1.50	3.00
OB08	Status LED, 3 mm low-current	Lite-On (typ.): LTL-4224 (typ.)	;	2	0.40	0.80
OB09	Selected lid magnet; one fitted plus two spares	K&J Magnetics: D22	;	3	0.50	1.50
OB10	Tamper-loop wire, 30 AWG wire-wrap spool	Adafruit: 1446	;	1	4.95	4.95
OB11	JST XH housings XHP-2/-3/-6 plus SXH contacts	JST: XHP-2/3/6, SXH-001T-P0.6	;	1	8.00	8.00
OB12	JST VH housings VHR-2N/-3N plus SVH contacts	JST: VHR-2N/3N, SVH-21T-P1.1	;	1	4.00	4.00
OB13	Insulated M3 standoffs 30 mm plus M2 hardware	Keystone/HH (typ.): assorted	;	1	8.00	8.00
OB14	USB-C data/charge cable	Anker (typ.): A8465 (typ.)	;	1	9.00	9.00
OB15	SWD programmer, 1.27 mm 10-pin, ST-LINK compatible	STMicro: STLINK-V3MINIE	;	1	12.00	12.00
DEV01	Firmware development board	STMicroelectronics: NUCLEO-L433RC-P	;	1	16.00	16.00
DEV02	USB Micro-B data cable	Adafruit: 592	;	1	3.00	3.00
DEV03	40-position 2.54 mm male header strip	Sullins: PRPC040SAAN-RC	;	2	0.70	1.40
DEV04	Dedicated firmware NFC module	Adafruit: 364, PN532 breakout	;	1	39.95	39.95
DEV05	I ² C FRAM development module	Adafruit: 1895	;	1	10.00	10.00
DEV06	0.1 Ω, 1%, 1 W current shunt	Vishay: WSL2512R1000FEA	;	5	0.60	3.00
DEV07	Two-position test terminal	On Shore Technology: OSTVN02A150	;	6	0.60	3.60
DEV08	10 kΩ, 1%, ¼ W test resistor	Yageo: MFR-25FBF52-10K	;	5	0.10	0.50
DEV09	1.62 kΩ, 1%, 0603 fixture resistor	Yageo: RC0603FR-071K62L	;	2	0.10	0.20
DEV10	Male-to-male jumper set	Adafruit: 1956	;	1	2.00	2.00
DEV11	Female-to-male jumper set	Adafruit: 1954	;	1	2.00	2.00
DEV12	Mini-grabber lead set	Pomona: 5250	;	1	8.00	8.00
DEV13	BNC-to-mini-grabber lead	Pomona: 6244	;	2	15.00	30.00

OB subtotal \$172.43; DEV subtotal \$119.65. DEV04 is an additional NFC reader for parallel firmware work. Assortment hardware/cable links may be generic searches; final counts follow released drawings/harnesses. Unused historical purchasing candidates are excluded.

3.3 Fabrication, labor and total

Fabrication service (Table 15)	USD
Main PCB, 100×80mm, 4-layer JLC04161H-7628, ENIG, 5pcs	55.00
Main-board via-in-pad process, epoxy-filled and copper-capped	80.00
Main-board stainless top stencil, 0.10mm	12.00
Hall PCB, 18×24mm, 2-layer, ENIG, 5pcs, panelized	6.00
DHL shipping, one consolidated PCB order	27.00

CU-JAS427 is \$39.68 plus an unquoted hazardous-materials fee; latch stock and pack lead time require confirmation. BOM Unit/Buy columns give fitted/purchased quantities for two assembled board sets plus spares; HALL references belong to the remote board. Linked MPNs are vendor pages/searches, not confirmed stock or quotes. The JLCPCB fabrication subtotal \$180.00 covers two board designs in one consolidated order, with a five-board lot of each. Main board: 4-layer JLC04161H-7628 baseline, ENIG, filled/capped via-in-pad and 0.10 mm top stencil. Confirm the actual stackup, controlled impedance, via treatment, assembly process and quote with the selected course-round or direct fabricator. A later respin is not included.

Labor and machine shop

Machine shop labor: The ECE 445 machine shop provides fabrication labor for course projects at no direct charge. Approximately 10 labor hours are estimated for enclosure fabrication, mounting features, and integration. Enclosure materials are budgeted separately at approximately \$75.

The published UIUC electrical-engineering starting salary of \$87,429 [28] corresponds to about \$42.03/h at 2080 h/year. The model uses a rounded planning rate of \$45/h and a 2.5 overhead multiplier. Each member contributes 10 h/week for 14 weeks, including the two early proposal/architecture weeks: $45 \times 2.5 \times 140 = \$15,750$ per member. These are estimated economic labor costs, not wages being paid.

Cost item (Table 16)	Basis	USD
Sena Tiryaki	140 h × \$45/h × 2.5	15,750.00
Serdar Alp Oguz	140 h × \$45/h × 2.5	15,750.00
Selim Mamak	140 h × \$45/h × 2.5	15,750.00
Machine-shop labor	ECE 445 machine shop; ~10 h estimated	0.00
Enclosure materials	Polycarbonate, aluminum, hinge, fasteners	75.00

Budget summary

Category (Table 17)	USD
Main PCB components / Hall components	160.99 / 5.16
Off-board hardware / development equipment	172.43 / 119.65
Fabrication / machine shop	180.00 / 75.00
Nonlabor subtotal	713.23
Engineering labor	47,250.00
Total project estimate	47,963.23

Excluded pending quotes: battery hazardous-materials fee, non-PCB shipping, incremental fabrication charges and any later PCB respin. Enclosure materials remain a \$75 allowance; shop labor has no direct charge. Lab supply, scope, DMM, electronic load, low-current meter, force gauge/dial indicator, temperature tools and drop/contact fixtures are assumed available. Confirm differential or clamp-probe access for LA-3; a suitable differential shunt fixture may substitute while preserving the measured current and voltage criteria. If equipment must be purchased, update this budget.

3.4 Weekly schedule and responsibilities

Each member owns one work package per week. Sena also prepares Tuesday meeting agendas and notes. Firmware development and simulation proceed in parallel with PCB procurement; physical acceptance starts on assembled PCBs.

Week of (Table 18)	Sena Tiryaki	Serdar Alp Oguz	Selim Mamak
Sep 22	Consolidate R&V and magnet analysis.	Finalize CAD, ERC/DRC, parity and fabrication package.	Rubric review and machine-shop package.
Sep 29	Assemble design report and figures.	Cost and tolerance analysis with simulation evidence.	Ethics, safety, references and project-page preparation.
Oct 6	Nucleo safe-init, Stop 2 and EXTI; design review.	PCB quotes, impedance/via process and assembly route.	Shop scope/drawing review, clearances and material pricing.
Oct 13	Demonstration evidence for the approved simulation-to-PCB workflow.	Oct 15 PCB order; parts, latch stock and pack lead-time checks.	Oct 16 drawing freeze: carrier, strike, plate, magnet holder and openings.
Oct 20	DESFire AES vectors and reference transcript.	FRAM/dual-header log and desktop verifier.	Harness crimp/continuity and fabrication liaison.
Oct 27	Flash bring-up; CM-1...4 and persistent lockout tests.	Assemble, current-limited rails with R601/R411 removed; safe states/I ² C/FRAM before Oct 29 revision decision.	Hall/loop qualification and noise/current fixtures.
Nov 3	NFC startup, timing and switched-power tests; progress demonstration.	TA/power-TA charger review and battery-free demo, then TA-present first pack connection and power tests.	Bench-supply latch characterization and thermal/flyback checks.
Nov 10	Logging timing, cuts, corruption and I ² C qualification.	Charging, USB and RTC acceptance.	Enclosure integration, Hall geometry, loop map and battery tray.
Nov 17	Mock demonstration; key/service authorization tests.	Defect triage, reviewed rework and affected retests.	Impact tuning/acceptance and sensor event logging.
Nov 24	Integrated 5-run script and evidence assembly.	Formal HLR acceptance with instruments.	Final alignment and 20-cycle mechanical run.
Dec 1	Final demonstration and presentation.	Measured-results tables.	Mechanical/safety results and notebook reconciliation.
Dec 8	Final report assembly.	Verification appendices.	Checkout, equipment return and project-page updates.

Record actual initial shop contact against the course September 21 milestone; a prepared package does not prove a meeting. November 23-27 Fall Break work depends on recorded lab access, so start essential acceptance beforehand. October 29 can address only faults already discovered. Later failures require reviewed rework/substitution and repeat tests; a new PCB needs a confirmed price/delivery plan and budget update. Do not assume another funded fabrication round.

4. Impact, ethics and engineering standards

The intended users are laboratories and other small organizations needing credential-controlled access and a reviewable history. False accusations and missed tamper detections are both failures: TL-2 and AT-5 therefore require no events during defined normal handling. The record identifies credentials and sensor observations, not people or intent. Organizations should disclose logging, limit export access and set retention/clear policies. [1], [13]

Social and cultural expectations about workplace monitoring differ. Users need clear notice, authorized export access and retention policies appropriate to their organization; sensor events must not be treated as proof of misconduct. Global deployment also needs review of local privacy, radio, battery-transport and waste rules, as well as component availability.

IEEE and ACM ethics guide safety, honest claims, privacy and attribution. The container is tamper-evident within its routed sensors and qualified conditions; it does not detect every penetration or bypass. Cryptographic card authentication is required, but the unkeyed history does not protect against malicious recomputation, whole-memory replacement, rollback or truncation. CRC/hash checks detect corruption and inconsistent edits. Loss of power does not close an open lid. Report these limits and incomplete tests transparently. Credit datasheets, the TI compensation starting values and archived simulation sources. [1], [13], [42]

Low standby demand, rechargeable main power and high-endurance FRAM reduce service and replacement waste. Actual runtime depends on NFC/latch/USB duty, leakage and self-discharge. Separate the rechargeable pack and CR2032 for approved recycling; enclosure materials and PCB use their appropriate waste streams. The \$713.23 hardware/service estimate includes development equipment and spares, not a production-unit quote. Availability and substitutes affect global sourcing. As with any lockbox, harmful contents remain a possible misuse; the design's intended contribution is accountable handling.

Standard / reference (Table 19)	Application and evidence boundary
ISO/IEC 14443-1...4; 7816-4 [2], [3], [37], [38]	13.56 MHz Type A proximity interface, ISO-DEP and APDU structure. Confirm antenna placement and actual credential exchange.
FIPS 197; FIPS 180-4 [4], [5]	AES-128 authentication and SHA-256 history/verifier; validate known-answer vectors.
USB 2.0, CDC-ACM, Type-C [6], [7], [33]	Full-Speed service, source-current permissions and CC attachment. No USB PD or BC1.2 detection is implemented.
NXP UM10204 [8]	I ² C 100 kHz, 4.7 kΩ pull-ups and measured rise-time acceptance.
IPC-2221B / IPC-2152 [9], [39]	Board spacing, conductor current and stackup. Original A0 baseline: 0.15 mm clearance, 0.20 mm tracks and 0.8-1.8 mm doubled latch spine; changed layouts require renewed checks.
IPC-A-610J / J-STD-001J; J-STD-020F [10], [34], [40]	Assembly acceptance and moisture/reflow handling. Follow each supplier's limits; a classification profile alone does not qualify assembly.
FCC 47 CFR Part 15 [11]	13.56 MHz radio and digital emissions. Using a commercial module does not certify the complete container.
UL 2054 / IEC 62133-2 [12], [41]	Battery safety design references; protection circuitry is not evidence of certification.
UN Manual §38.3 [35]	CU-JAS427 vendor states it is not tested. Supplier shipping process only; no team reshipment. Substitute a documented pack if transport or course requirements demand it.
RoHS 2011/65/EU, amended [36]	Component selection target; confirm declarations/exemptions per purchased MPN. Lead-free assembly is planned.

4.1 Safety procedures and remaining gates

The highest-consequence hazard is Li-Po thermal runaway caused by shorting, damage, excessive discharge or incompatible charging. Coil heat, stored boost energy, pinch points, loose magnets and test-instrument shorts also require controlled procedures. Follow course safety and battery rules. [14], [15]

Activity (Table 20)	Required procedure
Battery approval and charging	All members complete lithium-safety training. TA and power TA review charger/protection design before charge tests. Demonstrate charger function without a pack on the assembled PCB; first pack connection occurs with the TA present. Use a LiPo-safe bag during charge and discharge testing, supervise charging and monitor temperature. Confirm pack charge-temperature limits, protection limits and selected NTC response.
Pack installation and storage	Use only the approved protected pack at J501. Fit one verified, insulated 103AT-2 in thermal contact; insulate any unused pack sensor. Smooth insulated tray, strap retention, no fastener tips under the pouch, and separation from hot parts. Store at appropriate storage charge in a safe bag with insulated terminals. Swollen, punctured or hard-dropped packs are retired to department recycling. At low-battery lockout, end the session and promptly recharge or disconnect; residual drain continues.
PCB commissioning	R601 and R411 start removed. Use a current-limited supply, verify rails, flash safe-init and pass CM-3 before installing relevant links. Repeat checks for power-up, held reset, IWDG and ROM recovery. Disable/isolate unsafe recovery paths. Battery and USB logic may remain live despite removed load links.
Latch and stored energy	Use bench supply before approved pack testing. Fit the flyback diode for every switching event. Disabled boost has no output disconnect: measure TP7 before handling and treat it as live whenever powered. Start with an electronic load, single pulses ≥ 20 s apart, then staged coil trials. Normal pulse ≤ 1 s and period = $\max(5 \text{ s}, 20T)$; supervised abuse alone uses $\max(1 \text{ s}, 4T)$. Stop at 60°C or coil rise $> 20^\circ\text{C}$.
Measurements and mechanical work	Scope ground clips go only to circuit ground. Probe drain tip-to-ground; use a clamp or differential shunt within the coil recirculation path for LA-3. Never ground a floating/high-side node. Guard spring bolt/lid pinch points; retain magnets and keep loose magnets away from implanted devices. Use guided drop fixture, eye protection and an exclusion area.
Lab and stop conditions	Two-person work, especially first power-up and battery steps. Use ESD mat/straps, fume extraction and eye protection. Shop work follows staff training/access rules. Stop for swelling, abnormal heat/odor/noise, repeated current limiting or incorrect rails; disconnect when safe, quarantine the pack and contact staff before retry.

Changes since the proposal

Detailed design refined the existing risks by identifying stored boost-output energy and the lack of output disconnect, defining safe scope-ground connections, and requiring secure magnet retention. Latch loading and USB/charging limits were already recognized; their quantified limits and tests are now specified. These refinements add controls without claiming a newly introduced hazard class.

Release gates

Obtain staff decisions on the battery/protection policy and whether a Safety Manual is required. Confirm shop drawings/scope, enclosure material pricing, fabrication route/quote and required test equipment. Native CAD reconciliation remains unverified: apply $R502=3.65 \text{ k}\Omega$, $R503=68 \text{ k}\Omega$ and $R509 \text{ supply}=V_{SYS}$, check footprint/pin/netlist consistency, rerun ERC/DRC and regenerate the schematics before order release. Section 2.10 also requires a documented standby-budget decision. Complete firmware, confirm current/thermal/source limits, and record all physical acceptance results. Pending approval or measurement is a gate, not a completed result.

5. References

- [1] IEEE, "IEEE Code of Ethics," IEEE Policies, §7.8.
- [2] ISO/IEC, 14443, Cards and Security Devices for Personal Identification; Contactless Proximity Objects: Parts 1, 3 and 4, 2018; Part 2, 2020, with Cor. 1, 2021.
- [3] ISO/IEC, Identification Cards; Integrated Circuit Cards; Part 4: Organization, Security and Commands for Interchange, ISO/IEC 7816-4:2020.
- [4] NIST, Advanced Encryption Standard (AES), FIPS PUB 197, 2001.
- [5] NIST, Secure Hash Standard (SHS), FIPS PUB 180-4, 2015.
- [6] USB Implementers Forum, Universal Serial Bus Specification, rev. 2.0, 2000.
- [7] USB Implementers Forum, USB Type-C Cable and Connector Specification, release 2.2.
- [8] NXP Semiconductors, I²C-bus Specification and User Manual, UM10204, rev. 7.0, 2021.
- [9] IPC, Generic Standard on Printed Board Design, IPC-2221B, Nov. 2012; and Standard for Determining Current Carrying Capacity in Printed Board Design, IPC-2152, Aug. 2009. Selected design-reference editions.
- [10] IPC, Acceptability of Electronic Assemblies, IPC-A-610J, Mar. 2024; and Requirements for Soldered Electrical and Electronic Assemblies, IPC J-STD-001J, Apr. 2024.
- [11] U.S. Federal Communications Commission, Radio Frequency Devices, 47 CFR Part 15.
- [12] UL Standards & Engagement, Household and Commercial Batteries, UL 2054, 3rd ed., Nov. 17, 2021, rev. Mar. 10, 2022; IEC 62133-2:2017+AMD1:2021 CSV, ed. 1.1, Jul. 15, 2021. Citations do not establish selected-pack certification.
- [13] ACM, "ACM Code of Ethics and Professional Conduct," 2018.
- [14] ECE 445 Course Staff, University of Illinois Urbana-Champaign, "Safety."
- [15] ECE 445 Course Staff, University of Illinois Urbana-Champaign, "General Battery Safety."
- [16] Team 4, Project Proposal: Secure Chain-of-Custody Container, ECE 445, Sep. 17, 2026.
- [17] STMicroelectronics, STM32L433xx Datasheet, DS11449, rev. 8; and STM32L4 Advanced Arm-Based 32-Bit MCUs Reference Manual, RM0394, rev. 5.
- [18] STMicroelectronics, STM32 Microcontroller System Memory Boot Mode, AN2606, rev. 70.
- [19] STMicroelectronics, STM32L43xxx/44xxx Device Errata, ES0318, rev. 11.
- [20] NXP Semiconductors, PN532/C1 Near Field Communication Controller Datasheet; and PN532 User Manual, UM0701.
- [21] STMicroelectronics, Oscillator Design Guide for STM8/STM32, AN2867.
- [22] NXP Semiconductors, MF3DHx3 MIFARE DESFire EV3 Contactless IC Datasheet.

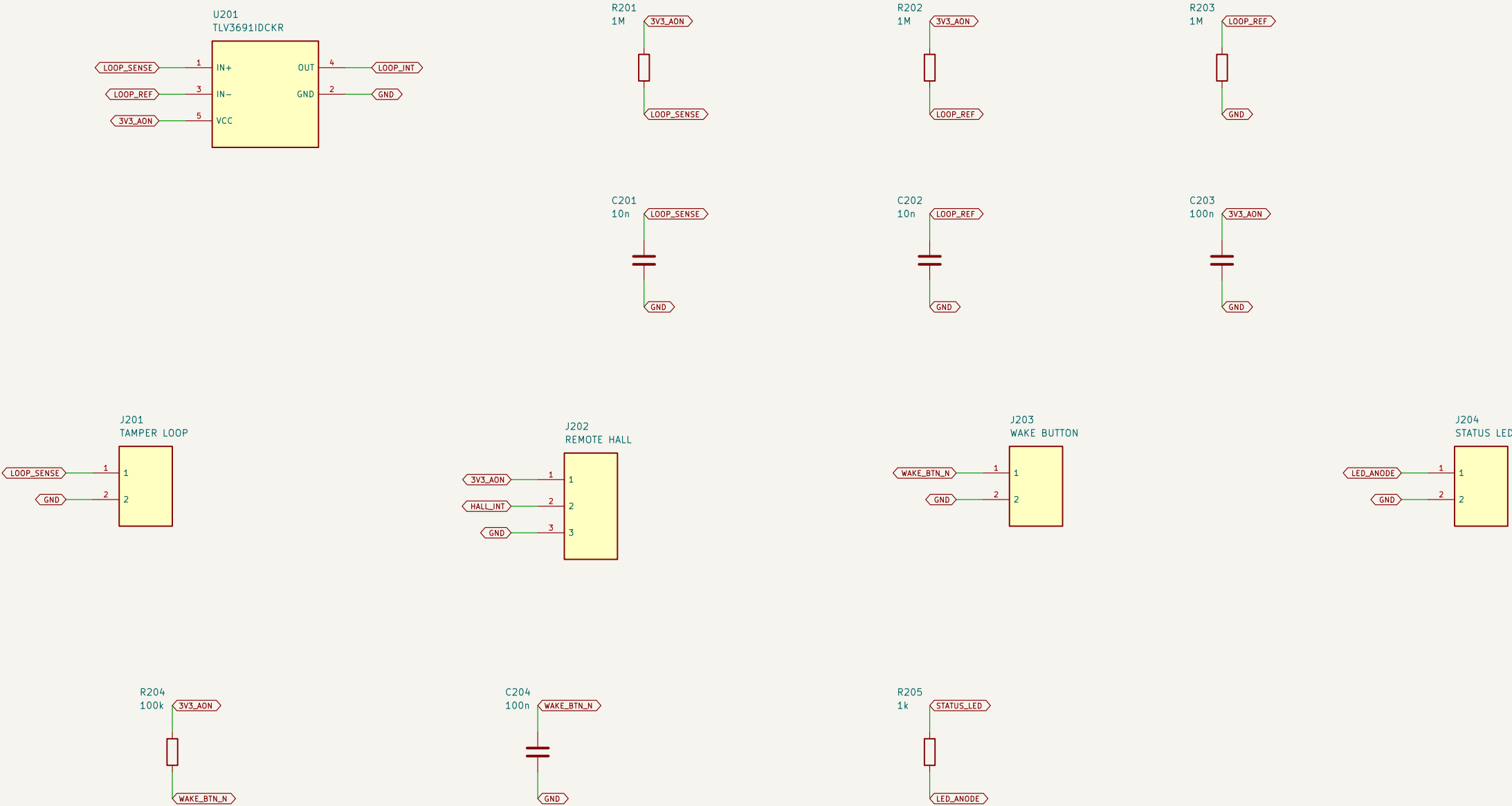
5. References (continued)

- [23] Texas Instruments, TLV3691 Datasheet, SBOS694A.
- [24] Texas Instruments, DRV5032 Datasheet, rev. H.
- [25] STMicroelectronics, LIS2DW12 Datasheet.
- [26] RAMXEED (Fujitsu), MB85RC256V FRAM Datasheet, DS501-00017-11v2-E.
- [27] Texas Instruments, TPS22917 (SLVSDW8B), TPS61088, TPS63900 (SLVSET3D), BQ24074 (SLUS810N), and SN74AXC4T774 (SCES898C) Datasheets.
- [28] Grainger College of Engineering, University of Illinois Urbana-Champaign, “Electrical Engineering; Outcomes,” 2024-25 cohort; reported average starting salary \$87,429.
- [29] K&J Magnetics, “D22 Neodymium Cylinder Magnet,” N42 product specification.
- [30] BatterySpace, “Polymer Li-Ion Battery Pack 3.7 V 3000 mAh (5 A Rate),” CU-JAS427; and linked 3.7 V/5 A protection-board specification. Confirm the installed board; the pack listing states it is not UN 38.3 tested.
- [31] Adafruit, “Lock-Style Solenoid; 12VDC,” product 1512.
- [32] Adafruit, “PN532 NFC/RFID Controller Breakout Board,” product 364.
- [33] USB Implementers Forum, Universal Serial Bus Class Definitions for Communications Devices, rev. 1.2, with errata/ECN through Apr. 3, 2025; and Communications Class Subclass Specification for PSTN Devices, rev. 1.2, Feb. 9, 2007, §§3.2.2-3.2.2.1. Bundle published May 28, 2025.
- [34] IPC/JEDEC, Moisture/Reflow Sensitivity Classification for Non-hermetic Surface Mount Devices (SMDs), J-STD-020F, Nov. 2022.
- [35] United Nations, Manual of Tests and Criteria, 8th rev. ed., ST/SG/AC.10/11/Rev.8, 2023, Part III, §38.3, with Amendment 1, 2025. §38.3.5 specifies test-summary information.
- [36] European Parliament and Council, Directive 2011/65/EU (RoHS), Jun. 8, 2011, OJ L 174, Jul. 1, 2011, pp. 88-110, as amended; including Commission Delegated Directive (EU) 2015/863, Mar. 31, 2015.
- [37] ISO/IEC 14443 series: Part 1, Physical Characteristics, 2018; Part 2, Radio Frequency Power and Signal Interface, 2020, Cor. 1:2021; Part 3, Initialization and Anticollision, 2018; Part 4, Transmission Protocol, 2018.
- [38] ISO/IEC, Identification Cards; Integrated Circuit Cards; Part 4: Organization, Security and Commands for Interchange, ISO/IEC 7816-4:2020.
- [39] IPC, IPC-2221B, Generic Standard on Printed Board Design, Nov. 2012; IPC-2152, Standard for Determining Current Carrying Capacity in Printed Board Design, Aug. 2009.
- [40] IPC, IPC-A-610J, Acceptability of Electronic Assemblies, Mar. 2024; IPC J-STD-001J, Requirements for Soldered Electrical and Electronic Assemblies, Apr. 2024.
- [41] UL Standards & Engagement, UL 2054, Household and Commercial Batteries, 3rd ed., Nov. 17, 2021, rev. Mar. 10, 2022; IEC, IEC 62133-2:2017+AMD1:2021 CSV, ed. 1.1, Jul. 15, 2021.
- [42] Texas Instruments, TPS61088EVM-677 Evaluation Module, User’s Guide SLVUAF2, Jun. 2015, Fig. 7 and Table 3, pp. 7-8. Compensation starting-value attribution; not project stability verification.
- [43] B. Guttman, D. R. White, and T. Walraven, Digital Evidence Preservation: Considerations for Evidence Handlers, NIST IR 8387, Sep. 2022, doi: 10.6028/NIST.IR.8387.
- [44] Infineon (Cypress), CY15B256J: 256-Kbit (32K × 8) Automotive Serial I²C F-RAM, datasheet 001-90843, rev. *I, Feb. 28, 2018, pp. 3, 10, 12, 15-17. Candidate contingency only.

	1	2	3	4	5	6	7	8
A	ECE 445 / TEAM 04 SECURE CHAIN-OF-CUSTODY CONTAINER							
	100 x 80 mm, 4-layer main PCB + remote Hall sensor board. Engineering prototype: read RELEASE_STATUS.md before fabrication or assembly.							
B	MCU / RTC / DEBUG MCU / RTC / DEBUG				TAMPER LOOP / DOOR INTERFACE TAMPER LOOP / DOOR INTERFACE			
C	ACCELEROMETER / FRAM ACCELEROMETER / FRAM				SWITCHED NFC / USB-C SERVICE SWITCHED NFC / USB-C SERVICE			
D	USB CHARGER / 3.3V BUCK-BOOST USB CHARGER / 3.3V BUCK-BOOST				11.5V LATCH DRIVER / BATTERY SENSE 11.5V LATCH DRIVER / BATTERY SENSE			
E					BATTERY ADC / TEST			
F	Interfaces: remote PN532 reader; door Hall board; normally closed tamper conductor; wake button; status LED; 9-12V cabinet latch; protected 1S battery with 10k NTC. No firmware or mechanical-security qualification is implied by the CAD checks.						ENGINEERING PROTOTYPE – SEE RELEASE STATUS ECE 445 – Team 04 Sheet: / File: ECE445_Team04.kicad_sch Title: Secure Chain-of-Custody Container Rev A0 Size: A3Date: 2026-09-24Rev: A0 KiCad E.D.A. 10.0.6Id: 1/8	
	1	2	3	4	5	6	7	8

Id: 2/8

TAMPER LOOP / DOOR INTERFACE



J201: continuous insulated conductor through one enclosure body, hinged lid, divider perimeter and cable passage. Intact R <=10k.
J202: separate Hall board at door magnet; pin 1 = 3.3V, 2 = output, 3 = GND.
J203: normally-open momentary wake switch. J204: external LED anode on pin 1.
Keep LOOP_SENSE / LOOP_REF clean and away from switching nodes; do not add leaky TVS parts.

ENGINEERING PROTOTYPE – SEE RELEASE STATUS

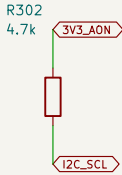
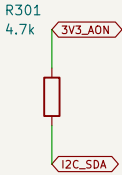
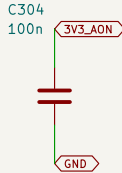
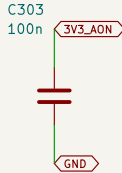
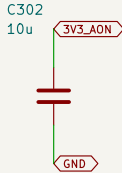
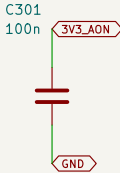
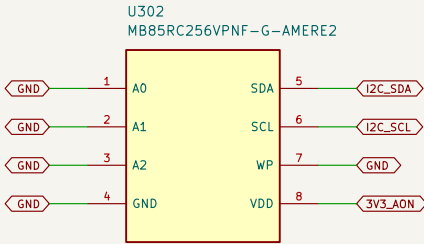
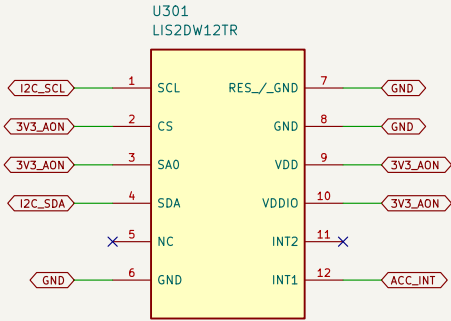
ECE 445 – Team 04

Sheet: /TAMPER LOOP / DOOR INTERFACE/
File: 02_Tamper.kicad_sch

Title: TAMPER LOOP / DOOR INTERFACE

Size: A3	Date: 2026-09-24	Rev: A0
KiCad E.D.A. 10.0.6		Id: 3/8

ACCELEROMETER / FRAM



I2C initial bus speed: 100kHz. LIS2DW12 SA0 high -> 7-bit address 0x19.
FRAM A2:A0 = 000 -> 0x50; WP tied low. Both devices remain on the always-on rail.
INT1 is the selected accelerometer interrupt. INT2 is intentionally unconnected.

ENGINEERING PROTOTYPE – SEE RELEASE STATUS

ECE 445 – Team 04

Sheet: /ACCELEROMETER / FRAM/
File: 03_Sensors_Storage.kicad_sch

Title: ACCELEROMETER / FRAM

Size: A3 Date: 2026-09-24
KiCad E.D.A. 10.0.6

Rev: A0
Id: 4/8

Id: 5/8

USB CHARGER / 3.3V BUCK-BOOST

A

B

C

D

E

F

A

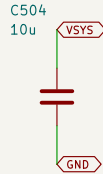
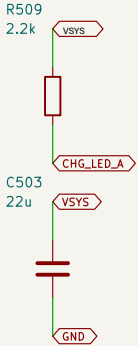
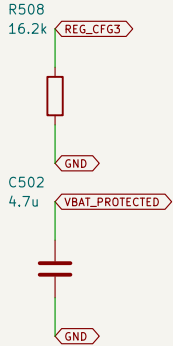
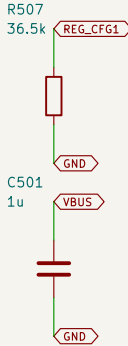
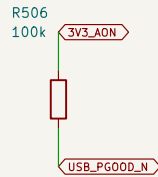
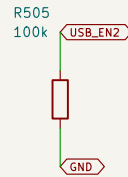
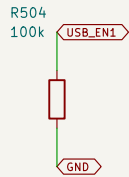
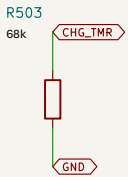
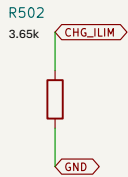
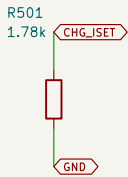
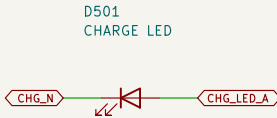
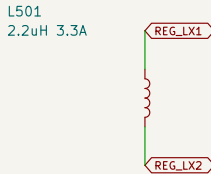
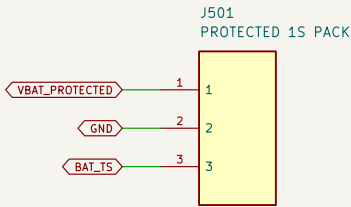
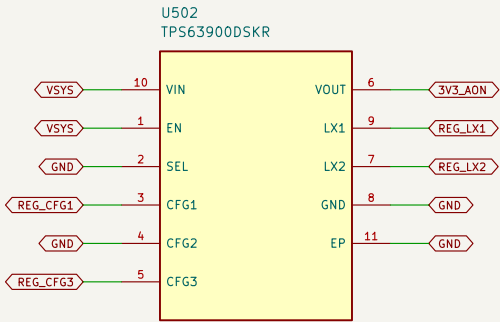
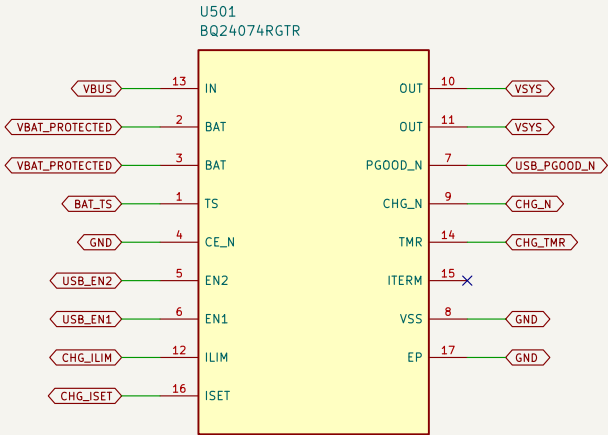
B

C

D

E

F



Corrected report circuit: R502=3.65k, R503=68k; R509 supply changed to VSYS. Apply these edits to native CAD and rerun release checks before fabrication. Use protected CU-JAS427 1S/3000mAh/5A pack and exactly one verified, insulated 103AT-2 thermistor; confirm the applicable pack limits. ISET is nominal 500mA. EN2/EN1=00 before configuration; 10 after >=500mA permission; 11 suspend. CE_N is grounded. TMR 68k: nominal 9.07h; initial bounds 6.73-11.45h.

ENGINEERING PROTOTYPE – SEE RELEASE STATUS

ECE 445 – Team 04

Sheet: /USB CHARGER / 3.3V BUCK-BOOST/
File: 05_Power.kicad_sch

Title: USB CHARGER / 3.3V BUCK-BOOST

Size: A3

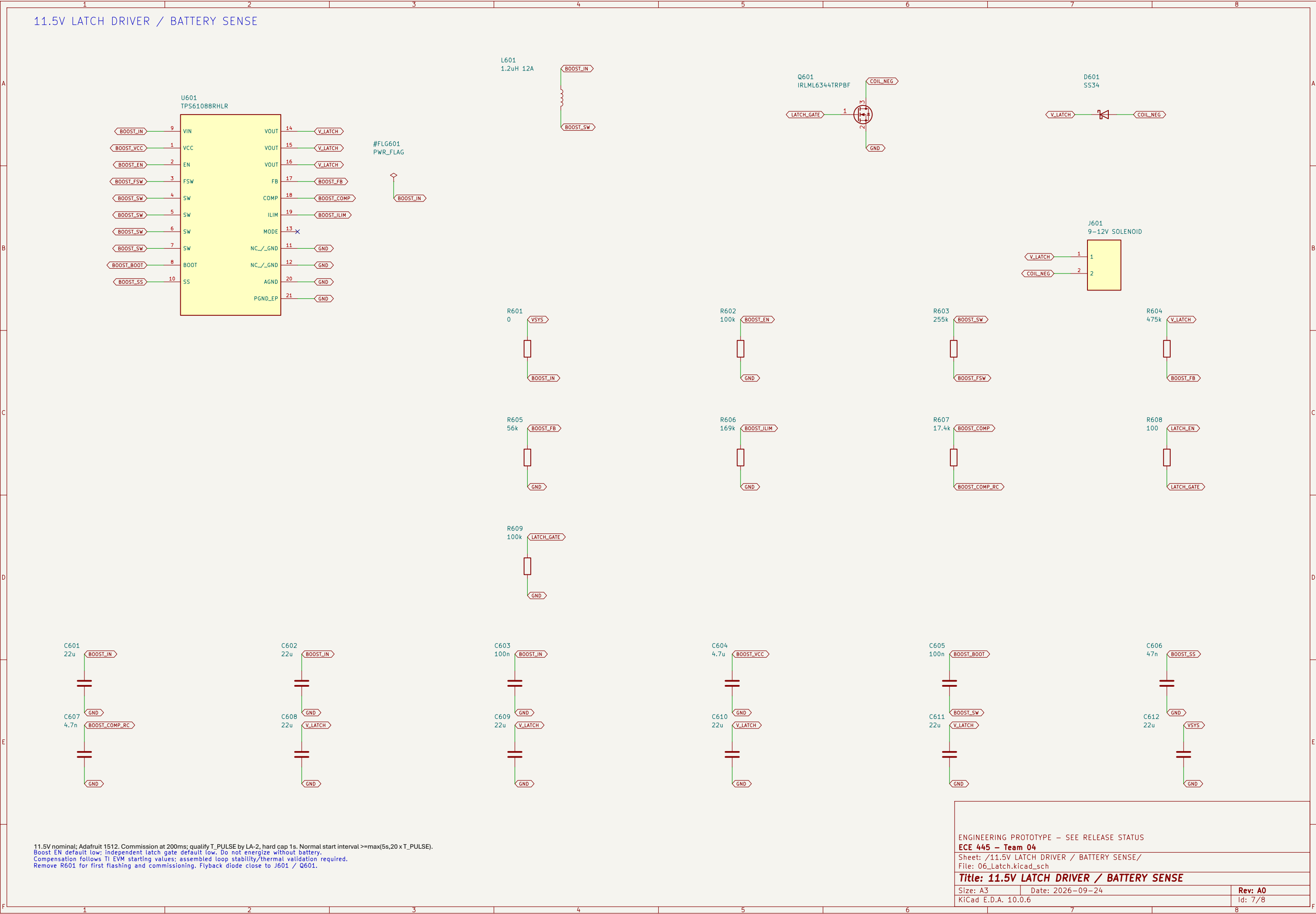
Date: 2026-09-24

Rev: A0

KiCad E.D.A. 10.0.6

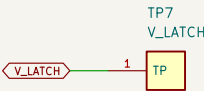
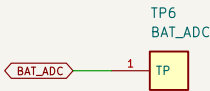
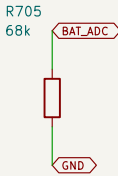
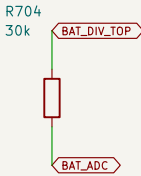
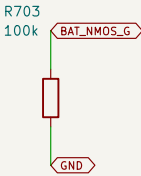
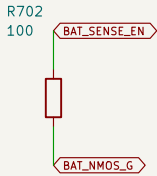
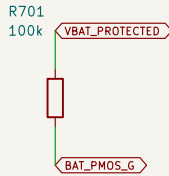
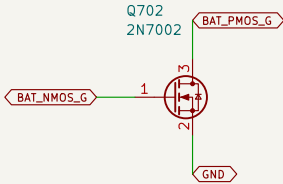
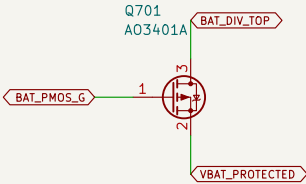
Id: 6/8

11.5V LATCH DRIVER / BATTERY SENSE



SWITCHED BATTERY ADC / TEST POINTS

PMOS source faces battery, body diode blocks battery-to-divider when disabled.
Enable BAT_SENSE_EN, wait >=2ms, discard first ADC sample. Divide by 68/(30+68).
A 4.2V battery gives nominal 2.914V at ADC. Firmware must deny latch below 3.6V resting
battery until source impedance and brownout behavior are physically characterized.



ENGINEERING PROTOTYPE – SEE RELEASE STATUS

ECE 445 – Team 04

Sheet: /BATTERY ADC / TEST/
File: 07_Battery_ADC.kicad_sch

Title: SWITCHED BATTERY ADC / TEST POINTS

Size: A3

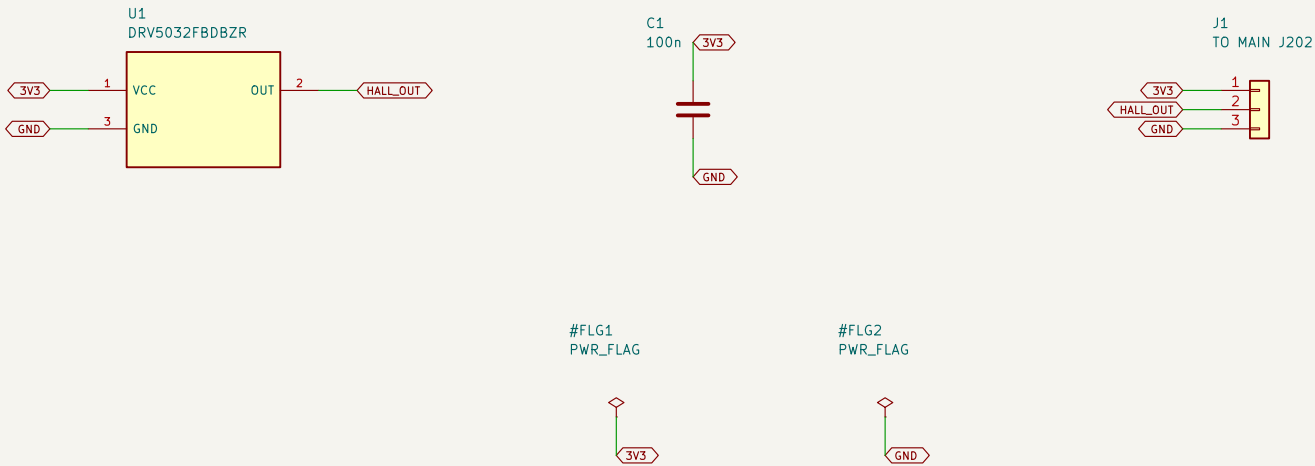
Date: 2026-09-24

Rev: A0

KiCad E.D.A. 10.0.6

Id: 8/8

REMOTE DOOR SENSOR



Mount near the door magnet, with the sensor at the board edge.
J1: 1 = 3.3V, 2 = push-pull OUT, 3 = GND. Wire to main-board J202 pin-for-pin.
DRV5032FB: 5Hz sampling, active-low detection, omnipolar. Do not add an output pull-up.
Mechanical dimensions: 18 x 24 mm. Two 2.2mm holes at (3,21.5) and (15,21.5).
Confirm magnet polarity/field, closed-door detection and released-door distance on the assembled box.