

Firmware 00-05-00 Cumulative Change Log

Baseline: v00.04.11

Target: v00.05.00

Updated: 2026-09-08

Status: implemented in the current version-5 production source

This document records the net implemented firmware and supporting-engineering changes between v00.04.11 and v00.05.00. It describes behavior present in the final version-5 source. Abandoned campaigns, deferred proposals, failed experiments, intermediate implementations that were later removed, and qualification-only behavior are not presented as released features.

Internal SD storage and logging

- Replaced production FAT32 logging on the internal SD card with dedicated HPT media format 2.0.
- Added three independently committed circular record lanes, A/B/C. Two matching valid copies are healthy, one valid copy provides explicit degraded operation, and loss of all valid copies is reported.
- Added 2,048-sector circular segments, bounded reclaim, whole-segment retirement, and redundant CRC-protected retirement metadata that survives reset.
- Added capacity validation for at least 90 days of minute records plus a 10% per-lane margin. Additional card capacity supplies rotation and retirement margin rather than extending the customer retention promise.
- Changed production log submission to bounded, non-blocking 64-byte record snapshots. Queue-full and unavailable-media losses are counted without blocking temperature control.
- Added bounded retries and failure handling so missing, unreadable, invalid, or failed SD media cannot prevent control, monitoring, alarms, the HMI, USB, or communications from operating.
- Added protocol-level card classification using CID, representative-sector reads, and HPT media validation. A readable card with the wrong format is reported as requiring initialization rather than as absent.
- Added explicit, guarded whole-card HPT initialization with repeated CID and sector-read validation immediately before the first destructive write. Firmware never formats or migrates an SD card automatically.
- Added read-only full-address scrub, lane-health, retirement, mismatch, record-loss, and replace-media diagnostics.
- Added startup and interruption recovery for committed history, including bounded recovery at qualified record, commit, reclaim, segment, and retirement-metadata boundaries.
- Retained FileX for removable USB media while removing it from the version-5 production internal-SD logging path.

History graph

- Changed the graph to use real persisted-record bounds instead of displaying a fabricated two-hour future extent.
- Added a stable sequence-published RAM snapshot so the HMI does not read a chart buffer while the SD owner is updating it.
- Added a bounded newest-history cache and a validated fast reconstruction path that falls back to full three-lane quorum resolution when a preferred-lane window cannot be trusted.
- Added live graph refresh as new records are persisted. An attached viewport follows the newest record at every zoom level; Pan Left holds historical position and Pan Right reattaches to the newest record.
- Preserved missing-data gaps and explicit power-off intervals instead of synthesizing continuous history.
- Added array-bound validation and invalidation of stale chart bounds after an SD media-generation change or destructive initialization.

Data-log export

- Reworked customer log export to read immutable HPT snapshots rather than the retired internal-SD FAT32 file layout.
- Added bounded timestamp-range lookup using durable per-segment timestamp envelopes and a bounded directory over the customer-visible retained suffix.
- Clamped an entered start date to the newest applicable boundary: the entered date, the oldest retained record, or the rolling 90-day export limit. The HMI explains an adjustment before continuing to the normal end-date entry.
- Enforced start-before-end, future-end, and exact five-minute minimum-range validation against the effective start.
- Added fail-closed export handling for snapshot reclamation, sequence gaps, malformed records, ambiguous copies, storage errors, and incomplete traversal. A staged prefix is never published as a successful complete export.
- Added actual/requested time and sequence ranges, gap and copy-health counts, record counts, byte counts, and phase timing to export status and CSV metadata.
- Changed publication to an atomic temporary-file workflow: write HPTE.TMP, verify counts, add the completion trailer, close and flush, rename to the selected CSV name, and perform a final media flush.
- Added a bounded SDRAM staging buffer and bulk HPT iterator while retaining a qualified 32 KiB maximum FileX write size for broad USB-drive compatibility.

USB mass-storage behavior

- Restored the broadly compatible v00.04.11 USB command and lifecycle baseline while retaining version-5 HPT export, firmware update, backup, WAV, and PID publication features.
- Increased the HPT publication write cap from the former 1 KiB behavior to the qualified 32 KiB limit.
- Corrected application media ownership, close, flush, rename, and remount handling across repeated USB sessions.
- Added strict Bulk-Only Transport Command Status Wrapper validation. Malformed or missing status fails closed, while a valid command failure remains distinguishable from a transport failure.
- Added session quarantine after a missing command-status response so firmware does not issue a new command into an indeterminate BOT session.

- Added one bounded root-port re-enumeration attempt for a final USBX enumeration failure.
- Kept optional SCSI commands optional. Normal publication does not require SYNCHRONIZE CACHE, START STOP UNIT, controller-driven VBUS cycling, re-enumeration, remounting, or full-file rereading after a successful write.
- Added a guarded USB VBUS adapter outside generated SSP code for diagnostics; it is not part of the normal production publication sequence.

Firmware update, backup, and file publication safety

- Added exact update-file validation for header CRC, format and product fields, fixed main-image length, audio length/alignment, total file size, and complete main/audio payload CRCs before QSPI erase begins.
- Added bounded payload reads, communications ownership, flash-ready polling, forced-stop handling, and NVRAM startup transfers so failures return instead of waiting indefinitely or underflowing timeout counters.
- Changed recovery-image publication to a temporary-file transaction with close, flush, backup of the prior image, rename, and final flush.
- Added complete USB payload validation before internal-flash replacement and preserved explicit failure status across the update reset.
- Added exact, case-insensitive filename and structure checks for firmware and WAV discovery.

Configuration persistence and safety

- Added a versioned SMI configuration fingerprint containing schema, magic, structure size, layout revision, machine type, generation, and block CRC.
- Added redundant configuration copies with newest-valid selection and repair of an invalid or older copy.
- Added complete factory-default construction when no supported current-SMI record exists; bytes from a rejected record are not carried into defaults.
- Added semantic validation for model/enumeration values, strings, booleans, finite setpoints and gains, calibration, alarm limits, loop timing, PID limits, and optional-controller relationships.
- Preserved a fingerprinted but semantically unsafe record for diagnosis while inhibiting effective heat. Startup does not silently clamp or rewrite the unsafe configuration.
- Changed configuration saving to a bounded three-attempt transaction with distinct committed, invalid, and exhausted-storage terminal results.
- Added transaction-keyed, reason-specific operator warnings so transient retries and recovered intermediate states do not produce false failure messages.

Temperature calibration and setpoint control

- Standardized the effective main-temperature calibration offset to the fixed absolute range -10.0 C through +10.0 C at 0.1 C precision.
- Applied the same limits to customer calibration and service 514, preventing repeated edits from expanding the allowed correction.
- Added endpoint clamping and press-and-hold repeat behavior to the calibration controls.
- Ensured the adjusted RTD temperature is the value used by the display, control, high-heat, alarm, and log-record paths.

- Added a guarded engineering setpoint mailbox and host-side setpoint/soak utilities. Accepted requests use the same validated setter and persistence path as the touchscreen and are limited to finite values from 0.0 C through 70.1 C. The interface is inert without debug access and is not a network or customer remote-control service.

Operator status and service functions

- Added reason-specific SD warnings for no readable response, sector-read failure, unsupported/invalid media, and installed media requiring HPT initialization. The warning confirms that temperature control remains active only when current configuration state supports that statement.
- Added service 467 for read-only protocol and CID identity reporting.
- Added HPT media classification, commissioning, health, range, graph, export, and recovery status surfaces.
- Routed the established service-471 format workflow to guarded HPT media 2.0 initialization.
- Added the shared services 480-489 qualification catalog for identity, scrub, initialization, lane diagnostics, wrap/reclaim/readback, controlled recovery, endurance, checkpoint continuation, and the ordered full run. Destructive entries retain explicit confirmation and identity preconditions.
- Retired the internal-SD FAT32-only services 469, 470, 472, and 474. Their service numbers now display a retirement notice rather than starting the old implementation.

Engineering, build, and release support

- Added managed Debug and Release build commands with stable artifact names and validated versioned ELF, S-record, and map copies.
- Added immutable candidate manifests binding source, configuration, embedded version, toolchain, artifact sizes, and SHA-256 values.
- Added manifest-bound bench programming, complete flash readback comparison, rollback capture, dual-J-Link bench inventory, and hostname-only remote bench access.
- Added executable model, static-policy, fault-injection, export, graph, SD, USB, configuration, update, calibration, and release-validation checks.
- Added exact-byte release publication safeguards, including preservation of canonical S-record line endings across Windows and Linux checkouts.

Final version-5 identity

The repository already records this cumulative implementation as production release v00.05.00:

- frozen firmware source commit: fa6f1a99099c02d8359ca6723e982ce48e4529f7;
- release tag commit: f14d089c;
- production candidate: 00.05.00-fa6f1a99099c-c33cda33c79a;
- Release S-record SHA-256:
C33CDA33C79A760BFE839503C18F5CFD4C614ADF0A00F41AF92360CF90EDB024.

Exact release provenance remains in Release/firmware-release.json and Release/RELEASE_NOTES.md.

Scope intentionally omitted

This change log does not claim abandoned or superseded work. In particular, it does not present the intermediate 00.04.13 internal-SD FAT32 formatter and FAT32 endurance services as version-5 features, does not treat diagnostic power cuts or forced USB faults as normal customer workflows, and does not claim an operator-accessible full HPT recovery function. Historical plans, incidents, failed trials, and qualification evidence remain available elsewhere in the repository without being part of this implementation summary.