PRODUCT

Avionics Ground System

Transportation Avionics Ground System Nxp Imx

SiliconCentric | Independent Verification & Validation

PRODUCT

Introduction

Our client is an avionics ground-support equipment maker. Their product is a portable line-test set: a test set that misreads a discrete can strand a serviceable aircraft or clear an unserviceable one. They came to us mid-development — interface board schematics complete, first prototypes running, design freeze one iteration away. The board is a standalone NXP i.MX design whose internal Cortex-M7 serves as the companion microcontroller, generating and capturing the deterministic bus traffic that the Cortex-A user-interface side cannot be trusted to time. We collaborated with them on this project by providing independent verification and validation of the board.

- Compute topology: a single i.MX package — Cortex-A core for the operator interface and test-management stack, internal Cortex-M7 for cycle-accurate ARINC-429 scheduling and discrete-I/O timing.
- Under validation: eight ARINC-429 channels (four transmit with line drivers, four receive), sixteen aircraft-convention discrete inputs (28 V/open and ground/open selectable), eight discrete outputs, an IRIG-B timing input, RS-422 x2, an isolated 28 V aircraft-power measurement channel, a galvanically isolated DC/DC power stage, eMMC, and a resistive-touch display.
- Program state: mid-development — prototypes on the bench, one layout iteration remaining before freeze.
- Independence: no technical, managerial, or financial stake in the design; airline and MRO customers of the end product weight independent evidence heavily.
- Bounded scope: independent validation only — no test-set feature development, no firmware authoring, no out-of-scope engineering.
- Working inputs: the hardware design package — schematics, ICDs, BOM — with no access to firmware source.

2

PRODUCT

Hardware Topology

The topology is a standalone SoC with the companion on-die: the M7 owns everything with a timing budget, the A-core owns everything with a screen. Scope enclosed the interface board, its buses, its isolation barriers, and its timing chain; the test-set application software and any airworthiness paperwork for target aircraft stayed outside.

- Topology classification: standalone SoC with internal Cortex-M7 companion; cores communicate over shared OCRAM with a mailbox, and the M7 exclusively owns the ARINC scheduler and discrete timing.
- The M7's job: ARINC-429 word scheduling at both 12.5 and 100 kbps rates, discrete edge timestamping, IRIG-B decode, and the deterministic behavior the product's measurements depend on.
- In-scope interfaces: ARINC-429 x8, discrete in x16 and out x8, IRIG-B, RS-422 x2, the isolated 28 V measurement channel, I2C (temperature, power telemetry), eMMC, display.
- Envelope in scope: −20 °C to +55 °C flight-line ambient, operation from both bench power and aircraft 28 V per MIL-STD-704-style quality, and the electrical noise environment of a live flight line.
- Out of scope: test-set application software, per-aircraft test procedures, and any certification sign-off — we produce the evidence; the client's assessor and their airline customers judge it.
- The i.MX family is among the six architectures Polaris already runs on, so the OS baseline was inherited and effort went to the board delta rather than silicon bring-up.

3

PRODUCT

Problem Statement

Prototypes worked in the lab, the application team was building UI against them, and one layout iteration remained — after which every hardware fault becomes a firmware workaround or a field problem. A test set is measurement equipment: an undetected hardware flaw does not just fail, it reports wrong results.

- Proven in isolation, never as a board: the ARINC line drivers and receivers carried vendor compliance data on vendor layouts — not with this board's isolated supply, its connector stack, its discrete-input dividers, or its IRIG-B front end sharing the same ground partition.
- Firmware coverage is feature-shaped, not board-shaped: the application exercises the ARINC channels its test procedures use, but the ground/open discrete mode, the second RS-422 port, the full IRIG-B amplitude range, and the isolated measurement channel's fault behavior fell outside every feature.
- No stress, no extremes, no duration: no −20 °C flight-line cold start, no +55 °C soak, no multi-day endurance, no aircraft-power transient and brown-out campaign, no operation-under-noise characterization — the daily environment of ground-support equipment.
- Nothing runs alongside development: validation was an end-phase gate, so a marginal receiver threshold would surface as intermittent test-set misreads in an MRO hangar — the kind of field report that ends an equipment brand's credibility.
- Airline procurement expects documented verification evidence for test equipment; ARINC-429 electrical conformance and timing accuracy claims must be backed by records, not asserted.
- The product measures other systems, so its own timing chain — IRIG-B in, M7 scheduling, timestamp out — must be proven to a tighter budget than anything it tests.
- One layout iteration remained: any fault found after freeze would be patched in firmware or lived with in the field.

PRODUCT

Customer Requirements

4

The client's requirements were direct: validate the whole board, under stated limits, before the freeze, with evidence that survives airline technical evaluation.

- Operating temperature: the board shall operate from −20 °C to +55 °C flight-line ambient, including cold start at −20 °C.
- Supply voltage: 28 V nominal aircraft power, steady-state window 22 V to 29 V per MIL-STD-704-style quality. The board shall survive transient spikes to 80 V for 50 ms without damage; over-voltage protection shall clamp above 32 V continuous.
- Brown-out: the board shall ride through input sag to 18 V and recover without operator intervention; below 18 V it shall shut down cleanly with no record loss.
- Over-current: the isolated DC/DC stage and each downstream rail shall have over-current protection tripping within 10 ms; a fault on the isolated measurement channel shall not propagate across the isolation barrier.
- Humidity: the unit shall operate at up to 95% RH non-condensing and shall not be exposed beyond that.
- Full-board functional validation: the A-core, the M7, all memory regions, all eight ARINC channels at both rates, all twenty-four discretes in both conventions, IRIG-B across its amplitude range, both RS-422 ports, the isolated measurement channel, eMMC, and the display — one integrated system.
- Coverage independent of firmware scope: every subsystem validated regardless of the application's test-procedure set, through a HAL built from the design package.
- Stress matrix: −20 °C to +55 °C sweep with cold-start cycling, 96-hour endurance under full bus traffic, aircraft-power transient and brown-out campaigns on the 28 V input, and injected-noise runs replicating flight-line conditions.
- Continuous validation alongside development: CI integration revalidating every firmware candidate on the prototypes through the freeze and beyond.
- Evidence: timestamped, operator-attributed, version-pinned records with bidirectional traceability, packaged for airline and MRO technical evaluations.
- A web console the client's verification staff run without embedded expertise, learned once.
- An immutable, append-only evidence store anchoring the freeze decision and the production baseline.
- Setup in minutes: a documented bench — board, bus simulator, programmable 28 V source, host — reproducible by any operator.

PRODUCT

Architecture

The interface board runs the validation OS, HAL, and client; an external x86 host runs the server, dashboard, and SDK. Execution stays isolated from data processing, and the board keeps its resources for representative behavior — necessary when the measurement under test is the board's own timing accuracy.

- Polaris OS (the validation OS) — a reproducible Linux image for the A-core booting to a known state, so prototype benches cannot drift apart.
- HAL — the single board-specific layer, exercising every ARINC channel, all discretes in both conventions, IRIG-B decode, RS-422, the isolated measurement channel, and eMMC behind a uniform interface that keeps the avionics-GSE suites portable to the frozen layout.
- Client — the on-target agent driving tests through the HAL; gRPC on Linux, FlatBuffers to the M7's FreeRTOS image; three timestamps per event (origin, relay, server); light enough that the timing chain being measured stays undisturbed.
- Server — orchestration, scheduling, and the append-only records store on the host, three prototypes in parallel, dashboard and API hosted.
- Dashboard — the console for the verification staff: provision a board, configure and launch, live per-channel ARINC word rates, discrete states, IRIG lock, rail telemetry, time-series review; every state-changing action operator-attributed.
- Python SDK — automation and CI; scripts everything the console does; C bindings served the timing-injection harness on this program.
- The OS and HAL are the two board-specific layers and were heavily modified for this board and this SoC; the client, server, dashboard, and Python SDK were configured to the client's requirements, but their core structure and working style remain the same across every board and every industry.

6

PRODUCT

Design

The binding constraints: a timing chain the product's credibility rests on, a −20 °C flight line, an isolation barrier whose integrity is a safety property, and aircraft-power quality that ranges from lab-clean to generator-cart noisy.

- Validation OS design — read-only rootfs, A/B partitions with rollback; boot optimized under 20 seconds because a portable test set that boots slowly gets left in the truck — the trade-off was dropping debug tooling from the image, recovered via an on-demand overlay. The M7 runs FreeRTOS with a static schedule matched to the ARINC frame timing.
- HAL design — partitioned by schematic sheet against ICD clauses; ARINC receive and discrete edges are interrupt-driven with M7 hardware timestamping since polling would destroy the timing evidence. A babbling channel can storm the M7, so per-channel rate limiting is built into the capture path.
- Client design — origin timestamps disciplined to the IRIG-B-locked clock when available, free-running otherwise, with the discipline state recorded — so no record ever claims a timebase it did not have; on power loss the client flushes raw records first, trading shutdown grace for complete evidence.
- Server design — three-timestamp causality orders a 28 V transient against the discrete misreads it caused; retention sized for 96-hour full-traffic runs on three boards; deployment on the client's isolated lab network, cross-site sync configured off.
- Dashboard design — per-channel ARINC error counters, discrete-state matrices in both conventions, IRIG lock status, and isolation-barrier telemetry are first-class views — what an avionics verification engineer triages first; run health and drop counts on every screen.
- SDK design — the client scripted the acceptance gate, the noise-injection matrix, and overnight endurance; the direct API path served single-channel bench checks, at the stated cost that those runs generate no records.
- OS and HAL design was board-specific and heavily reworked; the four upper components were configured to this client's verification workflow while their structure and working style stayed constant.

7

PRODUCT

Implementation

Work went to the OS delta, the HAL, and the avionics-GSE campaigns; the four upper components were configured, not constructed.

- Validation OS — Yocto image for the i.MX: inherited BSP and U-Boot, board device tree covering the ARINC interface logic, discrete banks, IRIG front end, and display, minimal kernel; OTA with A/B rollback; sub-20-second boot; per-build SBOM with CVE tracking; the M7 FreeRTOS image built in the same tree.
- HAL — implemented sheet by sheet and bench-verified as written: register interfaces to the ARINC transceivers, M7 DMA capture with hardware timestamps, discrete-bank drivers handling both aircraft conventions, IRIG-B decode path, isolated-channel measurement drivers; the design-package pass surfaced an ICD ambiguity — the ICD defined discrete input polarity as "active" without stating whether active meant 28 V or ground, while the schematic's dividers implied ground/open, a documentation conflict that would have inverted sixteen channels' worth of test results.
- Client — C++ daemon, event and polling paths, discipline-aware timestamping, power-loss-hardened shutdown, gRPC upstream, FlatBuffers to the M7.
- Server — telemetry receiver, versioned schema, scheduler, REST API, dashboard hosting, three-board parallelism.
- Dashboard — board provisioning, campaign configuration, live channel and discrete streaming, time-series review, export for airline evaluations, operator attribution.
- SDK — Python bindings, C timing-harness bindings, example scripts, CI wiring firing the acceptance suite on every firmware candidate.
- Board-specific: OS delta and HAL. Configuration: client discipline policy, server deployment posture, dashboard views, SDK harness glue.

PRODUCT

Test - IV&V

Testing ran stack-first, then OS/HAL, then the board across one-shot, long-running, event-based, and monitoring campaigns — with every dashboard-launched run committed to the append-only store.

- Stack self-verification: 100% test coverage of the client, server, dashboard, and Python SDK before it produced evidence about this board.
- OS/HAL verification: A/B boot and rollback exercised, OTA verified end to end, secure boot checked on accept and reject paths.
- Bench setup: board cabled to an ARINC bus simulator and programmable 28 V source, IRIG-B generator connected, provisioning from the dashboard — documented, repeatable, under thirty minutes.
- Functional campaign: per-channel ARINC electrical and word suites at 12.5 and 100 kbps, discrete matrices across both conventions and threshold ranges, IRIG-B lock across the amplitude range, RS-422 margin, isolated-channel accuracy against reference, display and eMMC checks.
- Compute and memory checks: DDR and OCRAM pattern stress across the −20 °C to +55 °C span, eMMC integrity through repeated unclean power loss, and mailbox latency characterized across DVFS states — the finding that later shaped the timing-discipline rule.
- Watchdog and reset campaign: induced hangs on both cores confirming watchdog recovery to a defined, visibly failed state — a test set must fail loudly, never report through a wedged timing chain — with the M7's static ARINC schedule verified to restart cleanly after every reset combination.
- Debug posture: JTAG access verified disabled in the fielded configuration, retained on prototypes where it anchored the M7 timing calibration.
- One-shot tests as the acceptance gate: one pass/fail per subsystem per firmware candidate.
- Long-running: the 96-hour full-traffic endurance held all eight ARINC channels at rate with snapshots, catching receiver channel 6's threshold drifting with board temperature — a bias-resistor tolerance stack corrected in the freeze layout.
- Event-based: silent runs recording on word errors, discrete misreads, IRIG lock loss, and rail events — this mode caught IRIG-B losing lock at the low end of its specified amplitude range, traced to an input comparator hysteresis choice, fixed before freeze.
- Monitoring: passive telemetry — rails, temperatures, isolation-barrier leakage, IRIG lock statistics — under representative traffic; the main finding surfaced here: the isolated DC/DC stage's switching noise coupled into the discrete-input dividers, producing false ground/open transitions on four channels whenever the converter ran above 60% load — a layout-level coupling that made the test set misread aircraft discretes on its own power stage's schedule.
- Instrumentation correlation: oscilloscope and differential-probe captures anchored the converter-coupling, threshold-drift, and IRIG findings to the records at the electrical level.
- Recording rule: every run launched from the dashboard is recorded, always, into the append-only store; the Python SDK can run 100% of what the dashboard can run — module, peripheral, or system level — for quick independent checks, and SDK-launched runs of this kind are not written to the records store. The store is the evidence; the SDK is the bench tool.
- Traceability: requirements traced bidirectionally to tests and records, schemas version-pinned, runs reproducible for airline technical evaluation.

9

PRODUCT

Deliverables

The client received the complete platform fitted to this interface board — source, records, procedures, no lock-in.

- Validation OS image with the full Yocto build system, recipes, and per-build SBOM.
- Board-specific BSP and HAL source for every subsystem, maintained against the design package through the freeze.
- Compiled client for the A-core plus the M7 FreeRTOS build.
- Server and dashboard as deployment-ready containers on the client's lab network.
- Complete suites — ARINC electrical and protocol, discrete matrices, IRIG-B, thermal, endurance, power-transient, noise-injection — with recorded prototype baselines.
- Python SDK with documentation, example scripts, timing-harness bindings, and CI integration gating every firmware candidate.
- The append-only records store as client property — the evidence base for airline and MRO evaluations.
- The independent validation report: the converter-to-discrete coupling, the channel-6 threshold drift, the IRIG amplitude finding, the discrete-polarity ICD conflict, metrics, pass/fail, coverage.
- Bench procedures for acceptance and re-runs; full documentation; no lock-in.

10

PRODUCT

Conclusion

A test set whose job is reporting the true state of aircraft went to design freeze with its own faults found and fixed: discretes that misread under converter load, a receiver that drifted with temperature, a timing input that quit at the edge of its spec.

- The converter-coupling defect was the expensive one — a test set misreading discretes in the field would have cost airline trust one hangar at a time; it cost a layout edit before freeze, with scope-anchored records behind the finding rather than anyone's assertion.
- The suites gate every firmware drop in CI and carry to the production build with only the HAL delta re-verified. We produce the evidence — the client's assessor and their airline customers judge it.

II

PRODUCT

Lessons Learned

The engagement sharpened our treatment of measurement-equipment validation, where the board's own accuracy is the product.

- Self-interference campaigns now run early on any board that both generates power and measures signals — the converter-load schedule was the key that unlocked the discrete misreads, and sweeping internal load states is now standard before functional depth; ICD polarity ambiguities on discrete conventions get resolved in document review, where this board's largest potential error lived.
- The A-core/M7 timing handoff carried a subtle trap: OCRAM mailbox latency varied with A-core DVFS state, jittering the M7's notion of when a test started by up to 40 µs — pinning the mailbox path and recording DVFS state with every timing measurement is now standard practice on i.MX timing-critical engagements.

CONTACT

SiliconCentric

EMAIL sandesh@siliconcentric.com

PHONE (669) 356-1998

WEB https://www.siliconcentric.com

ADDRESS San Jose, CA, USA