PRODUCT

Smart Thermostat

Home Appliances Smart Thermostat Ti Sitara

SiliconCentric | Independent Verification & Validation

I

PRODUCT

Introduction

Our client is a home-appliance maker. Their product is a smart thermostat — a consumer device that switches real HVAC loads — and its board had never been proven as a system. Mid-development, with rev A boards on the bench and a layout freeze approaching, we collaborated with them on this project by providing independent verification and validation of the board. The design is a standalone TI Sitara SoC: the Cortex-A core runs the display and connectivity stack, and the internal Cortex-M4 is the companion controller owning the sensing loop and the HVAC switching outputs.

- Compute topology: a single Sitara package — Cortex-A application core for UI and radio stack, internal Cortex-M4 for thermistor sampling, control-loop execution, and relay/triac actuation.
- Under validation: three relay drivers for HVAC stages, a triac dimming stage for a fan, four NTC thermistor channels, a capacitive-touch ring and wake sensor, a Zigbee/Thread radio module on SPI, a 2.4-inch display over parallel RGB, humidity and proximity sensors on I2C, and the 24 VAC power-harvesting supply with battery backup.
- Program state: mid-development — rev A functional but with known escapes, layout freeze scheduled, appliance firmware team ramping.
- Independence: we hold no technical, managerial, or financial stake in the design, and the finding that mattered most here went against the power supply — reporting it cost us nothing.
- Bounded scope: independent validation only; no feature development, no control-algorithm work, no product firmware authoring.
- Working inputs: the hardware design package — schematics, ICDs, BOM — with no firmware source access.

2

PRODUCT

Hardware Topology

The topology is a standalone SoC with the companion role on-die: the M4 runs everything that must survive when the A-core sleeps, which in a thermostat is nearly everything that matters. Scope enclosed the board, its switching stages, and its power states; the comfort algorithms and any safety-agency filing sat outside.

- Topology classification: standalone SoC with internal Cortex-M4 companion; A-core and M4 communicate through shared L3 SRAM with a mailbox, and the M4 holds exclusive authority over the relay and triac outputs.
- The M4's job: 10 Hz thermistor sampling, the hysteresis control loop, relay and triac sequencing with compressor-protection lockouts, and waking the A-core on touch or radio activity.
- In-scope interfaces: SPI (radio), I2C x2 (humidity, proximity, touch controller), parallel RGB display, four ADC thermistor channels, relay GPIO bank, triac gate drive with zero-cross detection, 24 VAC supply path with supercap-backed RTC.
- Envelope in scope: 0 °C to +40 °C ambient, 24 VAC input with the brown-outs and surges of residential HVAC transformers, and a duty cycle of years on a wall.
- Out of scope: comfort-control firmware, mobile-app integration, UL/EN 60730 agency testing — we produce integration evidence; the agency lab and the client's assessor judge it.
- The Sitara family is one of the six architectures Polaris already runs on, so the OS baseline was inherited and the effort went to this board's delta, not silicon bring-up.

3

PRODUCT

Problem Statement

Rev A worked well enough to demo and nobody could say more than that. The firmware team was about to build years-long-duty-cycle software on a board whose sleep states, switching stages, and sensing accuracy had only anecdote behind them — while a retail-channel launch date compressed everything.

- Proven in isolation, never as a board: TI's EVM proved the SoC, the radio module carried its own certification, and the relay vendor published lifetime curves — but this board's 24 VAC harvesting supply, its thermistor front ends, its triac zero-cross circuit, and its sleep architecture had never been exercised together.
- Firmware coverage is feature-shaped, not board-shaped: launch firmware needed two HVAC stages, not three, never drove the triac above half range, and treated the proximity sensor as optional — so the third relay, the triac's full range, and a sensor bus would reach production untested by that team.
- No stress, no extremes, no duration: no 40 °C soak with all stages switching, no multi-week endurance against relay and triac wear-in, no 24 VAC brown-out and transformer-surge campaign, no long-horizon sleep-current characterization — the exact life of a wall thermostat.
- Nothing runs alongside development: validation was an end-phase gate, so a defective sleep state would surface months later as battery complaints in field returns rather than as a finding on a bench.
- EN 60730-class agency review expects evidence that the switching stages behave under abnormal mains conditions; retail-channel quality audits expect return-rate projections grounded in test data.
- Sleep current is the product: a thermostat that misses its microamp budget drains its backup battery in the field.
- Compressor short-cycling from a relay-sequencing fault is an expensive appliance failure the thermostat maker would own.

PRODUCT

Customer Requirements

4

The client's requirements were direct: validate the whole board, under stated limits, with evidence usable for the layout-freeze decision, the agency lab pre-brief, and retail quality audits.

- Operating temperature: the board shall operate from 0 °C to +40 °C ambient.
- Supply voltage: 24 VAC nominal, operating window 18 VAC to 30 VAC. The board shall survive transformer surges to 40 VAC for 1 s without damage; over-voltage protection shall clamp above 30 VAC continuous.
- Brown-out: the board shall ride through 24 VAC sags to 16 VAC (furnace contactor pull-in) without reset; below that it shall transfer to battery backup with no record loss and no relay state change.
- Over-current: each relay stage shall be protected against load faults; the triac stage shall have over-current shutdown within one half-cycle. A shorted HVAC load shall not damage the board.
- Sleep current: deep-sleep current shall not exceed the design budget of 95 µA; battery backup shall hold the RTC and M4 sensing loop for 72 hours minimum.
- Humidity: the board shall operate at up to 90% RH non-condensing and shall not be exposed beyond that.
- Full-board functional validation: the A-core, the M4, all DRAM and SRAM regions, all four thermistor channels, all three relays, the triac across its full range with zero-cross verification, touch, display, radio, both I2C buses, and the 24 VAC supply path — one integrated system.
- Coverage independent of firmware scope: every subsystem validated regardless of the launch feature set, through a HAL built from the design package rather than the product firmware.
- Stress matrix: 0–40 °C sweep, four-week switching endurance across relay and triac stages, 24 VAC brown-out and surge campaigns, radio-coexistence checks, sleep-current characterization across all power states, and thermistor-accuracy verification — vibration waived by product profile.
- Continuous validation alongside development: CI hooks revalidating every firmware candidate on rev A and the frozen layout.
- Evidence: timestamped, operator-attributed, version-pinned records with bidirectional traceability for the agency file and retail audits.
- A web console the client's lab staff run without embedded expertise, learned once.
- An immutable, append-only evidence store whose rev A baselines anchor the frozen layout's comparison runs.
- Setup in minutes: standardized bench procedure — board, 24 VAC source, load bank, host — with no custom rig.

PRODUCT

Architecture

The Sitara board carries the validation OS, HAL, and client; an external x86 host carries the server, dashboard, and SDK. Execution stays isolated from data processing, and the board keeps its resources for representative behavior — decisive here, because sleep-current measurements are exactly what an intrusive toolchain contaminates.

- Polaris OS (the validation OS) — a reproducible Linux image for the A-core booting to a known state, one baseline for every board on the bench.
- HAL — the single board-specific layer, exercising the relay bank, triac gate and zero-cross path, thermistor ADCs, touch, display, radio SPI, and both I2C buses behind a uniform interface that keeps the appliance suites portable to the frozen layout.
- Client — the on-target agent driving tests through the HAL; gRPC on Linux, FlatBuffers to the M4's FreeRTOS image; three timestamps per event (origin, relay, server); its idle footprint small enough that sleep-state evidence stays valid.
- Server — orchestration, scheduling, and the append-only records store on the host, five rev A boards in parallel, dashboard and API hosted.
- Dashboard — the lab console: provision a board, configure and launch, live switching-state, thermistor, rail, and sleep-current telemetry, time-series review; every state-changing action operator-attributed.
- Python SDK — automation and CI; scripts everything the console does; C bindings available, unused 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.

PRODUCT

Design

The design drivers: a microamp sleep budget, mains-adjacent switching stages that must fail safe, a 24 VAC supply that browns out whenever the furnace contactor pulls in, and a years-long duty cycle compressed into a four-week endurance campaign.

- Validation OS design — read-only rootfs with A/B rollback; suspend-to-RAM support was kept in the validation image even though it complicates the update path, because validating the product's sleep states demanded the OS actually enter them — a trade-off accepted knowingly. The M4 runs FreeRTOS, matching the tick-suppression model the sleep campaign needed.
- HAL design — partitioned by schematic sheet, each function pinned to an ICD clause; zero-cross and touch events are interrupt-driven while thermistors poll at 10 Hz — polling chosen deliberately because interrupt-driven ADC watchdogs would disturb the sampling noise floor under test, at the known cost of missing sub-100 ms thermal transients, documented as a limit.
- Client design — origin timestamps at the driver boundary; during sleep tests the client parks itself and delegates event capture to the M4, trading direct observation for uncontaminated current measurements — the M4 relays its event log on wake.
- Server design — three-timestamp ordering ties a 24 VAC sag to the M4 reset it caused; retention sized for four-week endurance streams from five boards, with switching-cycle counters aggregated hourly — raw retention of every relay edge was rejected as storage without value.
- Dashboard design — sleep-current trend, relay/triac cycle counters, thermistor deltas against reference probes, and 24 VAC quality are first-class views; run health and drop counts on every screen for the lab staff.
- SDK design — the client scripted the acceptance gate, the switching-endurance matrix, and nightly sleep-current runs; the direct API path served single-relay bench checks, with the stated cost that those runs leave no records.
- OS and HAL design was board-specific and heavily reworked; the four upper components were configured to this client's lab workflow while their structure and working style stayed constant.

7

PRODUCT

Implementation

Work concentrated in the OS delta, the HAL, and the appliance campaigns; the upper four components were configured, not built.

- Validation OS — Yocto image for the Sitara: inherited BSP and U-Boot, board device tree covering the display, radio, touch controller, and ADC channels, kernel with suspend-to-RAM validated; OTA with A/B rollback; boot under 20 seconds; per-build SBOM with CVE tracking; the M4 FreeRTOS image built in the same tree.
- HAL — implemented sheet by sheet from the design package and bench-verified as written: ADC sequencing with oversampling for the thermistor channels, interrupt handlers for zero-cross and touch, GPIO sequencing with enforced dead-time for the relay bank, SPI timing for the radio; the package pass caught an ICD conflict — the zero-cross detector's output polarity was documented opposite to the schematic's comparator wiring, which would have fired the triac at peak mains voltage instead of the crossing.
- Client — C++ daemon, event and polling paths, sleep-aware operation with M4 delegation, graceful shutdown without record loss, gRPC upstream, FlatBuffers to the M4.
- Server — telemetry receiver, versioned schema, scheduler, REST API, dashboard hosting, five-board parallelism.
- Dashboard — board provisioning, campaign configuration, live switching and current streaming, time-series review, export for the agency pre-brief, operator attribution.
- SDK — Python bindings, example scripts per subsystem, CI wiring firing the acceptance suite on every firmware candidate.
- Board-specific: OS delta and HAL. Configuration: client sleep behavior, server aggregation policy, dashboard views, SDK examples.

PRODUCT

Test - IV&V

8

Verification ran stack-first, then OS/HAL, then the board across one-shot, long-running, event-based, and monitoring campaigns — every dashboard-launched run recorded 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 on a 24 VAC programmable source with an HVAC load bank, reference thermometry placed, provisioning from the dashboard — a twenty-minute documented procedure.
- Functional campaign: relay sequencing with lockout verification, triac full-range firing-angle suites against zero-cross, thermistor accuracy against reference probes, touch and proximity suites, display checks, radio PER runs, sleep-state entry/exit verification.
- Compute and memory checks: DRAM and on-chip SRAM pattern stress across the thermal range, mailbox and shared-SRAM integrity between the A-core and M4 under concurrent load, and boot-path verification through repeated 24 VAC brown-out and battery-transfer events.
- Watchdog and reset campaign: induced hangs on both cores confirming watchdog recovery with relay states held and compressor-protection lockouts preserved across the reset — a thermostat that forgets its lockout timer on reset short-cycles the most expensive appliance in the house; M4 authority over the switching outputs verified through every A-core reset combination; JTAG access was confirmed disabled in the production-intent configuration, retained on rev A for bench debug.
- One-shot tests as the acceptance gate: one pass/fail per subsystem per firmware candidate.
- Long-running: the four-week switching endurance logged every relay and triac cycle with periodic parameter snapshots, catching contact-resistance growth on relay 2 trending out of family by week three — a supplier-lot flag raised before production procurement.
- Event-based: silent runs recording on zero-cross anomalies, thermistor out-of-family readings, rail excursions, and unexpected wake events — this mode caught the touch controller waking the A-core roughly every 40 minutes on electrical noise from the triac snubber, a coupling that battery modeling would have blamed on software.
- Monitoring: passive telemetry — rails, board temperature, sleep current, 24 VAC quality — over multi-day runs; the main finding surfaced here: deep-sleep current measured 4.1x the design budget, traced to a GPIO bank left floating by the rev A layout, back-powering the display driver through its I/O pins.
- Instrumentation correlation: oscilloscope and precision source-measure captures anchored the sleep-current, snubber-coupling, and zero-cross findings to the records.
- 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.

9

PRODUCT

Deliverables

Delivery was the complete platform fitted to this thermostat 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 layout freeze.
- Compiled client for the A-core plus the M4 FreeRTOS build.
- Server and dashboard as deployment-ready containers in the client's lab.
- Complete suites — functional, switching endurance, thermistor accuracy, sleep-current, 24 VAC abuse — with recorded rev A baselines.
- Python SDK with documentation, example scripts, and CI integration gating every firmware candidate.
- The append-only records store as client property — evidence for the agency file and retail audits.
- The independent validation report: the sleep-current defect, the snubber-to-touch coupling, the zero-cross ICD conflict, the relay-2 lot flag, metrics, pass/fail, coverage.
- Bench procedures for acceptance and re-runs; full documentation; no lock-in.

10

PRODUCT

Conclusion

The layout froze with the floating GPIO bank fixed, the zero-cross polarity corrected, and the snubber coupling suppressed — three defects that would have shipped as battery complaints, blown fuses, and phantom wake-ups in customers' homes.

- The 4.1x sleep-current exceedance and the peak-voltage triac firing were both invisible to feature-level firmware testing and both caught from the design package and the bench, at the cost of a layout edit instead of a field-return program — with records the agency lab pre-brief used directly.
- The suites gate every firmware drop in CI and carry to the frozen layout with only the HAL delta re-verified. We produce the evidence — the client's agency lab and assessor judge it.

II

PRODUCT

Lessons Learned

The engagement moved power-state and mains-interaction testing to the front of our appliance pipeline.

- Sleep-current characterization now precedes functional depth on any battery-backed appliance board — the floating-GPIO defect was measurable on day three, and every week it stayed hidden was a week of firmware assumptions built on a wrong power budget; likewise, zero-cross and polarity checks against the schematic happen during document review, where this board's most dangerous defect actually lived.
- The A-core/M4 wake contract needs explicit adversarial testing: the M4 correctly ignored the touch controller's noise-driven interrupts, but the A-core's wake path did not, and the asymmetry hid until multi-day monitoring — asymmetric wake-source validation across both cores is now standard on every heterogeneous Sitara engagement.

CONTACT

SiliconCentric

EMAIL sandesh@siliconcentric.com

PHONE (669) 356-1998

WEB https://www.siliconcentric.com

ADDRESS San Jose, CA, USA