PRODUCT

Smart Grid Meter

Energy Power Smart Grid Meter Nxp Imx

SiliconCentric | Independent Verification & Validation

SiliconCentric

I

PRODUCT

Introduction

Our client is a grid-equipment manufacturer. Their product is a three-phase smart grid meter — hardware deployed in the hundreds of thousands and revisited roughly never. The client wanted the first-article boards independently proven before a single unit was scheduled for a utility pilot. The board is a standalone NXP i.MX SoC whose internal Cortex-M7 acts as the companion microcontroller, running the metrology sampling loop that the Cortex-A communications stack must never disturb. We collaborated with them on this project by providing independent verification and validation of the board.

- Compute topology: one i.MX package — Cortex-A core for the communications and data-management stack, internal Cortex-M7 for continuous metrology sampling and tamper supervision.
- Under validation: a polyphase metering AFE sampling three current transformers and a neutral shunt, voltage dividers per phase, a supercap-backed RTC, an NB-IoT module on UART with its own SIM and power domain, two RS-485 ports carrying DNP3, an optical maintenance port, anti-tamper switches and a magnetic sensor on dedicated GPIO, and eMMC.
- Program state: fabricated first articles, bench-powered once, metering firmware team staffed and waiting on hardware confidence.
- Independence: our assessment holds no technical, managerial, or financial stake in the design — and utility procurement teams weight independent evidence over vendor self-reports.
- Bounded scope: independent validation only — no metrology-algorithm development, no firmware authoring, no out-of-scope engineering.
- Working inputs: schematics, ICDs, and the BOM — the hardware design package — with no access to firmware source.

2

PRODUCT

Hardware Topology

Topologically this is a standalone SoC with the companion function on-die: the M7 owns the sampling loop and the tamper chain, the A-core owns everything that talks to the utility. Scope enclosed the board, its measurement chain, its backup-power behavior, and its communications hardware; legal metrology certification and the utility's head-end integration stayed outside.

- Topology classification: standalone SoC with internal Cortex-M7 companion; the cores share OCRAM with a mailbox, and the M7 holds the AFE, the tamper GPIOs, and the RTC.
- The M7's job: 4 kHz-per-channel metrology sampling, energy accumulation, tamper-event latching that must survive main-power loss, and RTC integrity.
- In-scope interfaces: the AFE's dedicated serial interface, SPI (AFE control), I2C (RTC, temperature), UART x3 (NB-IoT, optical port, console), RS-485 x2 (DNP3), eMMC, tamper GPIO bank.
- Envelope in scope: −25 °C to +60 °C outdoor-cabinet rating, three-phase 230/400 V measurement context with the board's own supply taken from phase A, sustained brown-out and outage profiles, and a 15-year target service life.
- Out of scope: legal-metrology type approval (MID/OIML-class), DNP3 head-end integration, firmware development — we produce evidence; the client's notified body and utility judge it.
- The i.MX family is one of the six architectures Polaris already runs on, so the OS baseline was inherited and the engagement's effort went to the board delta rather than silicon bring-up.

3

PRODUCT

Problem Statement

The boards were back, the utility pilot had a date, and metrology accuracy claims — the product's entire reason to exist — rested on an unproven measurement chain. Each component had pedigree; the assembled board had none, and in metering a silent hardware fault becomes a billing dispute at scale.

- Proven in isolation, never as a board: the AFE vendor's characterization used their reference layout — not this board's CT burden resistors, its anti-alias filters, its ground partitioning between the measurement and communications domains, or its phase-A-fed power supply.
- Firmware coverage is feature-shaped, not board-shaped: the metering firmware would exercise the AFE and NB-IoT daily, but the second RS-485 port, the optical port's full speed range, the magnetic-tamper sensor, and the RTC's backup-domain behavior fell outside every planned feature.
- No stress, no extremes, no duration: no −25 °C to +60 °C accuracy sweep, no multi-week continuous-accumulation endurance, no outage and brown-out campaign against the exact power-loss profiles a grid meter lives through, no NB-IoT transmit-burst testing against the board's own rails.
- Nothing runs alongside development: validation was an end-gate, so a measurement-chain defect would surface during the utility pilot as an accuracy dispute — the most damaging possible venue.
- IEC 62443 expectations on the communications path and DNP3 conformance expectations from the utility both demand documented evidence, and legal-metrology review later demands a traceable test history.
- The NB-IoT module's transmit bursts draw amps from a supply shared with a precision measurement domain — a coupling risk specific to this board's layout.
- A fleet recall on deployed meters means truck rolls priced per unit across an entire service territory; the economics forbid finding hardware faults after deployment.

PRODUCT

Customer Requirements

4

The client's requirements were direct: validate the whole board, under stated limits, with evidence that survives both a notified body and a utility procurement review.

- Operating temperature: the board shall operate from −25 °C to +60 °C outdoor-cabinet ambient, with metrology accuracy held across the full span.
- Supply voltage: board supply taken from phase A at 230 V AC nominal, operating window 184 V to 264 V (−20%/+15%). The board shall survive a phase-to-phase misconnection at 400 V AC without damage; over-voltage protection shall act above 264 V continuous.
- Brown-out and outage: the board shall ride through grid brown-out and outage profiles as recorded by the utility; on outage the M7 shall latch tamper and accumulation state with no record loss, and the supercap backup shall hold the RTC for a minimum of four weeks.
- Over-current: the supply path shall have over-current protection; NB-IoT transmit bursts shall not disturb the measurement domain's rails beyond the accuracy budget.
- Humidity: the board shall operate at up to 95% RH non-condensing per the outdoor-cabinet profile.
- Full-board functional validation: the A-core, the M7, all memory regions, the full AFE chain across all four current channels and three voltage channels, both RS-485 ports, NB-IoT, the optical port, RTC and its backup domain, every tamper input, and eMMC — one integrated system.
- Coverage independent of firmware scope: every subsystem validated regardless of the metering feature set, driven through a HAL built from the design package.
- Stress matrix: accuracy-relevant thermal sweep −25 °C to +60 °C, three-week continuous accumulation endurance, outage/brown-out campaigns replaying recorded grid events, NB-IoT burst testing with rail monitoring, and tamper-chain verification through power loss.
- Continuous validation alongside development: CI integration revalidating every firmware candidate on real first articles.
- Regulatory evidence: timestamped, operator-attributed, version-pinned records with bidirectional traceability, structured for the notified-body file and the utility's technical evaluation. The named regimes: IEC 62443 posture on communications, DNP3 conformance context, MID-class metrology review downstream.
- A web console the manufacturer's test lab runs without embedded specialists.
- An immutable, append-only evidence store — a chain of custody that a billing-dispute lawyer, not just an engineer, might one day read.
- Setup in minutes: standardized bench with a three-phase reference source, documented so any operator reproduces it.

5

PRODUCT

Architecture

The meter board runs the validation OS, HAL, and client; an external x86 host runs the server, dashboard, and SDK. The split isolates execution from data processing and preserves the board's resources for representative behavior — which in metering means the sampling loop ran undisturbed while tests observed it, because a loaded measurement domain is a wrong measurement domain.

- Polaris OS (the validation OS) — a reproducible Linux image for the A-core booting to a known state, giving every first article an identical software baseline.
- HAL — the one board-specific layer, exercising the AFE chain, both RS-485 ports, NB-IoT, the optical port, RTC and backup domain, tamper bank, and eMMC behind a uniform interface that keeps the metering suites portable to the production revision.
- 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); load kept off the measurement domain so accuracy evidence stays clean.
- Server — orchestration, scheduling, and the append-only records store on the host, eight first articles in parallel, dashboard and API hosted.
- Dashboard — the lab console: provision a board, configure and launch, live per-phase accuracy deltas against the reference source, rail and RTC telemetry, time-series review; every state-changing action operator-attributed.
- Python SDK — automation and CI; scripts everything the console does; C bindings available, unused here.
- 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: metrology-grade accuracy across an 85-degree temperature span, a 15-year service life compressed into weeks of evidence, power-loss behavior that must be flawless, and a records regime built for disputes as much as for engineering.

- Validation OS design — read-only rootfs, A/B partitions with rollback, secure boot through the i.MX HAB chain because a meter image with an unverifiable origin is an IEC 62443 finding waiting to happen; the trade-off is signing-infrastructure overhead per build, absorbed into the CI. The M7 runs FreeRTOS with tick suppression matched to the 4 kHz sampling frame.
- HAL design — partitioned by schematic sheet against ICD clauses; AFE data and tamper events are interrupt-driven — a missed tamper edge is an evidentiary hole — while RTC and temperature poll at 1 Hz. Interrupt-driven AFE capture on a shared interconnect can jitter the M7's frame timing, so the AFE path was pinned to the M7's TCM.
- Client design — origin timestamps disciplined to the RTC so accuracy records and grid events share a timebase; on outage the client's last act is flushing the tamper and accumulation state, trading shutdown margin for a complete power-loss record.
- Server design — three-timestamp causality orders an NB-IoT burst against the phase-A rail dip it caused; retention sized for three-week accumulation streams from eight boards; records signed at rest because the client's counsel asked what a billing dispute would subpoena.
- Dashboard design — per-phase error against reference, rail telemetry, RTC drift, and tamper-chain state are first-class views; run health and drop counts on every screen.
- SDK design — the client scripted the acceptance gate, the outage-replay matrix, and nightly accuracy runs; the direct API path served single-channel bench checks, at the stated cost that such runs produce no records.
- OS and HAL design was board-specific and heavily reworked; the four upper components were configured to this client's lab and quality workflow while their structure and working style stayed constant.

7

PRODUCT

Implementation

Effort went to the OS delta, the HAL, and the metering campaigns; the four upper components were configured, not constructed.

- Validation OS — Yocto image for the i.MX: inherited BSP and U-Boot with HAB signing, board device tree covering the AFE, RTC, NB-IoT power domain, and tamper bank, minimal kernel; OTA with A/B rollback; boot under 25 seconds; 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: the AFE's serial capture into M7 TCM via DMA, interrupt handlers for the tamper bank with latch verification, RS-485 drivers with direction-control timing, NB-IoT power-domain sequencing; the design-package pass surfaced a BOM error — the anti-alias filter on current channel 2 specified 1% capacitors on the schematic but the BOM carried 10% parts, a phase-error contributor caught before it could pass as an AFE calibration problem.
- Client — C++ daemon, event and polling paths, RTC-disciplined timestamping, outage-hardened shutdown, gRPC upstream, FlatBuffers to the M7.
- Server — telemetry receiver, versioned signed schema, scheduler, REST API, dashboard hosting, eight-board parallelism.
- Dashboard — board provisioning, campaign configuration, live accuracy and rail streaming, time-series review, export templated for the notified-body file, 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 timebase discipline, server signing and retention, dashboard views and export, SDK examples.

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 generated evidence about the meter.
- OS/HAL verification: A/B boot and rollback exercised, OTA verified end to end, the HAB secure-boot chain checked on accept and reject paths.
- Bench setup: board wired to a three-phase reference source and programmable load, RF path to an NB-IoT network simulator, provisioning from the dashboard — documented and repeatable in under thirty minutes.
- Functional campaign: per-channel AFE accuracy suites against the reference source, phase-linkage and neutral-shunt checks, DNP3 exchange suites on both RS-485 ports, optical-port speed range, NB-IoT attach and transfer suites, RTC drift measurement, tamper-chain suites including magnetic stimulus.
- Compute and memory campaign: DDR pattern stress across the −25 °C to +60 °C span, eMMC endurance profiled against the fifteen-year logging duty model, and cache/DMA integrity verified with the metrology path pinned to TCM — confirming the isolation the design review demanded.
- Watchdog and reset campaign: induced hangs on both cores confirming watchdog recovery without loss of accumulation or tamper state, and warm, cold, and outage-driven reset combinations verified to restart sampling within the accuracy budget.
- Debug and security posture: JTAG access verified locked through the i.MX fuse configuration on production-intent settings — an open debug port on a revenue meter is both an IEC 62443 finding and a tamper vector — with debug access retained on first articles for bench evidence.
- One-shot tests as the acceptance gate: one pass/fail per subsystem per firmware candidate per board.
- Long-running: the three-week continuous accumulation run compared energy registers against the reference standard daily, catching a slow divergence on channel 2 consistent with the anti-alias BOM finding and confirming the fix.
- Event-based: silent runs recording on tamper edges, rail excursions, RTC anomalies, and accuracy-threshold crossings — this mode caught NB-IoT transmit bursts dipping the analog rail enough to disturb channel 3's noise floor, resolved with a supply-domain change note for production.
- Monitoring: passive telemetry — rails, board temperature, RTC drift, backup-domain voltage — across outage campaigns; the main finding emerged here: the supercap backup, specified for weeks of RTC retention, drained in nine days, traced to a leakage path through a mis-specified ideal-diode controller that back-fed the dead main rail.
- Instrumentation correlation: precision power-analyzer and oscilloscope captures anchored the accuracy, burst-coupling, and supercap 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 for the notified body and the utility.

9

PRODUCT

Deliverables

The manufacturer received the complete platform fitted to this meter — source, records, procedures, no lock-in.

- Validation OS image with the full Yocto build system, HAB-signed boot recipes, and per-build SBOM.
- Board-specific BSP and HAL source for every subsystem, maintained against the design package into the production revision.
- Compiled client for the A-core plus the M7 FreeRTOS build.
- Server and dashboard as deployment-ready containers in the manufacturer's lab.
- Complete suites — accuracy, thermal, accumulation endurance, outage replay, NB-IoT burst, tamper — with recorded first-article baselines against the reference standard.
- Python SDK with documentation, example scripts, and CI integration gating every firmware candidate.
- The append-only, signed records store as client property — evidence for the notified body, the utility, and any future dispute.
- The independent validation report: the supercap leakage path, the NB-IoT rail coupling, the anti-alias BOM error, RTC drift data, metrics, pass/fail, coverage.
- Bench procedures for acceptance and re-runs; full documentation; no lock-in.

10

PRODUCT

Conclusion

A meter built for a fifteen-year life on a wall entered its utility pilot with its measurement chain independently proven and its worst defect — a backup domain that quietly died in nine days — already fixed in the production layout.

- The supercap leakage, the transmit-burst coupling into the analog domain, and the tolerance error in the anti-alias filter were all board-level faults no vendor datasheet or feature test would have caught; each cost a layout or BOM edit instead of territory-wide truck rolls and a billing-accuracy dispute.
- The suites gate every firmware drop in CI and the records store anchors the notified-body file, carrying to the production revision with only the HAL delta re-verified. We produce the evidence — the client's notified body and utility judge it.

II

PRODUCT

Lessons Learned

The engagement changed how we treat backup power domains and mixed-domain supplies on metering-class boards.

- Backup-domain endurance testing now starts on bench day one rather than in the environmental phase — the supercap defect needed nine days of wall-clock time to prove, and starting that clock late would have pushed the finding past the layout window; document review likewise now cross-checks every precision-path component tolerance between schematic and BOM, where this board's accuracy defect actually lived.
- On i.MX metering topologies the shared-interconnect path between the A-core and the M7's AFE traffic is a real hazard: eMMC bursts from the A-core measurably jittered AFE DMA completion until the path was pinned to TCM — isolating the metrology domain's memory traffic is now a standing design-review question before any metering engagement.

CONTACT

SiliconCentric

EMAIL sandesh@siliconcentric.com

PHONE (669) 356-1998

WEB https://www.siliconcentric.com

ADDRESS San Jose, CA, USA