PRODUCT

Portable Ultrasound

Healthcare Portable Ultrasound Zynq Ultrascale Mpsoc

SiliconCentric | Independent Verification & Validation

I

PRODUCT

Introduction

Our client is a medical-device company. Their product is a handheld ultrasound scanner built on a standalone AMD Xilinx Zynq UltraScale+ MPSoC: the Cortex-A53 application cluster runs imaging and UI, and the on-die RPU — a lockstep Cortex-R5 pair — acts as the companion controller for acquisition timing and battery safety. Their first-article boards had come back from fabrication, and their IEC 62304 development plan assumed the hardware worked, with no independent evidence that it did. We collaborated with them on this project by providing independent verification and validation of the board.

- Compute topology: a single MPSoC package; the A53 cluster plus programmable logic handle beamforming and image reconstruction, and the internal RPU runs the real-time acquisition and battery-supervision loops.
- Hardware under validation: a 128-element transducer interface, the analog front end and receive beamformer path through the programmable logic, the PLL clock tree feeding the AFE sampling clocks, 4 GB DDR4, eMMC, a battery gas gauge and charger on I2C, USB-C, Wi-Fi module on SDIO, and a 5-inch touch display.
- The client held fabricated first-article boards, powered once for a smoke test, with firmware development gated on hardware confidence.
- Independence mattered contractually: the design house that laid out the board could not credibly assess its own work, and we hold no technical, managerial, or financial stake in it.
- Scope was strictly bounded to independent validation — no feature development, no imaging-algorithm work, no product firmware authoring.
- We built everything from the hardware design package — schematics, ICDs, BOM — with no access to the client's firmware source.

2

PRODUCT

Hardware Topology

This is a standalone-SoC topology in which the application/companion split lives inside one package: A53 cores and FPGA fabric on one side, the lockstep RPU on the other, joined by on-chip memory and an inter-processor interrupt mailbox. The validation boundary enclosed the board and its envelope; the imaging application and any regulatory sign-off stayed outside.

- Topology classification: standalone MPSoC with internal RPU companion; APU–RPU interconnect is OCM shared memory with IPI mailboxes, plus a watchdog owned by the RPU.
- The RPU's job: sequence acquisition timing to the AFE, supervise the battery system, and hold a hard real-time deadline the Linux side is not trusted with.
- In-scope interfaces: the JESD-style AFE data lanes into the fabric, SPI (AFE control), I2C x2 (gas gauge, charger, touch, temperature sensors), DDR4, eMMC, SDIO, USB-C, MIPI-DSI.
- Envelope in scope: 10 °C to 40 °C ambient per IEC 60601 operating assumptions, a sealed handheld enclosure with no fan, and a 3.6 V single-cell battery system with hot-swap charging.
- Out of scope: imaging firmware, DICOM connectivity, and certification sign-off — we produce evidence for the client's IEC 62304/60601 case; their assessor and notified body judge it.
- The Zynq UltraScale+ family is one of the six architectures Polaris already runs on, so the OS baseline was inherited and effort went to this board's delta rather than silicon bring-up.

3

PRODUCT

Problem Statement

The boards existed, the imaging-firmware team had a committed start date, and the clinical-evaluation schedule was already promised to investors. The only proof of hardware health was device-level: the AFE vendor's characterization, the module vendor's numbers, Xilinx's silicon data. In a medical device, that gap is schedule risk and a design-history-file hole an auditor will find.

- Proven in isolation, never as a board: the AFE, the MPSoC, and the power system each had vendor reference data, but nothing had exercised this board's AFE lane routing into the fabric, its clock-tree distribution, its DDR4 topology, and its battery path together.
- Firmware coverage is feature-shaped, not board-shaped: the imaging team would drive the AFE, display, and DDR4 hard, but the USB-C data path, the second I2C bus, the charger's fault modes, and the RPU watchdog interactions sat outside every planned feature.
- No stress, no extremes, no duration: no soak at 40 °C in the sealed enclosure under continuous acquisition-equivalent load, no multi-day burn-in, no battery brown-out and hot-unplug campaign, no charge-cycle endurance — the conditions a handheld clinical device meets daily.
- Validation was penciled in as a pre-submission gate, meaning a marginal DDR4 channel would first appear as an image artifact in the firmware backlog, debugged by imaging engineers on a board they did not design.
- IEC 62304 requires documented, traceable integration evidence between hardware and software items; undocumented bench checks do not enter a design history file.
- Image quality depends directly on AFE sampling-clock jitter — a clock-tree problem here is a clinical-performance problem.
- The handheld thermal envelope was unproven: 12 W of compute in a sealed case that must stay within IEC 60601 surface-temperature limits.

PRODUCT

Customer Requirements

4

The client's requirements were direct: validate the whole board, under stated limits, with evidence formatted to survive a notified-body audit.

- Operating temperature: the board shall operate from 10 °C to 40 °C ambient. Enclosure surface temperature shall not exceed 43 °C at any point, per IEC 60601.
- Supply voltage: single-cell Li-ion, 3.6 V nominal, operating window 3.0 V to 4.2 V. The board shall survive input over-voltage up to 5.5 V on the USB-C input without damage; over-voltage protection shall trip at 5.5 V.
- Over-current: charge current shall not exceed 2.0 A; over-current protection shall trip at 2.5 A. Rail over-current on the 5 V and 3.3 V rails shall trip within 10 ms.
- Brown-out: the board shall shut down cleanly below 3.0 V cell voltage with no record loss and no memory corruption.
- Humidity: the board shall operate at 15% to 90% RH non-condensing and shall not be exposed beyond 90% RH.
- Full-board functional validation: all four A53 cores, both R5 cores in lockstep, the programmable logic paths, every DDR4 region, eMMC, the AFE control and data paths, both I2C buses, USB-C, SDIO, and the display — exercised as one integrated system.
- Coverage independent of firmware scope: every subsystem validated whether or not the imaging feature set touches it, through a HAL derived from the design package instead of the product firmware.
- Stress and environmental matrix: thermal sweep 10–40 °C with surface-temperature mapping, 120-hour endurance under sustained acquisition-equivalent load, battery brown-out and hot-unplug campaigns, charge-cycle endurance, and DDR4 margining at temperature.
- Continuous validation alongside firmware development: CI integration revalidating every firmware candidate on real boards throughout the program.
- Regulatory evidence: timestamped, operator-attributed, version-pinned records with bidirectional traceability, structured for direct inclusion in the design history file under IEC 62304 with IEC 60601 bench evidence.
- A web console the client's verification engineers can run after one afternoon of orientation, with a standardized bench procedure and setup measured in minutes.
- An immutable, append-only evidence store that becomes the qualification baseline for the next board revision.

PRODUCT

Architecture

The target board carries the validation OS, HAL, and client; an external x86 host carries the server, dashboard, and SDK. That split keeps test execution isolated from data processing and leaves the MPSoC's compute for behavior that resembles the field — necessary when the thing being measured is thermal load and memory bandwidth under realistic acquisition traffic.

- Polaris OS (the validation OS) — a reproducible Linux image for the MPSoC that boots to a known validation state, so the client's evidence never depends on a hand-configured board.
- HAL — the single board-specific layer; here it exercises the AFE control path, fabric data capture, DDR4, both I2C buses, the battery system, USB-C, SDIO, and display, and its uniform interface keeps the medical suites portable to the next board spin.
- Client — the lightweight on-target agent driving all tests through the HAL; gRPC on the Linux side, FlatBuffers to the FreeRTOS image on the RPU; three timestamps per event (origin, relay, server); light enough that thermal and bandwidth measurements reflect the product, not the tooling.
- Server — orchestration, scheduling, and the append-only records store on the x86 host, running three first-article boards in parallel and hosting the dashboard and API.
- Dashboard — the operator console: provision a board, configure and launch, watch live rail, temperature, and lane telemetry, review time series afterward; every state-changing action operator-attributed, which the quality team required for the design history file.
- Python SDK — automation and CI; scripts everything the console does; C/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 binding constraints were a sealed handheld thermal envelope, a battery-powered duty cycle with clinical charge patterns, sub-picosecond-class jitter sensitivity on the AFE clocks, and a documentation regime where every record may be audited years later.

- Validation OS design — read-only rootfs, A/B partitions with automatic rollback, and secure boot through the MPSoC's boot ROM chain, because an unbootable board inside a thermal soak wastes a day; the trade-off is a heavier image-update path, accepted. The RPU runs FreeRTOS in lockstep mode — Zephyr was considered and dropped because lockstep fault-injection hooks were already proven under FreeRTOS.
- HAL design — partitioned by subsystem with each function tied to a schematic sheet and ICD clause; AFE data capture is interrupt-and-DMA driven since polling would alias the jitter under test, while battery telemetry is polled at 1 Hz. A misbehaving AFE can storm the fabric interrupt lines, so storm detection and throttling are built in.
- Client design — origin timestamps taken at the fabric boundary so clock-anomaly records order correctly against thermal events; on battery-critical the client flushes records before the RPU forces shutdown, trading a 60 ms delay for zero evidence loss.
- Server design — three-timestamp causality lets a DDR4 correctable-error burst be ordered against the temperature ramp that provoked it; retention sized for 120-hour campaigns on three boards; records encrypted at rest because the quality system classifies them as device records.
- Dashboard design — surface temperatures, rail voltages, DDR4 error counters, and AFE lane status are first-class views, because that is what a medical verification engineer triages; run health and drop counts appear on every screen.
- SDK design — the client scripted the nightly acceptance gate and the charge-cycle matrix; a direct API path served quick single-peripheral checks at the bench, with the explicit trade-off that those runs produce no records.
- OS and HAL design was board-specific and heavily reworked; the four upper components were configured to this client's quality-system workflow while their structure and working style stayed constant.

7

PRODUCT

Implementation

Project work concentrated in the OS delta, the HAL built sheet-by-sheet from the design package, and the medical campaigns; the client, server, dashboard, and SDK stood up through configuration alone.

- Validation OS — Yocto image for the MPSoC: inherited BSP and boot chain (FSBL, ATF, U-Boot), board-specific device tree covering the AFE, gas gauge, charger, and display, kernel trimmed to validated drivers; OTA with A/B rollback; boot under 35 seconds including bitstream load; per-build SBOM with CVE tracking; the RPU FreeRTOS image built under the same tree.
- HAL — implemented subsystem by subsystem and bench-verified as written: memory-mapped control of the fabric capture blocks, DMA paths for AFE data, interrupt handlers for battery-fault lines, bus-timing work on both I2C segments. The design-package review surfaced an ICD conflict — the gas gauge and touch controller were both documented at I2C address 0x55 on the same bus — resolved before it could appear as an intermittent touch failure.
- Client — C++ daemon on Linux, event and polling paths into the HAL, hardware timestamping, graceful shutdown without record loss, gRPC upstream, FlatBuffers to the RPU.
- Server — telemetry receiver, versioned record schema, campaign scheduler, REST API, dashboard hosting, three-board parallelism, encrypted store.
- Dashboard — board provisioning, campaign configuration, live thermal and lane streaming, time-series review, PDF export shaped for design-history-file inclusion, operator attribution on every action.
- SDK — Python bindings, example scripts per subsystem, and CI wiring that fires the acceptance suite on each firmware candidate.
- Board-specific work: OS delta and HAL. Configuration work: client transport, server retention and encryption, dashboard views and export templates, SDK examples.

PRODUCT

Test - IV&V

Verification proceeded from the stack outward: prove the platform, prove the OS/HAL on this board, then run the board through one-shot, long-running, event-based, and monitoring campaigns — every dashboard-launched run landing in the append-only store.

- Stack self-verification: 100% test coverage of the client, server, dashboard, and Python SDK — the platform is proven before it produces evidence about anyone's board.
- OS/HAL verification: A/B boot and rollback exercised, OTA verified end to end, the secure boot chain checked on both accept and reject paths including a deliberately mis-signed bitstream.
- Bench setup: board cabled to the host, battery emulator and thermal chamber configured, provisioning from the dashboard — a documented, repeatable, sub-30-minute procedure.
- Functional campaign: AFE control and capture suites, per-lane data-integrity runs, DDR4 margin and error-counter suites, battery charge/discharge/fault suites, display and touch verification, USB-C and SDIO checks.
- Watchdog and fault-injection campaign: the RPU-owned watchdog exercised with induced A53 hangs, lockstep divergence injection on the R5 pair confirming detection and safe shutdown, charger and gas-gauge fault lines driven through every documented fault mode, and the APU–RPU boot-order and reset-ownership contract verified as its own suite.
- Debug posture: JTAG lockdown verified in the production-fused configuration — an open debug port on a device holding patient-adjacent records is a notified-body finding — with debug and trace retained on first articles to anchor the timing evidence.
- One-shot tests formed the acceptance gate: configure, execute, capture, one pass/fail per subsystem per candidate.
- Long-running: a 120-hour acquisition-equivalent soak with periodic snapshots exposed DDR4 correctable errors climbing above 52 °C die temperature, traced to a training-margin issue and resolved with a timing-parameter change and a respin note.
- Event-based: silent runs emitting records on thermal crossings, rail excursions, DDR4 error thresholds, and battery faults — this mode caught the main defect: AFE sampling-clock jitter rising past budget when the charger switched to fast-charge, a supply-coupling path from the charge pump into the clock-tree PLL that vendor data on any single device could not have shown.
- Monitoring: passive telemetry — surface and die temperatures, all rails, CPU and fabric load — alongside a representative acquisition workload supplied as a binary; surface temperature reached 2.3 °C over the IEC 60601 touch limit at 40 °C ambient, a finding that forced an enclosure and duty-cycle change.
- Instrumentation correlation: phase-noise-analyzer and oscilloscope captures anchored the jitter and charger 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: each requirement traced bidirectionally to its tests and records, schemas version-pinned, every run reproducible for the auditor.

9

PRODUCT

Deliverables

The client received the complete validation platform fitted to their board and silicon — full source, their records, no lock-in.

- Validation OS image with the full Yocto build system, boot-chain recipes, and per-build SBOM.
- Board-specific BSP and HAL source covering every peripheral, maintained against the design package and carried into the respin.
- Compiled client for the A53 cluster plus the RPU FreeRTOS build.
- Server and dashboard as deployment-ready containers configured for the client's quality-system bench.
- Complete suites — functional, thermal, endurance, battery, DDR4 margin, clock-integrity — with recorded first-article baselines.
- Python SDK with documentation, example scripts, and CI integration revalidating every firmware candidate on hardware.
- The append-only records store delivered as client property — design-history-file evidence in auditable form.
- The independent validation report: the charger-to-PLL coupling defect, the DDR4 margin finding, the surface-temperature exceedance, the I2C address conflict, metrics, pass/fail, coverage.
- Bench procedures for acceptance and re-runs; full documentation; no lock-in.

10

PRODUCT

Conclusion

The board's real defects — a clock tree that degraded under fast charge, a memory channel that erred when hot, an enclosure that ran over its surface-temperature limit — were found on the bench with instruments attached, not in clinical use. The respin absorbed all of them before the imaging team had written a line against the hardware.

- Four findings that would have surfaced as image-quality complaints and field returns were fixed in one planned revision, backed by assessor-ready records instead of internal assertion — months of misdirected imaging-firmware debugging avoided.
- The suites now run as the CI acceptance gate and the whole platform carries to the respin with only the HAL delta re-verified. The standing caveat holds — we produce the evidence; the client's assessor and notified body judge it.

II

PRODUCT

Lessons Learned

This engagement changed our sequencing for battery-powered medical boards: power-quality interactions and thermal mapping now precede functional depth.

- Charger and clock-tree interaction testing moves to the first bench week on any battery device with precision analog — the fast-charge jitter coupling was findable on day two with a phase-noise analyzer, and IEC 60601 surface-temperature mapping belongs in week one, not in the environmental phase.
- The MPSoC's OCM arbitration produced a real APU–RPU friction point: RPU deadline jitter appeared whenever the A53 cluster saturated DDR4, because OCM-resident RPU code still crossed the shared interconnect for peripheral access — the fix (dedicated LPD peripherals for the RPU) is now a standing design-review question we ask before any Zynq UltraScale+ engagement.

CONTACT

SiliconCentric

EMAIL sandesh@siliconcentric.com

PHONE (669) 356-1998

WEB https://www.siliconcentric.com

ADDRESS San Jose, CA, USA