

What to collect before you take over a Qorvo-based product

Collect these items from the outgoing team in the first month of a takeover. Each one protects your ability to patch, test, certify and ship the product that is already in the field.

☐ 1 Source and history

Full repositories, tags for every shipped version, branching rules

Why: fixes must start from the exact code in the field

☐ 2 Build

Toolchain versions, build scripts, container images, reproducibility notes

Why: an unreproducible build is an unpatchable product

☐ 3 Vendor software

SDK versions, patches applied to vendor code, binary libraries with versions and hashes

Why: binary components can only be updated by their vendor

☐ 4 Licences

SDK and stack licences, open-source obligations

Why: some licences restrict where code may be used or require source disclosure

☐ 5 Security

Signing keys and their custody, secure boot configuration, OTA infrastructure

Why: lost keys can make a field fleet unupdatable

☐ **6 Manufacturing**

Production test scripts, calibration procedures and stored values: antenna delay, crystal trim, TX power

Why: calibration knowledge is often undocumented and person-dependent

☐ **7 Test assets**

Test plans, HIL benches, phone and anchor matrices, sniffer captures

Why: regressions surface only on real radio set-ups

☐ **8 Certification**

FiRa, CSA, Bluetooth and CE/RED records, including declarations and test reports

Why: re-test rules depend on what was certified

☐ **9 Field data**

Crash logs, telemetry, open customer issues

Why: the real backlog is usually in the field

☐ **10 Compliance**

SBOM, vulnerability disclosure policy, support period per product

Why: CRA obligations continue through the handover

Signs of a healthy takeover: track them from day one

- Time to reproduce the shipped build
- Share of test cases automated and running on hardware
- Time from a field report to a triaged issue
- Age of open vulnerabilities in the SBOM
- Release cadence against the agreed calendar