Hardware and IoT test scoping questions

These are the questions a SilentGrid consultant asks when scoping a hardware and IoT security test. Answering them first makes the call shorter and the quote more accurate.

"Not sure" is a fine answer. Working out the unknowns is part of what the scoping call is for.

Questions marked **Sizing** help us prepare an accurate quote.

01 Before any test

What prompted the test, and what date does the result need to meet?

Why we ask: the reason sets the depth and report format, and the date fixes the testing window and any retest.

Will testing run against production, staging or a dedicated test copy?

Why we ask: production needs tighter limits on load, data and timing. A test copy allows more thorough techniques.

When can testing run, and are there change freezes or peak periods to avoid?

Why we ask: the schedule is built around them.

Will you want fixes retested?

Why we ask: retesting is agreed at scoping, so it is scheduled and priced from the start.

02 Hardware and IoT

How many device models or hardware revisions are in scope?

SIZING

Why we ask: each model has its own board, firmware and interfaces.

How many units can you supply, and can they be opened, desoldered or damaged?

Why we ask: firmware extraction can destroy a board, so spare units may be needed.

Which interfaces does it have: debug ports (UART, JTAG, SWD), USB, Bluetooth, Zigbee, cellular?

Why we ask: each port and radio adds its own test cases.

Are firmware images, update packages or schematics available?

Why we ask: they save extraction time and allow deeper analysis.

Are the companion app and cloud platform in scope?

Why we ask: the device is often the way into the backend that trusts it.

Where are the devices deployed: homes, hospitals, industrial sites?

Why we ask: it sets the threat model, including how much physical access an attacker is assumed to have.

Discuss your testing priorities

www.silentgrid.com/contact