Design and test strategy for IoT connectivity challenges

Patrick Mannion - October 30, 2017

A recent survey of nearly 600 designers interested in IoT design showed that the number one struggle they have is with connectivity. That doesn’t mean security isn’t a concern, it just may not be as troublesome to implement, once they get around to it.

A survey of 600 designers interested in IoT showed that connectivity is their biggest struggle. (Image source: EETimes).

As the recent call-to-action by Arm Technology’s CEO Simon Segar indicates, security is in large part a matter of everyone agreeing to do it in the first place. This idea led to his introduction of a Security Manifesto and the concept of a Digital Social Contract to help align the industry toward a common good, for users and for the IoT to progress to 1 trillion devices.

Getting to an acceptable baseline level of security is necessary and hard, but doable, with some attention up front and the willingness to do it. So why do designers struggle with connectivity? And how can that struggle be mitigated? The answer is a better appreciation and understanding of RF design and test.

In a conversation I had with James Park, the founder of Fitbit, he mentioned how the design of the original Fitbit got delayed for many months because the team determined they could design the RF portion themselves. They might have gotten it, eventually, but after three months, they gave in and asked for outside help. Apparently it boiled down to interference between the RF (Bluetooth) and digital circuitry that was solved with a revised layout. They got outside help, and the rest is history.
However, the problem remains: designing is fun, until testing begins, then the rubber hits the proverbial road. Software debug takes increasingly larger portions of design and development time, which puts pressure on test. However, giving short shrift to test, especially with respect to RF, can result in last-minute problems that can kill a production schedule.

**Solving for connectivity design and test best practices**

In his years at Rohde & Schwarz, Ak Emarievbe, co-founder and CEO of Belvor Technical Resources, has seen the problems designers get into on a daily basis. “The first thing designers need to understand are the needs of the device and application ranging from power requirements, coverage, data rates, mobility, delay time to mention but a few and then choose carefully from the many wireless options,” he said. These range from Bluetooth, Zigbee and Wi-Fi, to LoRaWAN and Sigfox for unlicensed-band wide-area coverage, and NB-IoT and LTE Cat M1 for licensed-band operation, also for wide-area IoT coverage.

The right radio access technology and RF design will ensure power consumption is minimized, and that there isn’t unnecessary RF power output, while ensuring the device is operable in all the target markets.

This latter point is critical, as many designers ultimately hope for high-volume, global market acceptance and success. This affects not only the type of interface, but also how it is designed in. The temptation may be to go with a chip-on-board design, especially where space is tight, but as Emarievbe points out, that slows down a design and increases overall cost of testing where a module might have been a better choice. Choosing which way to go requires analysis of the design’s form factor requirements, expected volumes, and time to test. A module will invariably have been tested to the required standard (i.e. Bluetooth) and also in most cases might have been FCC or ETSI certified for regulatory compliance.

“Often that’s not enough,” said Emarievbe. “Designs need to meet carriers’ [wireless operators] network requirements too.”

Like security, test is often an afterthought, and that’s where designers and schedules get burned. Emarievbe said that designers need to pay more attention to the design of the test bed, selecting the right equipment and test plans to match the application, and consider better all the test equipment sourcing options, such as lease versus buy versus rent to own. “Then there’s high-volume manufacturing; it has to be designed for manufacturability to make sure of even simple things such as the boards and antennas being on right and calibrated, with overall functionality verified before being shipped off to an end user.”

To help with these decisions and ensure an IoT design gets through the test phase as efficiently as possible, Emarievbe is giving a solid 3-hour course over three days on November 7, 8, and 9th, from 9 am to 10 am (PST).

Given as part of the EETimes University Series, the course is titled, “**Inside IoT - How to Defeat Wireless Device Test and Certification Challenges**,” and will address the major challenges and how to reduce test time and cost for any wirelessly connected device.

By the end of the course, designers will know:
The main wireless connectivity options and their design and test implications.

Why choosing pre-certified modules is helpful, but it's just the beginning of meeting standards, certification, and regulatory requirements.

What, exactly, are those requirements.

What to expect and how to plan accordingly so a product gets through design and test, on time and within budget.

Emarievbe has helped designers through the process, from design considerations, to test-bed development and strategies, compliance/certification through to high volume manufacturing test. “I know how hard it can be, but I also know how to address the design, test, and certification issues, where to go, what questions need to be asked, and who to talk to for a manufacturing solution.”

Seems to be a good fit for what ails us now. Note that the course is interactive, so you can ask questions live, or even get started here, in the comments section below.

—Engineer Patrick Mannion manages EE Times University. In a previous life, he was an editor and publisher on EE Times and brand director for EDN. He continues to write for EDN and Electronic Products, in addition to globetrotting for AspenCore and appearing in buzz package videos.

Related articles:

- IoT: We aren’t as ready as we think
- Designing IoT: Devices and Local Networks
- Which IoT protocol should you use for your design?
- IoT May Need Sub-50-Cent SoCs
- ARM CEO Sounds Security Alarm