DIGI FIELD GUIDE:

FIVE TIPS TO IMPROVE YOUR IOT DESIGNS

DIGI FIELD GUIDE: FIVE TIPS TO IMPROVE YOUR IOT DESIGNS

The Internet of Things (IoT) has evolved from a marketing buzzword to a strategic roadmap for many OEMs and technology companies. As a result of this shift, companies with expertise in devices like sensors, lights, pumps, or even home appliances are now being asked to quickly become experts in wireless and cellular connectivity. No matter how brilliant the engineering team is, the challenge of getting immersed in new technologies is sure to create a few bumps in the road.

As this disruptive new marketplace rapidly takes shape, many companies are simultaneously striving to achieve contradictory goals: being first to market and having the lowest-cost solution. This is leading many firms to create solutions with little attention to crucial factors such as total recurring engineering cost and adaptability to new technologies; while still omitting critical features in the final product.

Digi remains focused on connectivity technology, where we have been a leader for over 30 years. We work with customers every day to overcome the challenges they face in bringing to market new and innovative wireless products and solutions. We understand the challenges and mistakes that can arise and how best to anticipate and avoid them.

This field guide provides an overview of five ways to improve the design of your wireless IoT product, get to market faster, and increase the reliability of your solution. While this document focuses on the unique challenges of cellular technology, the concepts apply to any wireless technology (e.g. LTE-M, NB-IoT, Bluetooth Mesh, or ZigBee, for example).

Tip No. 1

THINK ABOUT SECURITY FIRST

As the number of IoT devices continues to grow exponentially, you need to make security a top priority for virtually any application – particularly if you're transmitting sensitive data. The troubling fact is, an estimated 70 percent of IoT devices are vulnerable to attack, so it is essential for developers to factor in this critical requirement from the beginning.

> Be sure to encrypt everything – even the data that's not sensitive.

Be sure to encrypt everything – even the data that's not sensitive.
Most companies today have or are implementing policies requiring all data that is transmitted over the air to be encrypted – regardless of how sensitive the data is. Even something as benign as the data from a water-tank sensor must be encrypted in order for an IT director to permit your product to be on their network. Nothing ends a sales meeting faster than an IT director saying they won't use your product because it is not secure.

Pre-configure your device to be secure.
The days of shipping a wireless device with a default ID and password (think: "admin/admin") are over. It's not enough to merely provide the user with all the tools needed to secure the device and encrypt the data. After all, if they fail to follow through, a security breach will still mean you could face unfavorable publicity or even legal liability. Make sure your product has out-of-the-box security – or force users to set proper passwords and encryption before they can use or deploy the product.

For a comprehensive overview of how to secure your device for your application, download your copy of "IoT Device Security Built-In, Not Bolt-On."

Tip No. 2

DESIGN FOR TODAY – AND TOMORROW

Companies are pushing hard to be first to offer IoT solutions in their respective markets. That emphasis on time-to-market oftentimes leads to some short-term design decisions with a narrower technology focus. While this may get you to market faster, it ignores the hard reality that wireless technologies, customer needs, and market dynamics are always changing.

For instance, if you choose cellular technology as your wireless standard for a new product, what happens when a large customer says they don't want cellular – it needs to be unlicensed bands, sub-GHz, or ZigBee? What if your competitors start implementing a new connectivity technology – can you transition quickly to catch up? No one can exactly predict what the future may bring, which is why it's essential to design in the flexibility to adapt.

A single-technology focus encourages engineers to design solutions (think boards and drivers) around one specific module and firmware interface. But when a new technology emerges, it usually requires a painful cycle of hardware and firmware redesign that can, in many cases, require the same time and cost as an original design starting from scratch.

The better technique: a modular design approach that supports multiple wireless technologies in the same footprint with a common command set and driver. This makes your solution more agile and adaptable to new wireless technologies.

Tip No. 3

DON'T FORGET REMOTE MANAGEMENT

Over-the-air and over-the-network firmware updates are commonplace in consumer electronics, and savvy technology companies understand a remote communication device must support OTA firmware updates to be considered secure. For instance, think of the smartphones, laptops, and tablets that constantly receive updates for new features, bug fixes, and security patches. Make sure your remote devices are backed by a solid infrastructure for executing over-the-air updates of the firmware on the communication interface.

This enables you to immediately address inevitable security vulnerabilities that virtually every product experiences over time. Without a cost-effective way to update these devices remotely, you could spend months or years with truck rolls and technician visits to every site. For instance, the Wi-Fi WPA2 vulnerability KRACK made many Wi-Fi devices using WPA2 insecure unless a firmware patch was applied. Remediating that vulnerability would be a costly headache without an infrastructure for remote updates.

Make sure your vendor has a remote-management platform for its products – and be sure that platform is highly secure. The annual cost of a remote-management solution is typically less than even a single truck roll to a remote site, so the ROI on these platforms is easy to justify.

Tip No. 4

GET SMART ABOUT CERTIFICATIONS

Whether it is FCC, CE, IC, or cellular carrier certifications, any new wireless product undergoes multiple certifications – which can create cost and schedule challenges because as many as 80 percent fail cellular certification on the first attempt. Radiated emissions, poor receive sensitivity, lack of support for key features, or poor antenna design are just a few of the hundreds of reasons products fall short. These failures can cripple a product schedule and decimate budgets. It's not uncommon for a certification failure to require a hardware redesign that can take six months or more.

Vendors often view certifications as a one-time cost, not realizing that every entry into a new geographic region can lead to significant design changes or even new wireless technologies to meet new certification or re-certification requirements. Even if you make no changes, certification bodies may change their standards that require you to re-certify your entire product line. For example, the Radio Equipment Directive (RED) in 2016, required almost every vendor selling a product in Europe to undergo some level of re-certification effort.

Purchasing a pre-certified module can eliminate many of the headaches associated with wireless certifications for the FCC, Industry Canada (IC), and CE Mark in Europe. When deploying a cellular solution, look for a module that is end-device certified. This eliminates the need to undergo a cellular certification process. A cellular module that is only listed as modular-certified does not eliminate the carrier certification process. If you implement a modular-certified device, you must still go through PTCRB, AT&T, and Verizon certifications, and you may need to repeat those processes with every new product variation or significant firmware change – or if your vendor changes the firmware on their module. Early in your design process, get answers to these key questions:

- Will this new product require a certification you've never done before?
- Will this product be sold across multiple countries or regions now or in the future?
- Do you lack the necessary expertise on staff to manage certification requirements for multiple countries?

If the answer to any of these is "yes," a pre-certified module or off-the-shelf gateway from a company with experience in global certifications can greatly simplify the design process and shorten your time to market.

Tip No. 5

CHOOSE A TECHNOLOGY PARTNER, NOT JUST A COMPONENT

In both the short- and long-term, the wireless gateway, module, or chipset you choose becomes a key component in your product. That's why it is critical to base your buying decision on more than what is on the data sheet or in the price quote. In many ways, your selection process extends beyond the component to include the vendor that stands behind the component. View your supplier as a partner, not a vendor. Some critical questions to ask before choosing a partner:

Will my partner be here in two years?
Beware of startups jumping onto the IoT bandwagon; as many as 60-90 percent of tech startups fail. You don't want to choose an IoT startup as your technology partner, only to subsequently find yourself on your own with no support and no options for future products.

Does my partner care about me?
No matter what you hear in a sales meeting, many module vendors focus only on very large deals. If you don't fit into their sweet spot, you might be waiting days for responses to simple support questions. The average command specification for a cellular module is 300-500 pages long, so you and your engineering team will have questions. Will you get the responses quickly enough to stay on schedule?

Does my partner have a wide range of product options or are they focused on only one thing?
A technology company focused on cellular may fit your needs today, but what happens when your customers need something different – like unlicensed bands, sub-GHz, or ZigBee? If your partner doesn't have technology breadth, you'll almost certainly incur a costly and lengthy redesign effort at some point. A good wireless partner is technology-agnostic and can help you with the technology that best fits your market and your customers, and not try to push you into one standard to win a sales contract.

Furthermore, a design services partner should deliver world class service that can support at any level or fill in any gap on your team whether it's coding software, designing electronics and PCBs, securing industry and government certifications, building and testing for security, optimizing for thermal and mechanical dynamics, designing for test and manufacturing - and the list goes on. It's critical to understand if your partner specializes in just one or two of these areas, or are they able to support you throughout the product lifecycle and ensure your project is a success.

SUMMARY

The IoT and wireless technology represent a massive market opportunity – but also extensive challenges for engineering teams tasked with designing next-generation products. Making the correct design decisions and taking a long-term view of your product and technology roadmap early in the design process will position you for success today and tomorrow.

Digi has the products, platforms, services, and expertise to fit your requirements no matter where you are in your design cycle. To reach out to an IoT expert today, please contact us.

Contact a Digi expert and get started today

PH: 877-912-3444
www.digi.com

Digi International
9350 Excelsior Blvd.
Suite 700
Hopkins, MN 55343

Digi International - Japan
+81-3-5428-0261

Digi International - Singapore
+65-6213-5380

Digi International - China
+88-21-5049-2199

Digi International - Germany
+49-89-540-428-0

/digi.international @DigiDotCom /digi-international

While every reasonable effort has been made to ensure that this information is accurate, complete, and up-to-date, all information is provided "AS IS" without warranty of any kind. We disclaim liability for any reliance on this information. All registered trademarks or trademarks are property of their respective owners.