The Connectivity Iceberg:

9 Hidden Costs That Can Sink Your IoT Ambitions

SORACOM
soracom.io

NEURONIC WORKS
neuronicworks.com

IoT Design and Connectivity

The Internet of Things (IoT) has revolutionized the way we interact with everyday objects and devices, creating new opportunities for businesses across industries.

NeuronicWorks, a product design and manufacturing company based in Toronto, Ontario, works alongside world-class connectivity partners like Soracom to provide cutting-edge IoT designs that meet today's reality and tomorrow's vision. Our team has a deep understanding of the latest technologies and trends in the IoT space, allowing us to create cutting-edge products that are human-centric, functional, reliable, sustainable, energy efficient, and recyclable.

In this eBook, Soracom clearly identifies some of the common hidden costs one might encounter while launching an IoT project. From the intricacies of product design and manufacturing to connectivity, encryption, and product maintenance, this eBook provides a comprehensive guide for anyone interested in learning about the total cost of ownership (TCO) of an IoT project. Whether you're a business owner looking to create a new product, or an individual interested in the latest trends in IoT, this eBook is an invaluable resource.

NeuronicWorks Inc.

Introduction

In business, as in life, it is always best to approach a new opportunity prepared. Launching an IoT project without a firm understanding of the risks and challenges involved in getting your deployment off the ground could see even the most creative innovations crash and burn.

Product Managers need to get a handle on any potential costs that may come their way before they start a project. Yet, while some expenses may seem obvious to even the most inexperienced entrepreneurs, the truth is that these costs are only the tip of the iceberg. You may have a fleet of devices ready to enter the field, but have you considered how you will manage these devices' lifecycles? Will you need to bring on engineers to maintain or scale your project? Will your devices need to cross international borders?

This eBook will help you socialize the total cost of ownership (TCO) of an IoT project, including some of the hidden costs you may not have previously considered. With our help, you should be able to bring your deployment to market while avoiding the TCO iceberg.

Contents

If you think you're ready to deploy a fleet of IoT devices, first be sure you can answer these 9 questions before you go to market.

How Are You Handling Your Hardware Needs?

At the most basic level, you will need a handle on the IoT devices that will make up your fleet. As IoT sensors, dev boards, and other equipment become more affordable, the question of whether or not to bring hardware development in-house or to utilize third-party vendors is one developer will need to tackle early on.

Though costs will vary pretty wildly depending on the functionality and complexity of the devices, custom hardware development can eat up as much as 80% of an IoT project's budget and can take anywhere from several months to several years to yield a working solution.

There are Five Major Stages of Hardware Development:

Preliminary Analysis

This stage aims to determine a Minimum Viable Product from which you can build your ultimate product. This means defining the core functionality, the scope of initial deployment, and establishing a budget, among other considerations. It also means getting buy-in from company stakeholders and system engineers.

Design

Now that you have established a game plan, it's time to figure out how you can make it happen. This means plotting systems and housings that fit your core functionality and use case, as well as a microcontroller that can enable these components to work together.

Prototyping

Once the design has been laid out, you must create a working version of your device. This could involve the fabrication of components, coding of software, and all manner of development, depending on the solution. Even well-thought-out products should anticipate creating several iterations before reaching a viable product.

Testing

Once you have a finished prototype, it's important to test it - and not only for its core functionality in a laboratory environment. Developers will want to test their devices in different environmental conditions, run the device for an extended period of time to test its power demands, analyze the integrity of the housing, etc.

Manufacturing

Once you have arrived at a viable version of the device, you can send it out for mass production. Whether you have the resources for such an effort or are sending your plans to a manufacturer, this can be a lengthy process.

Each stage offers potential pitfalls and rabbit holes that could eat up your budget, so newcomers to the process may want to find a design partner who can lead them through this stage of development in the most efficient manner.

The challenges don't end once your device is designed and ready to be deployed, either. You'll also need to provide unique credentials and certificates for every device in your fleet and manage each one. This is an ongoing process for IoT projects, as keys may need to be rotated from time to time.

You could manage this through a device management system using an over-the-air update mechanism or utilize the device's IoT SIM card as an authentication token. This allows smart connectivity solutions to do the heavy lifting for your cloud while providing advanced security when used as a root of trust.

2 What About Software?

Of course, hardware is only as good as the software that it utilizes, and there are many considerations you will want to get in front of before launching your IoT project.

The first thing that likely comes to mind is cost, and much of that will be wrapped up in your device's Firmware. If you are able to bring firmware development in-house, coding the software will be a considerable focus of your engineering team - as will testing it. This could mean taking on new personnel for coding or QA and potentially even project managers.

You'll want to be intentional about software design as well. Architecting your system to integrate firmware over-the-air updates (FOTA), for example, will make remote installation of new features, patches, and updates simpler but will involve recurring costs typically taken on by your IoT platform of choice.

Keeping your back end device-side can get pricey, so most deployments offload the real heavy lifting to the cloud. Yet cloud integration comes with its own set of costs. Will you develop your own server application, or will you rely upon established services like AWS or Azure? If you're using Cloud on your back end, you will need transport layer security on each device as well as an encryption resource. This means designing your device with enough memory to process encryptions, as well as a battery big enough to support this function.

Battery life should be a central consideration in the design phase, with engineers needing to find ways to get the most out of fairly small batteries. This can be as simple as balancing functions with sleep modes during periods of inactivity to technological solutions like energy harvesting.

Most IoT devices also lack sufficient security measures, boasting factory default passwords and out-of-date or otherwise unpatched software. Though some countries have begun introducing legislation to address this issue, anyone designing their own IoT deployment will want to consider utilizing more secure software practices.

Of course, this all presupposes that you have access to an engineering team. This brings to mind the next question.

Energy Harvesting

Methods for harvesting energy from the external environment include:

- Thermoelectric conversion
- Solar power
- Wind energy harvesting
- Radio frequency signals
- Vibrational excitation

Energy harvesting can obviate the need for battery replacements, making it a great way to manage TCO.

3

Can You Afford Your Own Engineering Team?

Hiring your own engineering team can be costly, with just the salary of an IoT Solutions Engineer averaging around $100,000 USD.[1] When trying to understand the total cost of ownership for your organization as a whole, you will have to weigh the value added by having an in-house engineering team versus the potential return on investment.

Engineers are an essential part of any IoT deployment, so it's important to understand what they do before making a decision to outsource your development. Some of the responsibilities entrusted to IoT engineers include:

- Designing your deployment to meet end goals
- Creating and developing devices, sensors, and software
- Designing, coding, and testing new features
- Updating and patching software as needed
- Correcting issues with UX, network connectivity, and platforms
- And more.

While there is no reason these things could not be addressed by a third-party organization, maintaining an in-house engineering group could expedite the process. With an external team, you must set expectations, boundaries, and timetables but are still at the mercy of another group's schedule and capabilities.

[1] IoT Solutions Engineer Salary, Comparably.Com, retrieved 2 December 2022

By bringing this function into your organization, you have more control over the workflow process, and prioritization of tasks, as well as the capabilities of the individual engineers brought into the project. This can be make-or-break for an IoT project, as speed-to-market is a major concern for any organization.

Bringing your engineering resources in-house also offers you the ability to proscribe the specific skill sets that will comprise your development team. If you are building an application off of Raspberry Pis, for example, finding an engineer with expertise in Python means your team can more nimbly work through the device's main programming language.

Of course, this decision is largely contingent upon a firm understanding of what your engineering needs will entail. How often will you require software updates? Will you offload provisioning and credential management to a smart connectivity provider? Do you have plans for expansions? Further iterations of your application?

Getting ahead of these questions informs whether or not an in-house engineering team is a worthwhile investment for your application.

4 Do You Have a Plan to Maximize Battery Life?

Of course, one of the key goals behind preventative maintenance is to avoid the costly downtime associated with a device losing power. Between the loss of functionality, the cost of staffing to replace the battery, and the equipment charges themselves, battery-related downtime can be expensive. To this end, it's also wise for project architects to get the most out of the battery life for each and every device in the field.

Though you can anticipate that a device's designed functionality will be the largest drain on its battery's power, there are a number of more subtle factors that could be sapping its energy. Atmospheric conditions, for example, could impact a battery's performance. Everything from the ambient temperature to the moisture levels to even the electromagnetic traffic within an area can affect the power demands and constitution of the battery.

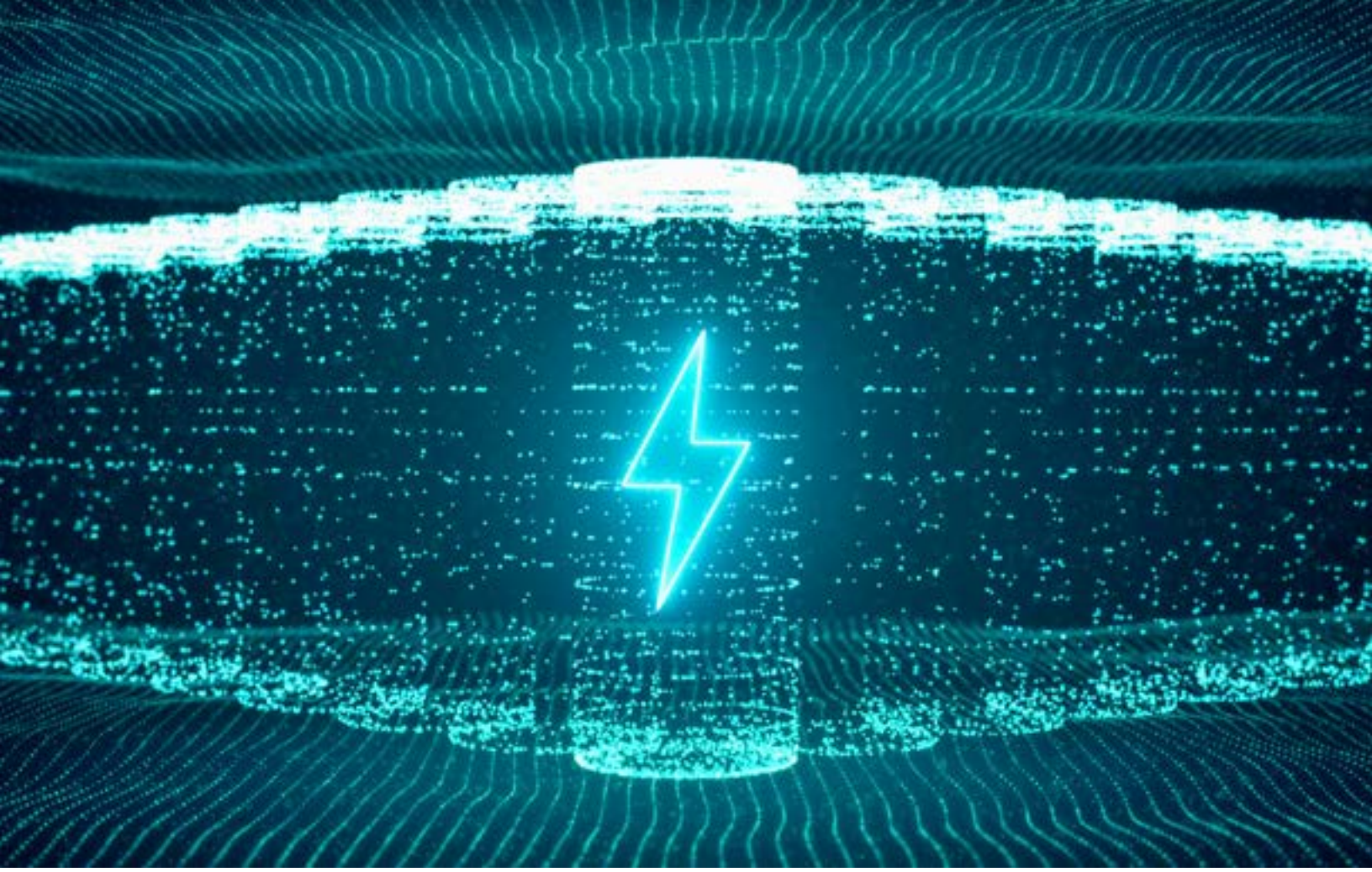
This is to say nothing of the unseen energy drains in your device's day-to-day operation. Say an unexpected information packet comes in while the device is in standby or sleep mode. When a device is interrupted during a sleep cycle, it must power on and utilize the battery to perform its function, switching out of a rest pattern and using more energy than had been planned.

In this above scenario, a smart connectivity provider can provide a secure private network between your devices and the backend to avoid this unwanted interruption, but there are many ways to architect your IoT system to maximize your device's battery life. These include:

Choose the Best Connectivity Technology
Once you know your project parameters, explore whether low-power connectivity solutions like LPWAN may be sufficient for your data transmissions.

Test Your Batteries Outside of the Lab
Though you may test your devices in a secure environment, that may not be indicative of how they will perform under real-world conditions. Before you scale, test your batteries for signal integrity and power consumption in your actual deployment location.

Manage Device Status
Devices that require infrequent data collection and uploads should be placed into standby or sleep mode when not in active use.



Control the Size of Data Packets

Managing the size and frequency of data packets can help ensure consistent and more easily managed power consumption. If your application allows, ensuring that data is only transferred when it meets your size or complexity requirements (and not before) could help prolong battery life.

Define Essential Processes

Ensure that only essential processes are a part of your operation. Disabling peripherals or turning off geo-location services when not in use, for example, can reduce staring on a battery.

The power demands of a project are multifaceted, so understanding the demands of your battery will help you streamline your operation to maximize its output.

5 How are You Managing Product Lifecycle?

Once you have actually launched your IoT solutions in the field, how do you plan to keep those devices running? What is your strategy for replacing or retiring older assets? How do you plan to roll out updates and patches? The product lifecycle is full of potential pitfalls and hidden costs, so it's important to understand what precisely you should be mindful of before you get started.

Provisioning

At the beginning of a product's lifecycle, the device needs to be able to establish stable and secure connections to your network and IoT platform. From this platform, you will need to manage the authentication process for connected devices to ensure secure and steady uptime while denying any unwanted intrusions. This is a key point for securing your network from data theft, DoS attacks, and more.

Configuration

Establishing data collection links and introducing basic configuration procedures will be obstacles unique to each and every deployment, but some things are fairly universal. You will want to account for remote access for controlling and monitoring your fleet once it's in the field. You likely need to set up both device- and group-specific controls as well. Understanding the needs of your deployment and devices is paramount to proper configuration.

Deployment

Managing the logistics of shipping and deploying a product is a multifaceted challenge. In addition to tariffs, shipping demands, and other complications that could arise from this early stage, there are power and connectivity considerations to be made before the devices even reach their final destination. Questions such as "Will your product be able to ship in standby mode, or must it remain active?"

Maintenance

Being able to remotely monitor devices in the field allows for predictive and preventative maintenance of your deployment, as well as issue upgrades and patches as needed. Planning for remote access could save considerable manhours by eliminating the need to send teams into the field for a malfunctioning device and can prevent costly downtime.

Decommissioning/Deactivating Devices

Occasionally, a device will outlive its usefulness and need to be retired or replaced. Do you have a plan for recycling or re-using your devices? If you opt for battery-powered devices, do you have a proper disposal plan for the discarded batteries? Do you have easy access to replacements?

One example of a hidden cost that IoT developers may face is the potential to be charged for devices that may not even be in use.
Depending on the deployment, some devices may not be required at certain times (eg, seasonal equipment cycles or devices in transit), yet without updating the status of the SIM within these devices, they can incur regular charges. By working with a smart connectivity provider, however, users can instead suspend the SIMs during these periods, only reactivating them when they are needed.

6 What is Your Plan For Maintenance/Support?

Once your devices have gone afield, you will need a strategy to help support those deployed assets and keep them running. There is any number of potential issues that could arise to help shift the TCO of your deployment away from profitability, so you'll want to be sure that the connected devices can be remotely accessed from the central IoT platform.

Remote access can allow users to monitor their devices in individual and group settings, enabling them to better track performance, anticipate issues, and address problems as they appear. Reports indicate that IoT-empowered predictive maintenance can reduce the maintenance costs of industrial deployments by upwards of 40 percent, reduce equipment downtime by up to 50 percent and reduce equipment capital investment by 3-5% by extending the useful life of machinery[2].

This monitoring will allow you to stay on top of elements of the device's performance, battery life, and any atmospheric conditions that may put the device at risk of damage or otherwise impact its performance. When combined with modern AI technologies, the data drawn from this monitoring can also help anticipate wear and tear on the physical device or power events that could impact your fleet.

AI Empowered Predictive Maintenance

AI can quickly compare current status readings to historical data to gain essential insights for improved performance.

Say your devices are using more data than you had planned for. By looking into communication over the cellular link, users can analyze packets being sent and received by their devices. This can allow users to review the procedures and processes to assess where the issues lie and what needs to be changed or updated to suspend unnecessary communication. This can allow them to deduce whether the problem can be addressed with firmware updates or if the configuration needs to be reworked.

Depending on the deployment, you will also likely need to plan for ongoing support of your fleet. IoT devices, by and large, are created with inadequate security measures, making patching and updates a necessity to protect data. Will you have the infrastructure in place to make these updates remotely, or will you need to manually update each individual device in the network? Waiting around until a problem arises only creates more issues (and costs), so plotting ahead is the best solution.

[2] Unlocking the Potential of the Internet of Things, McKinsey Digital, June 2015

7

Do You Need Global Connectivity?

A firm understanding of your IoT deployment will include an appreciation for the boundaries to which your connected devices will need to adhere or traverse. Will your devices be confined to a proscribed area within a controlled environment, or will your aspirations take your devices beyond regional and national borders? Some organizations may require truly global connectivity to operate effectively, and though it is certainly an attractive option to be able to transmit to and from the cloud wherever you may go, it can be a costly endeavor.

It can be a challenge to find a single mobile network operator (MNO) that can accommodate global connectivity. This could mean that an organization will be forced to rely upon the services of multiple MNOs simultaneously, something that comes with several challenges on its own.

Central to these challenges is the logistical conundrum that comes from managing multiple contracts, multiple service terms, multiple pricing structures, and potentially even carriers in multiple regions. It's also likely that spreading your connectivity across multiple carriers carries additional costs, as volume discounts are less likely when the data is spread out.

The solution here is simple - find a connectivity partner with access to multiple carriers that can give customized rates across multiple regions. This obviates the inefficiencies of juggling multiple contracts and provides you with more flexibility to bargain with potential carriers. Finding a connectivity partner that offers plans with no commitment and pay-as-you-go pricing can help manage the total cost of ownership of your operation.

You'll also want to seek out a carrier with contingencies that can protect your solution from downtime. A good partner will foster connectivity across multiple carriers, meaning when one goes down, another will take its place to help ensure consistent connectivity for your deployment.

Even if global connectivity is not needed in the short term, are there plans for your deployment to scale in the coming months/years? It may be worth speaking with a potential connectivity partner about their global connectivity options just in case, lest you miss out on an opportunity while seeking out a more comprehensive provider.

Global Connectivity Requires Global Security

Sending devices afield across international borders opens up a world of opportunities for incursions or device theft. Multilayered security and real-time monitoring of both devices and the network can be implemented during the design stage and provide a more comprehensive defense against would-be attacks.

8

How Will You Encrypt the Data You Produce?

A 2020 report found that 98% of all IoT device traffic is unencrypted[3]. Though organizations like AWS have attempted to mitigate this through managed keys that provide base-level encryption, data security is something that should be at front of mind for any project getting off the ground.

Due to their lack of computational power, size limitations, and the cost of components, most commercially available IoT devices are shipped with insufficient protections. That can mean anything from default passwords to weak authentication protocols, to insecure string-handling functions. It also means the organizations behind IoT projects will need to look to enhanced security measures if they truly hope to keep their data from falling into the wrong hands.

To this end, data encryption is essential to maintaining the integrity of an IoT network. Properly done, encryption ensures that data can only be accessed by those with the appropriate permissions and keys by making said data undecipherable to anyone without the required permissions.

[3] 2020 Unit 42 IoT Threat Report, Unit 42, March 2020

There are varying levels of encryption, with some of the most popular forms being:

Triple Data Encryption Standard (DES)

An evolution of the traditional DES, this utilizes 3 56-bit keys to secure networks.

RSA

An asymmetric encryption that utilizes a public key to encrypt the data and a private one to decrypt it.

Blowfish

This symmetric cipher splits data into separate 64-bit blocks and encrypts each one individually.

Twofish

The updated form of Blowfish, Twofish utilizes 256-bit blocks to encrypt the data.

The Advanced Encryption Standard (AES)

The most prominent algorithm in North America, it uses keys in 128-, 192-, and 256- bit formats. It is considered resistant to all but brute force attacks.

Elliptic Curve Cryptography (ECC)

Prominently employed to protect the interactions between websites and their users, ECC uses a 256-bit key that provides the same level of security as a 3 MB RSA key.

It is important to understand the kinds of encryption that are appropriate for your deployment. How sensitive is your data? Are you in an industry that is often targeted by malware and hackers? Have you faced incursions in the past? These questions can help define the level of security most appropriate for your deployment and help you control security costs as a result.

If you don't need full end-to-end encryption, for example, you could likely work with your smart connectivity provider to utilize secured links to receive data and only encrypt the data before it is sent over the public internet or to an unfamiliar network,

9

Is Your Connectivity Smart?

While connecting to the internet is a service that many can provide, not all connectivity providers are created equal. Smart Connectivity is a full-suite solution that offers more than just a portal to the internet, it offers a more holistic approach to IoT development - one that looks beyond mere connectivity toward the factors that can help control project costs.

This chiefly happens by offloading much of the network's communication overhead to the connectivity partner. We've already touched a bit on this in previous entries, but some connectivity solutions include value-added services and features that can take some of the strain off of your network. A proper smart connectivity solution could provide developers with services such as:

- Authentication
- Provisioning
- Cloud integration
- Data Encryption
- Etc.

What is Communication Overhead?

When a computation or process takes up too much time, memory, bandwidth, or other resources, creating an unnecessary drag on performance.

One example that may go overlooked can be seen in the headers that help to route IP packets across the network. The computational power required to parse this information may seem small at first, roughly a byte or so, but aggregated across an entire network of devices, it can add up quickly. A smart connectivity provider can more easily identify the source of the data and convert it to the appropriate format without requiring that additional metadata to identify a packet. This reduces data consumption, improving your cost structure incrementally.

Smart Connectivity providers can also offer security options, such as private networking that can keep your devices and backend away from the public internet. In addition to the enhanced security that this lends your personal data, this can also prevent interruptions in workflow from incoming packets that could create drains on a device's batteries. This is another incremental performance boost, but it can all add up on a larger deployment.

Left unchecked, any number of things could cause a project's costs to spiral out of control. Yet with this list of common pitfalls for IoT deployments, you should be able to get a better handle on the total cost of ownership for your project.

Here is a quick checklist of questions you will want to understand about your project to avoid the TCO iceberg:

- ✔ **What are your hardware needs?**
  - What functions does the device need to perform?
  - Do you require a custom device, or can you work with existing hardware?
- ✔ **What are you doing for software?**
  - Will you be developing your firmware in-house or relying upon existing solutions?
  - Do you have plans for offloading your back end to the cloud, or will those processes be performed device-side?
- ✔ **Do you need an in-house Engineering team?**
  - Can you afford a team of engineering professionals?
  - What skillsets does your deployment need to succeed?
  - Does the speed of development offset the cost?
- ✔ **What are you doing to maximize battery life?**
  - Is your device performing any unnecessary functions?
  - Can you easily switch between active and standby modes?
  - Does your test environment replicate the atmospheric conditions of your deployment?
- ✔ **How are you going to manage the product lifecycle of your deployed devices?**
  - How will you be provisioning your fleet of devices? What about configuration?
  - Will you be able to ship devices in standby mode during deployment/transit?
  - Do you have a plan for decommissioning/recycling devices at the end of their life cycle?
- ✔ **What is your plan for maintenance/support?**
  - Can you remotely access/monitor your deployed devices?
  - Can you patch/update your devices remotely or do you need to send a technician to replace parts?
- ✔ **Is Global connectivity a necessity?**
  - Will your deployment be crossing international borders?
  - If so, is your connectivity provider able to support connections across the globe?
  - If not, are you prepared to navigate multiple MNO contracts?
- ✔ **How will you secure your data?**
  - Are you working with a connectivity provider that can encrypt your data for you?
  - Do you need enhanced security beyond base encryption?
- ✔ **Are you working with a Smart Connectivity provider?**
  - Can your connectivity provider support your plans for scaling?
  - Can they help offload tasks from your backend?
  - Can they help secure your data?

SORACOM

A Smarter Connection

Success in IoT requires a deep understanding of hardware, software, cloud architecture, and connectivity... at the very least. That technical complexity has a lot to do with why most IoT projects never get past the prototype stage. But IoT is a team sport, and choosing the right partner can go a long way toward smoothing the path to success.

Since 2015, we've worked with developers around the world, from startups to global enterprises, to bring IoT projects from prototype to full worldwide deployment. We've grown to now serve over 10,000 customers worldwide, and we've learned a lot along the way.

Ready to get started with Soracom?
Our team of IoT experts is always ready to talk about your requirements.

To book your free IoT consultation, visit soracom.io/contact.