IoT Planning - Seven Key Questions for Highly Effective M2M deployments

By Ian Marsden Eseye CTO & Founder

If you want to utilize IoT and are preparing for a connected device deployment, you'll probably have worked through many scenarios and options. M2M IoT is a complex area. Each question can lead to more questions, resulting in a mind-stretching number of inter-related choices. How do you ensure your project is a business success throughout its lifecycle?

Rapid global adoption ensures IoT continues to grow at pace, with many new and developing projects and supporting services. To make sure you get your deployment right in the long-term, we would like to share some of our experience and expertise. We've been delivering IoT for over 10 years and have over 1,000 globally connected customers, spanning 130 countries, delivering 1m+ live connections. We specifically provide project expertise and services for global cellular connectivity and device optimization. We are the only AWS IoT Strategic Partner for connectivity.

Here is a small selection of the headline questions you should ask. Many more will become important as you develop your project:

1. What are the best options for device connectivity: wired, WiFi, radio or Cellular?

If a wire or WiFi, do you have control over the setting in which the device will exist? Do you know how much the installation of network cabling or infrastructure at each location will add to the cost of your project? Do you control the WiFi? If you don't, but link to it, how will you ensure you stay connected at each location when something happens on-site? If Radio and you're deploying worldwide, how will you ensure you adhere to local legislation regarding frequencies, transmitter powers and the approvals you'll need for each country? If Cellular, to what extent can you be clear about where devices will be located and whether they are fixed or moving? A general rule is: the more global and the more areas your devices are entering, the more you'll need to invest in the planning and the device.

2. How much money will lost connectivity and down-time cost me?

We advise you to calculate this carefully, and we can help. You might be surprised at the speed at which the numbers escalate. For example, single network operators average around 80% coverage at the locations in which IoT devices are installed; Eseye, with dynamic multi-operator SIM technology, averages over 98%. The more downtime costs you, the more you should invest in build and connectivity options. You should also estimate the cost of onsite maintenance visits and do everything you can to minimize these. Early procurement savings may have long-term negative results on the project if ongoing costs escalate.

3. How should I specify and build devices that will connect and stay connected, wherever they are deployed?

Do you fully understand the range of environments the device is expected to work in? This knowledge is crucial and has significant impact on the hardware and software choices you will make. Will you go in-house or use a third-party contractor for design, and how much are you prepared to spend on device hardware? Eseye has over ten years of device optimization experience on more than 200 projects, and also manufactures high-end Hera routers, so knows well that there are pros and cons to both approaches. This is another area where early planning and investment will reap rewards further down the line.

4. For cellular connectivity, how can I contract and connect my devices in multiple locations, regions and countries?

If you plan to manage this in-house, you'll need to build expertise and capacity. For global deployments you'll need to understand local regulations which, for example, can stop a standard roaming SIM card working in a number of countries. Nor is the legislation as light or simple as you might wish: different countries require different certification and are subject to local laws. In terms of contracting with Mobile Network Operators (MNOs), if you engage in a multi-country deployment, be prepared to find their world fragmented. There are around 800 MNOs worldwide (source GSMA), and individual contracts will result in you having to manage across multiple SLAs, languages, customer support centers, data price points and billing formats. Plus, if your business case requires over 80% network coverage, you'll need to contract with at least two different network operators in each country. There are also in-

country roaming rules you need to keep on top of. An alternative is to engage with companies like Eseye, who become a single point of contact and contract, and manage all of the above.

5. Using customer support services, how can I make sure I get problems fixed quickly?

When you have issues, and there will be some, resolutions will be quicker and more successful if you can talk direct to IoT experts who understand the device and the way it might operate on the network. Not all MNOs deliver this, so make sure you check and get references on customer support from existing clients with similar scale deployments to your own.

6. What cloud storage should I use and how will I make sure data can be reported and analyzed effectively?

This is the essence and value of IoT: to be able to gather information from all devices and centrally view and manage them, in order to save or make money, or to deliver some other kind of impact, such as social or environmental. There will be a budget and benefit analysis to undertake, but you have two main routes to choose from: either build in-house server and developer capacity or buy-in Cloud services and configure your project around their rules. Your requirement may be so unique you have no choice but to retain a developer team and to build and manage in-house hardware and analytics software. However, for most, customizable off-the-shelf storage and analytics solutions will be fit for purpose and give better value and scope to scale. Bear in mind that the bolt-on data analysis and security device management software that companies like AWS are developing will continue to add services; just as long as you are willing to configure by their rules, e.g. MQTT (Message Queuing Telemetry Transport). On this note, in establishing their rules, cloud providers have invested thousands of hours designing, building and testing for reliability, in the wide variety of real work scenarios. Whilst you may initially find adhering to some of the design rules and standards difficult and will be tempted to design a simpler custom solution, think hard about whether this is a sensible and scalable, long-term strategy.

7. How can I ensure my deployment is as secure as possible throughout its lifecycle?

It is essential to consider the implications of someone getting into your system before it happens, and to invest at the right level. We advocate and provide a range of advanced security features, which bring new, more affordable protection, and at the same time adhere to the security requirements of AWS Cloud. As you prepare your devices and connectivity you should decide where your security boundary is and plan accordingly. Give serious consideration to contracting in third-party penetration testing experts and ensure your team is keen to encourage this.

We have only touched the surface here and hope we have helped you to consider the complexities involved and decisions you need to make. IoT may appear alarming but each one of these, and other significant related questions, has been addressed successfully in numerous Eseye projects. After all, there are 20 billion devices out there, so please let us help yours to be a success.

Contact Us:

eseye.com

Contact sales@eseye.com

Please follow us on:

@eseyem2m

eseye

facebook.com/eseyeM2M