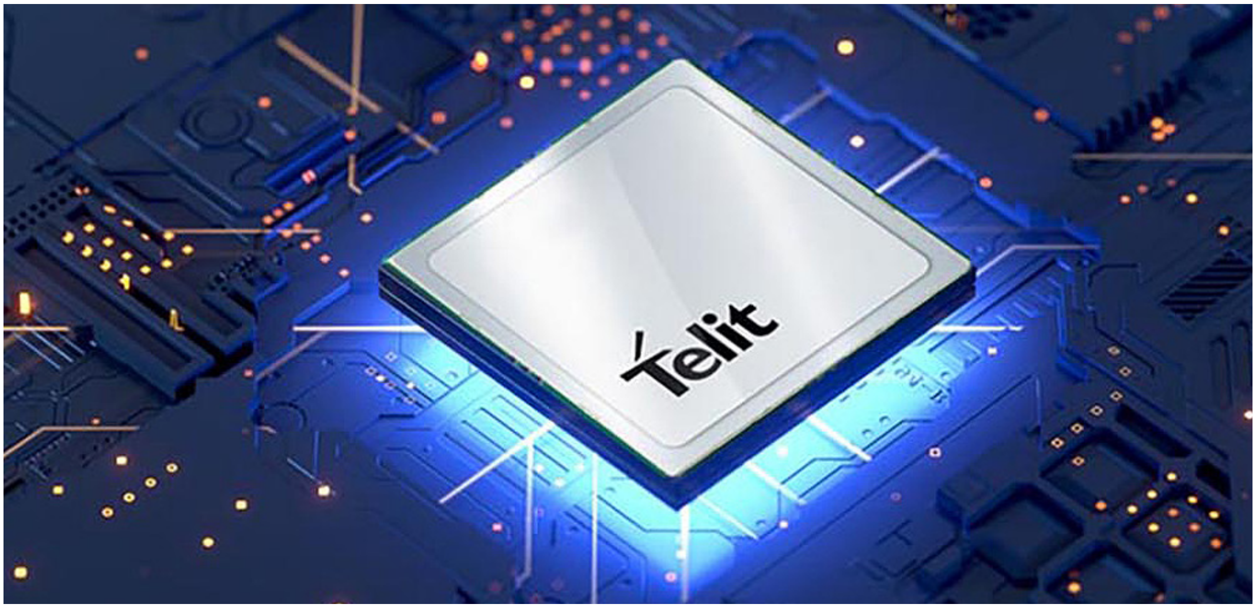
What You Need to Know to Make the Best IoT Module Selection



TELIT WHITE PAPER 05.2020

Introduction

Look Beyond the Chipset to Secure Cellular Connections in the Field.

From powering smart building devices to supporting public safety, companies rely on Internet of Things (IoT) modules to dramatically grow their business, increase operational efficiency and deliver real-time insights and outcomes to their partners and customers. However, the lack of standards is leaving many companies to focus on simple use cases instead of realizing the full value of IoT.

IoT is no longer a question of "if" and "when" companies will embrace it but rather a plan for today's deep operational transformation and the future. Now that the technology has grown in importance, the floodgates have opened and released a seemingly endless array of one of the most crucial components of any IoT deployment — cellular IoT modules.

Considering the critical role they play in a successful IoT deployment, cellular IoT module function must always be appropriate, consistent and sustainable. These small communication adapters and computing devices allow physical objects to connect and interact with wireless networks as they transmit the data that devices sense, collect and store.

Contents

Cost of Connectivity Remains High, While Hardware Has Become More Affordable

Although the price tag for IoT modules has steadily decreased in recent years, wireless connectivity remains a distinct service that is far from commoditized. Most newcomers to IoT employ a commodity electronic component selection model matching needed capabilities or desired use cases with the lowest price possible. However, there is a greater need to ensure choosing IoT module and services providers carefully.

Pricing models for IoT connectivity plans may differ not only on cost per megabyte used but also on additional charges. For example, value-added services, monthly or annual fees, number of connections, or volume of data allowed can be bundled into one packaged price. In the case of cellular low-power wide-area data plans, however, charges could include each message transmitted and exchanges in addition to the megabyte.

Even though functions of different IoT components are generally similar, businesses should still consider the risk, sustainable interoperability, committed capacity and expertise required to deploy and run a successful IoT project. In this white paper, we'll explore how these aspects of your cellular IoT module investments can impact the security and connectivity of your assets and processes.

Break Free from Risky Opportunism to Advance with Long-Term Technological Commitment

Fast-paced innovation, growing globalization and the constant threat of cyber attacks are making the IoT market susceptible to opportunism. As quickly as technology and business needs evolve, low-cost IoT vendors enter the market ready to deliver cutting-edge modules that address the latest concerns. However, history has shown that their commitment only lasts until return targets are met for opportunistic investors at which time they simply dissolve.

Since module-level components are easily produced from chipset vendor reference designs, low-cost vendors can demonstrate a tempting, robust portfolio of offerings. They claim that their innovations' ruggedness, reliability, dependability matches competitor solutions. However, their relatively low investment in research, development and production suggests that in-service performance over years and decades may be limited to future designs that may or may not work well with existing modules.

Risks of Working with a Budget IoT Vendor

For most businesses, this go-to-market strategy poses significant risks. Take, for example, smart vending machines. A cellular communications outage can cost thousands in revenue, even if it is for just a few hours. When the connection ceases to work, the device stops — as well as data exchange, automated ordering and transactional operations.

As many businesses who have gone one round with commodity vendors already know, it does not take many outages at peak demand to wipe out the savings promised by a low-cost module — regardless of whether the machine is near concession stands at a major ballpark or in a break room at a small startup. Every time a company needs to dispatch a maintenance team to repair a machine, initial savings on the one-time purchase price of the module can quickly turn into a burdensome cost compounded by lost revenue.

Despite promises, low-cost providers cannot guarantee long-term support, global certifications and guidance on programming interfaces, continuous cybersecurity upgrades, enduring device pinout, connectivity footprint, power supply specifications and more. Instead, all too often, the relationship ends as soon as the technology order is fulfilled and delivered. Additionally, since many have not been in mainstream markets for very long, verifying quality and longevity claims against track record is not an option.

Understand the Fundamental Difference Between a Low-Cost Module and a Low-Cost Vendor

Cellular IoT modules are not a commoditized business expense — they are an investment in the long-term backbone of business models, organizational processes and customer experiences. A single unplanned interruption in the operation of any module could translate into failure that could disappoint everyone the business touches — customers, suppliers, partners, employees, shareholders and even executives.

This disappointment is what can happen when a low-cost provider redesigns a cellular IoT module. However, this doesn't mean that all inexpensive modules are poor investments that make deployment unsustainable over the long haul. When sourcing a module from a low-cost vendor, businesses need to consider if they can take the financial risk. They should also contemplate if they have the wherewithal necessary to handle a mass failure situation when the vendor no longer supports additional development needs, bug fixes and code updates. Risk and exposure are mitigated if, instead, the low-cost module is procured from an established brand.

Product lifecycles vary from customer to customer, which means the components they integrate must be just as flexible. Components for data storage, power and processing are not exposed to the risk of forced obsolescence. These devices don't rely on external factors to operate. In contrast, cellular modules will only work if they comply with the standards (that continuously change) current for the mobile network at the time they go into service.

A sound IoT investment — like most technology purchases — is a matter of simple math. Every module provider should be required to provide evidence of operational compatibility throughout the intended life of the device and business contract. Brand name vendors can show their cellular IoT modules — even low-cost ones — enhance and modernize their customers' IoT systems over product lifecycles while maintaining backward compatibility with form factors and logical interfaces.

Choose an IoT Vendor Committed to Future-Proofing Your Investments

The purchase of a cellular IoT module is an investment in the business's future success. It is crucial to know everything about the vendor supplying the module to understand the quality of the product and the level of support available. For example, vendors running on razor-thin profit margins often curtail financing of a global network of field engineering and tech support hubs, R&D efforts and quality management — limiting any opportunity to leverage reference design notes from cellular chip providers to develop relevant, secure and fail-safe innovations.

As a leading provider of cellular technology for home and business security and alarm systems, Telit nearly two-decade history of helping businesses succeed in a challenging marketplace. Throughout this time, we have seen industry leaders such as Ericsson, Nokia, Motorola, Enfora, Novatel and Option enter and leave the module market. Some players couldn't commit the resources required for the continued development and maintenance efforts that customers need to be successful.

Telit's story is very different. We give every customer our long-term commitment and investment in their success. Based on our years of experience working with a variety of businesses, including many of the world's top brands, we have come to understand well what combination of edge-to-cloud enabled modules, connectivity plans and managed services; and web-enabled platforms will work for each customer. This setup has proven to be an excellent enabler of fast IoT deployment solutions and business growth.

Even though Telit does offer low-cost modules, we ensure every IoT solution component available in our portfolio future proofs customers' business models as they securely and reliably power the edge of their network of devices. More importantly, we continuously focus on delivering low-cost variants with three core promises that every customer can trust — dependable, available for the long term, and broadly certified.

[05.2020]

Telit reserves all rights to this document and the information contained herein. Products, names, logos and designs described herein may in whole or in part be subject to intellectual property rights. The information contained herein is provided "as is." No warranty of any kind, either express or implied, is made in relation to the accuracy, reliability, fitness for a particular purpose or content of this document. This document may be revised by Telit at any time. For most recent documents, please visit www.telit.com

Telit