How to make wireless IIoT work for your business

Laird™
CONNECTIVITY

Five factors to consider if you're building a wireless IIoT solution

IoT, or the Internet of Things, means a lot of things to a lot of people. At its core, it's about connecting the real world of products and environments to the internet where that data can be used to help improve life. Unfortunately, that's a really broad description. It's how we end up with the endless list of IoT niches we see today: smart cities, smart buildings, industrial Internet of Things (IIoT), M2M, consumer IoT, eHealth and many more

To cut through a lot of confusion and help you decide if you want to read this whitepaper, ask yourself three questions:

1. Do you belong to an enterprise looking to create revenue from your customer base through a connected solution?
2. Do you consider your business to be mission-critical? That could mean many things, but some examples could be helping your customers meet regulatory compliance, preventing downtime of expensive assets, or protecting the health and wellbeing of patients. It does not include helping your customers perfectly toast bread at precisely 6:45am each day.
3. Are you looking for help on selecting the right sensing and connectivity technologies for your IoT architecture?

If you answered yes to one or all of the above – great! We think you'll get something out of this white paper. Let's get started.

This whitepaper examines the benefits as well as the complex challenges that accompany the implementation of an enterprise-grade, revenue generating IoT solution. Navigating the system complexity, creating the appropriate connectivity architecture, managing effective security, are some of the challenges that must be addressed and solved for an effective, profitable and scalable system. This paper highlights the following five factors to consider when building an IIoT solution:

1. Top IoT challenges
2. What your competitors are doing – example applications
3. Architecting your IoT solution
4. Choosing a connectivity option
5. Selecting a cloud solution

For the sake of simplicity, we'll call you an original equipment manufacturer (OEM) in this whitepaper. That could mean you actually manufacture equipment such as medical devices, industrial pumps or devices in commercial restrooms. Or it could mean you develop a software solution that uses data from other companies' equipment and sensors to drive insights for customers. ▶

This whitepaper examines the benefits as well as the complex challenges that accompany the implementation of an enterprise-grade, revenue generating IoT solution.

The importance of connected products to OEMs

OEMs are increasingly under pressure to build their business – outperform competition, increase revenue and grow profit margins. When manufacturers are looking to improve their business or systems, when they're seeking to drive business growth, they typically don't go out searching specifically for an IoT or connected system. What these business drivers are seeking is simply a way to increase the size and profitability of their business. They are looking for a solution that will meet their business outcome goals.

Although it's true that an IoT system and the data that results from it can vastly transform a business, most manufacturers are looking for ways to achieve one or more of the following:

- Help your customers have the best possible experience and uptime with your products
- Help your customers reduce their own costs by automating a previously manual solution (We're looking at you, Mr. Clipboard)
- Help your engineers and product managers understand how your customers use your products
- Help your field service teams be more efficient and profitable

To put it simply, IoT just isn't that interesting unless there is a solid business case surrounding it; an obvious reason to build a connected system. It's important to emphasise to potential customers how an IoT system can help them make great strides towards achieving their business goals.

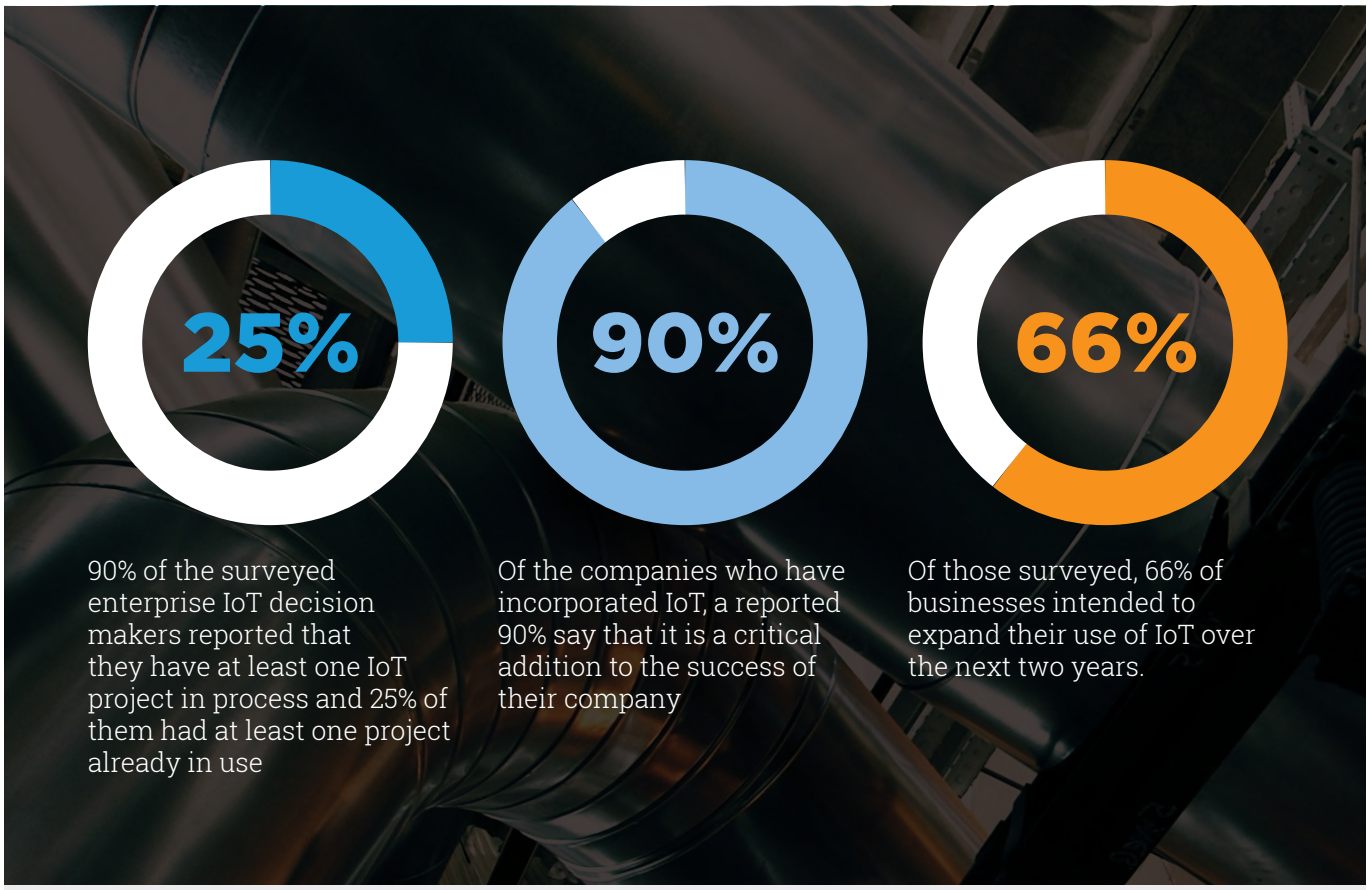
But if you're reading this whitepaper, it's probably a safe bet that you've already figured this one out. Your job now is to make that business case a reality, preferably stumbling as few times as possible along the way.

Top IoT challenges

Connected solutions can generate a lot of useful insights, but in between your things, the internet, and the insights you seek are infinite combinations of specialised technologies: wireless, sensors, operating systems, cloud, containers, security, SaaS systems, analytics engines and user interfaces. Piecing these technologies together into a value-driver is fraught with challenges, including:

- Picking winning technologies in your solution that will stand the test of time
- Assessing and maintaining return on investment (ROI) for both upfront development as well as ongoing costs of maintenance
- Integrating legacy products and systems
- Finding the diverse skill sets necessary for successful IoT implementation
- Ensuring that your IoT system is secure

In spite of this, adoption of IoT across industries continues to increase at a fast pace. According to the most recent **IoT Signals** survey completed by **Microsoft**, 82% of the surveyed enterprise IoT decision makers reported that they have at least one IoT project in use. Of the companies that have incorporated IoT, a reported 90% say that it is a critical addition to the success of their company, with a 96% reported satisfaction rate with the results. ▶



It's evident that the move towards IoT systems continues to grow. Also, according to the Microsoft survey, 90% of businesses were already IoT adopters with 66% planning on expanding their IoT implementations over the next two years. As these businesses experience an increased ROI, they are also likely to continue to look for new ways to use this IoT technology, especially as additional innovations such as artificial intelligence (AI) and 5G emerge.

Simply put, companies that successfully deploy connected solutions to the benefit of their business will thrive, and those that don't will fall behind. 90% of the surveyed enterprise IoT decision makers reported that they have at least one IoT project in process and 25% of them had at least one project already in use. Of the companies who have incorporated IoT, a reported 90% say that it is a critical addition to the success of their company. Of those surveyed, 66% of businesses intended to expand their use of IoT over the next two years.

Prerequisites

There are a few important decisions you'll need to make that are out of the scope of this whitepaper. Before selecting an IoT architecture, it's vitally important that your organisation is aligned on where you stand on the following:

- How do you plan to monetise your IoT solution? As previously discussed, will you be helping your customers? Engineering team? Field service organisation?
- What equipment or environmental data (temperature, vibration, usage or current) do you need to drive the insights you desire. This expertise likely already lives in your organisation. If you don't know, that's OK – but you should be ready to cast a wider net and give yourself a longer leash on a proof of concept phase to learn what's necessary to gather and what isn't.
- Your organisation's long-term IoT strategy – where do you plan to invest your resources and gain an edge? Do you need machine learning experts? Full stack developers? Big data analysts? This whitepaper assumes, as we see with many of our customers, that the data you gather, the algorithms you develop, and the cloud systems you intend to build are going to be your company's secret sauce for IoT.
- Where is the data you need? Is it already living in unconnected legacy equipment? Does it need a new sensing capability?
- What's going to collect that data? Do you need to install new equipment? Retrofit legacy products? Can your customers install this equipment or do you need to send out installers to your customer sites?
- In what type of environment is your equipment and how will it get out? Will you have Wi-Fi access? Cellular reception?

Understanding these basic realities will help guide which architectures and technologies might be a good fit.

Example applications

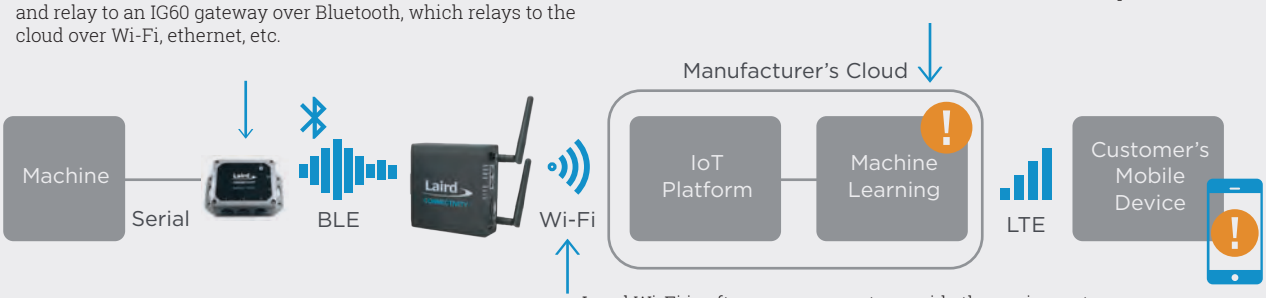
To get you started down the right path, below are some examples we've seen: ▶

Smart industrial support systems

Solution architecture

Legacy equipment frequently uses RS-232 (serial) based-protocols. A BT610 sensor can extract useful data over wired serial connection and relay to an IG60 gateway over Bluetooth, which relays to the cloud over Wi-Fi, ethernet, etc.

Machine learning algorithms in the cloud can predict failures and warn customers with alerts to their smartphone



Local Wi-Fi is often an easy way to provide the equipment secure connectivity to the manufacturer's cloud environment

Several customers we work with design and manufacture equipment that keeps mission critical systems running. For example, it could be a cooling system that's keeping a semiconductor laser etcher running, a compressor system keeping lubricant running through a fabrication machine, or a backup power system connected to hospital refrigerators.

In any of these scenarios, these manufacturers put their companies and brands on the line to guarantee reliability and uptime. When their equipment fails, it causes other major systems to fail, causing their customers to lose thousands of dollars an hour from lost production.

For this class of company, a connected solution offers several paths to monetisation:

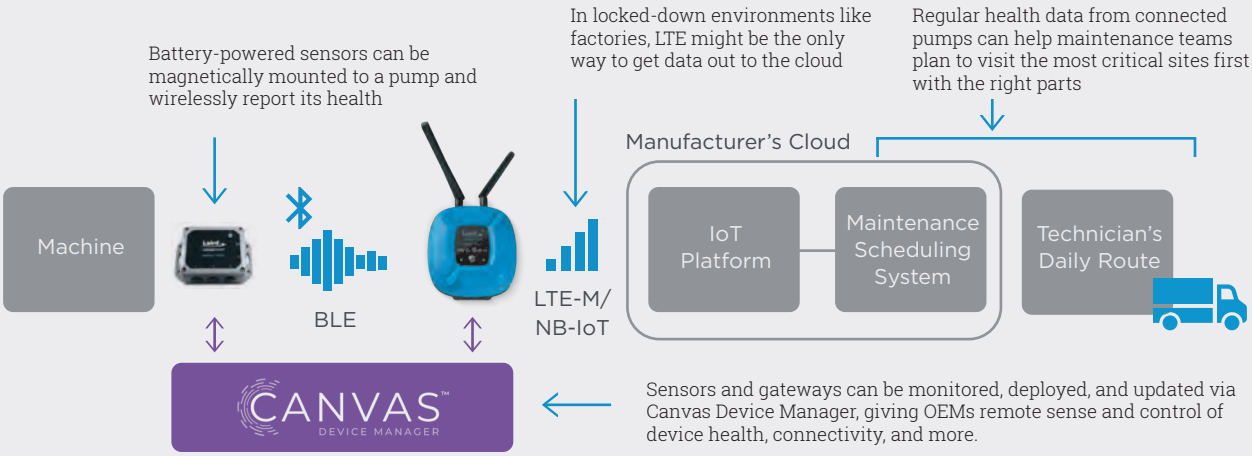
Offer higher levels of service level agreements (SLAs) to their customers from the ability to monitor equipment in the field and predict failures through a connected solution.

Increase revenue from aftermarket parts or consumables by ensuring customers properly maintain the equipment.

Reduce field services teams' costs by allowing them to optimise routes and service the most urgent issues first. ▶

Connected pumps and compressors

Solution architecture



Some technologies and inventions are high-end and trendy. Others are a less glamorous but no less important. For example, consider pumps and compressors. We have customers whose main priority or function is to provide equipment that pumps drinking water to both urban and rural areas as well as to treat and remove wastewater.

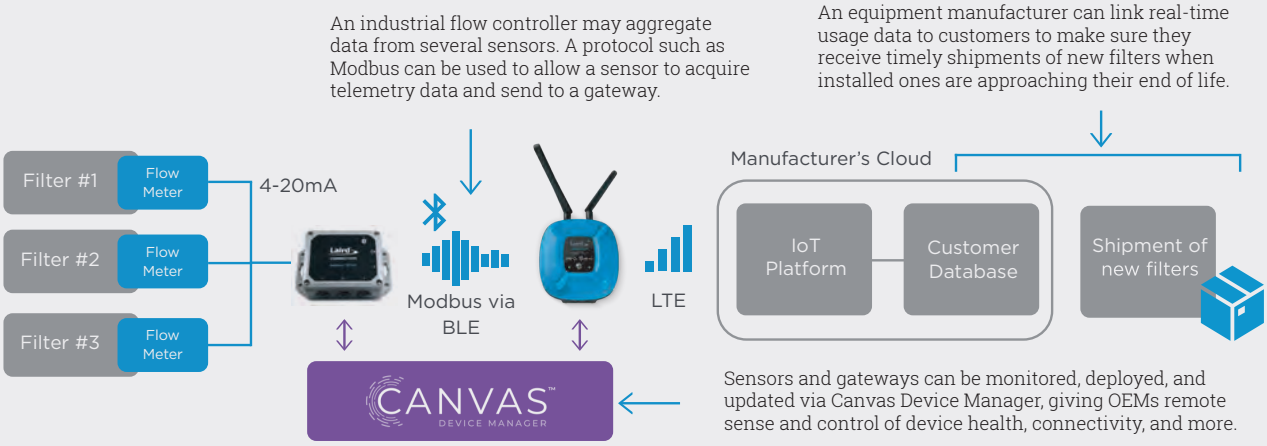
Not a fancy technology but it certainly plays a critical, life-saving role. If critical installations such as wastewater pumping stations, water treatment plants, and irrigation systems fail, it not only creates increased mechanical expense and the expense involved with business down-time, it threatens life and livelihood of those who rely on the services the equipment provides.

For this type of company, a connected solution offers the following possibilities for enhanced business opportunities:

Provide cost savings to their customers by enabling remote monitoring of in-service equipment. With this ability to remotely monitor equipment, customers are able to perform predictive maintenance techniques rather than routine preventative maintenance – equipment is only serviced when necessary rather than on a time-based schedule. This decreases the number of unexpected mechanical failures, prevents unnecessary equipment down-time, and minimises the need for personnel to manually inspect critical installations.

Increase revenue by providing a system for their customers to receive operational data that can enhance or guide business goals. ▶

Filtration systems
Solution architecture



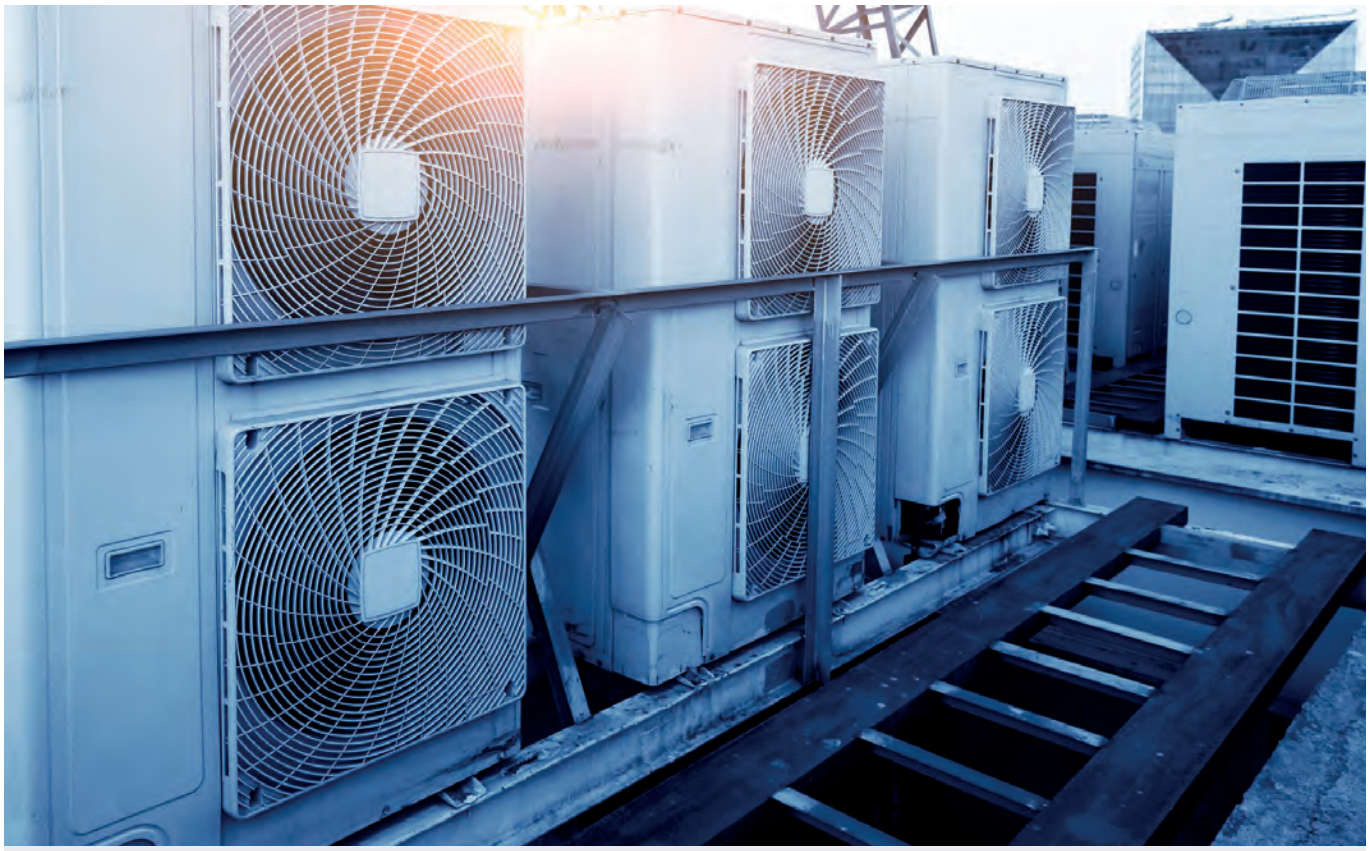
Probably a less life-critical example but still a solid application of a connected solution can be seen in the beer-brewing industry. Considering the increasing amount of beer competition and knowing that beer drinkers are often very particular about their beer selection, breweries strive for high quality and consistency in their brewing process. Companies that provide filtration systems to these breweries could benefit from the business opportunities a connected solution provides.

There are multiple ways that a connected system could enhance a company's offerings or services and therefore their financial bottom line.

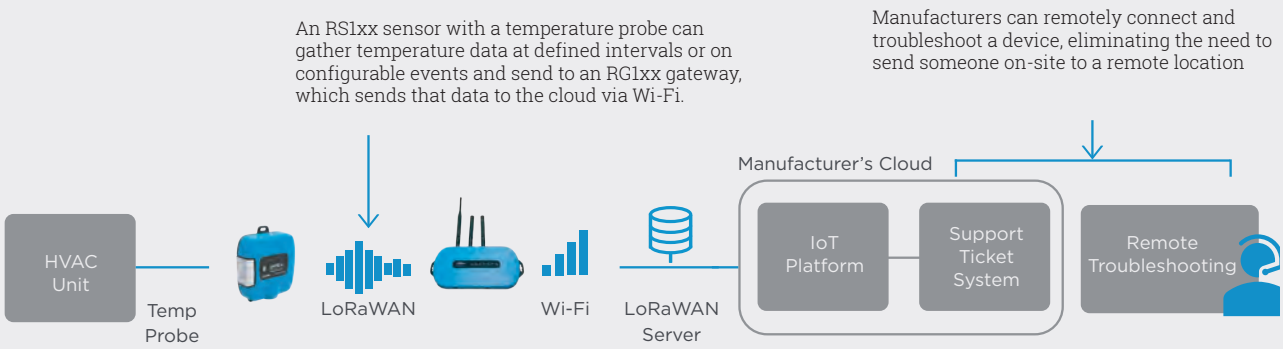
In addition to previous examples such as enabling predictive maintenance and decreasing field service team costs, the following are also possible with a connected solution in the brewing industry:

Provide their customers the ability to easily monitor the entire brewing process to ensure production consistency and quality. The ingredients that go into beer can vary from year to year depending on environment conditions, such as weather and soil. From the data provided by a connected IoT system, brewers can make the necessary adjustments to ensure each batch of beer tastes as it should.

Create a connected system for their customers that operates in a secure environment and ensures no loss of data even when Wi-Fi connectivity is not available. ▶



HVAC monitoring
Solution architecture



Downtime in any manufacturing plant is a threat to the business. As the old saying goes, "time is money". When a plant is idle, for whatever reason, it's a financial risk to the business. A connected IoT solution could enhance business success for any type of manufacturing plant where asset management, operational efficiencies, and safety are critical factors. Take, for example, a company that provides gear drives to manufacturing plants.

For this type of industry, offering smart gear drives as part of a connected system could enhance business opportunities in a variety of ways:

Offer real-time monitoring of equipment to ensure optimal performance and maintenance needs.

Provide on-demand information to customers.

To ensure efficient product installation as well as historical and analytical data to assess equipment performance.

Enable predictive equipment analysis to not only allow timely maintenance but to also ensure a safer work environment for employees. ▶

Connect to legacy sensors
Analogue and/or digital IO sensors that already exist in your system communicate data to a wired communication bus sensor via a modbus. The sensor then delivers the data to a gateway, which communicates with the cloud.

Connect to wireless sensors (battery-powered)
Battery-powered Bluetooth or LoRa sensors communicate wirelessly to a wired communication bus which then delivers data to and from the cloud.

Direct integration
Your machine or device contains an integrated module or modem to directly communicate to and deliver data to and from the cloud. An example module is the Laird Connectivity Pinnacle 100 multi-wireless modem.

Architecting your IoT solution
Choosing connectivity options

With an IoT connected system, data is mission critical. Most of the value to your business comes from the resulting data once it's transitioned to the cloud. To complicate this issue, industrial buildings and factories frequently have harsh radiofrequency (RF) environments and are, at times, in remote locations with poor carrier coverage.

But, how exactly do you get this data? How is this data effectively moved to the cloud? The first step is to determine which connectivity options are available to you. Here are some things to consider:

- What connectivity options are available at your site? Will the local IT allow you to access and use the Wi-Fi network? If not, are you able to run Ethernet cable?
- Are there currently sensors available to use with the system or will you need to install new ones? How will you power the sensors? Are they battery-operated?
- Is a wireless connection an option for the sensors based upon the environment? Is the environment conducive to the use of sensors?

With an abundance of technologies available at your fingertips such as Bluetooth, Wi-Fi, LoRa and cellular, along with cloud systems to collect, store and analyse data, where do you start? How do you even begin to choose the correct connectivity choice for your industrial IoT systems and applications?

Connectivity architectures
As shown in the previous examples, there are many ways to move the data you need for your connected solution to the cloud. Here are some generic examples to consider.

Selecting a wireless technology
There are four main wireless technologies that should be considered for connectivity in a wirelessly connected system: Wi-Fi, Bluetooth, cellular and LPWAN. Connectivity can be embedded within the device or added on with external modules and devices once the device has been deployed. Market expectations are that new smart devices have connectivity embedded within the device, but many businesses still utilise legacy devices which must be taken into consideration. Gateways can also be used to collect data on a local level then manage the connection to a cloud server for the transmission of this data. In this way, not every device or sensor must be connected to a cloud or network server.

Wi-Fi
Wi-Fi, in general, is a technology that uses radio waves to transmit information at specific frequencies. It enables high-speed and secure communication between a variety of devices, without wires, over both short and long distances. More specifically, enterprise-grade Wi-Fi, in contrast to consumer-grade, provides a higher-level of service when it comes to performance, security, standards/compliance, and life-cycle management – factors that are important for connectivity in any IIoT system. The latest Wi-Fi devices using Wi-Fi 6 and 6E frequently support some of the most current security offerings, such as WPA3.

Bluetooth
Bluetooth is a wireless technology that allows mobile Bluetooth devices to exchange data over short distances. The original classic Bluetooth was designed to continually ▶

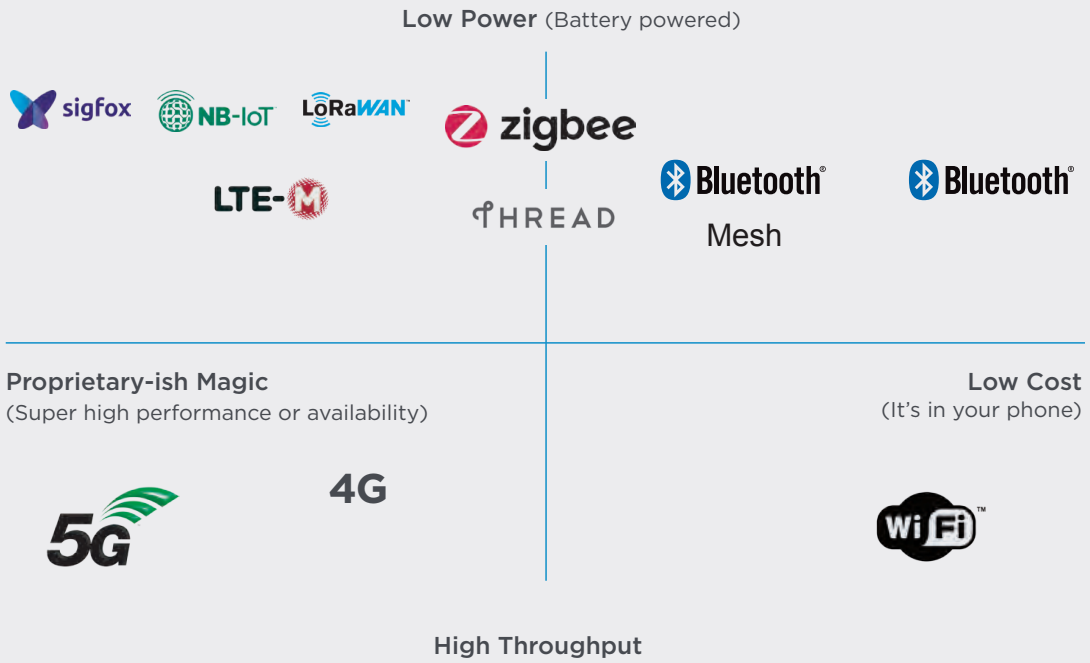


Figure A

Figure 1 provides a basic overview of each of these wireless technologies in regard to cost, performance, and level of power and/or throughput. In general, low-cost versus high performance and low power versus high throughput.

stream data over short distances. Since its early days as a means to connect earbuds to your phone, Bluetooth has rapidly evolved as a low-cost, solidly performing option for wireless sensor applications.

The more recently developed Bluetooth Low Energy, also known as BLE or Bluetooth LE and introduced in Bluetooth 4.0, is a low power yet robust technology intended for situations where battery life is more important than high data transfer speeds.

Bluetooth 5 introduced a popular new feature called the LE Coded PHY. Use of this technology can provide up to four times the range as previous versions of Bluetooth, at the cost of a lower data rate. This trade-off has proven a popular choice for battery-powered wireless sensors.

Adopted in 2017, Bluetooth mesh is a networking Bluetooth technology that replaces the one-to-one Bluetooth exchange with a many-to-many relationship between Bluetooth devices. Mesh networks, in general, can effectively meet communication requirements over large areas while monitoring and managing many devices. Bluetooth mesh networking, more specifically, accomplishes these things while also maintaining compatibility with current devices and, because it depends on Bluetooth LE technology, does so with low-energy efficiency.

LPWAN

Rather than being a single technology, low power wide area network (LPWAN) is a broad term to describe a group of protocols that operate using low powered devices to communicate small amounts of data over long distances.

There are several technologies competing within the LPWAN realm including LoRaWAN and cellular protocols such as LTE CAT-M1 and narrowband IoT (NB-IoT). With some applications, using a LPWAN protocol like LoRa operating in the 900 MHz range allows greater range and better propagation through various building materials than Wi-Fi or BLE. The cellular LPWAN technologies like LTE CAT-M1 and NB-IoT are becoming very effective in connecting remote sensor devices. These protocols are different from standard cellular services because they are meant to support low data rates at much lower cost than support for standard voice and data cellular service.

Wireless gateways

Within the IoT, we are seeing growth in the adoption of gateway technology. A gateway is a physical device or software program that serves as a connection point between the cloud server/application and devices and/or sensors. All data moving to the cloud, or vice versa, goes through the gateway, which can be either a dedicated hardware appliance or software programme. Smart devices along with sensors can generate thousands of data points per second. With a gateway, devices can collect and pre-process or package the data locally before sending it on to the cloud. In this way, the end user can minimise the volume of data needed to be sent and can manage a secure connection through the internet and into the target cloud provider. Because the gateway manages information moving in both directions, it can protect data from leaks and IoT devices from being compromised by malicious outside attacks.

A gateway can support multiple connection technologies such as Wi-Fi, BLE, LoRa, Ethernet, and serial port ▶

connections. Most deployments use the ethernet or a Wi-Fi connection to the local area network as the doorway to manage the cloud connection. If using the local area network is not feasible, then a cell modem can be integrated into the gateway to utilise cellular connectivity to connect back to the cloud. The LTE CAT-M1 and/or NB-IoT service connections can be a cost-effective egress technology for lower data rate applications.

Understanding telemetry vs. device management

It's important to understand the difference between two main functions of cloud services. The first is what we have been discussing for the majority of this whitepaper: getting data from devices and performing monitoring or analysis to create valuable insights and deep information. This is what we refer to as telemetry data. It is distinct from the second main function of the cloud, which is device management.

Device management is monitoring the status of devices in your cloud solution, including any error or debug information, software updates, provisioning and deployment, security analysis, and more. Where telemetry is interested in the data that applies to the application, device management is interested in the status and health of the sensors and gateways themselves.

Selecting a telemetry system

There are many cloud solutions from which to choose once a business or manufacturer has a clear understanding of their specific telemetry needs. Even though most major cloud IoT platforms have a proprietary element to them, not choosing one is not really an option due to the fact that cloud-based services are a must for the vast majority who manage a connected IoT system. Also note that choosing a proprietary cloud solution is a far better option than trying to build your own. Even **GE**, in its financial prime, failed to develop a cloud platform despite investing billions of dollars.

The following are some important factors to consider when selecting a cloud platform.

Who offers compelling IoT, analytics and machine learning capabilities? While technologies such as message queueing telemetry transport (MQTT) are frequently available on nearly any IoT platform, edge and container technologies, robust database options, analytics tools, and particularly machine learning and artificial intelligence are not universal. Some platform providers are ahead of others.

Which cloud platform will reliably still be around in five or ten years? Longevity is important when it comes to producing and marketing stability to ensure a product's lifecycle can be supported. Companies in general are not permanent nor are they static and this applies equally to cloud solutions. Companies can go out of business or simply change their strategies or services which has the potential to disrupt critical day-to-day data management.

Which cloud service provider is adding new features and additional capabilities more consistently or rapidly? Technology is always evolving. New ideas lead to new features at a fast pace. To ensure an IIoT system is utilising the most advanced capabilities is important especially considering the pressure to outperform the competition as well as increase revenue and profit margins.

Although most major cloud IoT platforms have a proprietary element to them, not choosing one is not really an option due to the fact that cloud-based services are a must for the vast majority who manage a connected IoT system.

How many devices will be connected to the cloud solution? How much data will the cloud solution be managing? When selecting a cloud service, it's important to understand both the devices the manufacturer needs and the data that will be transported to and stored within the cloud. Scalability is the ability of an IIoT and cloud system to grow and successfully manage the increased demands of this growth. This is one of the most important features to consider with a cloud solution and a company's failure frequently comes from an inability to successfully scale up or down to meet its changing business needs.

Which cloud service provider offers the most solid technology and development ecosystem and partnership for the business? As noted in this paper, the implementation of an industrial IoT system is complex and challenging. It involves creating the appropriate connectivity architecture, managing regulations and security, as well as other vital considerations. It only makes sense to choose a cloud solution that offers the advance knowledge and experience as well as strong partnership to ensure an IIoT system's success.

Selecting a device

Management solution

In addition to finding the right telemetry partner, finding a fully-featured device management solution is critical not just to the reliability of your devices, but getting them into the field in the first place.

Device management begins with a comprehensive security architecture, continues through deploying and provisioning devices remotely in the field, and continues throughout the life cycle with vulnerability monitoring and security updates. A fully-featured device management solution needs to stay in step with real-world threats, and ensure that devices are checked against security issues and provided with over-the-air fixes as needed. ▶

The following are important questions to ask when choosing a device management solution:

Does your chosen partner meet or, ideally, exceed legal security requirements and regulations? For an IIoT system to be deployed successfully and effectively, it must be deployed securely. As the move towards IIoT systems continues to grow along with the ongoing rapid influx of global connectivity, security becomes a greater challenge. Along with cybersecurity concerns, understanding laws and regulations regarding cloud-based data adds another layer of complexity to the business equation. Not only are regulations forced to evolve along with technology, laws also differ from country to country which adds to the difficulty.

The right cloud solution for a manufacturing IIoT system can not only help navigate these regulations, but it can also ensure the tightest possible security and over-the-air (OTA) security updates.

Does it scale? As we previously mentioned, failure often comes from an inability to scale an IIoT system to match business growth or, when applicable, business downturns. It's one thing to manage a system that includes a few connected IoT devices and a local cloud, but it's a far different matter to deploy and maintain a largescale IIoT system in a challenging environment with an increased criticality of connectivity and data delivery. Not only is scaling a system expensive, it also requires additional resources and technical know-how. For OEMs and other manufacturers, trying to accomplish this internally, versus provisioning from an external cloud solution partnership, often leads to IIoT business failure.

Is it extensible to integration with your telemetry solution? Not all cloud solutions play nicely with each other. In general, the largest telemetry platforms, like **AWS** and **Azure**, are dominant enough in the marketplace that third party providers' software can be integrated into their toolkits. However, as previously discussed, with this comes a requirement for significant development on the part of the OEM.

Does a native device management platform already exist for the devices you're using? In the classic build vs. buy decision, the convenience of relying on an existing device management platform can save OEMs significant development efforts, given that the platform meets the previously discussed requirements.

Laird Connectivity's Canvas Device Management platform, which is already available for the IG60-BL654m BT610, and MG100, is powered by partner **EdgeIQ**. The device management platform simplifies workflows for configuration and maintenance of IoT device deployments. Easily set-up your devices, monitor performance, and keep software up-to-date across your entire IoT device fleet.

Laird has partnered with EdgeIQ and other industry leading cloud-based and SaaS providers, so that our customers do not need to integrate multiple third party components themselves. We've bundled everything together to fully integrate with your network infrastructure. Benefit from remote firmware updates, remote configuration and remote device health monitoring, all with seamless operation of Laird Connectivity sensors and gateways.

Conclusion

It's understood that manufacturers are increasingly under pressure to encourage business growth by improving efficiency, decreasing operational costs and strengthening customer relationships. It's also understood that an effective IIoT system and the resulting data can vastly transform a business. As we stated earlier, despite the fact that IIoT systems are complicated and difficult to manage, the adoption of this technology across industries, including manufacturing, continues to increase at a rapid pace.

Simply put, don't try to rebuild what already exists. Find an IoT and cloud solution partner who can help make the best technology decisions for your IIoT system, allowing you to focus on your areas of expertise and getting the value out of the IoT data the system provides.