IoT for Industrial Markets

By Glenn Longley, FreeWave Technologies, Inc.

With modern industrial technology, an organization can make intelligent operating decisions because it can establish connectivity to all of its assets in industrial facilities or the field across any distance. Communications and process technology advancements continue to enable more data collection than ever before from an ever increasing number of sensors monitoring almost anything. When industrial automation was first picking up speed in industries like oil and gas, there was a heavy focus on how supervisory control and data acquisition (SCADA) systems helped collect and transfer critically important data. SCADA systems are still relevant today, but as communications technology evolved, especially with the adoption of wireless Machine-to-Machine (M2M) communications becoming important in allowing operators to access more data from more access points. More recently, the concept of the Internet of Things (IoT), or the idea of complete connectivity, has begun to be adopted by industrial markets. While each of these concepts – SCADA, M2M and IoT are unique – they have the same basic premise, and that is providing reliable, cost effective communication solutions by enabling data transfer from sensor to server, and ultimately the data user.

What is IoT?

IoT is all about comprehensive connectivity with internet protocol or IP technology. With a fully connected wireless infrastructure there are more sensors and more data points, which ultimately leads to a safer environment, cost savings and increased monitoring and automation. For example, if there are technologies collecting data or controlling processes in locations that are hazardous for people, an organization can protect its employees through automation by limiting the need to access those locations. IoT supports better asset monitoring because with technologies like wireless I/O there is opportunity to access more key points in the field for data collection. Like with SCADA and other industrial control systems, any move from manual to automated processes tends to bring significant ROI from time and labor savings, as well as increased efficiency.

As IoT rolls out, and a fully connected environment is in place, it also opens up more opportunities for sharing, storing and accessing data, which will lead to new business opportunities and streamlined operations. The collection and transfer of data from the field asset is a requirement in many critical industries such as oil and gas, agriculture, municipal operations, water/wastewater, and electric power. The systems in the industrial sector have developed into a full-scale Industrial Internet of Things (IIoT) or Industry 4.0 that relies on wireless M2M connectivity to collect, transport and process mass amounts of data for organizations with ease.

Power of Data with IIoT

There is no denying that the data collected from assets is extremely valuable. Complete connectivity through IIoT technology can further help organizations connect and collect more data. With wireless technology in particular, it is now possible to reach the most remote locations and transfer data reliably. Industrial organizations are creating a connected infrastructure with IP connections, rather than using

more traditional serial technologies. With IP enabled sensors or IP/IIoT enabled Access Gateways, the data generated by sensors at an asset location can be valuable to more than just the central control system. This might mean M2M communication with sensors talking directly to each other. It may mean that multiple systems consume the live, real-time sensor data directly from the field. It may even mean that operators connect their sensors directly to the cloud or back office systems. If there is a way to share critical data that addresses security issues and can help provide information to key data users, then that information becomes increasingly valuable.

Wireless in the IIoT space

IIoT isn't necessarily a new concept; connectivity in order to collect data is a huge component of both SCADA and M2M. Wireless is a beneficial tool in the IIoT that enables enhanced coverage to help an operator with remote assets ultimately deploy more sensors that are monitoring the right values at the right locations at the right rate. While wireless technology is not an absolute requirement in IIoT, an operator is less likely to get the ubiquitous coverage that is expected today if they select a wired only solution. Essentially, an industrial operator could have a completely connected facility with everything wired, but the expense to do that is generally prohibitive if they have a lot of remote assets. Extending coverage of assets and facilities that stretch across an entire city, or a series of plants, often creates cost and logistical issues when dealing with wired technology. Wireless, on the other hand, lets organizations establish connectivity in places that are not feasible in the wired world.

Although many industries are moving towards being completely connected via IIoT, it remains highly fragmented in the industrial world. Industrial markets are diverse and require different solutions based on specific considerations for security, networking, technology and daily operations. With wireless technology, however, the concept of a standardized IoT world becomes more probable. Consumer technology, for example, uses standards to ensure interoperability and allow for commodity type parts. While some of this commercial, consumer grade technology is "good enough" for industrial applications, many applications still require a level of industrial design and hardening that consumer grade products do not have. However, this presence of consumer technology in the industrial space and has the potential to push other IIoT technology towards more standards-based connectivity.

IIoT and Security

Security will ultimately be the limiting factor on how much IIoT is deployed. The traditional trade off of is either "easy to use" or "secure", but not both is still relevant. IIoT solutions often utilize some of the widely deployed security technologies from the Internet to avoid the custom, one off solutions of past industrial security, if it was used at all. IP technology makes it easier to deploy and talk to sensors, but it also makes it easier for intruders to see and snoop on your valuable data streams. With the use of TLS/SSL and basic AES-128 data encryption, even in an IIoT environment where data moves across an open network and it is assumed that an unauthorized party could potentially see the traffic on that network, secure connections can be established. When the data is properly encrypted, an unauthorized party cannot access the data even if they can see it in the network. In wireless connections, standards based connections will allow relatively easy access to the network itself, leaving just the software

encryption to stop snooping. With proprietary wireless links that several wireless providers offer provide a more difficult to snoop connection, a network is going to be less vulnerable assuming similar levels of encryption and security protocols are used. Frequency Hopping Spread Spectrum (FHSS) radios for example make it much more difficult to access data from that network, which adds another layer of security, but it doesn't replace the need for security in the actual data stream on the network and the technology must be able to address these security concerns.

Oil and Gas Example

Oil and gas is a security-conscious industry. The data that is transmitted via IIoT technologies can be extremely useful, if it can meet the security requirements while data is being transferred. For example, the data could identify the utilization or failure rate of a certain type of control equipment. If the failure rate of this equipment was consistent and data was then accessed and analyzed by the producer or trade group, they might be willing to pay users for that data. If efficiency can be improved by just a small percentage then there are billions and billions of dollars to be saved by creating efficiencies. These are the same promises of SCADA, however with IoT the industry is now looking at how every single asset, across every facility can be connected through the internet (or an intranet), making data readily available to key decision makers.

The Advantages and Benefits of Wireless for IIoT

Fundamentally, wireless provides connections for any piece of data that an industrial organization would like to connect to. With I/O there is the ability to connect sensors to servers and wirelessly move data no matter where the asset is located. With IIoT, the right wireless technology in place can provide the infrastructure needed to move data in even the harshest industrial settings.

There are multiple options for establishing IIoT, from FHSS and I/O technology, to WiFi, cellular or satellite. Each technology is suited for specific settings. For example, on the consumer level it is fairly easy to piggyback on an existing WiFi connection in order to enable an IIoT environment. However, in an industrial setting there are more challenges such as remote locations, long distance coverage needs, weather exposure, and noisy radio frequencies, harsh environments, etc. In these instances, a more industrially hardened solution will most likely have more success.

For example, if there is one truck with a cell connection on it that returns geolocation information once a day, or once an hour, a cellular connection might make sense for the wireless connection. In that type of environment there isn't a large complex infrastructure, so a cellular type of technology may be a viable option. However, when the goal for IoT is to connect assets and there is a specific area that needs coverage, there are wireless technologies that allow the operator to build that network to bring data back in, either for fixed assets or by connecting mobile coverage for a specific area. Wireless I/O can enable the transfer of sensor data from just about any point in the field, even if the asset is extremely remote with unusable cell connections. This type of technology typically has the encryption features to protect proprietary information by keeping it on the internal network. FHSS technology also provides another level of security and reliability in these types of environments. The protocols for this type of installation are still based on IoT; however the connection is via intranet or a private network. This

ensures that critical data will not be accessible by the outside world. No matter what type of technology is selected, the key to success in an industrial environment is the ability to make a connection at any point that it is needed and to safely transfer that data back to the stakeholders who will be using the information.

IoT Application Examples

IoT is being picked up in almost every industrial market, whether it's oil and gas, electric power, water/wastewater, agriculture, municipal, and many more. The use of automation in oil and gas is widespread. The ability to improve efficiency and save money drive this demand for SCADA data and the ability to do it through IoT will only continue to drive the demand for automation technology. Electric power and water/wastewater have also increased the adoption of automation technology. Power outages in remote locations that once took days to find and fix can be resolved in hours. As SCADA data continues to solve real world problems and lead to cost savings, the demand for IoT will continue to grow.

Another example is the general municipal market. Street parking in a city that is connected with IoT technology via sensors can push data to the cloud that is then used to notify consumers via a smartphone app. People visiting the city would then be able to identify and locate open parking spaces. In a parking garage, this type of app could help someone determine how many levels they will need to go in order to find a parking space versus endless winding through every level.

IIoT in agriculture could provide data about how much water was dispersed throughout a field or rainfall levels. This is connecting sensors both to the direct and indirect consumers and linking that data with a wide range of sources to make more intelligent decisions. There are many, many opportunities across the industrial world for IIoT, and the industries will need the connectivity through sensors and I/O points to be able to accomplish a complete IIoT infrastructure.

Conclusion

IoT for industrial markets provides the same connectivity in the industrial space as we see growing in the consumer space. Everything will be connected and for industry, that means anything can be monitored. As with all technologies and improvements, this evolution will not grow just because we have the technology to connect sensors to servers; it will grow because of compelling business cases to take the new technology that allow you to monitor and connect anything and solve problems of today, tomorrow and things we haven't thought of yet by enabling an operator to move data from wherever it is collected to wherever it needs to go. It creates an environment where it is possible to connect any type of sensor to a server with any type of data to and from any location. With these pieces in place, businesses can make intelligent decisions on how to spend their resources. Industrial operators and decision makers need to consider not only the right technology for their needs, but should be careful in their selection of wireless IoT providers. A reputable provider will go above and beyond simply offering a product. If there is difficulty establishing a connection to an asset, they will work on a solution. IoT is all about connectivity, and without a provider who is willing to make sure that happens, important data will be lost. Without that data there are missed opportunities. IIoT is about enabling those opportunities.