Wireless Sensors In Real-Time

Aaron LaJoie, Electrochem Solutions

The ability to make real-time decisions based on pressure, temperature or flow measurements while a process is running can provide significant advantages in a measurement and control system. These advantages can be expressed in different ways, such as cost savings through improved resource management or reduced reliability upon mobile workers. While measurement data can be used to dynamically control a process, it can also be displayed over a network to allow remote monitoring of the process status in real-time.

Rising pressures, temperatures or vibration intensity can easily be adjusted, if need be, if the appropriate personnel is aware of faulty conditions. As data is collected for process control or a system control and data acquisition system, it can also be archived for future reference when a review of process trends could provide additional improvements.

While wireless sensing clearly offers advantages, the adoption phase moves at a slow pace in many industries due to inaccurate perceptions. One of the main reasons wireless technology is yet to be fully adopted is price. Many organizations have not taken the time to explore the benefits achieved via wireless sensing in comparison to the price of implementing the technology. Similarly, a company may be content with their existing wired system and be reluctant to make the switch.

In 2009, a leading exploration company in the oil and gas industry saved almost $200,000 in installation costs alone by implementing wireless sensing. Digging trenches to install conduit and other signal wires can be very costly, and the process needs to be repeated for every new job, whereas wireless sensors are a one-time cost.

The second issue stems from concerns with the technology itself, namely latency, which is considered critical and can vary depending on which technology is chosen by an organization. However, latency is an inherent trait of all wireless. Unlike a conventional analog signal, there are delays associated with the analog-to-digital conversion process, as well as radio frequency transmissions. The time it takes from the start of the conversion process when the raw measurement is taken until the wireless signal from the sensor is received at the gateway or modem is considered to be the total latency time. The latency for each wireless technology differs.

Having said this, a wireless sensor network would never be as fast as a standard wired sensor network. Of the determinism that occurs between each layer of the wireless protocol (network, security, application, etc.), each takes a different amount of time, and this is all generally longer than its corresponding layer embedded in the wired versions of the protocols. Many wireless protocols also have to maintain very strict timing to ensure data packets are routed and delivered to the proper locations on time. Maintaining this adds to the total determinism and

latency of the system.

What to Expect from Wireless

Each wireless protocol has advantages. For instance, the ZigBee protocol offers low latency within the millisecond range and the ability to scale a large network. Bluetooth has slightly higher latencies, but significantly higher data rate capabilities, whereas WirelessHART offers channel hopping and can interface with hundreds of thousands of HART sensors and equipment that may already be located within the field. In addition, one WirelessHART network has a maximum size of about 100 devices.

Security is another concern when considering wireless adoption. 128-bit AES encryption is used across the majority of platforms. There are several extra precautions that can be taken in order to further protect wireless data, but it should be noted they do not offer advantages over standard encryption; they just add a simpler layer of security on top.

For example, ZigBee has a well-defined packet structure. Portions of this structure can be formatted in a unique fashion by making alterations to the application layer of the protocol. Only those who know the exact format of these packets can properly decode the data. However, AES encryption contributes to overall latency by making wireless transmissions slightly longer. This increases the demands of battery consumption.

The most pressing issue that companies face is the question of overall reliability. What happens if a node fails? Is the data stored anywhere to be retrieved at a later time? How does the technology function in a particular environment? Without explaining every possible scenario, we can look at several specific features of wireless technology that can help eliminate many concerns.

Signal strength is one of the best indicators of reliability. If a strong signal exists, there would be no communication loss. However, if the signal weakens, this may raise concerns regarding loss of communication links, and more importantly, loss of data. There are a few factors that can affect the strength of a wireless signal, such as interference with devices that produce a large amount of electrical or radio frequency noise, as well as a wireless device’s ability to coexist with other wireless devices, perhaps of a different protocol, such as Wi-Fi.

A common practice to ensure the receipt of a strong signal in a particular working environment is to conduct a field test, which is conducted by the manufacturer and would consist of going into a typical working environment, and positioning the wireless devices in common locations where heavy interference may occur. The devices would stream data packets back to a gateway device while being monitored.

For example, imagine there are steel barriers in direct line of sight from the wireless sensor to the gateway device that is stored in a control room. If the signal strength is strong and reliable under these conditions, then it is safe to believe that the

wireless signal would be accurate under all conditions in that environment. In contrast, if the signal is weak or no signal is found, then alternative options would have to be explored.

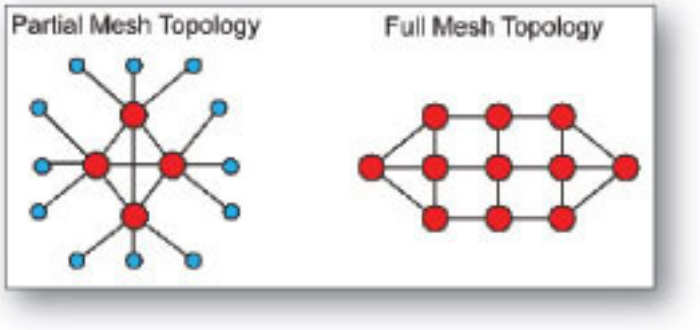

Figure 1: Meshing Diagram

One option would involve the use of a higher gain or directional antenna to improve signal strength. Another is the ability to use a meshing system. Meshing is the ability to use devices known as routers or repeaters to essentially extend wireless signals and make communication paths more reliable. When a wireless sensor network exists with meshing capabilities, various communication paths can be created, as seen in Figure 1. In partial mesh topology, nodes are only connected to certain other nodes, but in full mesh topology, every node is connected to one another. This way, if a device loses communication, perhaps by loss of battery power, an alternate communication path is automatically created, greatly reducing the chance of data loss. While Bluetooth operates primarily on a master/slave relationship, ZigBee and WirelessHART support meshing. In Figure 2, we can see a common configuration of a ZigBee mesh network consisting of end devices, routers and coordinators. Coordinators and routers can communicate with any other device, but end devices can only communicate with routers and coordinators.

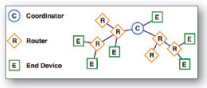

Figure 2: ZigBee Wireless Networks

A typical WirelessHART network configuration is an example of a full mesh network topology. In addition, ZigBee has a retry metric that offers the ability to resend data if the original message was not properly sent and received the first time. In ZigBee, there are proper sequences that need to take place, such as acknowledgments between the wireless device and the gateway when a data packet is transmitted. If an acknowledgment does not occur on both ends, it is assumed that the data was lost and then attempted to be resent. This is a parameter that can be configured similar to other ZigBee parameters.

Powering Up—Wirelessly

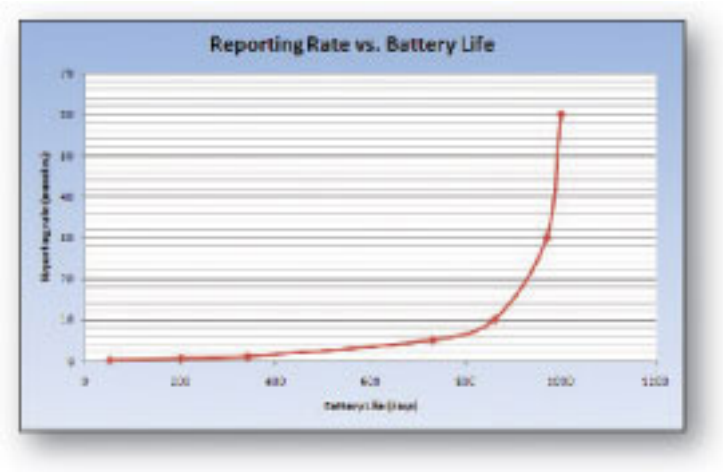

Figure 3: Battery Life Chart

It should be noted that many of the features mentioned above have an effect on the battery life of the wireless sensing devices. One example of this is turning on 128-bit encryption, which tends to consume slightly more battery life than if it were off. Similarly, the latency and/or response time of wireless sensors also have a large effect on expected battery life, as seen in Figure 3.
Many wireless sensors have programmable transmission frequencies; in other words, it is easily adjustable to ask the device to transmit a reading once every minute or 10 times per second. Considering the actual radio frequency transmission consumes the most battery power, we can expect to see a shorter battery life from a device that transmits 10 times per second. For this reason, a consumer may choose a ZigBee-enabled device. ZigBee is known for its ultra-low power requirements. The transmission rates are programmable, along with the actual transmit power. ZigBee devices also resort to a very low power mode when the device is not transmitting in an effort to conserve power.

After discussing the sensing side of the wireless equation, it is also imperative to understand the receiving portion, also known as the gateway device. Gateways are used to receive wireless signals, but more importantly, process the data to allow interface with a company’s existing control equipment. These gateways offer numerous hardware interfaces, such as serial RS-232 or USB and digital I/Os or relays, as well as software interfaces, such as MODBUS-RTU or TCP/IP, OLE for Process Control (OPC) or FTP and Telnet. Common applications involve connecting a gateway device to a CNC machine’s controller through RS-232.

Wireless pressure sensors can monitor clamping pressures on tooling pallets inside of machines to verify that parts are being machined properly. These measurements would be provided to the machine’s controller through MODBUS-RTU. If the clamping pressure is too low, the machine’s cycle would automatically cease, preventing the destruction of accompanying machine parts. Another option would be for temperature measurements to be wirelessly transmitted to a gateway device. This data would be processed and published to a company’s network or existing historian software over an Ethernet connection having an OPC interface.

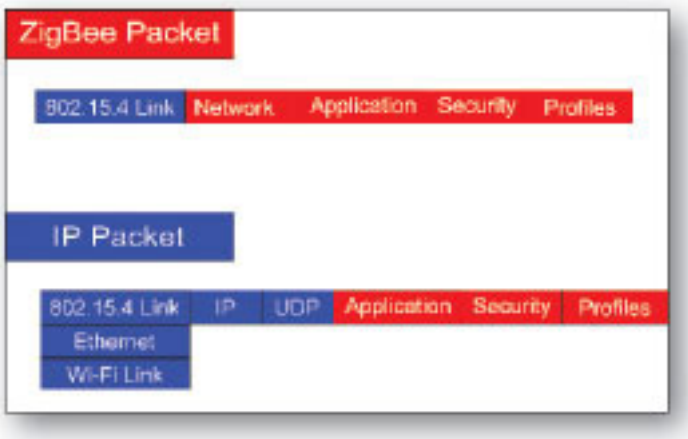

Figure 4: ZigBee Message over IP

Recently, many companies have shown great interest in having the ability to control all of their sensing needs via the Internet. ZigBee, for example, is one of the first wireless standards to adopt a functional IP protocol and set of IP-connected devices that can interoperate natively with other IP-connected devices. ZigBee's proprietary IP protocol, implemented in the application layer, is designed to easily integrate existing ZigBee devices. The standard ZigBee data packet structure is combined with a conventional IP data packet, as seen in Figure 4.
The goal is to define a compact, low-traffic message format that can support embedded systems that are attached to low-bandwidth, low-power networks. Devices are allowed to communicate with one another by implementing manufacturer-specific application profiles. These profiles are a set of parameters that define communication channels and other vital settings to assure proper communication and operation between devices. ZigBee/IP profiles also allow for larger sensor networks and increased network security.

Another main focus of this protocol is to fit the needs of extremely resource-constrained devices. Unlike HTTP or XML, which require more resources to decode and process, the binary messages created by ZigBee are simpler to implement and are much better suited for low-bandwidth networks.

Aaron LaJoie works for Electrochem Solutions Inc. For more information, please visit www.electrochemsolutions.com *[1].*

Links:
[1] http://www.electrochemsolutions.com