AS SEEN IN THE SUMMER 2008 ISSUE OF...
Valve MAGAZINE

THE RELIABILITY AND SECURITY OF WIRELESS VALVE MONITORS

THE INTRODUCTION OF THE WIRELESS HART PROTOCOL IS ONE OF THE THREE TOP AUTOMATION TRENDS OF 2008, ACCORDING TO THE ARC ADVISORY GROUP OF BOSTON. AND A QUARTER OF THE RESPONDENTS TO A POLL CONDUCTED LAST YEAR BY *INTECH* MAGAZINE CALLED WIRELESS THEIR "BIGGEST CHALLENGE OF 2008."

BY KURTIS JENSEN

Wireless technology is a hot button for anyone involved in the design, operation, maintenance or upgrading of process industry plants. This is because it promises to lower construction costs while greatly expanding the ability of personnel to monitor and communicate with equipment in remote or hard-to-reach areas.

If you knew when valves were not performing, you would be more reactive. You could avoid sending personnel into undesirable conditions just to verify a valve's position. You could even eliminate the need for someone to check the status due to a new regulation, allowing you to do more with the resources you have. Or, you may want to keep a watch on certain manual valves, but power is nowhere near. These are only a few compelling reasons for considering wireless technology for a variety of valve applications.

The first wireless transmitters of pressure and temperature data are already working in the field, and wireless devices to monitor valves and provide feedback are on the way. But end-users want assurances of reliability and security before they will be willing to commit to a new technology.

The single most important factor in adopting any new technology is reliability, and wireless is no different. Security is equally critical, so wireless applications will be subjected to the same scrutiny as information technology (IT) systems with respect to their security. Unless the reliability and security of wireless instruments are as good as or better than existing wired systems, why even consider their use?

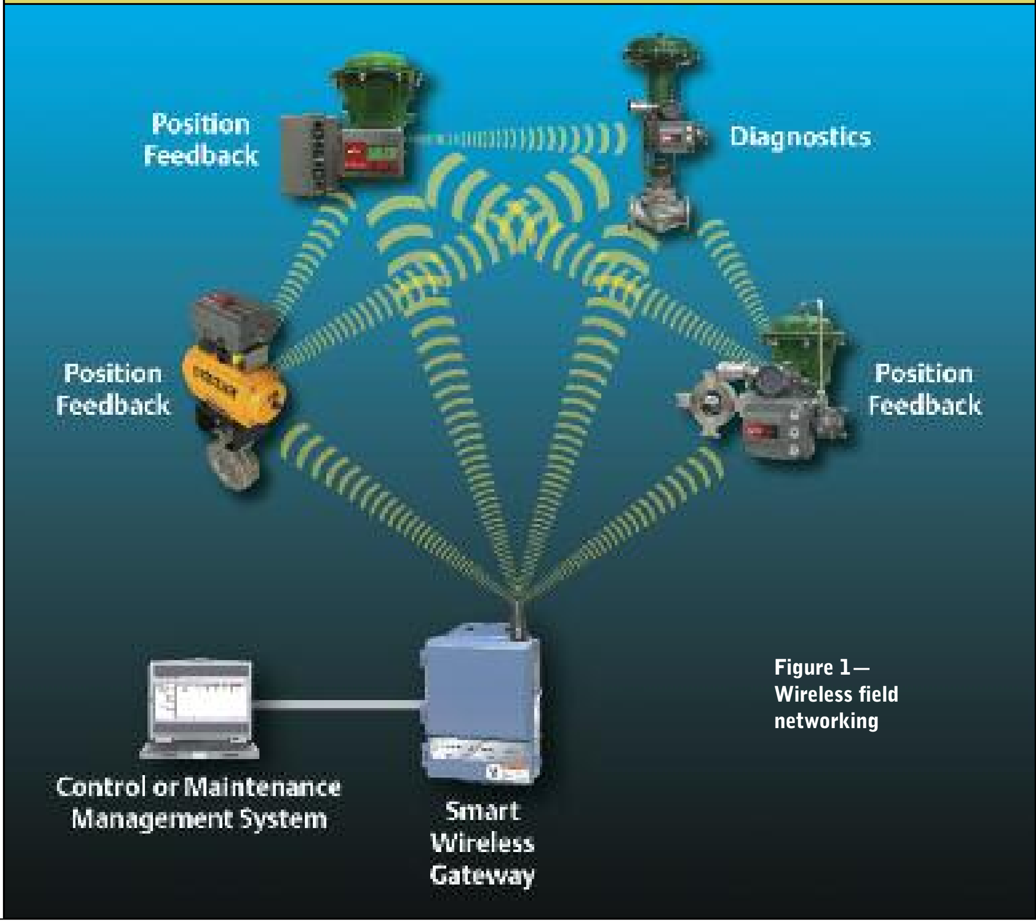

Figure 1—Wireless field networking

Reliability's a Real Consideration

The reliability of wireless systems depends on having multiple paths of communication so that if one device fails or is blocked, another path can be taken. This is solved through the use of "mesh networks" that offer many different paths for transmissions to follow in order to reach the gateway (or receiver), which directs the communication to a control system or other appropriate locations in the plant. The mesh provides redundancy that yields a high level of communication reliability no matter what permanent or temporary obstacles may exist between the transmitting device and the gateway. This is *not true* of all wireless systems.

Another assurance of reliability is an electronic technique called "frequency hopping." If one of the assigned frequencies is jammed or compromised by noise or other interference, the wireless transmitter senses the problem and automatically uses another channel.

With multiple paths between devices and many frequencies available, the reliability of wireless networks is at least equal to wired systems, and they are not subject to power outages or inadvertent damage to cables. The mesh network concept and frequency hopping techniques are included in the already-approved WirelessHART standard to which the smart wireless system adheres, as well as the pending ISA100 standard.

Devices based on this technology have been proven in use to demonstrate greater than 99% data transfer reliability.

A large number of wireless transmitters rely on battery power with battery life typically running between 5 to 10 years, depending on how fast a given device updates. This is a distinguishing characteristic between wired and battery-powered devices. Wired instruments send information almost constantly, whereas wireless devices may operate on a one-minute schedule, remaining at rest most of the time and coming to life just long enough to transmit an update. This can be done more often if required by the situation, but with a corresponding reduction of battery life. In addition, these devices provide an estimate of remaining power life that enables scheduled maintenance.

Serious About Security

A very real issue with all wireless transmissions is that some outsider might be interested in intercepting or altering the data. Security is taken very seriously by IT experts, who have identified several important elements to wireless transmission security.

The first of these is encryption, a method of seemingly random symbols that surround each transmission. Even if the message is intercepted, it takes too long to decode to be of use. Encryption keys are changed frequently so that anyone trying to read intercepted messages by comparing them will not be able to break the code before it is changed.

In addition, each transmission must be authenticated, meaning that the sending and receiving devices must recognize each other, or the transmission will be ignored. Another step is data verification by the receiving device. The authentication and verification rules are built into the devices, so no foreign device will be able to intercept a transmission or send bogus information to the receiving station.

The channel-hopping feature discussed earlier protects against jamming of channels by either intentional or non-intentional sources, which is the final key to secure wireless transmissions.

Again, all of the required security features are built into the smart wireless system.

Advantages Over Wired Applications

Wireless offers many advantages over wired applications in the right circumstances, but wireless should not be viewed as a direct replacement for wired instrumentation. Wireless devices are typically slower but can be installed in a matter of minutes. They can often be installed where wired devices cannot—in hard-to-reach locations, in areas hazardous to plant personnel, where power doesn't exist and where running wires is not allowed or prohibitively expensive, to name a few.

Initially, most wireless devices will be used for monitoring remote but critical sites to improve operational awareness of certain equipment. Wireless transmissions will overlay existing operating architectures at many sites. In such cases, additional wiring is not needed, and existing wired networks are not impacted.

A second stage of wireless development will occur when outdated wired instrumentation is replaced by wireless (Figure 1, page 22). The farther an operation is removed from the control center, the more attractive wireless will become for full control functionality. Driven by lower engineering and installation costs, wireless upgrades will be simpler and easier to implement because new conduit and wires will be eliminated.

Other advantages of wireless technology include:

- Reduced project reviews so projects are completed faster
- Intrinsic safety, due to low power consumption
- Manually operated equipment easily added
- An additional layer of assurance in safety-related applications

Motivation for Wireless

The ease and simplicity of implementing wireless technology can be a strong motivator, especially when minimal engineering effort is needed for the important coordination-of-project reviews. As work forces diminish, anything that requires less effort by a smaller and less experienced staff becomes a motivator.

Improving operational effectiveness is perhaps even more important. This includes reducing the number of times operators or maintenance personnel must go out to touch equipment and the amount of time needed to take corrective action when necessary. In some cases, regulatory agencies are demanding more information about operating equipment, especially valves. This may include more frequent measurements that use a structured or automated collection process.

A smart wireless solution does not require a large investment in site surveys or an existing wireless infrastructure. An available startup kit includes the gateway and a few field devices to measure or monitor selected sites. A self-organizing mesh network can often be operating in a matter of minutes, and more transmitters can be added easily and seamlessly as budgets evolve.

It's Here Now

Gaining the benefits of the valve applications outlined above requires a solid foundation of wireless networks and control infrastructure. To meet this need, the wired and wireless worlds are integrated in a single, scalable infrastructure that helps end-users optimize applications across an entire operation. In effect, the benefits of the digital plant architecture are extended to assets that were previously out of physical and economic reach.

This approach is based wholly on open standards so designers can choose from a variety of wireless solutions without being tied to a specific technology or vendor.

The self-organizing mesh technology that is the basis for WirelessHART has been tested and proved in the field. Each wireless device in a self-organizing network can act as a router for other nearby devices, passing messages along until they reach their destinations. If there is an obstruction, transmissions are simply re-routed along the mesh network until a clear path to the gateway is found.

As conditions change or new obstacles are encountered in a plant—such as temporary scaffolding, new equipment, or a parked construction trailer—these wireless networks simply reorganize. All of this happens automatically, without any involvement by the user. This capability provides redundant communication paths and better reliability than direct, line-of-sight communications between individual devices and their gateways.

This self-organizing technology optimizes data reliability while minimizing power consumption. It also reduces the effort and infrastructure necessary to set up a successful wireless network. Traditional point-to-point wireless networks require costly and time-consuming site surveys to be certain that every node in the system has a line-of-sight path. Such a network can require up to three times as many infrastructure nodes as an efficient self-organizing network.

These self-organizing field networks use IEEE 802.15.4 radio technology with channel hopping as the physical layer. They are designed and tested to be tolerant to interference and can co-exist with other wireless networks in a plant. The networks are also highly scalable with low latency.

The cornerstone of this system is the wireless gateway, which can serve up to 100 wireless field devices on a single network or on multiple networks. In the future, remote operations controllers will also operate as gateways. These gateways pass on the field-generated information to the control system where appropriate alarms can be established to notify operators of changes occurring in any of the monitored devices. Diagnostic data are passed to asset management software to be processed and made available for use by maintenance personnel.

Wireless on Valves

Most operations have a large number of "blind valves" that are either manual or semi-automatic but provide no valve position feedback, normally because of cost or location. As such valves age, their performance can degrade to sluggish, slow operation. The true position of the valve may be questionable, and operators have to start visiting certain trouble-prone valves to verify their position. Where valve position monitoring does not currently exist, wireless monitoring is a great way to start using this technology with minimum risk.

There is also an excellent opportunity to obtain previously unavailable performance information, sometimes called "stranded diagnostics," from many valves, such as automated control valves. Digital valve controllers generate useful diagnostic information, but the data cannot be captured remotely because the plant does not support a digital architecture. If a valve is not actually closed when it is supposed to be, leaking steam or a process chemical can cost thousands of dollars without anyone knowing about it. A wireless device could provide assurance of the closed position, thus eliminating an operator's "blind spot." At a minimum, this would result in decreased response times to developing problems—and it could help prevent expensive losses.

The wireless infrastructure will be largely incremental, allowing reexamination of previous automation decisions for improved process operations and safety. In both cases, valve health issues can be discovered before they affect the process.

Wireless monitoring of valves not only makes sense but can be done today. For those considering wireless, look around at your valves and ask how you can be more responsive when their performance starts to degrade. At the same time, you can make better use of personnel by not having to send them out to check valves as often, if the same valve information can be obtained wirelessly. And it's being done—today. **VM**

Kurtis Jensen is an Instruments Product Manager at Emerson Process Management, representing Fisher and Valve Automation Products. His responsibilities include control accessories and related field instrumentation. Reach Jensen at kurtis.jensen@emerson.com.

FISHER®

EMERSON™ Process Management