Wireless Technology & Best Practices To Reduce Project Costs

by: Mark Menezes

The benefits of wireless seem obvious – "no wires". Despite this, fewer than 1% of installed measurements in process plants and mills are wireless. Fortunately, real and perceived obstacles to wireless deployment are being overcome with improved technology, most recently the "self-organizing network".

Other obstacles are not based on technology, but on the lack of security, standards, and consensus on appropriate applications, so are best addressed with a discussion around "best practices". Users can now consider adding measurements previously impossible to cost-justify, improving safety, reliability, efficiency and environmental compliance.

Why Wireless Measurement?

Wireless gives users low-cost access to additional measurements which would otherwise have been too costly to install. Examples from early adopters include:

- *Environmental:* advise in real time when pressure relief valves open and close, minimizing fines from regulatory agencies
- *Personnel Safety:* annunciate activation of emergency stop buttons, pressure and temperature switches and other alarms to the centrally-located operator
- *Health:* monitor water temperature and pressure at eye-wash stations, minimize "clipboard carrying" trips to the field to record data
- *Process Optimization:* monitor and trend additional process temperatures, pressures, flowrates for online and offline process optimization
- *Equipment Reliability:* monitor pump and motor vibration and temperature, strainer plugging, hot spots
- *Process Availability:* communicate open/close status of manual bypass valves to the centrally-located operator
- *Temporary Measurements:* test, verify and optimize operation of boilers, compressors and other capital equipment requiring performance contract
- *Portable Measurements:* measure and record flowrates, pressures, temperatures and levels for test skids and flow provers

Wireless, like bus technologies such as FOUNDATION® fieldbus (Ff), offers reduced installation cost, plus easy access to multiple process and diagnostic variables per device. Integrating Ff can be problematic when the installed control system is old or at capacity, so this technology is usually considered for greenfield installations or significant plant expansions.

With wireless, incremental devices can be easily added to any "brownfield" installation, even where the existing wired infrastructure is full. New wireless points can be seamlessly integrated, with full access to multiple variables and device diagnostics.

Wireless and Ff savings vs traditional point-to-point wiring include material – wire, junction boxes, cable trays, conduit, IS barriers, and DCS I/O cards, racks and power supplies – plus engineering, procurement and installation labour.

Total installed cost of a traditional point-to-point wired measurement can be two-to-ten times the acquisition cost of the transmitter itself. Where an individual device can provide multiple process variables – for example, a temperature transmitter with 8 inputs, or diagnostics – savings are multiplied. Additional benefits come from reduced physical space requirements, and from the increased flexibility and ease of expansion of a wireless or Ff system.

Self-Organizing Networks

Wireless devices have been used for decades to connect a few remote points – the "island of automation" – to the central control system. In some applications – water and waste treatment, oil and gas production – the majority of points are distributed over these islands. A Supervisory Control and Data Acquisition (SCADA) system – rather than a traditional PLC or DCS – is needed to tie them together.

While these solutions will continue to be used in these widely-distributed applications, the most interesting new development for a typical process plant is the self-organizing network. Each transmitter contains a smart RF radio. While RF is a "line of sight" technology, it's more flexible than infra-red, for example, and can work through most walls and gratings, and around smaller pipes and pumps. Devices which are within say 250 m, and not blocked by large, solid vessels or thick, reinforced walls and floors, can communicate directly with the gateway. In a "mesh" topology, a device which cannot see the gateway needs only to see another device, so a data packet can "multi-hop" between as many devices as necessary until it gets back to the gateway.

This mesh architecture is ideal in a plant environment, as it allows devices to see around tanks and other solid metal obstacles without the use of tall, costly antennas or repeaters. Once the system reaches sufficient density, the user can safely assume that any new device will be able to see at least two other devices, so failure of any one device will not affect network communications. In a "self-organizing" mesh network, the devices will automatically form the multi-hop connections back to the gateway, and re-form those networks dynamically as new devices and obstacles are added. This ensures the highest possible reliability with minimal configuration effort, and avoids the cost of a site survey.

Installation benefits are maximized when the self-organizing network devices are powered by internal batteries, with Class1 Div1 hazardous approvals for the transmitter+battery system. This is achieved by using devices designed specifically for process wireless applications, as opposed to simply combining off-the-shelf transmitters and radios.

Conventional devices can use up to 20 mA continuous current, simply to drive the analog output. A wireless pressure sensor can run on 1 mA, a temperature sensor even less. Plus, these devices can be designed to minimize turn-on time, making it practical for a device to power up to take a reading for only 1 second per minute, for example. Taken together, these capabilities can provide 5-7 year battery life in typical applications. The battery is user-replaceable in the field, without jeopardizing area approvals or requiring hot work permits.

Best Practices – Security, Standards, Applications

Before the user evaluates a particular wireless technology, they should consider:

- *Security:* does the solution ensure that the data is available, valid and accessible only to authorized users?

• *Standards:* is the solution "open", allowing seamless integration with devices from multiple suppliers; or, does it lock the user into a single supplier?
• *Appropriate applications:* although some suppliers promote "wireless everywhere", responsible bodies including ISA SP100 recommend wireless only for specific types of applications.

Careful, prior evaluation of all three of these factors is even more important with wireless than with other "new" technologies. With wireless, problems may not become apparent during the typical 3-6 month trial/acceptance period. So, a solution which seems to work well during a trial or visit to a reference site can cause problems in future years when the system is scaled-up, if these three factors have not been addressed.

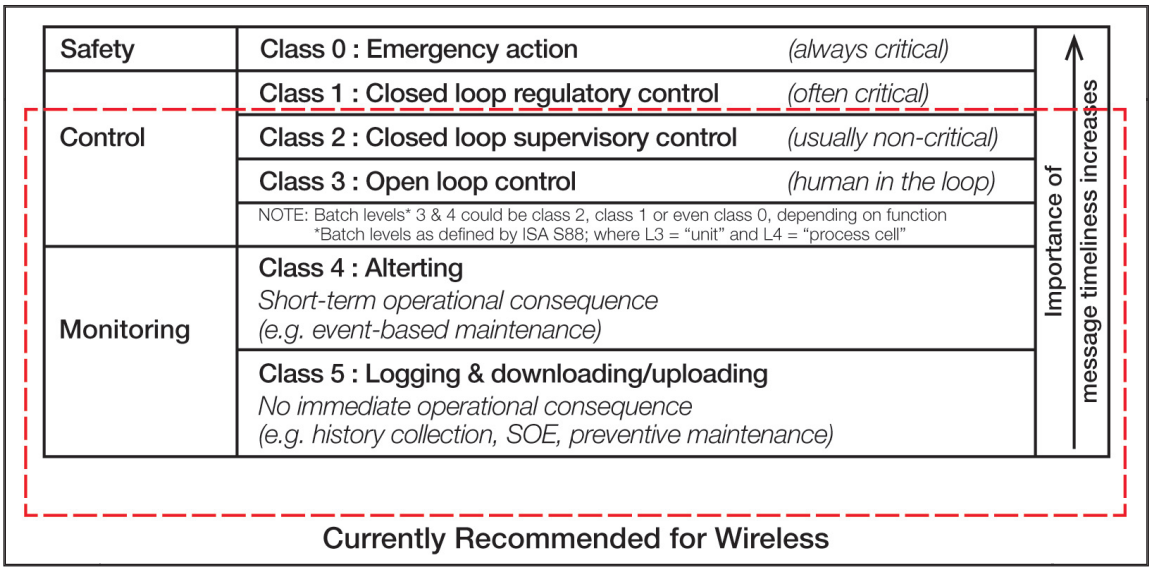

Figure1: Guidelines established by the ISA SP-100 committee

Security

Security is important because wireless data and devices can be accessed outside the plant fence, which bypasses the usual plant security. Related to security is reliability. A reliable system design ensures that data gets through every time. A secure system ensures that data that gets through is valid data, and only allows access to those who should have access to the devices and data. Both safety and reliability can be impacted deliberately by hackers, or accidentally by devices that can physically block or interfere with the radio spectrum.

Robust security provides multiple levels of protection against interference and attack. First, to ensure reliability, the system must be frequency agile – meaning that if a particular frequency becomes blocked, the radio will try again at another frequency.

In theory, licensing and operating at one fixed frequency will eliminate the risk of interference. In reality, in a typical plant environment, much of the interference is generated not by other radios but by devices that generate spurious, random emissions, like welding torches, variable-speed drives, etc.

So, while fixed-frequency, high powered radios may be preferred in remote oil/gas-field applications, lower powered frequency hopping provides better reliability in crowded plant applications – plus, the well-behaved network is less likely to interfere with other in-plant networks.

Second, all data should be sent with encryption, so someone listening in – easy to do with a RF scanner and a laptop – will not be able to decode the message and steal data. Related is authentication/verification – so only valid devices can gain access to the system.

Finally, even the most secure design can be defeated by poor password/code management. Instead of using static keys, the system should generate dynamic, rotating keys, and automatically update all devices periodically.

To add a new device to the network, the user would use a handheld to configure a network name and "join key" (similar to WEP on a wi-fi network), but only the encrypted rotating key would be broadcast over the network.

Open Standards

Many wireless products being installed today use proprietary communications, so the user is forced to buy devices – now and forever – from that one supplier. Beyond the obvious issues from a non-competitive environment, the user should be concerned about the risks of obsolescence. Proprietary devices can thrive in a standards-free environment, but experience has shown that once widely-supported open standards appear, those standards are embraced and the proprietary devices soon disappear. For example, although proprietary protocols were widely-used in the 1980s and 1990s, the only smart transmitter protocols to survive today are the open protocols – Ff, Profibus, and HART.

Depending on the application, open wireless standards either exist or are emerging in the short-term. For example, for communication between "islands of automation" – clusters of widely-separated devices – Wireless Ethernet is well established. For cell phone data, the most widely-used open standard is GSM.

The ideal open standard for communication between the wireless gateway and host is OPC (OLE for Process Control), typically over Ethernet, while RTU Modbus is supported by even the oldest host.

The relevant standard for in-plant applications is WirelessHART®. This open protocol – ratified in September 2007 - is supported by the more than 200 members of the HART User Group, and is backward-compatible with the 20 million+ installed base of wired HART devices. So, a user can use the same handhelds, and the host will display the device data using the same device driver, including recent EDDL enhancements, as with their existing wired HART devices.

Suppliers can easily redesign their HART product portfolio to work with WirelessHART – over 1000 HART devices are registered with the HART Foundation. This ensures that devices will be available for almost any application within a relatively short time, in contrast to the early years of Ff, when "niche" technologies were not available with Ff from any supplier. Eventually, users will choose to add wireless capability to existing, installed HART devices.

Since the devices are (presumably) already wired, the benefit will be to access diagnostics and secondary variables and support remote maintenance, rather than to save wiring costs.

Appropriate Applications

While wireless offers significant benefits, and robust security and open standards minimize risk, the user needs to use wireless only in appropriate applications. The best wireless designs can provide high data reliability – 99.9%+ – by ensuring that all data transmissions require a read receipt, and that data is automatically re-transmitted as often as necessary if blocked or interfered with. However, no design can guarantee that every single message gets through immediately, leading to variable latency.

The system designer should only consider wireless if all users of the data can tolerate this variable latency – the data will always arrive, sometimes in less than 1 second, but sometimes in 10 seconds, or longer. Since the data is time-stamped, latency does not affect the validity of trends or event logs, so this is normally acceptable in monitoring, trending or open loop control. However, variable latency is normally not acceptable for closed loop control or safety applications. For this reason, the ISA SP-100 committee has established guidelines (Figure 1).

Wireless technology should therefore be used for monitoring, logging and remote maintenance applications only. If the user has a project which includes both monitoring and critical control/safety points, one option might be to hard-wire the control and safety, and use wireless for the monitoring points. Or, the user can locate the critical control and safety logic in a local controller or PLC, or – in the case of Ff – in the devices themselves. Updates from the local controller can then be communicated wirelessly to the central host – variable latency will affect only the updates or operator commands, not the local control itself.

A more creative approach can be considered when new points are being added in an area with existing, full infrastructure (junction boxes, trays, DCS I/O, etc). Here, the user may choose to convert existing, wired monitoring to wireless. Then, that freed-up infrastructure can be re-used for the new critical control/safety points. From the installation savings alone, the user can often pay for a new wireless infrastructure, easily expanded in future.

Users should be careful not to base latency expectations on the trial/acceptance period, or a short visit to another similar site. By analogy, think of using Family Service Radios, which use RF radio technology. A pair of radios may work extremely well during the "trial" at the local mall, with minimal interference, multi-km range and short latency. When the system scales up and interference increases, range decreases and data latency increases ten-fold.

Over time, as wireless technology and user experience evolves, these guidelines will probably be relaxed, and in the future it's conceivable that wireless devices might even be used for the most critical control and safety applications.

Best Practices - Summary

Users can now consider adding measurements previously impossible to cost-justify, improving safety, reliability, efficiency and environmental compliance. New wireless self-organizing network technology provides significant benefits in reduced installation cost, flexibility and easy access to MultiVariable™ devices and diagnostics, all with seamless integration to legacy hosts.

To maximize benefits and minimize long-term risk, the user should:

- Consider wireless for new monitoring and logging applications
- In legacy plants, consider using wireless to free up existing wired infrastructure for critical new points.
- Satisfy themselves that any proposed solution incorporates robust security and open standards

Mark Menezes, P.Eng. has a degree in Chemical Engineering from the University of Toronto and an MBA from York-Schulich. He has 17 years experience in industrial automation, including 7 years with control systems and loop controllers, and 10 years with measurement. Presently, Mark manages Emerson Process Management's measurement business in Canada.

Emerson Process Management