Industrial Wireless Instrumentation
Adoption Considerations

Paul Sereiko, AIW LLC
Jay Werb, AIW LLC

User Adoption of Wireless Instrumentation

This paper covers a variety of end-user considerations in adoption of industrial wireless instrumentation.

In Clayton Christensen's model of innovation, low-cost products initially take a beachhead position with simple applications at the lower end of a market. From that starting point, they then work their way up market. A tipping point occurs when mainstream users discover that the low-cost products can be used in high-end applications.

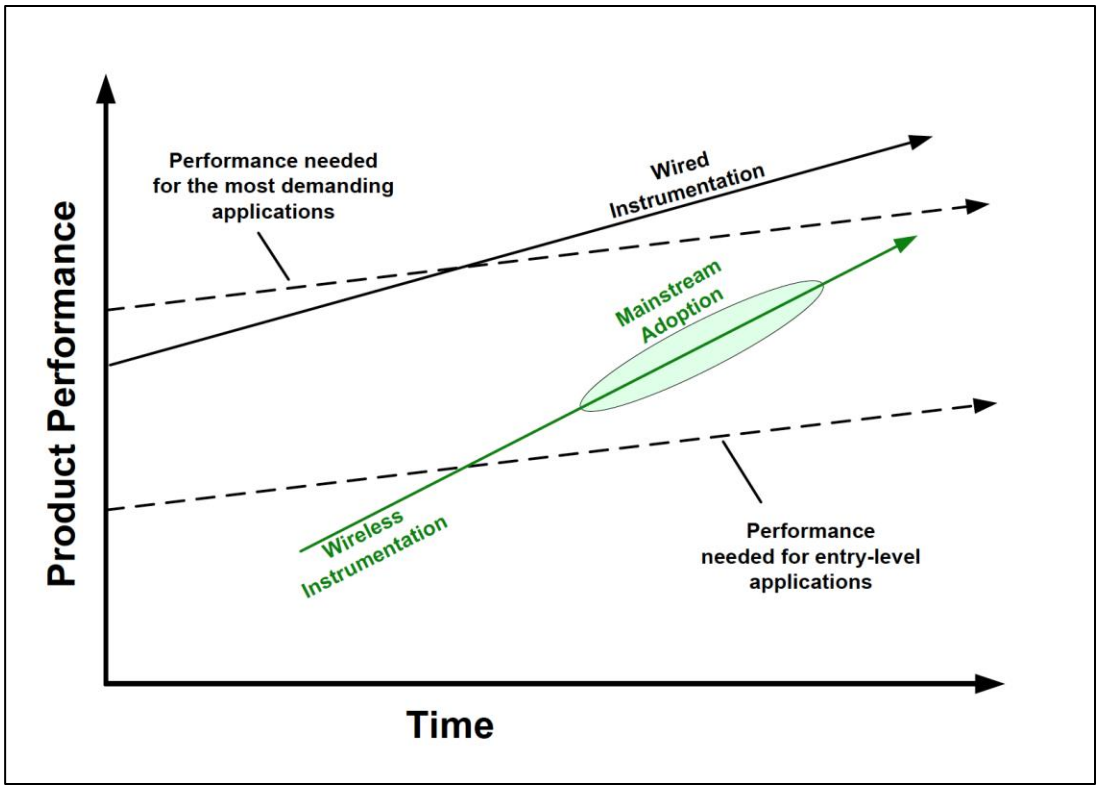

Figure 1 – Christensen's innovation model adapted for industrial wireless instrumentation

Industrial wireless instrumentation is rapidly becoming the technology of choice for a growing class of applications. A wireless deployment can enable significant cost savings compared to an equivalent wired installation, resulting in 20-30% savings in simple configurations. Cost reductions can be even more compelling in scaled installations or in remote locations. Where wiring is cost-prohibitive or

infeasible, wireless enables best practice instrumentation wherever it is needed for efficient and safe industrial operation.

The cost advantages of wireless instrumentation improve with scale. In a wired system, the cost of each additional instrument involves extra wiring and all of the associated labor, equipment, and maintenance. A wireless system, if designed for scalability, can accommodate additional devices with the same infrastructure and no additional wiring. For the first time, applications involving hundreds or thousands of points can be reasonably contemplated.

Until fairly recently, most users and experts viewed wireless instruments as intrinsically inferior to their wired counterparts, with wired instrumentation always being preferred when economically feasible. As experience with wireless technology grows, this attitude is shifting, with wireless becoming the default user selection for well-proven applications. Today, major users require cost justification for wired instrumentation in applications where wireless has been demonstrated to exceed user requirements.

Wired Versus Wireless Instrumentation

Table 1 summarizes the main functional differences between wired and wireless instrumentation. Some of the listed characteristics, such as fading and interference, relate to radio considerations. Other characteristics, such as battery replacement, relate to energy constraints when wireless instrumentation operates in locations where no power is available.

Table 1 – Principal differences between wired and wireless instrumentation
Courtesy AIW LLC

	Wired Instrumentation	**Wireless Instrumentation**
Installation	Wiring feasibility and cost o Data and power o Cable length; Configuration rules Infrastructure equipment	Access point architecture and placement Range to access points and neighbors Mesh network design
Instrumentation	Full range of available instruments o No battery constraints Proven in use for decades o Generally SIL rated Continuous reporting	Partial range of available instruments o Wireless adapters if power available Proven in use for years o Sometimes SIL rated Periodic reporting
Performance	Bus capacity o e.g., 4-20 mA Reliable until the wiring fails o Corrosion, vibration, etc	Data freshness & availability o e.g., 30 sec @ 99.99% Shared channel capacity o e.g., 90,000 timeslots/min Channel transients o Fading, interference, blockage, etc.

Management	Add wiring & equipment as needed Fix wiring after it fails Monitor instrument reporting	Short-term management: o Redundancy for automatic self-healing Long-term management: o Monitor network diagnostics o Anticipate systematic problems o Reconfigure wireless infrastructure o Battery management o Radio spectrum management
Security	Physical security of device and wire	Physical security of device Management of credentials and keys Network diagnostics
Redundancy	Extra wires for redundancy	Radio mesh Radio as complement to wired link

Major advantages of wireless instrumentation include:

- Lower cost, especially when large numbers of instruments are installed.

- Manageability. When wired connections fail, they are typically complete failures that occur without notice. Although wiring typically fails at connection interfaces, any physical point along the route is a potential failure point. Wireless failures are usually transient, and those transient problems can mostly be avoided by preventative maintenance linked to wireless diagnostics.

- Flexibility. After a wireless system is installed, it is easy to add new wireless instruments and also to report more data from existing instruments using wireless adapters.

- Security. Wireless security extends to the field instrument and does not rely on physical security of the transmission medium. (Some fieldbus technologies assume that field wiring is secure and therefore have no cryptography on the field instrument.)

- Redundancy within a wireless network. Typically, a wired instrumentation relies on a single wire to each instrument, with various opportunities for failure. A well-designed wireless system has redundancy built in at all steps in the transmission chain without any failure-prone connectors. Field experience is demonstrating that a redundant wireless channel can be every bit as reliable as a non-redundant wired channel, particularly when wires are long and/or subjected to challenging conditions.

- Redundancy at the plant level. A wireless system can be used to add redundancy to wired reporting, with the same data reported through wired and wireless channels. Similarly, when field instrumentation is involved in an independent protection layer (IPL), wireless may provide an advantage if another IPL uses available wiring.

Table 1 also suggests a set of generally agreed disadvantages of wireless instrumentation at this time. These considerations can be generally grouped as battery-related and radio-related.

Disadvantages of battery-powered operation include:

- Battery maintenance. Battery maintenance of wireless devices constitutes a factor that somewhat offsets wireless cost savings. In addition, if battery maintenance is not performed correctly, the instrument will eventually fail. A well-designed wireless solution should ensure that battery replacement occurs in conjunction with an instrument's general maintenance interval.

- Limited wireless instrumentation. Today, there is a limited range of available wireless instrumentation. A HART or Modbus wireless adapter can convert a wide range of wired instruments to wireless, but only if the wired instrument has the power to operate. In locations where wireless is needed, there may be no source of external power, and that limits the instrumentation options. For example, users have told the authors that no battery-powered clamp-on flow sensors are available today (mid-2014). However, new wireless products are being rapidly released to meet market demand.

- Continuous sampling. In some cases, it is not technically feasible to sample and report process data continuously under battery power. Wireless instruments can be configured to report process data frequently in critical applications, with predictable battery life impacts, but only if the sensor has the energy to collect the data in the first place.

Disadvantages of radio operation include:

- Procedural barriers. Wired instruments have been used for decades, and processes for specifying and approving wired systems are well established at user sites. Many of these same users do not have clear processes for approving wireless, particularly when safety credit is involved. At the time of this writing, wireless is rarely if ever used for automated Safety Instrumented System (SIS) applications at many sites due to procedural impediments (including but not limited to SIL requirements). Wireless Safety Related Alarms (SRA), such as gas sensors reporting to an operator, can be considered non-SIS and are being embraced as such at a growing number of sites.

- Statistical nature of radios. Radio performance is statistical by nature, with packet errors and retries being fundamental considerations for any wireless system design. Performance requirements are probabilistic, for example, a data freshness requirement of 30 seconds with 99.99% availability. A well-designed wireless system will have plenty of margin built-in and extensive network diagnostics that detect loss of margin even while the system achieves its performance objectives.

- Limited reporting rates. Wireless instruments and systems can be configured to support reporting as frequently as every second with a transmission latency of a fraction of a second. Sub-second reporting rates are not typically used for battery-powered instruments at this time.

- Spectrum management. Wireless instrumentation shares the radio spectrum with other systems and applications. Spectrum management generally needs to be considered when each new wireless system is installed, and should also be continuously monitored. As noted above, a well-designed wireless system will have performance margins built in and will include extensive diagnostics to detect loss of margin due to radio interference and other considerations. Wireless systems generally

support radio diagnostics, including metrics that are specifically intended to detect and blacklist problematic radio channels automatically.

Based on real-world experience with all of these factors, users of industrial wireless are quickly learning that wireless can deliver more than adequate performance for a very useful range of applications.

Application Classes for Industrial Wireless Instrumentation

Industrial wireless instrumentation is being applied to a wide variety of applications today. **Figure 2** represents one way to summarize concisely the major application areas, sometimes called application classes.

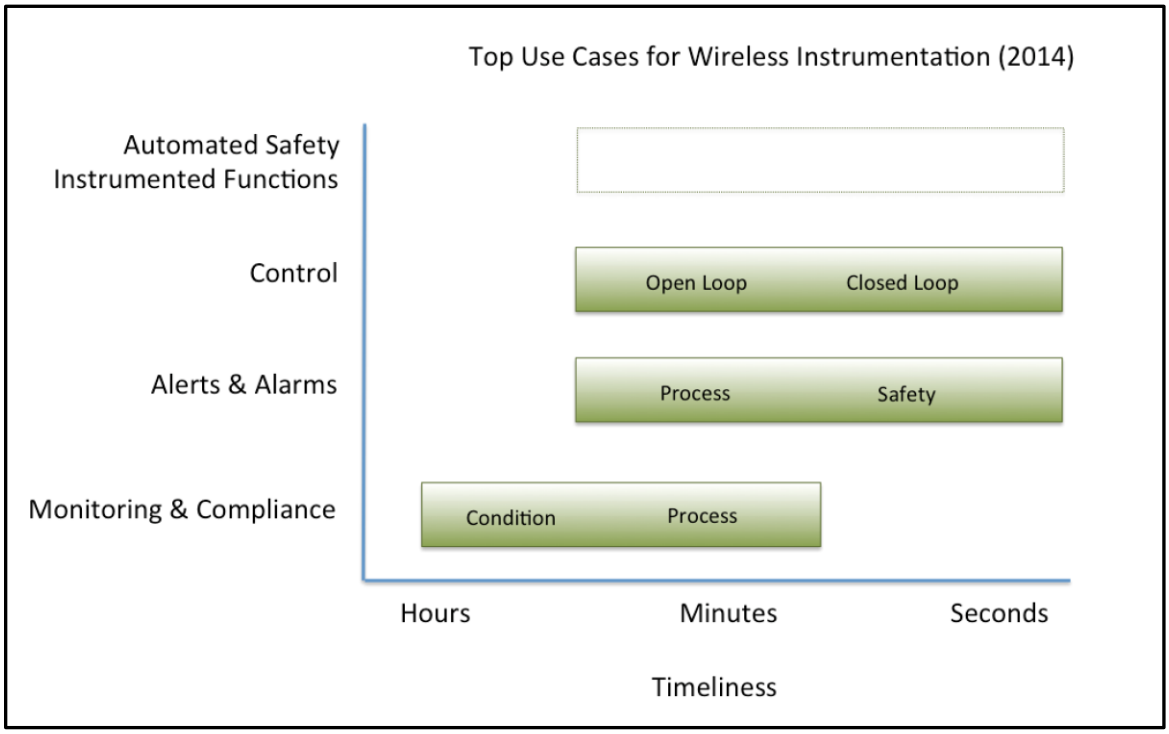

Figure 2 – Current landscape of industrial wireless instrumentation
Courtesy AIW LLC

The vertical axis shows general classes of applications:

- Monitoring and compliance applications track the status of equipment or a process state, such as temperature or vibration. Monitoring has been characterized by ISA100 as "without short-term consequences." Monitoring data is archived for subsequent review and may or may not be displayed to operators. Monitoring corresponds to ISA100 Application Class 5.

- Alerts and alarms track the status of a process state, such as temperature, or a safety state, such as hydrocarbon gas level. Exceptions are reported to an operator for appropriate action. Alerts and alarms correspond to ISA100 Application Class 4.

- In control applications, wireless is somehow involved in a control loop. “Open Loop” (ISA100 Application Class 3) means that a user is in the loop; “Closed Loop” means that the loop is automated. Some users make a further distinction between outer loop (ISA100 Application Class 2) and inner loop (ISA100 Application Class 1).

- In an automated safety instrumented function (SIF), a set of equipment is intended to reduce the risk of a specific hazard in an automated safety loop. Automated SIF roughly corresponds to ISA100 Application Class 0.

The green boxes in **Figure 2** indicate where wireless instrumentation is targeted, in actual practice at this time (2014). This is intended as a statement of fact, not to imply that wireless is unsuitable for other applications. For example, some wireless systems claim to support sub-second reporting rates, but sub-second timing is not shown in **Figure 2** because few wireless instruments today are so configured. Similarly, wireless instrumentation for automated SIF is shown with a dotted line to suggest that it is feasible but not to our knowledge being adopted by many users at this time.

A given instrument might be used for multiple application classes at the same time. For example, a temperature-monitoring instrument can be primarily intended to log compliance of a process state. In addition, when exceptions are detected, process alarms are reported to an operator, who can intervene by adjusting a valve. If the valve needs to be adjusted within 10 minutes of an exception, that would typically be classified an alarm. If response time is several hours, the application might be classified as an alert or as monitoring.

Condition Monitoring

Condition monitoring involves monitoring the condition of equipment in order to identify a developing fault. Condition monitoring may be applied to rotating machinery, steam traps, pipes, or other equipment. Candidates for wireless condition monitoring are items of equipment that are periodically inspected using handheld diagnostic tools, but that are subject to failure between inspections. Wireless instrumentation can provide more seamless visibility of equipment condition, allowing maintenance to be scheduled or other actions to be taken to prevent failure and/or avoid its consequences.

Rotating equipment is a commonly cited example of condition monitoring that is suitable for wireless. A plant may have hundreds or thousands of locations where rotating equipment is subject to failure. Vibration sensors on rotating equipment can be used to predict failures, with enough notice so that preventative maintenance can prevent an operational disruption.

Corrosion monitoring is another use case for industrial wireless. NDT (non-destructive testing) techniques are commonly used in periodic inspection of pipes and other equipment that is subject to corrosion. Similar capabilities are increasingly being offered in wireless products, providing an easily installed and easily moved corrosion monitoring capability at speeds approaching real-time.

Steam trap monitoring is another major use case for wireless. Steam traps discharge condensate, air, and other gases from a steam system while preventing the escape of live steam. Steam traps are high-precision devices that are subject to eventual failure. Improper steam trap operation can quickly result in process problems, such as temperature exceptions. A wireless steam trap monitor can provide notice

of a root cause maintenance problem before it negatively impacts the process. Today, users are planning deployment of thousands of wireless steam trap monitors per site.

Process Monitoring

Process monitoring involves tracking the status of a process or state where no immediate consequences are involved. Use cases include history collection, sequence-of-events logging, or event trapping with a long time scale for resolution.

Wellhead process monitoring is a common use case for wireless. A problem wellhead may be instrumented permanently or temporarily and data collected over a period of time to track performance or identify root cause problems. The wireless aspect makes it easy to instrument a wellhead temporarily and then relocate the wireless equipment to another wellhead as needed.

Remote wellhead monitoring is a potentially game changing application for upstream operation. A geographically distributed collection of brownfield wellheads can be retrofitted with wireless sensors, with process data transmitted to operations centers located in an office building hundreds or thousands of miles away. On-site personnel can be deployed as needed to handle exceptional circumstances.

Process monitoring may be required to demonstrate process compliance, such as in chemical or pharmaceutical manufacturing. Wireless sensors periodically report temperature, pressure, or other data that is archived in a historian application, thereby demonstrating the compliance of a process.

Process monitoring is commonly combined with alarming. When sensor data is out of range, an alarm can be sent to an operator. When the required response time is long, such as 8 hours, the application may still be considered monitoring. No exact definition has been agreed industry-wide that distinguishes "monitoring" and "alerting."

Alerts, Alarms, and Safety

Alarming involves an out-of-bounds condition that is reported to a user or system. Yokogawa Electronics Corporation has reported that over 50% of their wireless instrumentation projects require a 1-10 second update period. Cited applications include gas detection, fire detection, monitoring for operation (power), monitoring for safety (steel), cold temperature monitoring (gas), and tsunami detection. All of these can be considered "alarming" applications.

Many users have used the term "alarm" in alignment with ISA-18.2-2009, *Management of Alarm Systems for the Process Industries*. In that standard, an alarm is defined as "an audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a response." The essential element of this definition is the response to the alarm.

The term "alert" is generally used for applications with less rigorous requirements than alarms, for example maintenance alerts where the user response is not specific or time-critical.

According to IEC 61511-1, regarding safety alarms:

> *Where actions depend on an operator taking specific actions in response to an alarm (for example, opening or closing a valve), then the alarm shall be considered part of the safety instrumented system [SIS] (i.e., independent of the BCPS [Basic Process Control System]).*
>
> *Where actions depend on an operator notifying maintenance to repair a faulty system in response to a diagnostic alarm, this diagnostic alarm may be a part of the BCPS but shall be subject to appropriate proof testing and management of change along with the rest of the SIS.*

In practice, SIS alarms (by the definition above) are commonly used today. For example, a wireless gas detector alarm in the control room may require manual actions to evaluate the alarm, activate deluge, shut down processes, or other defined action.

A "safety-related alarm" designation can be applied to an alarming application that is a candidate for safety credit as an Independent Protection Layer. To simplify approvals, <0.9 availability may be claimed (SIL 0), thereby classifying an alarm as BCPS. Regardless of an alarm's classification, high reliability is invariably a key objective.

It is well established that an alarm system must be designed for effective handling of individual alarms during normal operation and handling of many alarms during a major plant upset. ISA-18.2-2009 suggests that an average of 2 alarms per 10 minutes is the maximum manageable by a single operator and that rates approaching 10 alarms in 10 minutes may not be reliably sustainable by an operator for long periods. Wireless has the potential for supporting many more alarms than have been feasible in the past, so alarm management is an essential consideration in a scaled wireless implementation.

Control Over Wireless

Control is an important application class for wireless. **Figure 3** shows a reference physical configuration of a wireless control system.

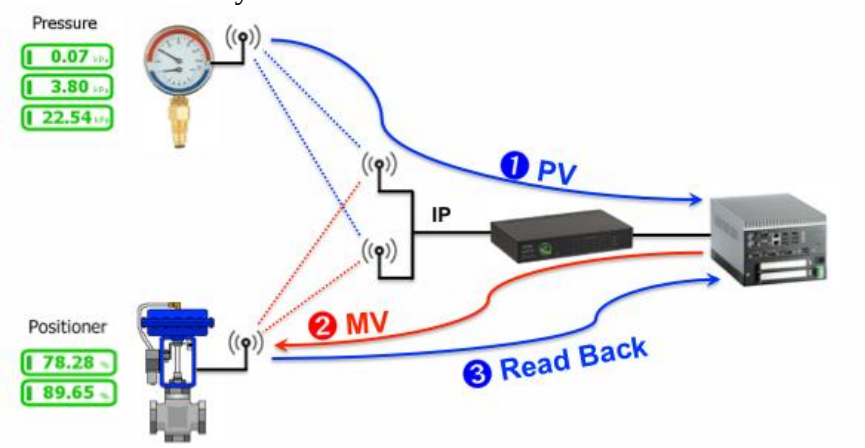

Figure 3 – Control over wireless

A wireless pressure sensor is illustrated on the top and a wireless positioner on the bottom. Both have redundant wireless connections that directly communicate to a high-performance IP backbone that may be wired, such as Ethernet, or wireless, such as a Wi-Fi mesh. Once a message is on the IP backbone, it is forwarded quickly and reliably to a controller via a gateway.

Figure 3 shows one wireless hop between the wireless devices and the high-performance IP backbone, a typical configuration for a fully wireless control system.

Figure 3 also shows the data flow. A process variable (PV), pressure in this case, is published to the controller. Based on this input and other considerations, the controller sends a manipulated value (MV) to the positioner. The positioner sends the actual position back to the controller. All of this needs to happen on the time scale required by the process, such as 1-2 minutes for a slowly changing process or 1-2 seconds for more traditional control.

In practice, a control solution does not have to be 100% wireless. The input device may be wireless and the output device may be wired or vice versa.

An entry-level wireless control architecture is shown in **Figure 4**. A wireless transmitter periodically publishes data to a controller through a wireless network. The controller executes control logic and uses wired fieldbus communication to transmit commands to a positioner. The input is wireless, but the output is through a wired connection.

Figure 4 – Wireless sensor, wired actuator

Figure 5 shows the reverse. On the right, a wired input device transmits sensor data to a controller, where control logic is executed. Then actuation occurs via a wireless link through an ISA100 network.

Figure 5 – Wired sensor, wireless actuator

Figure 6 shows a common configuration, with a wireless sensor providing secondary input. On the right, the primary loop is wired. On the left, a wireless sensor provides a secondary input that would be otherwise unavailable.

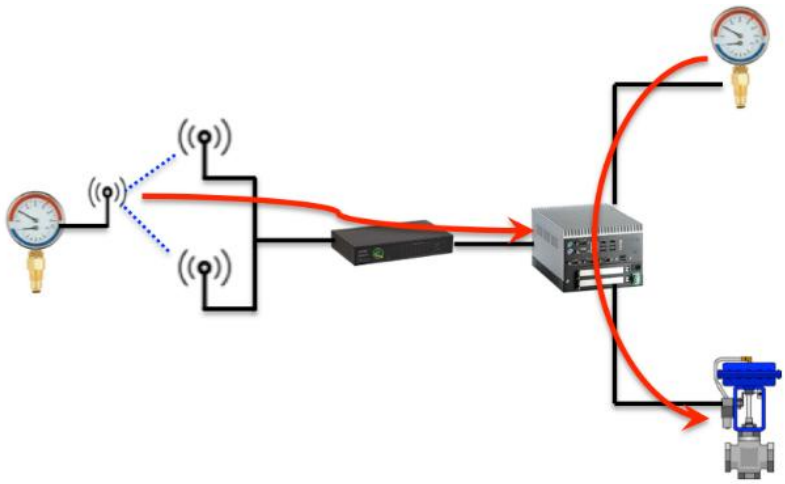

Figure 6 – Wireless sensor for secondary input

Early implementations of control-related applications tend to be hybrids of wired and wireless. As users become more comfortable with wireless, fully wireless solutions can be realistically considered.

Wireless Instrumentation Performance

Figure 7 shows a conceptual picture of a wireless instrumentation network. Exact features will vary depending on particular products and configurations, but the general principles apply across a range of solutions.

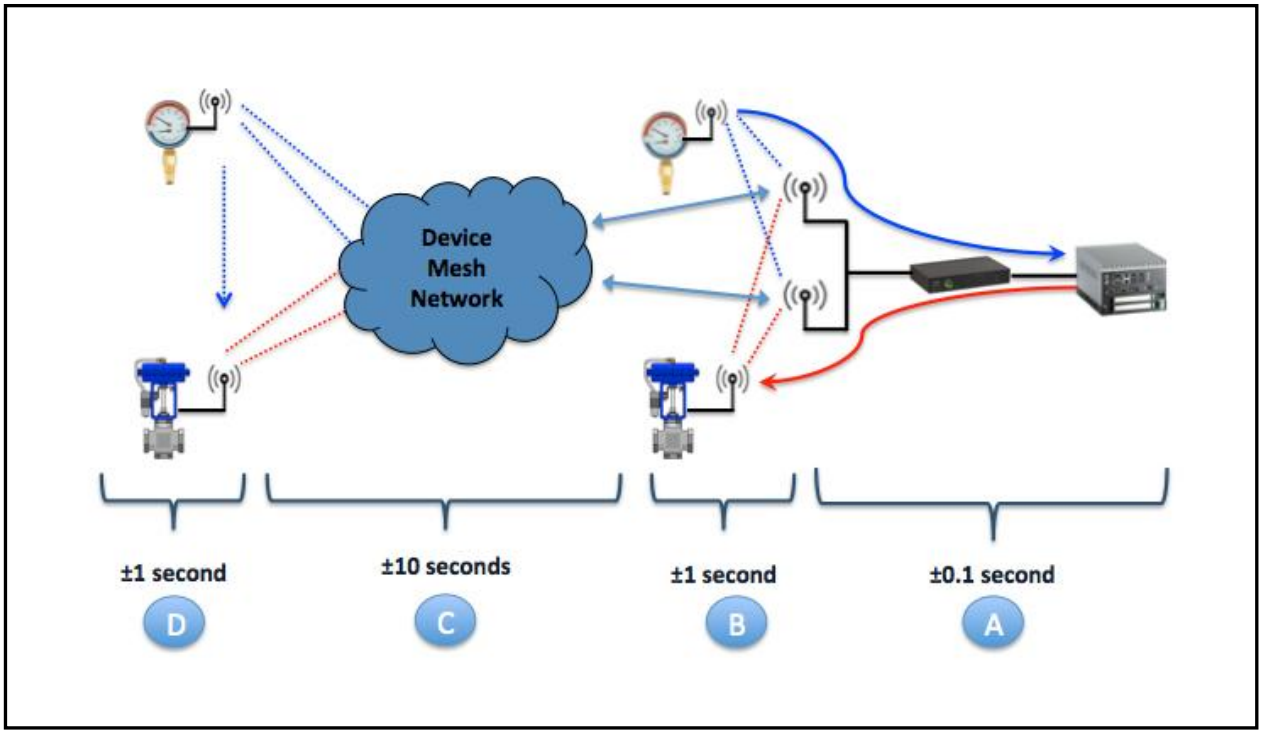

Figure 7 –Wireless Sensor Network Topologies

A. *Backbone:* A backbone network is shown that provides sub-second latency, which is typical for various IP-based solutions. The backbone may itself be wireless, such as a Wi-Fi mesh, an LTE digital umbrella, or a point-to-point solution. While different backbone solutions provide a variety of performance parameters, the principle is that backbones usually provide higher performance than is available in a battery-operated device mesh.

B. *Star to Backbone:* Some devices are shown connected to the backbone in a redundant star configuration; with each device having multiple backbone connections, particular in support of time-critical control or alarming applications. Since the backbone connection is "always on", latency on the order of 1 second can be supported.

C. *Device Mesh Network:* On the same network, but typically with lower priority, a device mesh supports a population of devices with performance requirements measured in 10s of seconds.

D. *Peer-to-Peer:* Mesh devices that are in proximity to each other may be configured to communicate directly, not through the mesh, and thereby provide point-to-point performance that is measured in seconds.

In actual practice, the "Device Mesh Network" performance can also be in the ±1 second range in structured configurations. Device mesh performance is primarily constrained by energy limitations of devices that participate in the mesh. For example, when a battery-powered field device is called upon to provide frequent routing services to neighboring devices, that reduces the device's energy budget to perform its primary function (e.g., to measure and report a level). When ±10 second numbers describe device mesh performance, this usually reflects a design that protects the battery life of routers.

Suppliers have addressed this by introducing specialized devices in the mesh to act exclusively or primarily as repeaters and/or by limiting the number of nodes supported per repeater. Such configurations have demonstrated field performance on the order of 1 second in controlled multi-hop topologies.

Adopting Wireless Instrumentation – User Considerations

Until this point, this paper has focused on the vocabulary of wireless instrumentation and differences between wireless instrument networks and their wired counterparts. As wireless instrumentation moves from an innovative proof-of-concept technology to scaled deployments users must review and likely revise policies, procedures, and organization responsibilities to assure responsible wide-spread deployment of wireless instrumentation. In our work with users we've used the following framework to help guide the transition from a wired-centric to a wireless-centric mindset.

Audit and Assessment of Current Situation

We start with an audit of existing practices occurs to better understand how the organization has handled the emergence of wireless instrumentation to date. We have found that independent of or despite any corporate edicts, plans, or initiatives, brownfield users have wireless instrumentation installations. Therefore major consideration is given to the following topics:

- Existing Installations
    - What are the existing wireless instrumentation installations?
    - Who is responsible for monitoring performance of and ongoing maintenance of these installations?
    - How was budget and safety approval secured for the existing installations?

- Technical Practices
    - What is the current state of the organizations technical practices?
    - Are practices updated to consider wireless instrumentation?
    - Is there a clear definition of when a wireless implementation is appropriate for a specific application?
    - Are there any regional regulatory impediments to deploying wireless?

- Organization structure
    - Is the technical and safety authority for wireless instrumentation centralized or dispersed throughout the organization?
    - Is there sufficient internal knowledge of the benefits and limitations of wireless instruments?
    - Has the responsibility for assuring standardized, high-quality wireless installation, DCS integration, and ongoing network and device management been established?

Once a thorough understanding of the current wireless instrumentation deployment environment is understood the user can assess the best way to effectively continue scaling their wireless instrumentation installations.

Approved Applications

Figures 2 through 7 in this paper depict performance metrics and typical block diagrams for various wireless instrumentation and/or actuation deployment scenarios. As a function of safety considerations, corporate culture, application requirements, available technology, industry and a range of other factors users must uniquely and periodically assess which applications are suitable for wireless systems. An honest and well-documented assessment of this question is a requirement for minimizing organizational dissonance with regard to future wireless deployments. **Figure 8** shows a simple tool that we use to summarize a user's wireless preferences. We have found this tool to be helpful starting point in design of systems, policies, and procedures.

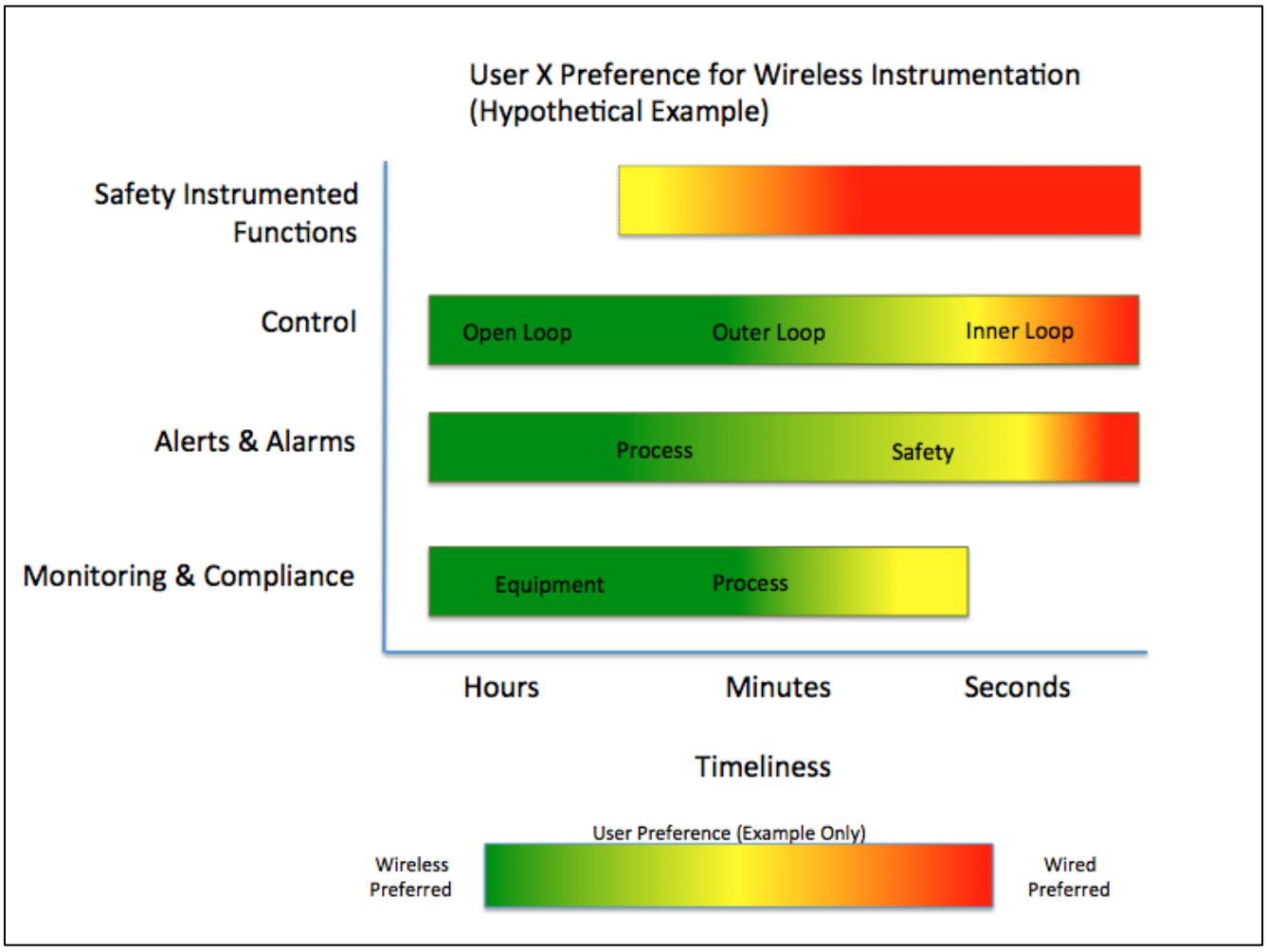

Figure 8 – Wireless Preferences of a Hypothetical User
Courtesy AIW LLC

In this example the user has clearly defined application types and timeliness requirements that are approved for wireless deployment. Coupled with acceptance procedures for reviewing yellow and orange applications this framework can be used to expeditiously move wireless projects through an approval cycle.

Point of Authority

Organization structure in process industry facilities is continually evolving with technology. Witness the development of IT organizations over the past 20 years as a case in point. Wireless instrumentation systems represent a new technology that requires feasibility input from four current organizations:

- Controls engineering must assess the ability of the **instrument** to be installed, maintained and operated within the performance requirements of a given installation.

- IT is concerned with ability of the instrumentation **network** to be secure, have adequate bandwidth, appropriate redundancy, and ability to scale to assure transport of instrumentation data.

- Safety must consider the **application** being deployed and the probabilistic nature of wireless data delivery in the context of the process to properly assess IPL's, suitability for alarming, and ultimately facility risk.

- Finally operations will need trained staff to install, provision, calibrate, and maintain devices, including battery replacement.

Users must decide how the various decisions associated with wireless deployment will be made. In a Single Point of Authority model, one group is given responsibility to become the wireless experts and work across functional boundaries to implement the wireless deployment plan and all associated policies. In a decentralized model, wireless experts are installed in each functional area and work together to generate wireless policy.

Implementation

Wireless is now at a stage where major users are rolling out wireless programs. The "tipping point" for industrial wireless occurs when major users switch from an ad hoc approach to wireless campaigns. In a bottom-up ad hoc approach, small wireless systems are installed one-by-one to address specific problems, relying on the passion of proactive early adopters. In a top-down campaign, solutions are rolled out to meet business. A good process allows for both approaches, with successful ad hoc systems being a laboratory for future wireless campaigns.

Some considerations in a scaled campaign are listed below.

- Deployment plan
    - Ad Hoc as a precursor to Scaled
    - Wireless umbrella vs. Bottoms Up
    - Highly engineered vs. Mesh
    - Single supplier vs. Multiple

- Procedure & Systems revision
    - Structured and simplified process for approvals
    - Installation standards
    - Post installation maintenance

    - Wireless performance dashboard

- User and Management Training
    - Vocabulary
    - Wireless Instrumentation Standards – ISA100.11a & WirelessHART
    - Comparison to "consumer" standards – WiFi, ZigBee
    - Understanding performance limitations

Conclusion

Industrial wireless instrumentation is widely considered suitable for monitoring, control, and alarms, including safety alarms. Systems may be deployed using an ad hoc methodology to get started, followed up by a campaign-style methodology to achieve strategic benefits.

Users must recognize that wireless instrumentation is a new technology platform. To properly and safely scale wireless instrumentation network for the enterprise requires shifts in policy, procedures, and organizational behavior.