Industrial wireless provides obvious and substantial benefits for installation, commissioning and maintenance of process systems. The ISA100.11a standard for wireless applications in the process automation industry was designed with control in mind. Ignace Verhamme explores the potential for its use, and what to expect in the future, both in terms of technical developments and user acceptance.

ISA100.11 covers five classes of use taking in applications as diverse as factory automation, location services and logistics. However the process industries are the vanguard users of ISA100.11-based systems. When discussing specific performance characteristics, we will consider ISA100.11a systems and hardware as implemented by Honeywell marketed under the name OneWireless for the worked example, since this is the area with which the author is most familiar. However, the control properties discussed are applicable to all ISA100.11a implementations, irrespective of the vendor. Differences in performance parameters will of course apply and must be considered on an individual basis.

Consider closed-loop control, as shown schematically in the block diagram (Fig. 1). The action in the controller block can be any control scheme suitable for the process to be controlled, such as PID control. Since there are currently no wireless valve positioners commercially available, the measurement block considered here is a wireless ISA100.11a device. ISA100.11a is an open wireless networking technology standard developed by the International Society of Automation (ISA).

**Fig.1. Block diagram of a closed control loop.** The action in the controller block can be any control scheme suitable for the process to be controlled, such as PID control. Since there are currently no wireless valve positioners commercially available, the measurement block considered here is a wireless ISA100.11a device.

A closed-loop control system as depicted in Fig. 1 has requirements that apply to digital control systems in general; they are not dependent on the technology used or the communication
protocol. These requirements are termed Critical to Control (CtC). They include deterministic and real-time (RT) behaviours, reliability, minimum sampling rate, scalability and security.

**Deterministic behaviour**

A deterministic system will always produce the same output from a given starting condition or initial state. For example in a process system, that would bring the process value to the setpoint within an RT constraint. So for process control purposes, timing is an essential part of the deterministic requirement. This is why a DCS is fundamentally different from a PLC - the cycle time in a pure PLC is not deterministic.

In general, a simple control loop cyclically acquires a single point from an input channel, processes it, and outputs a single point on an output channel. This process is repeated in cycles of exactly the same time for the system to be called time-deterministic and, therefore, suitable for process control. This requires exact timing of the input, which - referring to Fig. 1 again - is the measurement block’s output.

An important timing property is jitter - cycle time variation, such as start, duration and end. Jitter ideally should be zero as it can result in unacceptably poor control, so deterministic control and an RT system go hand-in-hand.

The following concepts implemented in the ISA100.11a protocol guarantee deterministic behaviour:

- All devices operate in a wireless ISA100.11a subnet communicate at a pre-determined time and a pre-allocated frequency channel with a pre-determined channel hopping sequence.

- Based on Time Division Multiple Access (TDMA), ISA100.11a technology divides time into configurable length timeslots, which typically range from 10 - 14ms.

- Wireless transmissions occur in bursts at clearly pre-determined times.

Collision-free, deterministic communication between two ISA100.11a devices occurs in dedicated timeslots. This communication typically will be related to the measured process values, which is time critical. This confirms that ISA100.11a is effectively suited for control purposes, and ISA100.11a-based systems support the deterministic timing requirement critical to control.

**ISA100.11a Infrastructure**

- **Gateway**: An interface between the wireless and plant networks, or directly to an end application on a plant network. Note that a gateway can be implemented as a single or redundant device.

- **Backbone router**: A field device, which has a field network interface and a backbone interface. Backbone routers enable the external backbone to carry native ISA100.11a protocol by encapsulating the protocol data unit for transport. A backbone is a (preferably high data rate) data network that could be an industrial Ethernet, IEEE 802.11-based wireless mesh.
network, a WiMAX network, or any other network within the facility interfacing to the plant's networks.

- **Routing device**: These devices can provide range extension for a network and path redundancy by routing ISA100.11a communication received from other ISA100.11a I/O devices. The router device can also be an I/O device, such as a wireless ISA100.11a transmitter in which case it routes its own data in addition to data received from other I/O devices. Routing devices have the capability to participate in a self-organizing sensor mesh.

- **Non-routing (I/O) device**: An input or output field instrument with the minimum characteristics required to participate in the network. The I/O role provides no mechanism for forwarding messages or routing any other device. This device can range in functionality from a wireless transmitter configured as a non routing device, to the least-complex devices with the potential for very low energy consumption. Some vendors of ISA100.11a wireless devices refer to the topology with non routing devices as a Star Network. This concept of non-routing devices will be shown to be essential in the realm of wireless control.

- **Provisioning or portable device**: Used to provision ISA100.11a devices, that is, inserting the required configuration data including the security key into a device to allow it to join a specific wireless industrial sensor network.

**Fig. 2. Schematic representation of the ISA100.11a infrastructure.** The ISA100.11a standard defines the many basic functions that improve data transfer reliability in communication. Within a ISA100 based wireless network, devices can have different roles; I/O (input/output), routing and I/O plus routing.

The timing property not considered is jitter. The sensor mesh architecture supported by ISA100.11a offers the advantage of flexibility and inherent redundancy, but can lead to poor control quality. The deployment of a star network is probably ideal because non-routing transmitters connecting to the backbone wireless mesh substantially reduce jitter.
Note that ISA100.11a also includes shared timeslots for alarms and bursty traffic, and it supports publishing, client/server, alert reporting, and bulk transfer traffic - such support for non-deterministic communication appears to be unique for ISA100.11a.

**Real-time behaviour**

A system is RT if the total correctness of an operation depends not only upon its logical correctness, but also upon the time in which it is performed. In other words, an RT deadline must be met, regardless of system load. An RT system has two important properties - throughput and latency. Jitter is sometimes included as another crucial timing property of an RT system.

Throughput (processing) performance traditionally lies with the controller's CPU (and possibly I/O card) processing capabilities. With digital smart transmitters such as Foundation Fieldbus or ISA100.11a transmitters, part of the processing has moved into the field and takes place within the transmitter itself.

A key control system property is latency; the end-to-end delays associated with communication, computation, and actuation. Typically, the greater the latency, the poorer the quality of control, because actions can only respond to delayed measurements. In general, latency should be an order of magnitude less than the smallest lag in the loop.

As far as throughput is concerned, there is no difference between a wired system with smart digital transmitters and an ISA100-based wireless system - effectively, there is no notable difference in control loop performance between a wired and wireless solution.

**Sampling rate**

The minimum sampling rate is crucial to control. Current control systems use digital computers for control action, requiring sampling of the analogue signals received by transmitter sensors. For a controller to work correctly, the time between samples must be small compared with the dominant time constants of the process to be controlled. In brief, the Nyquist-Shannon theorem - applied to a control system - can be expressed as follows: *To achieve good performance with digital control, it is necessary to sample the controlled variable at a rate faster than twice the highest frequency significant for control.*

Take, for example, a control loop using PID where derivative action is applied. To prevent excessive valve activity in the presence of higher frequency noise, it is usual to condition the controlled measurement with a low-pass filter of which the time constant is a small fraction of the derivative time constant. Sometimes, this results in a required sample interval less than a second. A general rule is to make the period between the scans less than one-tenth of the dead time, or one-twentieth of the lag in the process response. In practice, a one second sampling rate has seldom been a problem for all but the fastest process responses.
Reliability

System reliability depends on component reliability. It is difficult for every component to function correctly at any instance, yet a critical requirement for a process automation system is uptime - equivalent to system availability, which is a measure of control system reliability. To get the required system availability, the following need to be considered: redundancy; fault diagnostics and announcement; the application of distributed systems; and the inclusion of 'failure signals' separate from the process 'values'.

With the advent of smart transmitters, A/D conversion units are found in the transmitter itself rather than on the DCS input cards, with a digital communication link from transmitter to DCS. Foundation Fieldbus transmitters and ISA100.11a wireless transmitters are like this. Both are bi-directional digital protocols.

Since smart transmitter sampling is carried out in the transmitter, the reporting rate (the rate at which the transmitter publishes the measured value on the ISA100 network) has to be considered. ISA100.11a foresees devices with reporting rates of 100ms or faster. However, using current technology, this reduces battery life and, therefore, reliability. Today's commercially available transmitters operate at a reporting rate typically an order of magnitude slower.

Some wireless transmitters can be configured for a reporting interval of down to one second, making them suitable for closed loop control for all but the fastest processes. This reporting interval in medium-to-larger size installations may become impossible when transmitters need to act as routers in addition to their transmitting task. This is why, to realise a minimal reporting interval, a wireless transmitter in a control loop will typically be configured as a non-routing transmitter.

In addition to system uptime or availability, wireless system data reliability is important. In terms of system availability, Honeywell's ISA100.11a OneWireless system is considered here. This provides availability through component reliability, redundancy (in the meshed wireless network and in the gateway), diagnostics and application of distributed systems.

Since the wireless network is meshed with inherent built-in redundancy, its availability is higher than that of a traditional wired connection (it is difficult to cut a wireless connection in air). However, data reliability is a concern where interference could hamper communication. Interference is mitigated in ISA100.11a by the following:

• Direct-sequence spread spectrum (DSSS) modulation technique - this makes the ISA100.11a signal look like noise to other wireless systems.

• Spatial diversity - Two field access points receive transmission from the field instrument.

• Frequency diversity - Frequency hopping over the available channels in the bandwidth of the device's transmitting frequency.

• Dynamic power control - Reduces possible interference with other wireless networks.
• Channel black listing and adaptive channel hopping - Avoids congested channels.
• Implementation of IEEE 802.15.4-2006 - Proven to coexist in very congested environments.
• Careful management of the ISA100.11a wireless network implementation.

Power considerations

The reliability of the components of a control system with wireless transmitters introduces a potential failure mode typically unknown to a wired equivalent: battery life. The battery life of a wireless field device needs to be taken into account when calculating the availability figure. The battery life can be directly translated to a Mean Time To Fail (MTTF) number. A number an order of magnitude lower than the MTTF value of the other system components will drastically reduce the overall system availability to a level where it may no longer meet the uptime requirement.

The reporting rate and routing characteristics of the transmitter impact battery life. As previously established, a one second reporting rate is a good figure for use with control. With the current technology of fuel cells, it is not evident to implement a wireless field network suitable for control with routing transmitters. In particular, when we consider scalability where more than a few transmitters are deployed, the MTTF of the battery of the routing transmitter and, in extension, the entire control system drops to an unacceptable low value.

In fact, it is fair to say that battery life is probably the single most limiting factor in adaptation of wireless technology for closed loop control. Battery life extension to make ISA100 transmitters suitable for control is reached in a number of ways:

• Reduction of reporting rates by synchronizing measurement transmission with the control execution, or even more advanced by transmitting only when the rate of change of the measured value exceeds a certain threshold. This technique of synchronized sampling with exception reporting extends battery life, but only in the case of latency-tolerant control applications, where the reporting rate effectively can be reduced. Obviously, this also reduces the scope of control applications.

• Adaptive transmission power control, where the ISA100.11a field device dynamically selects a transmit power level during runtime operation. This technique optimizes power consumption and hence battery life.

• Use of non-routing transmitters in a star network, which is by far the most effective, highly recommended and (in most control applications) the only possible way to extend battery life.

Externally powered wireless transmitters mitigate this problem. In this case, only the ISA100.11a device communication is wireless; the power supply still requires wires.
ISA100.11a wireless protocol: Honeywell XYR 6000 transmitters

Scalability

A process automation system needs to meet the CtC criteria regardless of size. The deterministic and RT behaviours should not be affected by controller load or the communications infrastructure. Field signals sampling needs to be executed at exactly the configured frequencies, at exactly the same time in the scanning cycle independent of the number of connected field devices. System uptime should meet the minimum requirement of availability critical to control, regardless of the number of components added to the system. However, realistically, a CtC performance requirement will eventually be violated when expanding a process automation system. Note, therefore, the boundaries within which CtC performance is guaranteed.

An ISA100 wireless infrastructure's size, both geographically and in number of wireless devices, can affect parameters critical to control. Consider the following:

• As the covered area expands, and/or wireless transmitters are added, the required number of hops between transmitters and field access points may increase to a level where communication becomes too slow to meet the requirement for deterministic and RT behaviour. To limit the number of hops in an ISA100 implementation, a backbone wireless mesh and non-routing transmitters will be needed.

• To attain the required level of sampling and reporting rate in larger ISA100 installations, using non-routing transmitters will be the only option.

• An infrastructure having a mesh architecture increases reliability. When deploying routing transmitters forming a self-organised mesh, the availability will increase with increase in ISA100 transmitter numbers. However, as the number of routing field devices increases, field device battery life and, therefore, availability, becomes problematic. The only two viable options for control are externally powered or non-routing transmitters connecting to a backbone mesh of field access points.
Security

Security has become an essential requirement for process automation systems. This is a critical characteristic of such systems in general, irrespective of the physical layer for the communication link (wired or wireless).

With a wireless infrastructure, security measures are specifically needed to assure confidentiality (privacy), authentication (ID verification), message integrity (tamper-proofing), non-repudiation (proof of transaction) and availability.

To obtain such security, there are a number of different technologies and security measures that can be implemented. However, it is noteworthy that cyber security researchers working for the US government were unable to hack the OneWireless infrastructure. Specifically, they were unable to disrupt or manipulate sensor to field access point (multinode) communications.

The outlook

The vast majority of wireless transmitters installed are used for monitoring purposes - indeed, practically all wireless field devices are input only. The output devices currently available are discrete outputs. As yet, there are no industrial wireless analogue output devices, such as valve positioners, on the market. One of the technical challenges is the required power and the load that operation of these devices puts on batteries.

Even in the absence of wireless analogue output devices, it is possible, under certain conditions, to include a wireless transmitter in a closed-loop control scheme with the output device being wired. However, end users will need time to adopt this concept, and must become more comfortable with wireless technology before it will be widely used for control. Eventually, though, there will be a general application of wireless devices for control purposes.

To make wireless technology more suitable for closed-loop control, work is being carried out into improving battery life using long-life fuel cells and energy scavenging (energy derived from external sources such as solar PV, wind and kinetic energy). Work is also being carried out to improve reporting rates and the bandwidth of the ISA100 backbone mesh - the latter to allow high bandwidth applications.

It is also expected that the applications scope will need to be widened to take in, for example, safety. Another aspect is increasing interoperability with wired protocols. An example is where the ISA100 backbone mesh will serve as the HSE backbone for FF H1 (31.25kbps) segments.

Finally, control in the field will be required, so that control function blocks will reside in the wireless field device. This will allow closed control loop solely on the wireless network. Eventually, there will be plants using ISA100 wireless field devices that will download their firmware automatically from a cloud computing service accessible over a secure Service Node connection. The ISA100 devices will then be deployed as part of a closed control loop.
The conclusion is, therefore, that an industrial wireless solution based on the ISA100.11a standard can effectively be used with closed loop control applications.

_Ignace Verhamme_ is EMEA Solution Consultants Manager, Honeywell Process Solutions

(This article appeared on the Industrial Ethernet Book (www.iebmedia.com). The original can be found [here](http://www.iebmedia.com).)