Monitoring Systems

/ SORTING OUT WIRELESS

VAISALA

Monitoring Systems: Sorting Out Wireless

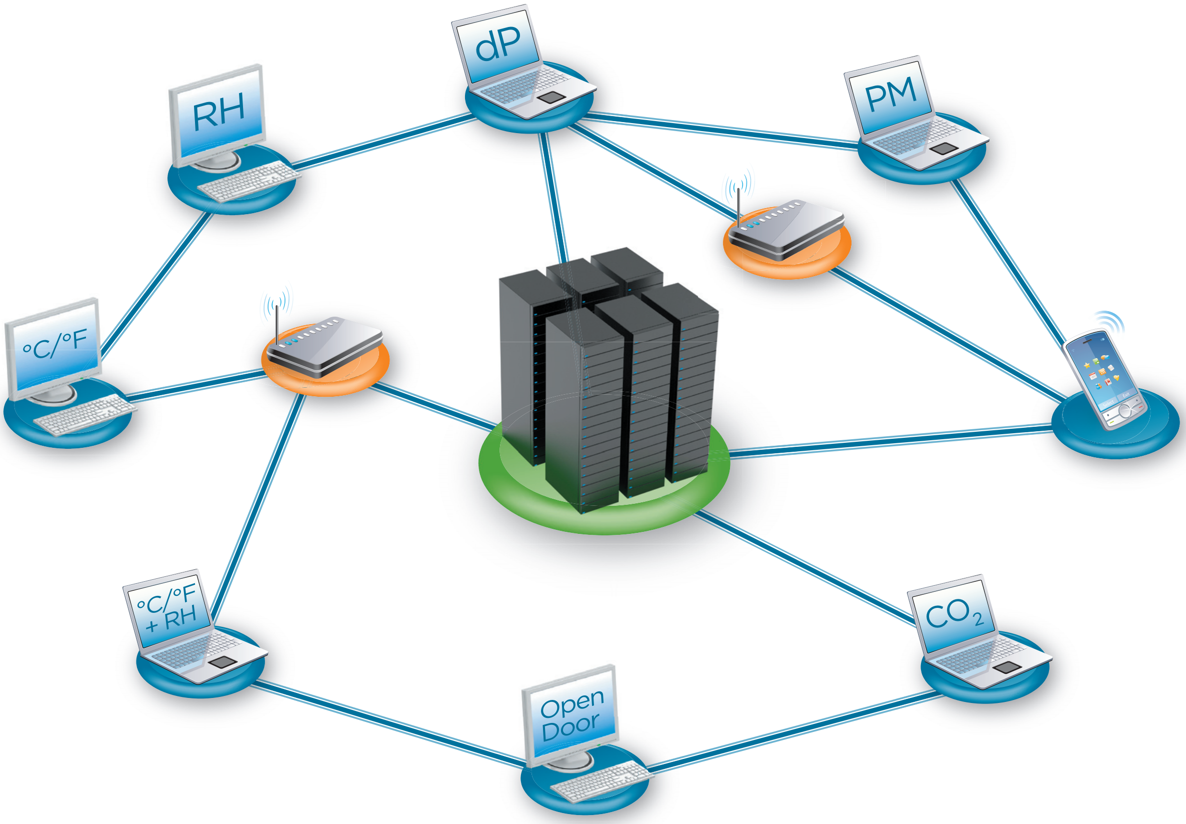
Monitoring systems for temperature, humidity and other parameters continue to proliferate in FDA/GxP regulated industries, which has made selecting a monitoring system no easy task. The systems can become complex, sometimes involving hundreds of sensors in a variety of settings, and anyone involved in these projects will have to make many decisions. One of the most complicated decisions for monitoring systems is selecting the connectivity that will allow the sensors to speak to a central processing unit. Decisions on connectivity will depend on the importance of the data for regulatory purposes, as well as logistical concerns such as the placement of access points for transmitters. In this article we simplify the challenge by describing the most common methods of connecting sensors to a monitoring system. Then, we list eight key considerations for selecting a wireless option that will work with your application.

What does wireless mean?

Let's start by defining the term "wireless." Whether you are monitoring warehouses, stability rooms, or freezers, the issues are the same. It's important to distinguish between power supply and signal output because the term "wireless" can apply to both. Power supply is simple; a device is either connected by wires to a source of electricity or it runs on batteries. Signal output is more complicated; wireless can be any method of communication that literally does not use wires. This is typically done over radio frequencies (RF). There are different frequencies and data formats to choose from. The two most common are WiFi and "other." WiFi is familiar to most people because it is a common computer network protocol. If your facility is already using WiFi, it can be convenient to run your wireless monitoring system over this existing infrastructure. WiFi protocol is a global standard, assuring that most WiFi equipment is interoperable. If you explore this route, consult with your information management people early in the selection process. They are usually responsible for the WiFi network and may have to approve of any system that runs on the network.

The somewhat vague category of "other" refers to systems that use standard or proprietary protocols and operate on a variety of different frequencies. These systems have some benefits, e.g., they can be designed to operate over longer or shorter distances than WiFi and do not have to share any existing networks within the facility. However, these systems require their own network of radio devices. If you plan to monitor areas that are spread out in your facility, you will need many of these devices. If a WiFi network already exists, it may not be necessary to create an entire new network. Proprietary RF networks may have less flexibility or be incompatible with regulations in other parts of the world, limiting the ability to create global networks for monitoring in widely distributed locations.

While the reliability of wireless systems is debatable, a well-configured system combined with good hardware will contribute greatly to data integrity and security. However, even the best wireless system can be compromised in two ways. First, all radio devices are subject to interference from other devices that create electromagnetic radiation (EMR). Obvious sources are hand-held radios and cordless phones. Less obvious sources of interference are microwave ovens and large electric motors. Second, the propagation of RF signals can be limited by physical obstacles, such as walls, racks full of products, and large metallic objects. These barriers to transmission can be taken into consideration during the planning, installation, and testing of wireless devices, but it's important to remember that the physical configuration of an area may not be the same six in months' time. This is especially true in large spaces used for storage or other activities that change regularly.



Just as one system can monitor multiple parameters and provide multiple outputs, such as reporting and alarming, multiple modes of connectivity can be used to customize a system to your applications.

Three different ways to achieve connectivity

Modern monitoring systems include measurement devices and event sensors that are typically connected to a computer that is hosting software for collecting this data. These devices can be connected to a network in several different ways:

- **Fully wireless devices:** Run on batteries and transmit data wirelessly via radio frequency to a receiver.
- **Hardwired devices:** Powered by permanently installed electrical connections and transmit their data over wires.
- **Hybrid devices:** Hardwired to a power source and transmit measurement data wirelessly; can use power over Ethernet (PoE), etc..

Fully wireless devices run on batteries and transmit information wirelessly. These devices are easy to install (no wires!) and can be the most economical option for a facility that does not have convenient sources of power at the monitoring points. The biggest downside is the need to change the batteries. If there are only a few sensing devices this is not a problem. However, when the number of devices increases, it can become a substantial task to stay on top of battery management. Devices in high risk areas where the measurement intervals are shorter tend to run through batteries more quickly. The ease of moving fully wireless devices is a double-edged sword; devices can easily be moved to locations where connectivity is marginal, causing inconsistent data transfer and a gap in the measurement records.

Hardwired devices sidestep the issue of batteries and all issues related to RF communication. Many consider them the “gold standard” of reliability. The main downside to hardwired devices is the time and cost associated with running wires for power and signals. Power over Ethernet (PoE) can simplify installation by providing both power and communications in one cable, which is typically a CAT5 cable that is connected to a PoE enabled server. When planning the installation of any hardwired device, it is important to consider the power source and what might happen to the monitoring devices and system in the event of a power outage. If the power source is not backed by generators, it may be wise to provide an uninterruptable power supply (UPS) for devices that are monitoring critical areas. PoE devices get their power from computer servers that are usually backed up with generators or large UPS systems.

Hybrid devices come in many flavors. They may transmit data wirelessly but be powered with internal battery backup. A battery-powered device that also has on-board memory can ensure that data is recorded autonomously and continuously even during power failures or extended blackouts. Hybrid devices are versatile and can be used to create workarounds for challenging situations. It is possible to combine hybrids with different configurations on the same monitoring system (e.g., some wireless, some PoE, some fully wireless). The downside to hybrid devices is the extra care necessary to specify and implement a system correctly. Hybrid devices may be slightly more expensive than simpler devices.

Eight Key Considerations

There is no single best way to configure connectivity in your monitoring system, but there are eight key considerations for planning or expanding your monitoring system:

1. Number of devices in the system (complexity)
2. Quality and performance of devices (accuracy of measurements; reliability)
3. Nature of the space where monitoring is required (e.g. small chamber, research lab, warehouse, etc.)
4. Existing infrastructure (electrical power, presence of WiFi, and Ethernet data drops)
5. Human resources required to install the envisioned system (running wires; happens once)
6. Human resources required to maintain the envisioned system (battery changes, happens regularly)
7. Desired and/or required data integrity (some data gaps OK vs. gap-free data)
8. The requirements and preferences of other system stakeholders (Quality, Information Management)

The need for monitoring systems is often driven by a combination of regulatory pressure and risk analysis. Most regulatory bodies provide guidance on what needs to be monitored while your risk analysis helps to define the criticality of specific measurements/events and what they mean to your organization. These are separate subjects not addressed here, but they are directly applicable to monitoring system choices. Devices and connectivity are only part of the bigger picture.

Further Reading

- **"Vaisala Veriteq Continuous Monitoring System Common Configurations"**
  http://www.vaisala.com/Vaisala Documents/Technology Descriptions/CMS-Common-Configurations-EN.pdf
- **"Wireless Networking in the Developing World"**
  This free e-Book focuses on telecommunications, but contains comprehensive introductory chapters that describe wireless technologies in detail. http://wndw.net/pdf/wndw2-en/wndw2-ebook.pdf
- **"How to Identify Wireless LAN Deployment Risks"** a brief tutorial by Jim Geier of Wireless Nets Ltd.
  http://www.wireless-nets.com/resources/tutorials/identify_wireless_lan_deployment_risks.html

VAISALA

For more information, visit
www.vaisala.com or contact
us at sales@vaisala.com

Ref. B211156EN-A ©Vaisala 2011