Three things to consider when planning an industrial wireless network

Justin Shade
Product Marketing Specialist — Wireless I/O and Network
Phoenix Contact USA

The overall acceptance of industrial wireless is growing, which is the major factor in making it easier to implement. During the past decade, users have become more comfortable with wireless. They understand that there isn't one specific wireless technology that fits every application, so they need to determine which technology best fits what they are looking to do.

Having installations to point to and a system integration channel with experience installing wireless systems goes a long way toward educating users about and ensuring easy installation of wireless systems.

How do I decide what wireless technology is right for my application?
Wireless can be broken down into two types, public and proprietary.

In a proprietary system, such as frequency-hopping spread spectrum (FHSS), the wireless modules must all belong to the same platform from the same manufacturer. Products from each manufacturer communicate a little bit differently, and provide differentiating features from those of other manufacturers. Also, a proprietary system creates an inherent level of security, because a would-be hacker cannot add just any module to the wireless network.

With a public system (such as Wi-Fi or Bluetooth), users can generally intermix wireless modules from different manufacturers. This increases interoperability between platforms and manufacturers. It also gives the user more freedom to choose the type of module he or she would like to use based on his or her needs.

From the applications side, the specific industrial protocol used (i.e., Modbus, EtherNet/IP, PROFINET) is typically not tied to any wireless technology — but the way you plan on implementing the protocol over the wireless network, and your expectations of the system, could help determine which wireless technology you choose. These industrial protocols, for the most part, do not work in conjunction with one another without the use of a server that can bridge the two protocols.

Do I need to test my wireless system?
In most cases, it is a good idea to do an on-site test of a wireless network before installing it permanently. An area might look as if it is free of obstructions or wireless frequency, but without testing, you never know what might cause interference problems to your installation. A wireless module with built-in tools like a Wi-Fi scanner or a low-function spectrum analyzer can help you best tune the wireless system to work in the environment where you are looking to install the system.

How can I ensure that my wireless network is secure?
Security is an important concern in any network. While wireless presents special challenges, there are many ways to make a wireless system secure. The first step is to make sure the installation area (panel, antenna mounting area, etc.) is located in a physically secure area. This means locking the panel where the wireless module is, not allowing access near the antenna assembly and limiting access to the wireless system to only approved personnel.

The next step is to change the default login information to the Web-based management of the wireless module (assuming the device has Web-based management, as most do today).

(over)

P.O. Box 4100, Harrisburg, PA 17111-0100 | Phone: 717-944-1300 | Fax: 717-944-1625 | Technical Service: 800-322-3225
E-mail: info@phoenixcon.com | Website: www.phoenixcontact.com

Many users make the mistake of not changing the wireless module's default parameters, so that anyone who has read the product's user manual can access the programming information.

As mentioned earlier, if a proprietary wireless technology will work for the application, going this route adds a level of protection, because it restricts the devices on the wireless network to a single manufacturer's wireless platform. To gain access to your network, you would need to know what platform of wireless module you were using before even being able to start thinking about how to gain access to the network.

Lastly, if the wireless platform you are using allows over-the-air encryption (which most do these days), turning on that encryption creates a secure path over the air. Using the WPA2-AES level of security and encryption is considered "un-hackable" by today's standards. When setting up security, you should always choose the highest level of encryption available, giving you the most secure system.

Conclusion

Do your research, and get the right parties involved. Some applications are straightforward, but for more complicated applications, consider hiring a system integrator who specializes in wireless installations. Enlisting the service of a system integrator at the beginning of your project may cost you a little more upfront. However, if a system is implemented correctly, this investment will pay for itself by preventing problems down the line.

P.O. Box 4100, Harrisburg, PA 17111-0100 | Phone: 717-944-1300 | Fax: 717-944-1625 | Technical Service: 800-322-3225
E-mail: info@phoenixcon.com | Website: www.phoenixcontact.com