Overcoming Concerns about Wireless PACs and I/O in Industrial Automation

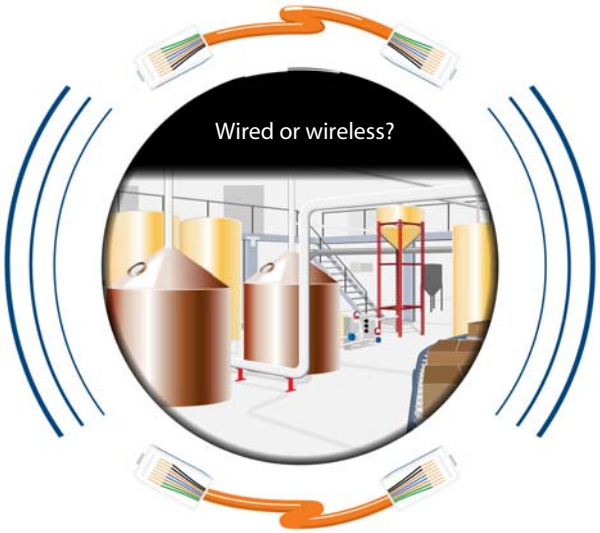
Industrial Automation Flirts with Wireless

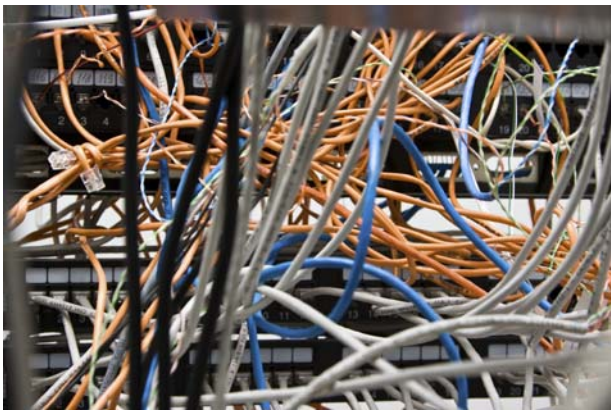
The automation industry increasingly finds wireless attractive, and for several reasons.

- Running a wired network incurs significant labor and material costs, while wireless networks cost far less.
- Wireless offers connectivity for remote areas or areas not currently served by wired networks.
- Wireless controllers and I/O can manage devices and processes even in inaccessible areas, or areas where network wiring is difficult or impossible to install.
- And wireless can offer a way to provide proof-of-concept for a new project before incurring the expense of a wired network.

For all these reasons, automation engineers are beginning to seriously consider wireless solutions (specifically WLAN, wireless Ethernet, or Wi-Fi) for all or part of their applications.

But with all these good reasons to use wireless, several concerns remain. Among them are security, network performance and reliability, availability and cost of I/O components, and the necessity of choosing between wired and wireless solutions up front.





Security

Wireless network security has been notoriously easy to compromise. Just stand outside an apartment building with a laptop and check the available wireless networks. How many can you access without even a password? But while personal wireless networks often remain insecure, security standards for business, industrial, and government use have been developed over the last several years and adopted by most organizations.

The earlier WEP (Wired Equivalent Privacy) security algorithm, which was found to have serious flaws, has been superseded by much stronger and more secure transmission algorithms.

Wi-Fi Protected Access (WPA), including the Temporal Key Integrity Protocol (TKIP), replaced the older WEP algorithm in 2003. The more recent WPA2, introduced in 2004, uses the even more secure Advanced Encryption Standard (AES) 802.11i algorithm.

WPA2's AES algorithm is compliant with National Institute of Standards and Technology (NIST) FIPS 140-2, required by some government agencies and corporations. These standards can protect a robust communication system.

For secure communications, WPA2-compliant products should be used for industrial wireless implementations today.

Wireless PACs and I/O in Industrial Automation

Network Performance and Reliability

The reliability of a wireless network depends on a number of things, including network size, physical environment, number of network users and how heavy their use is, and interference from other devices.

For a small all-wireless network, devices may perform well in *ad hoc* mode (peer to peer), where each device can detect and communicate with any other similarly configured device within range. This mode requires a smaller expenditure on network hardware and can be especially useful for a temporary wireless network. For a larger network, *infrastructure* mode is usually more suitable. Infrastructure mode routes communication through one or more wireless access points (APs).

Since wireless communications are based on radio signals that travel through air, physical environment plays a clear role in how well the network performs. Any obstacle—wood, metal, concrete—will impede the signal as it travels. The solution is to strategically place APs, wireless routers, and wireless repeaters as needed to cover the entire area requiring wireless transmission.

Network reliability also depends on the number of network users and the nature of their use. Simple data transfer usually requires little bandwidth; heavier use, such as transferring large files or interacting with multimedia, can slow network traffic considerably. Networks using the 802.11a or g standard are faster (maximum 54 Mbps) than those using 802.11b (maximum 11 Mbps).

RF (radio frequency) interference and EMC (electromagnetic compatibility) problems reduce network reliability when other devices—such as cordless phones, Bluetooth devices, even microwave ovens—interfere with wireless signal reception.

Reducing interference from other devices may involve changing channel frequency within a range or moving into a less crowded frequency. Wireless networks compatible with 802.11b and g standards, for example, use 2.4 GHz, a frequency shared by many devices. Moving to an 802.11a-compatible system, which uses 5 GHz, might offer less interference, although range may be shorter.

Wireless standards also differ in the number of non-overlapping channels they allow: 802.11b and g allow only three, so frequencies must be reused when more than three APs are required in the same system. More channels are available in 802.11a.

Availability and Cost of I/O Components

While concerns about wireless security and performance are generally shared by users of all wireless networks, the concern about availability and cost of I/O components is unique to the automation industry.

Currently, most automation manufacturers who supply wireless products offer product lines that differ substantially from their regular lines.

A wireless solution may have been acquired by purchase or developed by a separate division, for example. Or a subset of the regular product line may be adaptable for wireless use by module carriers or similar devices.

However, these solutions can cause problems for the automation customer.

As part of a separate wireless line or as a subset of regular products, wireless I/O may not include features the application requires—or features that just make design easier, such as simpler methods of wiring to field devices. If an application needs specific signal inputs or channel-to-channel isolation, for example, the wireless I/O product line may not include them. Limited availability may mean costly workarounds or even eliminating wireless as a possibility.

To set up any size wireless network, automation engineers usually find they must buy special wireless components, such as module carriers, I/O modules, racks, and terminations. In nearly all cases, customers who install a wireless network for automation must carry a separate inventory of spares in addition to those required for their wired systems. Special components and additional spares increase the cost of a wireless system.

The best solution is to look for a manufacturer whose wireless line encompasses a large array of reliable I/O and requires very few extra components. Ideally, look for a manufacturer whose I/O line is independent of network type.

Necessity of Choosing Solutions Up Front

Another concern of automation engineers in using wireless technology stems from the availability and cost issues just discussed: if the wireless version of their vendor's product line is different, engineers must choose at the beginning of a project whether to use wired or wireless communications. They must specify components and commit to a networking method up front.

Having to commit to a network in the early days of a project sets in stone portions of the system design, from overall approach to details of field connections.

If the chosen method proves disappointing, changing it means significant additional time and expense not only to buy, install, and configure new components, but also to redesign.

And these additional costs often include more than just I/O and network hardware components; they may also include software costs for licensing, training, and programming wireless I/O.

Ideally, wireless I/O from automation manufacturers would act more like the typical laptop computer, which includes both wired and wireless capability and can therefore adapt to a wired or wireless network, while offering the same functions and using the same software with either method. Long after you purchase the laptop, you can choose the network type or change from wired to wireless as circumstances dictate.

Addressing Wireless Concerns

Automation manufacturers could go a long way toward addressing engineers' concerns about wireless if they could do just four things:

- Include broad support for wireless standards—not just 802.11b—to give engineers options to improve individual system reliability.
- Include support for the best available security standards.
- Offer a full range of wireless I/O—ideally the same product line used for wired networks—and reduce the number of extra components or adapters needed for a wireless installation.
- Design controllers and I/O that can communicate with both wired and wireless Ethernet networks, as needed.

Let's see what this improved wireless system would look like.

Broad Support for Wireless Standards

Including broad support for wireless standards, manufacturers could go beyond 802.11b and give automation engineers additional options to address their individual wireless applications.

If support were included for all three of the most commonly used wireless standards in the world today—IEEE-802.11a, b, and g—engineers could use wireless access points, routers, and repeaters from nearly any vendor to build their wireless networks.

Depending on system needs, they could choose the higher 5 GHz band to avoid interference from other devices, or they could choose a faster standard for higher throughput. They could also choose between ad hoc and infrastructure modes to suit the size and design of the network.

Support for the Best Available Security

For system security, WEP is no longer sufficient, and even WPA is less than ideal. WPA2 encryption algorithms with 802.11i AES provide the robust protection industrial wireless applications normally require.

However, since some applications may use an older standard or not require highly secure transmissions, support for all three standards—WEP, WPA, and WPA2—should be included for backwards compatibility.

Full Range of Wireless I/O and Reduced Number of Wireless Components

From the automation engineer's viewpoint, a separate product line for wireless—or a subset of the normal wired product line—is difficult to work with. But being able to use the same I/O components in both wired and wireless networks would save time and money during design, implementation, and use.

- In the design phase, the engineer could specify I/O with confidence, knowing that he could use any I/O in the product line and that it would work with either network.
- During implementation, the same methods and costs for installing I/O and wiring to field devices would apply to both networks; there would be no need to retrain technicians. If communication is changed from wireless to wired at any time in the project, no additional costs would be incurred for I/O or field wiring.
- During system use, just one set of spares would need to be stocked for maintenance, even if both wireless and wired I/O were in place.

In addition, wireless would be considerably more attractive if manufacturers required fewer wireless components overall. Both initial system costs and the cost for stocking spares would be lower.

Wired and Wireless Support in Controllers and I/O

For real flexibility, wireless controllers and I/O should support both wired and wireless communication, just like a laptop computer. If they can be used either wired or wirelessly—or, even better, both at the same time—difficult network decisions won't have to be made at the beginning of a project. If an engineer designs a project using wireless technology and then discovers a wired network would be better, he can still use the same hardware.

Adding a wireless interface to wired controllers and I/O also offers new options for segmenting networks. For example, critical I/O and controller traffic could use the wired network interface, while less critical maintenance, troubleshooting, or local HMI tasks could be done wirelessly with a similarly configured laptop computer.

As in a laptop computer, the functions available in the controller and I/O should remain the same, no matter which network is being used. Only the physical medium would be different, so all I/O features and supported protocols would be the same.

Even software would not have to change. Because control and HMI programs would run on wired and wireless networks with no modification, there would be no additional cost involved for licensing, training, programming, and maintenance.

One Manufacturer's Response

One automation manufacturer who has incorporated many of these solutions into its wireless offering is Opto 22. The company recently added wireless capability to its SNAP PAC System™—an intelligent, distributed system suitable for industrial automation, remote monitoring, and data acquisition—and to its SNAP I/O™, which can also be used as remote I/O with Allen-Bradley® Logix PLCs and PC-based control systems.

- In Opto 22's SNAP PAC System, control is distributed among programmable automation controllers (PACs) and intelligent remote I/O processors (called

brains). These controllers and brains also handle all communications for the system.

- The same brains, or intelligent I/O processors, provide both local processing and communications for SNAP I/O used with A-B and PC-based systems.

Opto 22 has added wireless LAN capability to these controllers and brains without removing the communication functions that are already there.

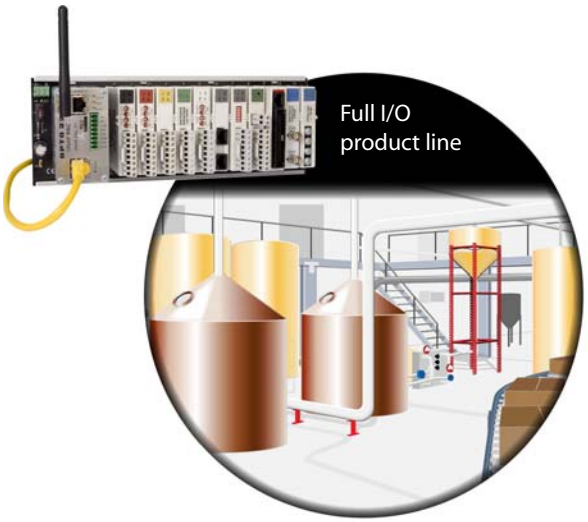
Wired and Wireless Support

A SNAP PAC controller, for example, has two independent Ethernet interfaces (two IP addresses; two network interface cards, or NICs). These two interfaces can be used for redundant links or for segmenting networks. Adding wireless support means that the PAC now has three Ethernet interfaces (three IP addresses; three NICs)—two wired and one wireless. If desired, the wireless controller can segment a wired from a wireless network and provide a redundant link as well.

A SNAP PAC brain, in contrast, has two *switched* Ethernet interfaces (one IP address; one NIC). The switched interfaces allow these intelligent I/O processors to be daisy chained, if needed. Adding wireless support to the brain means adding a second IP address, so the brain can communicate through either a wired or wireless network, as required by the application.

These controllers and brains retain the same functions whether they are used wired or wirelessly.

All the standard industrial protocols supported by the wired Ethernet interface are fully supported over wireless. These protocols include ODVA's EtherNet/IP™, Modbus®/TCP, OptoMMP, SNMP, SMTP, and FTP.



In addition, the same control and HMI development software is used regardless of physical network. Because the physical layer is abstracted, control programs running on the PAC require no modification for wireless communication.

Communications for both wired and wireless networks are set up in the same configuration software and can be done at the same time, or one network type can be added later.

Full I/O Product Line

Because Opto 22 adds wireless capability by modifying only its controllers and brains, the company offers the same I/O modules, racks, and other components whether the application is wired or wireless. No additional wireless components are needed.

The full line of analog, digital, and serial SNAP I/O modules is available for engineers to use with either network—an important point, since the company is well known for the breadth and reliability of its I/O.

Existing Opto 22 customers will also find it easy to experiment with or switch to wireless: they can simply exchange the existing brain or rack-mounted controller with a wired/wireless one. The mounting rack, I/O modules, field wiring, and all other communication and processing functions remain intact.

Support for Multiple Wireless and Security Standards

Opto 22's controllers and brains support 802.11a, b, and g, in both ad hoc and infrastructure modes. Engineers can use the higher frequency 802.11a standard at 5 GHz to avoid interference; they can use the faster 802.11g standard if that provides better performance.

Engineers can also use WPA2/AES algorithms for secure transmissions in infrastructure mode or, if need be, use WEP or WPA for backwards compatibility. All three standards are supported by Opto 22's controllers and brains.

Conclusion

Opto 22's wireless solution is currently unique in the industry in addressing several concerns automation engineers have about wireless I/O. With Opto 22's wireless controllers and I/O:

- Wireless system security can use the latest standards set by government and industry.
- System performance and reliability are maximized by broad support for wireless standards, giving engineers choices in how to implement system design for the best results.
- The company's complete line of analog, digital, and serial SNAP I/O modules is available for wireless use. No extra accessories are required for wireless, and the same spares are stocked for both wired and wireless portions of the system.
- The choice of a wired or wireless network can be made or changed at any time during the project, because the same hardware can switch between wired and wireless communication—or do both.

More About Opto 22

Opto 22 was started in 1974 by a co-inventor of the solid-state relay (SSR), who discovered a way to make SSRs more reliable. In the late 1970s the company developed the red-white-yellow-black color-coding system for input/output (I/O) modules, which is still a standard in the industry. As one of the original developers of the OPC interoperability standard, Opto 22 has consistently built products on open standards rather than on proprietary technologies.

The company first entered the wireless field in early 2000, when it became the first automation vendor to launch a wireless LAN I/O product. Two years later the company partnered with wireless leaders Nokia, AT&T Wireless, and Kyocera to deliver wireless remote monitoring and data acquisition solutions to manufacturers.

The company is probably best known for its high-quality SSRs and I/O. Quality is built into Opto 22 products: products are made in the U.S.A., and every I/O module is tested twice before leaving the factory in Temecula, California. The company does no statistical testing. Because the company builds and tests its own products, Opto 22 guarantees all solid-state SNAP I/O modules for life. Product support for all products is free.

For more information on wireless I/O and other products, visit www.opto22.com or contact Opto 22 Pre-Sales Engineering.

Opto 22 wired/wireless SNAP programmable automation controllers and SNAP I/O

Opto 22 • 43044 Business Park Drive • Temecula, CA 92590-3614 • www.opto22.com
SALES 800-321-6786 • 951-695-3000 • FAX 951-695-3095 • sales@opto22.com • SUPPORT 800-835-6786 • 951-695-3080 • FAX 951-695-3017 • support@opto22.com