

Wireless for Industrial Control: I can get to the data, now what?



Introduction

Technologies that enable factory and sensor equipment to connect to the network typically focus on connecting equipment "A" to workstation "B" over network "C". That's all fine and well if, at the end of the day, the data gets used. It all starts with connecting the equipment to the network. Choosing the right technology provides a path for future capability enhancements. Actually getting the data delivered over the network is often left to the IT professionals, but a basic understanding of the architectures is fundamental to getting the right capability out of the network. At the end of the day, unless there's compelling application of the data to real problems, it's a pointless exercise. The whole reason to extend access to industrial equipment is to provide a value to the enterprise.

Connecting to the data source

One of the biggest misperceptions of a wired network over a wireless

network is the range. Wire seems so much more capable of carrying signals than the air, although, in practice, the range limitations are similar. For the last 100 meters, wireless networks are much more flexible in terms of installation and changes than wired networks.

While the equipment costs of a WiFi installation is typically higher than a wired Ethernet network, the installation costs are normally lower. The labor costs involved in running a datacomm cable to each piece of equipment on the factory floor can be quite high, especially when there is no existing datacomm infrastructure. Once the facility has been wired, any equipment changes incur additional wiring costs. WiFi networks don't have these costs for installation and changes. The same installed WiFi equipment can be moved without additional labor for cabling.

Given the range, cost and installation issues, WiFi is often the best choice for connecting equipment and sensors to a network. Since most of the information has to be ultimately connected to an Ethernet network for transport to its ultimate destination, a local server or over the Internet, WiFi makes sense as the wireless technology of choice. Data is kept in an IEEE 802.3-type packet from the source to the ultimate destination, using an industry-standard infrastructure.

Embed Quatech's Airborne™ 802.11b Wireless LAN Node Module into OEM applications in as little as 6 weeks.

- Highly integrated 802.11b wireless module with radio, base-band & application processor
- Built-in web server enables drop-in LAN and Internet connectivity
- Quick time-to-market & reduced development costs
- Reduces need for RF and communications expertise
- Integrated RTOS and TCP/IP Stack
- Configurable serial, digital & analog I/O ports

Delivering the data

There are three basic network architectures used to deliver data from the source (equipment or sensors) to the ultimate user of the data on the network. The equipment may be a server to a client on the network, the equipment may be a client to a server on the network, or the equipment may be a web server to a browser on the network. Each of these architectures has distinct advantages and the best architecture for the application will depend on how the data is to be used.

A server-to-network client scenario is called “pull” architecture. The network client initiates data transfers and “pulls” data from a server attached to the equipment as needed. The network client is often a custom program for interacting with the data. In the classic Industrial Control environment, the equipment is usually an OPC (OLE for Process Control) server, and the client is a SCADA (Supervisory Control and Data Acquisition) application. “Pull” architecture is best used when data or control access to the equipment is only needed periodically.

A client-to-network server scenario is called “push” architecture. Here, equipment has data that needs to be delivered and the equipment initiates the transfer. The network server may be a custom application for monitoring the equipment, or a database server that stores the data for future analysis. This architecture is used for alerts and alarms, or recording status changes for future records or analysis. “Push” architecture is best used when equipment has a stream of data, or decides that data is available to use.

A Web server is a special type of “Pull” network where a standard web browser on the network client is able to present a portable graphical MMI to the equipment data. The interface is portable because a wide variety of computers and operating systems have standard W3C (World-Wide Web Consortium) browsers either built-in or available. Whether the client is a PC, MAC, Unix or Linux machine or just a browser terminal, they can all access and display the graphical interface provided by a Web server, even an embedded Web server. The standard browser interface allows this architecture to be easily used from any location over the Internet.

Using the data

There are several compelling reasons to connect equipment over a network. Since equipment can be configured electronically (through a serial port) it makes sense to use a network to enable remote equipment configuration and access to operating status. The equipment operational history can be retrieved and stored for later analysis or recordkeeping. For configuration and status, networked equipment can be interactively diagnosed remotely, leveraging technical resources geographically.

Most modern equipment has some capability of being electronically configured typically using a serial port. Equipment configurations and recipes can be developed and stored on the network, and deployed over the network to the equipment when required. This allows for a quick and consistent configuration

of the equipment, and minimizes human error. This is especially helpful in high-mix or quick turn-around environments where configurations change frequently. Centrally managing configurations ensures greater repeatability and less set-up and verification time for the organization.

Light bars are wonderful, but you have to look at them. A condition requiring attention may go unnoticed because the operators are working elsewhere. With a network connection, operational status can be relayed virtually anywhere. Standard e-mail messages can be sent to an “inbox” on a desktop, to cell phones and pagers as text messages. This allows equipment to directly communicate with the operator required to resolve the issue.

There are several industries where product and process traceability is a requirement. Both the food services and medical industries require traceability of product back to the process. Using a “Push” architecture, process equipment can send operating conditions and status to a database for recordkeeping and analysis. If there is quality control issue, it can be traced back in time to the process state when the product was made for much better analysis.

When a line is down, the quicker the problem can be isolated and identified, the sooner the line will be back up and operational. A Process Engineer can immediately examine the status of the equipment from his desktop and solve the problem. With networked equipment accessible over the Internet any issue can be dealt with immediately. Wireless networks add the benefit of technicians and engineers being able to connect directly to the machine, without having to “plug-in.” Notebook and handheld computers with off-the-shelf WiFi adapters can communicate directly with the equipment right on the shop floor. This brings all of the desktop tools right to the equipment, further enhancing the configuration and diagnostic capabilities.

Conclusion

There are compelling business cases for network-enabling industrial equipment. Standard networks can extend equipment accessibility to the shop floor into the office, and beyond the building to different sites. This ability allows creative organizations to leverage their resources geographically. Because the IT industry has already developed the architectures to move and manipulate this information, there is much less R&D required to deploy solutions. Wireless WiFi networking makes sense because it has all of the advantages of Ethernet, without the cabling and access limitations.