

New Standards-based Web-enabled Technologies Streamline Wireless Network to I/O Interface



Introduction

Wireless networks make a lot of sense in monitoring I/O for control systems. Along with the ability to rapidly deploy devices without extensive plant wiring, there are also a number of unexpected benefits. While more complicated to configure for operation, wireless networks provide features for overlapping networks in the same area, as well as for limiting access to critical networks through data encryption and security. With the flexibility and diversity of wireless network I/O adapters, ranging from simple serial bridges, through sophisticated command-based processors with integrated Web servers, many problems can be solved with a minimum of custom programming. The added benefits of standard protocols include the ability to route data over the Internet, providing the opportunity for centralized technical services operating over broad geographic regions.

Understanding Access Points When Connecting to a Network

Wireless adds additional complexity to networked devices. Not only do you have the traditional IP concerned with how to get onto the wired backbone. Wireless network traffic typically uses an Access Point (AP) to bridge between the wired and wireless networks. WiFi networks have both unique channels and Service Set Identifiers (SSID) that need to be assigned before data can travel across the wireless segments onto the wired subnets.

Unlike traditional Ethernet connectivity that only provides one channel to the network (the port you plug into), WiFi provides up to 14 distinct channels for network traffic, depending on your country profile. Each Access Point is configured with a channel and an SSID. In a typical deployment, all Access Points on the same subnet will have the same SSID. For example, all of the Access Point on the Manufacturing subnet may have the SSID "MFG".

Any client device on the Manufacturing subnet will need to be configured with that SSID, ensuring that data traffic will go onto the Access Points appropriate subnet. A Client device needing to use the Manufacturing subnet would be configured with an SSID of "MFG"

**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

and would never transfer data over the Engineering subnet. The Client device is dependent on which subnet it associates with for proper operation and allows multiple, distinct subnets to operate in the same physical environment.

Unlike wired Ethernet, where the physical cables force a one-to-one association between Client device and the network, Wireless networks have an implicit many-to-one relationship between potential Client

devices and the wired Ethernet backbones, through the Access Points. This open relationship between the Client and the Access Point, as well as through the Access Point into the wired backbone, is the basis of much concern. This issue is addressed by Wired Equivalent Privacy (WEP) Security designed to provide encrypted data streams as well as access control between Clients and the Access Points. By encrypting the data between the Client and the Access Point, only Clients with the private key information can successfully communicate with the Access Point. There were some early implementation issues with WEP, but the current generation has done away with the previous generation static key assignments. Breaking into today's wireless networks is significantly more difficult.

Working with I/O Interfaces

The simplest interfaces to I/O devices are wireless-to-serial bridges. This allows a network device, such as a PC or server, to communicate with an RS-232, RS-422 or RS-485 I/O device. Simple programs, Network OPC servers or other PC-based applications can, using the proper protocols, go out and query a wide variety of I/O devices. By placing most of the intelligence on host computers on the network, these devices can be quickly deployed, configured and operational.

Other application specific wireless devices include the digital or analog I/O functionality. These devices tightly couple the I/O with the wireless network. Although the overall flexibility is limited to the designed-in I/O functionality, for dedicated applications they provide significant value. By integrating I/O functionality and sometimes even the OPC server code into the wireless I/O point, deployment and configuration becomes simpler because there is less code to deploy on network computers. For focused applications, this can often more than make up for any reduction in flexibility.

Data Usage Optimization

It's one thing to connect I/O devices to the wireless network, but another to actually use the data. There are as many ways to use data as there are ways to collect data. Simple serial bridges rely on the network computer to

perform all the processing. Devices with embedded I/O capabilities often provide a higher-level command set for interacting with the I/O. Newer Web-based interfaces provide a sophisticated interface without deploying additional software – a huge savings in development time and resources.

Application specific command sets, for configuring, interrogating or assigning I/O ports are common for integrated wireless-to-I/O units. They provide a simple capability for applications to inquire or manipulate the I/O points without getting bogged down in sophisticated protocols. This allows rapid development and deployment of monitoring or HMI interfaces for applications.

With the development of more intelligent wireless adapters, Web-based interfaces provide a sophisticated way to combine graphics and monitoring functions for I/O devices. Web page development provides a convenient way to deploy graphic HMI interfaces without requiring any software to be installed on network computers. So any computer, anywhere, can have full HMI access to the controlled features. In addition, many wireless handheld computers also have browser software that allows engineers and technicians to walk the floor and inquire or configure settings in the device, without plugging in.

With the I/O connected to a network, a number of interesting possibilities open up in the maintenance and operation of control systems. If the network uses industry standard protocols, such as TCP/IP, access is expanded beyond the local area networks, out onto the Internet. This opens up opportunities for centralized engineering and technical support over a wide geographic range. Remote engineers have the ability, through the Internet, to immediately access, query, configure and monitor equipment operation without having to travel, or rely on a local technician to follow instructions and relay observations. This dramatically reduces the time for diagnostics and repair.