Industrial Communications

Ira Sharp, Marketing Manager for I/O and Network, Phoenix Contact

The times they are a-changing… In an “on-the-go” world, the need for information is great. With smart phones and other devices, we expect our news instantly, anywhere we might be. These devices drive great demands on the need for network communications and available information.

Things are no different in the industrial world. While we may not wait for a newspaper to get our media updates, we do wait for our maintenance team to make their rounds reporting equipment issues. Or, we wait for the production team to collect shift data to define how effective processes are running. Making these processes more efficient requires better, faster data with less user interaction and more advanced automation.

This advanced automation needs faster, more available and easier-to-use communications infrastructure. Ethernet has provided an effective, easy-to-use method of communicating all types of data. Ethernet makes it possible to transport data over standard copper cables, or through media converters using fiber, cellular or radio networks. With Ethernet as a common communications platform, an industrial automation system can combine any of these media interchangeably. This provides an effective way to network assets that were not previously obtainable because of location or costs. While the user must consider and understand the pros and cons of each medium, the underlying network will still function as expected if each medium is used correctly.

This article will focus on the different media that can be used to communicate Ethernet data, including standard copper Ethernet cables, fiber optic, cellular, Wi-Fi and 900 MHz wireless. In addition, it will define steps to protect the automation system from tampering and outside attacks that are a risk in an easy-to-use infrastructure such as Ethernet.

Standard Ethernet Cables
Standard copper Ethernet cables are the traditional way to transmit Ethernet data

in a local network. These cables are generally used with a variety of devices, such as unmanaged and managed switches, routers and firewalls.

An unmanaged switch is the most basic way to connect multiple Ethernet devices on a network. Unmanaged switches will learn the network's connected devices and route Ethernet data as needed. This is a very basic device and requires no configuration. However, with the lack of configuration comes the inability to make any advanced network decisions about how data should flow. The unmanaged switch does not allow for redundant topologies.

Managed switches give the network designer the ability to decide what type of traffic is permitted to flow through the switch. For example, if a particular Ethernet device needs priority, quality of service (QoS) can be used to ensure that device's traffic is handled prior to a lower priority device. In addition, Virtual Local Area Networks (VLANs) can be created. This segments Ethernet devices that share the same network medium, allowing for greater security and reduced traffic flow. Finally, managed switches enable redundancy protocols such as Rapid Spanning Tree Protocol (RSTP) or Fast Ring, providing an automatic failover connection for Ethernet devices to ensure the uptime a control system needs.

Routers

Routers can be used to connect different local networks. This allows systems to operate within their own local network, while allowing access from a "higher level" device to multiple local networks. For example, routers in an industrial control system commonly allow access from the IT department or from an ERP system into the production network.

With this type of access, it is important to control what devices can be accessed. This is a function of a firewall. The firewall is a list of network rules defining which devices are allowed to talk with other devices, and what type of information can be retrieved from these devices. For example, an ERP system typically needs production data, such as real-time updates on the status of manufacturing and the quantity of goods being produced. However, you generally do not want the ERP system to have any "control" over the production network. A firewall will accomplish this by limiting the access between the ERP system and the production network.

Sometimes, the distance is too great or cable runs are too costly for standard copper Ethernet cables. In these cases, alternatives must be explored. If distance is the issue, fiber optics can be used. Fiber is a great means of Ethernet communications. It can be connected up to 80 km and provides immunity against interference, because the transmitted signal is light – not electrons over a copper wire. This is ideal when networking in high EMI/RFI areas.

Wireless Options

If cabling in general is not an option for network connectivity, wireless is a great alternative. There are two basic wireless options: private radio and public radio. With private radio, the customer owns the network and has complete control. This "locked down" network provides an added layer of security as it is inaccessible from

devices outside the network. However, because this is a dedicated network, a network infrastructure will need to be created.

Wi-Fi is an ideal means of wireless communications for many applications. 802.11g offers speeds up to 54 Mbps, and 802.11n offers speeds up to 600 Mbps. Many different types of devices can be networked using this technology. Wi-Fi is also a public standard, which means third party devices can be configured to access the network.

An example of a Wi-Fi automation application is networking automated guided vehicles (AGVs). It is not possible to wire an Ethernet connection to a roving vehicle, and the use of brush arms can be costly to install and maintain. Wi-Fi communicates Ethernet data to the roving devices.

With the accessibility of the network from third party devices, a laptop or even an iPad could serve as a mobile operator panel. This mobile operator could check network status, define current position and data values, or even make program changes. The access of all devices on the Wi-Fi network is secure, as all devices must either share a similar passphrase called a PSK (pre-shared key) or have a certificate, which is used as part of 802.1x, to access the network. These are very robust forms of security when used within WPA2, the latest in Wi-Fi encryption and security.

Wi-Fi is great for applications that require fast speeds at shorter distances (generally less than 3,000 feet). For greater distances, proprietary radio can be used. Proprietary radio capabilities vary from manufacturer to manufacturer. For example, Phoenix Contact offers a proprietary technology called Trusted Wireless. Trusted Wireless operates in the 900 MHz range and uses 1 W of transmit power with frequency-hopping spread spectrum (FHSS). The 900 MHz Trusted Wireless technology is designed for use in the USA and can provide Ethernet connections at speeds up to 500 Kbps over 10-20 miles or through walls in plant. This type of radio is ideal for a Supervisory Control and Data Acquisition (SCADA) network that will cover a large area.

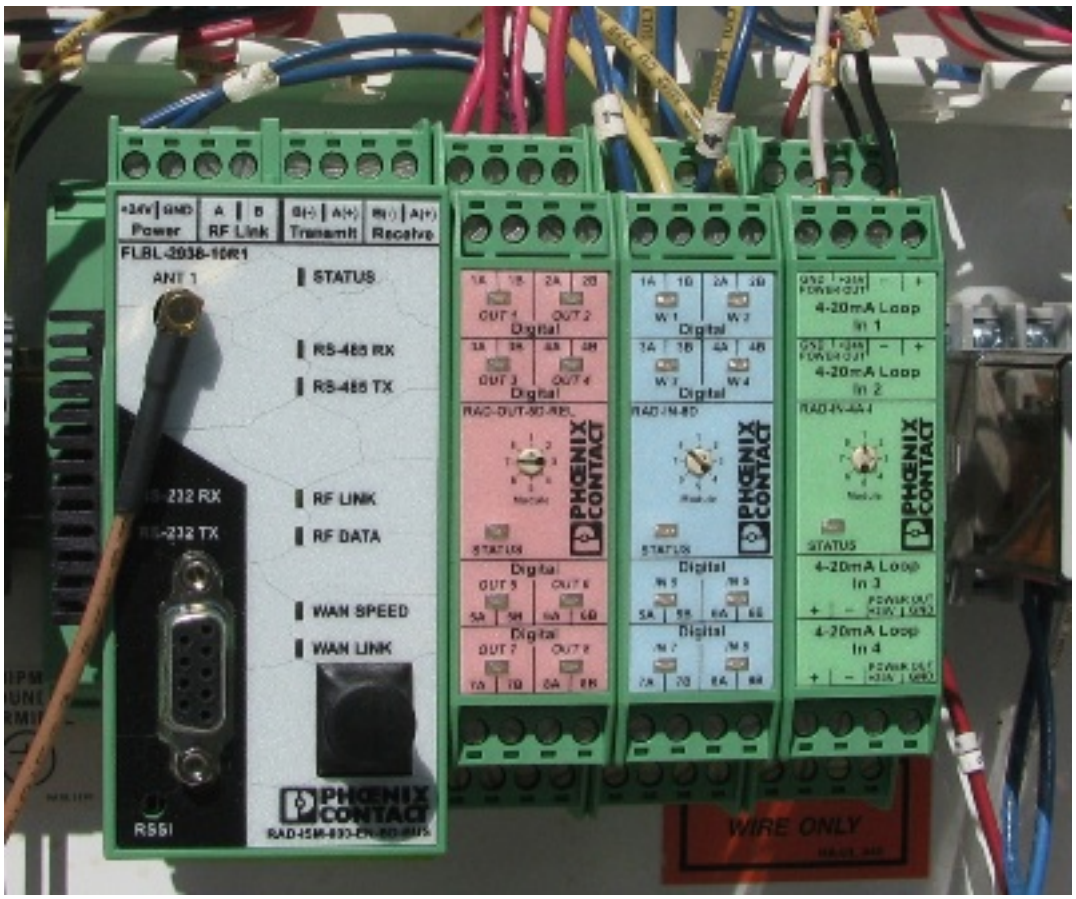

Figure 1*: Proprietary radios (such as this one used to automate an irrigation system at a golf course) can often cover longer distances than Wi-Fi radios, making them ideal for large SCADA networks.*

Cellular

If a proprietary system does not cover the required distance, or if network connections need to cover a large distance and are mobile, cellular technology is an option. Cellular allows easy network connections around a town, city or even around the world. With cellular, the industrial automation network will no longer be contained by a private network, as the cellular infrastructure is a public system. There are many safeguards in place to keep data secure over the cellular network and to add security. Specifically, virtual private networks (VPNs) can help secure data communications. By combining VPNs and the cellular network, Ethernet connectivity can be achieved virtually anywhere there is cellular access.

Today’s industrial networks need to be faster and more flexible than ever before. Industrial Ethernet – whether wired or wireless – can meet these demands. An engineer needs to determine many factors to determine what medium is best for a particular network, and to ensure that the proper security measures have been taken. Ultimately, an industrial Ethernet system can help a facility run more efficiently, decrease day-to-day costs and increase profits.

Figure 2*: Advanced Ethernet components such as managed switches, routers and VPNs can enhance the control capabilities and increase the security of an automation network.*

www.phoenixcontact.com [1]

Posted by Janine E. Mooney, Editor

March 16, 2012

Links:
[1] http://www.phoenixcontact.com