PART 1

OPTIMIZE ETHERNET/IP

Learn how to cost-effectively apply IEEE 802.11a/b/g and proprietary frequency-hopping wireless technologies to EtherNet/IP networks.

By Gary Enstad, Wireless Application Development Engineer and Jim Ralston, Northeast Regional Sales Manager, ProSoft Technology

The use of Ethernet for industrial networking is growing rapidly in factory automation, process control and SCADA systems. ODVA's Ethernet Industrial Protocol (EtherNet/IP™) network standard is gaining popularity as a preferred industrial protocol. Plant engineers are recognizing the advantages of Ethernet-enabled devices, such as ease of connectivity, high performance and cost savings.

While EtherNet/IP has many advantages, cable installation to hard-to-reach locations or moving equipment might not be reliable or cost-effective. Wireless Ethernet technologies have emerged that now can reliably reduce network costs while improving plant production.

However, applying these technologies isn't simple. Industrial Ethernet systems vary in bandwidth requirements, response times and data transmission characteristics. This article explores how to apply IEEE 802.11a/b/g and proprietary frequency hopping (FHSS) wireless technologies to EtherNet/IP networks for industrial automation systems.

EtherNet/IP Characteristics

EtherNet/IP is a network protocol defined by ODVA (www.odva.org). As an open standard, vendors can implement EtherNet/IP communications in their devices without licensing fees. Many vendors have adopted EtherNet/IP, including Rockwell Automation. The company selected the protocol as one of three preferred networks on its Logix controllers, in addition to DeviceNet™ and ControlNet™.

An important part of the EtherNet/IP standard is the definition of Common Industrial Protocol (CIP™) messaging. CIP defines the information packet recognizing that the message attributes will vary as applications vary. Therefore, the CIP message definition takes into account a range of applications, including programming/diagnostics, data collection, programmable logic controller (PLC) or programmable automation controllers (PAC) data exchange, and I/O communications, along with safety critical and motion-control applications.

EtherNet/IP uses the standard seven-layer Open Systems Interconnection (OSI) model for protocol definition, as shown in **Figure 1**, with CIP at level seven.

Implicit versus Explicit Messaging

CIP defines two types of connections. The first is Explicit CIP, which uses TCP/IP for its communications protocol. Explicit

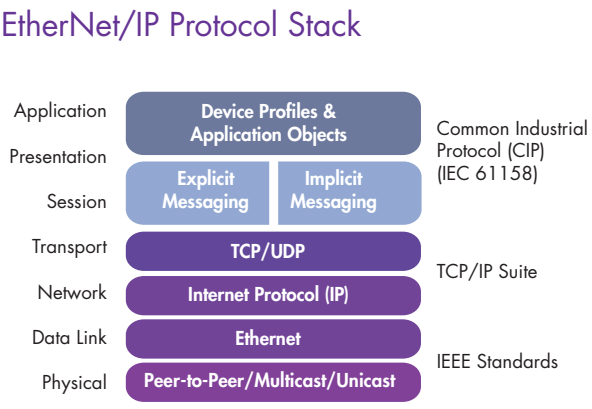

Figure 1. EtherNet/IP uses the standard seven-layer OSI model for protocol definition.

messages are unscheduled and use a request/response communications procedure or client/server connection. Examples of Explicit CIP include executing a MSG statement between PLC/PAC human-machine interfaces (HMI), device diagnostics and program uploads/downloads.

The second type of CIP is Implicit. It uses User Datagram Protocol (UDP/IP) for its communication mechanism. Implicit connections are time critical, scheduled, and use a requested packet interval (RPI) parameter to specify the rate at which data updates.

Implicit connections use UDP packets to produce/consume data over an EtherNet/IP network. The UDP packets usually are multicast if more than one data consumer exists. This multicast address is assigned by the EtherNet/IP interface and is unique for each produced tag.

Multicast IP addresses are used to make the network more efficient. A data producer can produce data for multiple consumers. By using multicast packets, many devices can receive or consume this packet without the producer having to send it to each consumer.

EtherNet/IP I/O blocks can support two major implicit connection types: direct and rack optimized. A direct connection is a real-time, data-transfer link between the controller and a single I/O module.

Rack optimization is a connection option in which multiple discrete I/O modules in a chassis can be consolidated to use a single connection. Analog modules typically can't be rack optimized, and each analog channel uses a separate CIP connection.

Proper network design is critical for implicit networking systems to achieve predictable "deterministic" I/O performance. Proper design also helps to ensure that I/O traffic doesn't "leak" outside of the automation network, causing network degradation.

ODVA recommends specific design strategies to ensure optimized network performance, such as segmentation (isolating sub-networks), the use of managed layer-two switches (IGMP snooping and multicast packet filtering) and high-speed network infrastructure (100Base-T or faster). Wireless design is particularly critical because wireless is, generally, slower than wired networks and exists on a shared media.

CIP Safety

CIP Safety™ is an extension of standard CIP. CIP Safety simply extends the application layer by adding a CIP Safety layer to it. CIP Safety is used when stop-on-a-failure is required to assure human safety. It has many triggers in place to detect critical and noncritical errors and to close the connections to assure a safety condition.

New specifications enhancements have been added to allow safety applications to have longer fault tolerances and the ability to help maintain operations over wireless networks. These enhancements include extending the RPI multiplier and the ability to configure the packet time expectation.

These parameters are especially helpful in the wireless world because latency tends to be higher. This setting also could allow radio-frequency (RF) packets to be retransmitted if required to assure the safety packets get though. These changes lend themselves to make CIP Safety well-suited for wireless communications.

Value of Wireless in EtherNet/IP Applications

While EtherNet/IP networks grow in popularity, in many applications, conventional wired Ethernet infrastructure is not a practical option, and an alternative option must be sought. In these cases, properly implementing wireless networks can reduce total costs and, in many situations, improve reliability and increase plant production.

Wireless as an Alternative to Cable Installation

The cost of installing cable in industrial plants is a function of the material costs plus the labor charges. Cable installation cost estimates range from $20 to $2,000 per foot, depending on installation challenges (distances, obstacles), environment and local labor costs. Factors that impact total cable installation costs include:

- Distance and number of locations.
- Conduit design and installation.
- Trenching.
- Fiber optic cable & infrastructure (e.g. fiber switches).
- Hazardous location regulations.

When the total cost of cable installation is calculated, you can compare it to the total cost of wireless. Wireless total costs include the wireless hardware (including wireless nodes, antennas and cables), antenna installation (if applicable) and personnel training.

However, even when factoring in these additional costs, the wide swing of costs involved in wired installations make it unsurprising that in many cases, the savings realized by wireless are dramatic and significant.

Properly implemented wireless sometimes offers better reliability than cabled systems because there are fewer mechanical connections to fail. If the cable is broken by moving equipment, severed during construction or damaged by vibration, production may be down for hours until the problem is located and corrected.

Wireless also offers electrical isolation like fiber optics offer, eliminating potential surge damage from ground plane transients.

Finally, wireless helps reduce project time because it's typically quicker to install than wired systems. This is especially beneficial in systems that move over time, such as mining operations, or for reconfiguring plant-floor production equipment.

Wireless in Mobile Equipment

Wireless can significantly benefit moving production equipment, such as material handling systems in which controllers and I/O are on moving platforms. Examples include overhead cranes, transfer cars, stacker/reclaimer cranes, automatic guided vehicles (AGV), conveyor systems and rotating packaging machines.

Mechanical Ethernet communications methods, such as festoon cable systems, flex cable, slip rings and rails, are prone to frequent maintenance and sudden failures. These systems often have high acquisition costs, especially when supporting Ethernet. Many of these mechanical systems are being retrofitted with wireless as production shutdowns become more frequent.

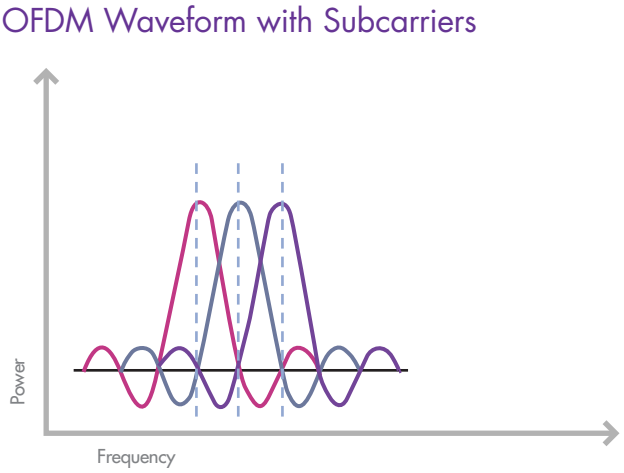

Figure 2. Direct Sequence and Orthogonal Frequency Domain Modulation use a wide channel within the band to simultaneously modulate a highly encoded bit pattern.

Wireless as a Leased Telephone Line Alternative

For distant sites, leasing phone lines for Ethernet communications is common. Most phone companies offer a range of digital services from 56 Kbps up to multiple Mbps.

Unfortunately, many remote industrial sites, such as pump stations, well heads and storage tanks, may be too far away from the telecomm infrastructure to support higher-speed services. This can sometimes lead to telephone line reliability issues. Private RF systems, such as spread spectrum, are managed by the user and don't rely on any third-party services.

Cost is another issue when leasing telephone digital circuits. Monthly charges can be several hundred dollars or more per site. Because these reoccur monthly, you must set a significant budget just for communication. The initial cost of a private RF system may be higher, but it has no significant reoccurring costs. Return on investment for a complete wireless system might only take several months.

Wireless Considerations: TCP/IP or UDP/IP

Before selecting the wireless technology, it's important to consider the EtherNet/IP application and determine if it will be based on TCP/IP, UDP/IP or a combination of the two. This is important because TCP and UDP protocols behave differently over wireless networks.

UDP/IP is typically used in implicit messaging systems in which controllers communicate to I/O blocks over Ethernet media. TCP/IP is much more common because it's the basis for explicit messaging between controllers, HMIs, remote programming and data collection.

Ultimately, the automation architecture will determine the EtherNet/IP protocol type and appropriate wireless technologies.

Wireless Technology

The most common approach to wireless Ethernet is RF transmission in the spread spectrum bands. Globally, the

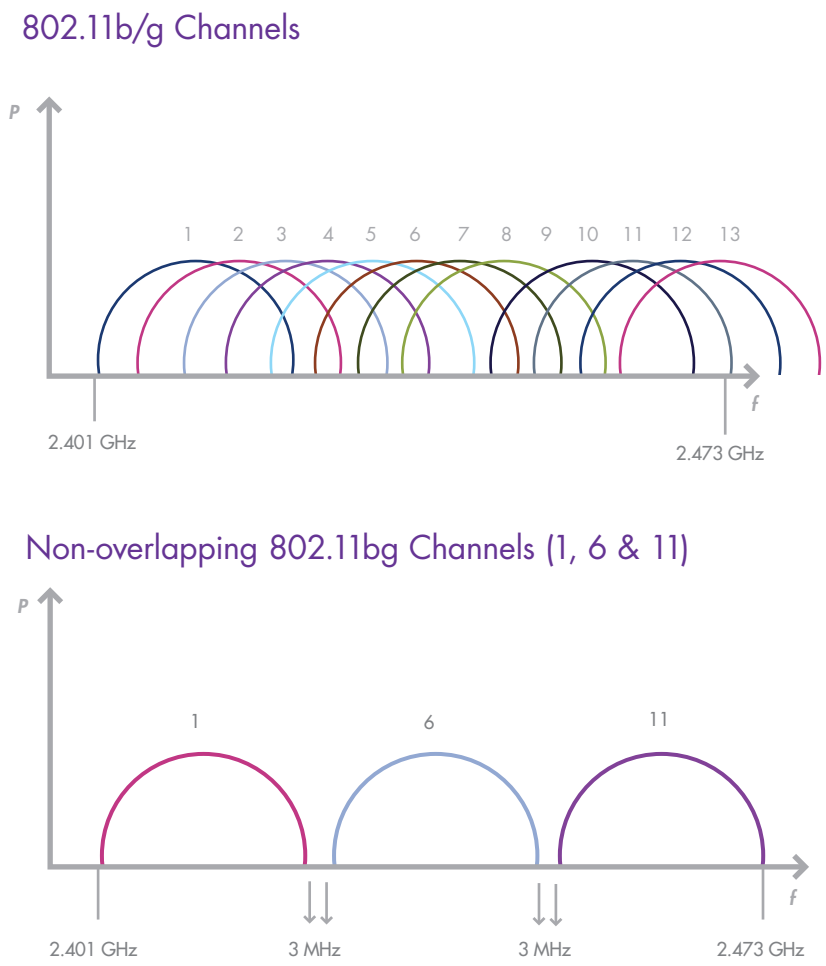

Figure 3. IEEE 802.11n will incorporate Direct Sequence and Orthogonal Frequency Domain Modulation techniques. The wide-band modulation offers high speed, but it is more prone to noise problems when multiple systems are operating in close proximity. IEEE 802.11b/g has 13 available channels (top), but only three channels don't overlap (bottom).

2.4 GHz and 5.8 GHz bands are available for license-free use in most countries.

Spread spectrum means spreading the RF energy across the entire, or wide portion of, the spectrum. This permits high-speed communications, and operates in "noisy" environments that have multiple RF systems.

Three major methods of spreading RF energy exist: Direct Sequence (DSSS), Orthogonal Frequency Domain Modulation (OFDM) and FHSS. Each method has advantages and disadvantages.

DSSS and OFDM use a wide channel within the band to simultaneously modulate a highly encoded bit pattern (see **Figure 2**).

DSSS and OFDM offer the fastest spread spectrum data rates because the wide channel permits complex modulation schemes to be transmitted. OFDM uses a complex modulation technique and is capable of high data rates and low latency. Latency is the transmission time a packet takes from one end to the other.

OFDM also is significantly more immune to multipath fading, a problem caused by RF reflections that often affects high data rate systems. Slower-speed FHSSs are relatively immune to multipath.

DSSS and OFDM are the methods used by all popular open Wi-Fi standards, including IEEE 802.11b, 802.11g (both transmitting in the 2.4 GHz band) and 802.11a (transmitting in the 5 GHz band). IEEE 802.11n is nearing ratification, and it will also incorporate these techniques.

While the wide band modulation offers high speed, it's more prone to noise problems when multiple systems are operating in close proximity. For example, the 2.4GHz band used by IEEE 802.11b/g has 13 available channels (11 channels in North America), but only three channels don't overlap (see **Figure 3**). This is one of the challenges that IEEE 802.11n will address.

Because of overlapping channels and the popularity of Wi-Fi systems in plants, band crowding and RF saturation can lead to poor wireless performance.

Frequency hopping is a popular technique for industrial systems because it has outstanding noise immunity techniques. Unlike Direct Sequence and OFDM, FHSS uses many smaller channels in the spectrum and rapidly changes channels, or "hops around," from channel to channel (see **Figure 4**).

FHSS has a high RF energy per bit ratio. By incorporating error-correction techniques, FHSS offers the best chance for successful data transmission. This is because the transmitter will send the packet over and over again using different channels until an acknowledgement is received.

The disadvantage of FHSS is that it's slower than Direct Sequence/OFDM and has longer data latency. Most FHSSs are limited to 1 Mbps or lower RF data rate. However, if the data rate is fast enough for the application, the reliability of FHSS

is tough to beat, especially in high noise environments.

IEEE 802.15.1 (Bluetooth®) is one of the few open standards incorporating FHSS. Because of IEEE 802.15.1's distance limitation, Bluetooth devices seldom are applied to Ethernet systems. Most industrial FHSS modems are proprietary, meaning that each manufacturer uses its own technique. And, vendor X usually won't communicate with vendor Y.

While this is a potential disadvantage for commercial systems, it can be desirable for industrial systems for two reasons: security and isolation from the wireless IT system.

Because industrial FHSS technologies typically aren't based upon an open standard, the manufacturer can use unique authentication processes and sophisticated encryption techniques to ensure high security levels. While security has significantly improved in Wi-Fi systems with Wi-Fi Protected Access (WPA™) and Wi-Fi Protected Access 2 (WPA2™) standards, hackers will continue to look for holes.

Fortunately, many industrial Wi-Fi manufacturers now include an option to hide the access point by not transmitting its Service Set Identifier (SSID) beacon, effectively hiding the access point from potential hackers. Other security techniques include cryptographic encryption, key management and rogue access-point detection. This provides the same high degree of security that FHSSs provide.

FHSS also offers plant managers the ability to operate their own wireless network separate from the IT department. Because of the popularity of 802.11 technologies for wireless network access, warehouse bar code systems and video surveillance, proprietary FHSSs could be the best choice for industrial systems.

Wireless Considerations: Frequency Band Selection

Considerations for selecting the frequency band for EtherNet/IP communications include:

- Required data rate.
- Distance.
- Line-of-sight (LOS) obstructions.
- Modulation technique.
- Band availability (government regulation).
- Band saturation (crowding).

You also should consider spectrum management issues if wireless already is in place or planned for the future.

License-free communications using the spread-spectrum bands is popular for industrial Ethernet systems. Three major spread spectrum bands are available in the Americas and Australia:

- 902 MHz to 928 MHz
- 2.4 GHz to 2.483 GHz
- 5.1 GHz to 5.8 GHz

Most countries in Europe, Africa and Asia permit license-free communications in the 2.4 GHz and 5 GHz bands, but local regulations vary and should be investigated to assure compliance.

Data rate and distance are the first major considerations in frequency band selection. Generally, frequency band and range (distance) are inversely related; the higher the frequency, the shorter the range (all other factors being equal). However, data rate and frequency band are directly related; the higher the frequency, the faster the potential data rate.

The other major consideration is band usage and management. Many plants use the 2.4 GHz extensively for IT and inventory systems. Therefore, the 900 MHz band (for slower speed systems) or 5 GHz band (for higher speed) might be the best choice for industrial wireless systems.

Wireless Considerations: Importance of Line-of-Sight

Antenna placement is a key consideration. Today's spread spectrum systems perform best with clear, unobstructed LOS between antennas. If obstructions exist, such as metal structures, concrete walls/floors, trees, etc., then communications will be impeded. In many industrial systems, however, obtaining clear LOS might not be practical or possible.

Fortunately, the lower-frequency 900 MHz band offers relatively good reflectivity and penetration characteristics. Using frequency-hopping techniques in the 900 MHz band has the best chance to provide reliable data transmission in applications without clear LOS, although at relatively slower speeds.

Applications without LOS always should be thoroughly tested before implemented.

For longer-range outdoor systems, clear LOS between antennas is even more critical. Additionally, RF transmission theory dictates that the earth can reflect the signal in a way that can improve or impede the signal. A buffer zone between the earth and the LOS also is needed for maximum signal levels. This area is called the Fresnel Zone (see **Figure 5**), and it's important when engineering the antenna system, particularly antenna height.

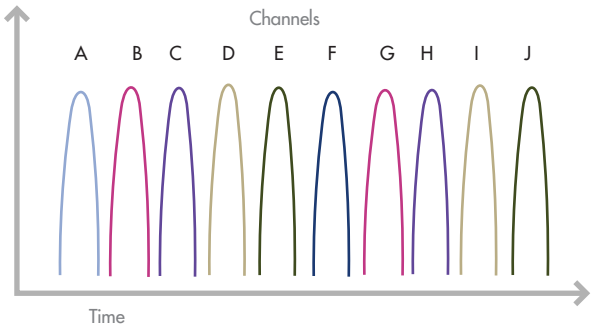

Figure 4. Frequency hopping is popular because it has outstanding noise immunity techniques. It uses many smaller channels in the spectrum and rapidly changes channels, or "hops around," from channel to channel.

Wireless Considerations: Multipath

Multipath is caused when the directed and reflected signals arrive and combine with different delays and amplitudes (see **Figure 6**).

The delayed signals are produced by reflected and scattered signals arriving at the receiver from different paths. This causes propagation delay.

These additional signals might completely cancel out the original signal, referred to as multipath fading. Or, these signals might be combined by superposition to create delay at the receiver. This delay is referred to as delay spread, defined as the difference in propagation delay between the directed (LOS) signal and the reflected signal.

The delay spread's tolerance varies among different radio manufacturers. Lower-cost radios often will have a lower number and be more susceptible to the multipath issue.

Large open areas with reflective surfaces, such as metal, typically are more prone to this phenomenon. But some wireless technologies are more likely to experience multipath fading issues than others. FHSSs are nearly immune to this problem, while older DSSS is very susceptible. OFDM is much better at handling multipath than direct sequence, so it's a good choice when you need high-speed data transfer.

Systems that are 802.11-based also might offer the option for a second receive-only antenna. By mounting a second antenna a few inches away from the main antenna, the radio receiver can determine which signal is best to use. This is referred to as antenna diversity, and it's one way to reduce multipath problems.

Sometimes making just slight adjustments to antenna positions in systems experiencing difficulties also can reduce problems.

Wireless Considerations: Contention

In most working environments, other wireless devices of some kind are in use. The IEEE 802.11 specification makes it possible for these devices to work well with the same proximity. Contention is the ability to capture the RF channel, use it, and share it with other RF devices on the same frequency.

If too many transmitters are on the same frequency, contention can be an issue because getting on the channel might be difficult and time-consuming as other users contend for that channel. Carrier Sense Multiple Access (CSMA) and Clear Channel Assessment (CCA) are the collision detection mechanisms used to help ensure that no two radios on the same channel transmit at the same time.

As previously discussed, frequency band management and channel allocation helps to ensure dependable wireless performance. This is especially crucial when wireless is applied to high-speed I/O systems. Dedicated "clear channels" are best for these demanding applications. They help ensure reliable coexistence of multiple RF systems.

Wireless Considerations: Interference

Many plant engineers are concerned that emissions generated by industrial equipment may interfere with wireless systems. DSSS, OFDM and FHSS are all capable of reliable transmission in noisy industrial plants where variable-frequency drives (VFD), high-voltage substations and even arc welders are in operation. Most interference problems are the result of other wireless systems operating in the same band or channel, and not from industrial equipment. □

Radio Frequency Path Terrain Profile

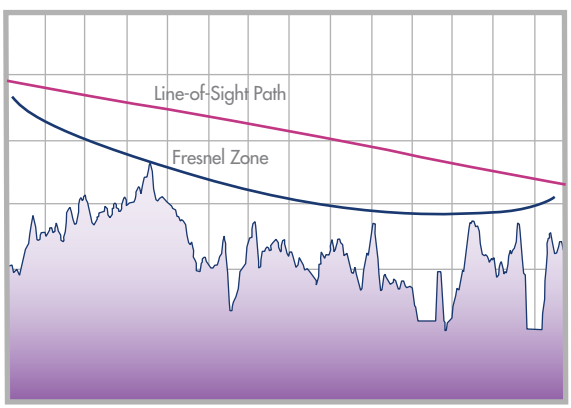

Figure 5. Radio-frequency transmission theory dictates that the earth can reflect the signal in such a way to improve or impede it. A buffer zone, called the Fresnel Zone, in between the earth and the line of sight also is needed for maximum signal levels. The Fresnel Zone is important when engineering the antenna system.

Multipath Phenomena

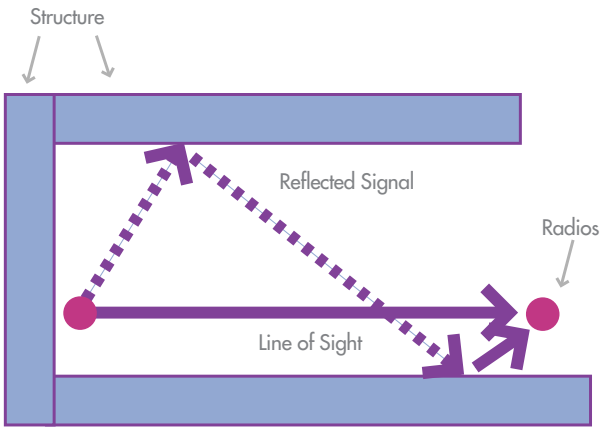

Figure 6. Multipath is caused when the directed and reflected signals arrive and combine with different delays and amplitudes. The delayed signals are produced by reflected and scattered signals arriving at the receiver from different paths, resulting in propagation delay. These additional signals might cancel the original signal completely.

Part II of this article will appear in the October 2009 issue of The Journal and will address EtherNet/IP reliability and performance over wireless links, and emerging technologies.

Gary Enstad, genstad@prosoft-technology.com, has a B.S. in Electrical Engineering and has been involved in wireless design and technical support for more than nine years. He is Wireless Application Development Engineer for ProSoft Technology's wireless division in Madison, Wis.

Jim Ralston, jralston@prosoft-technology.com, has been involved with the design and support of industrial wireless systems for more than 12 years. He is the Northeast Regional Sales Manager for ProSoft Technology in the Pittsburgh area.

ProSoft Technology, Bakersfield, Calif., participates as an Encompass™ Product Partner in the Rockwell Automation PartnerNetwork™. The company offers communication modules and network solutions that include in-chassis, protocol interface products, in-rack flow computers and PCs, standalone gateways and wireless communication networks.

ProSoft Technology, Inc.
www.rockwellautomation.com/go/p-prosoft
Rockwell Automation Encompass Product Partner Program
www.rockwellautomation.com/go/tjencompass