CONTROL ENGINEERING

Industrial Ethernet Implementation eGuide

Sponsored by:

B&B ELECTRONICS

Make The Right Connections

About B&B Electronics

For over 30 years, B&B Electronics has designed and manufactured rugged, reliable data communications systems for commercial and industrial applications.

As a proven technology partner to customers that include Fortune 100 companies, system integrators, value-added resellers (VARs), and distributors, B&B has experience working with a variety of products and technologies—from legacy serial devices to Ethernet, USB and wireless (including proprietary RF, industrial Wi-Fi and cellular). Its vast product inventory includes interface converters, switches, hubs, extenders, data acquisition equipment, and other device connectivity and data networking solutions.

Headquartered in the U.S., with distribution in over 60 countries around the world, B&B products are found wherever conditions demand rugged, reliable data connectivity solutions. At its U.S. headquarters in Ottawa, IL, B&B provides engineering, manufacturing, service and warehousing. Additional engineering functions are performed by its Quatech division in Hudson, OH. Activities at the European headquarters, located in County Galway, Ireland, include service, support and warehousing. Manufacturing, engineering and design for the latest broadband wireless products designed for M2M applications are handled at the Conel division, located in the Czech Republic.

In addition to delivering data communications solutions that are easy to install and use, B&B provides reliable technical support and detailed product documentation. Its technical experts have extensive experience assisting customers with system design, product selection, installation and troubleshooting. B&B also offers custom product design and manufacturing services to fit any unique engineering application.

B&B's recent acquisitions include Quatech (embedded wireless specialists), IMC Networks (experts in media conversion and fiber optics), and Conel (experts in cellular networking). By merging with these companies, B&B has extended the B&B product line and expanded the company's engineering expertise, while maintaining B&B's high standards for rugged reliability in data communications products and solutions.

Tips and Tricks: Six Overlooked Places to Use Industrial Wireless

How Wi-Fi industrial wireless communications can save time, trouble, and money

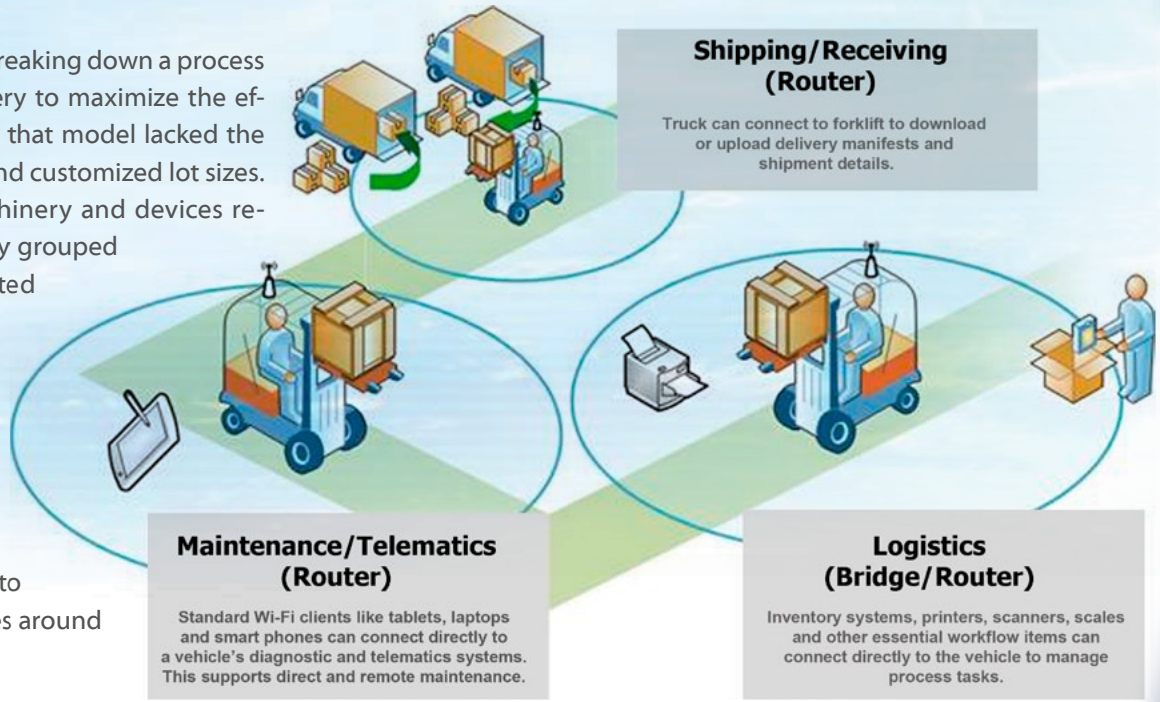
Technological advances like multiple-in-multiple-out (MIMO) transmitting and receiving are making Wi-Fi increasingly useful in industrial applications. Bandwidth and reliability have increased dramatically, and implementation costs have dropped. It's worth rethinking some of the ways in which industrial data communications have been made in the past and considering where Wi-Fi can fit into the mix. Here are six overlooked locations to consider industrial wireless communications.

1. Flexible work cells

Industrial assembly was traditionally done by breaking down a process into individual steps and positioning machinery to maximize the efficiency and throughput of each machine. But that model lacked the flexibility needed for the production of small and customized lot sizes. The solution is the work cell, where the machinery and devices required for a specific project can be temporarily grouped together, and released for other uses as dictated by circumstances. But that means recabling the work cells every time there's a change. Wi-Fi makes it easier, and cheaper, to set up and rearrange work cells.

2. Mobile connections

In a shipping and receiving application, a Wi-Fi access point enables mobile equipment to stay connected to the network, even as it moves around a plant. Cable connections don't allow for much mobility. In applications like shipping and receiving, where the value of mobile machinery like forklifts is greatly enhanced if those devices have network connections, an industrial-grade Wi-Fi wireless access point (such as the APXG-Q5420 from B&B Electronics) can keep mobile equipment connected to the network even as it moves around a plant. A truck could connect to a forklift to download or upload delivery manifests and shipment details. Inventory systems, printers, scales, and other tools can communicate directly with a vehicle to expedite workflow. Wi-Fi clients like laptops, tablets, or



smartphones can connect directly to the vehicle. Even vehicle maintenance is simplified, as onboard diagnostics and telematics can be monitored directly or from a remote location.

3. Network-enabling legacy devices

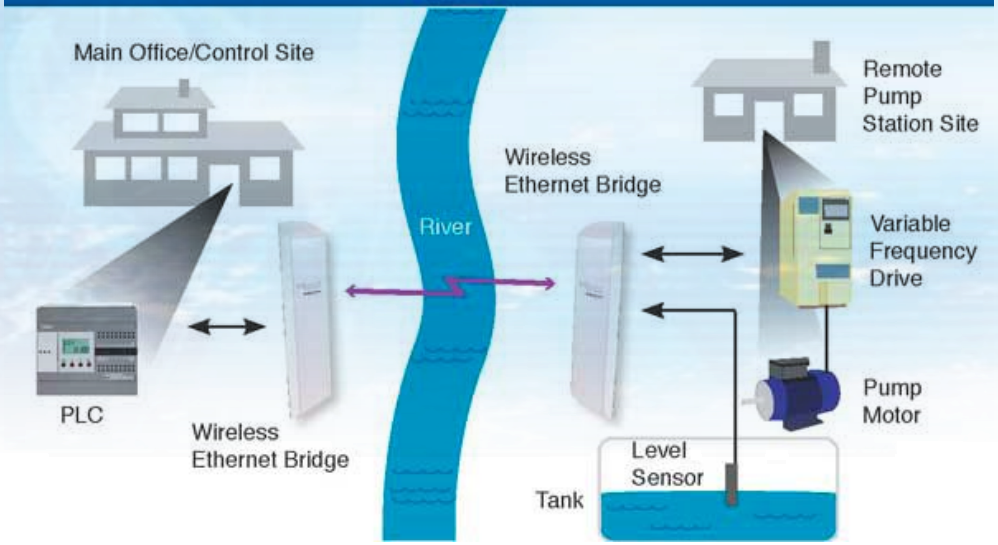
The enormous installed base of devices using serial communications isn't going anywhere any time soon. But as newer protocols like Ethernet and Wi-Fi have appeared, it is becoming harder to find laptops or computers equipped with serial ports.

One solution is to equip serial devices with wireless Ethernet serial servers. Wireless serial server technology can turn a serial device into one more node on the network and give it communications capabilities that it was never designed to possess. A serial device could also be equipped with an embedded Wi-Fi access point module (like the APMG-Q551 from B&B Electronics), which creates a self-sustaining wireless hotspot much like the one at the corner coffee shop. Handheld Wi-Fi clients can then connect to it using Android, Apple iOS, or Microsoft Windows operating systems.

4. Cable vulnerability

Although network cables are commonly run under floors, or through walls or drop ceilings, some portion of the cable must eventually be exposed as it makes the final run to an attached device. That's not a big issue in an office environment, but in industrial applications, that final run leaves a cable vulnerable to serious damage. Cables may be crushed by moving machinery, stepped on, pulled, bent, or soaked in damaging fluids like solvents. And when cables fail, installing new cable is often cheaper and easier than tracking down the fault point in the existing installation. If this happens often enough, it will ultimately create a confusing rat's nest of old and new wiring.

Remote Pump Station Application



The problem is magnified in temporary installations at remote locations. Imagine setting up a large generator system for a remote construction site or to provide temporary power after a natural disaster. You'd need to tie together everything from supervisory control and data acquisition (SCADA) to Modbus network communications, and you'd be working in a slightly disorganized environment full of moving vehicles and workers. Murphy's Law tells us what would happen to any exposed cable. Trenching your cable would help, but it would add time and expense to the project. And the final run would still be highly vulnerable. It would be easier to do the job with Wi-Fi.

5. Hard-to-wire locations

Sometimes you just can't wire a widget. The expenses involved in running cable over a river or highway, for example, can be prohibitive. Even an indoor installation

can be problematic, depending on where a device needs to be placed. And moving data any significant distance over cable will call for expensive fiber optic cables, receivers, and transceivers. Fiber optic cable provides for enormous bandwidth and, as demonstrated by the telcos, it will carry data across entire continents. But how many applications would actually require that much range or bandwidth? For far less money you can install off-the-shelf Wi-Fi bridges (such as the GhostBridge from B&B Electronics), which can create connections with speeds of up to 150 Mbps at distances of up to 15 km, depending upon local conditions.

6. Hazardous locations

In 1989 a solar flare created a magnetic storm that knocked out the power grid for all of Quebec, Canada, by inducing unexpected current on the power lines. Industrial motors and other high-power devices create magnetic fields that will affect nearby copper cabling in much the same way, though on a smaller scale. With luck, the only result will be data transmission errors and blue screens. But more serious events will damage expensive equipment.

And the greater the distance between connected devices, the more likely it becomes that communicating devices will be getting their power from different building ground references. When they do, copper cable can create a ground loop path. Again, you'll be able to count yourself lucky if the only result is a blue screen.

These problems can't be addressed with ordinary surge suppression, which only tries to limit spikes between the signal and ground line. (When the ground line rises, as it does in ground loop situations, surge suppression won't stop it.) You could install isolators, which allow the lines to float while keeping the local side at the proper ground and signal level. And you could invest in fiber optics, which are natively immune to electromagnetic interference (EMI), spikes surges, and ground loops.

But if you'd prefer to save yourself some money and trouble, you could just use Wi-Fi.

Mike Fahrion, the director of product management at B&B Electronics, is an expert in data communications with 20 years of design and application experience. He oversees the development of the company's rugged M2M connectivity solutions for wireless and wired networks based on serial, Ethernet, wireless, and USB communication technologies. Fahrion is a speaker and author who writes a self-described politically incorrect newsletter, "eConnections," with more than 50,000 monthly subscribers.
www.bb-elec.com

Edited by Mark T. Hoske, content manager, Control Engineering, CFE Media, mhoske@cfemedia.com.

Industrial Ethernet Signal Clarity

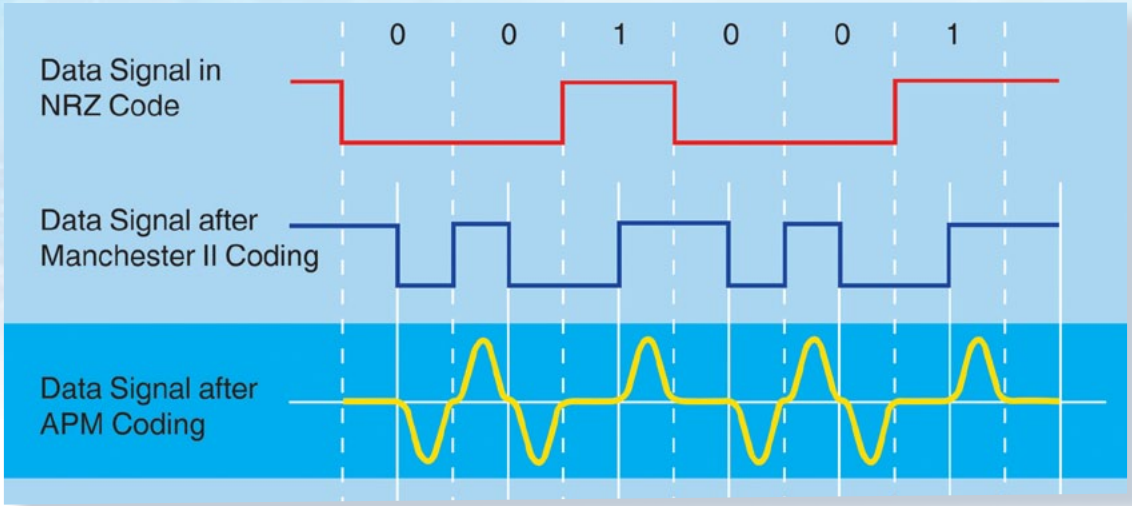
Best practices and latest technologies help ensure that the information received over industrial Ethernet networks represents the desired measurement or instructions. These include proper grounding, cable routing, proper shielding, and cable length.

Ethernet protocols securely transmit data from source to sink. "Securely" in this context means that data sent by A and received by B is either:

- Identified as uncorrupted
- Clearly identified as corrupted such that repeat mechanisms take over, attempting to resend the data and get an uncorrupt copy to B.

It should be understood that Ethernet protocol designers tried to protect that data as much as possible. The Ethernet frame (level 2 of the OSI 7-layer model) uses a 32-bit cycle redundancy check (CRC) that is so hard to trick that the reception of unidentified but still corrupt data is so unlikely that it can be ignored. As a consequence, it is up to the installer and user to not undo these efforts through poor installation. In situations where plant noise can interfere with the data on the wire, several things can happen.

- If the occurrence of the interference is infrequent, the data will eventually reach B undisturbed. Unfortunately, the requirement to repeat the transmission delays the arrival of data.
- In another situation, A may never be able to successfully transmit the data to B before it gets a new update. When that happens, the data arriving at B is "jumping" more than it would under better circumstances, another possible consequence of delayed reception.
- The third and the worst-case scenario is that A simply cannot transmit any data to B. Still, users of well-designed communication systems can be quite confident that any data they are getting is good. In other words, the "network signal clarity" is a given.



Once one identifies bad installation practices as the main reason for data arriving at B late or not at all, it is helpful to know the elements of good installation practices.

Proper grounding

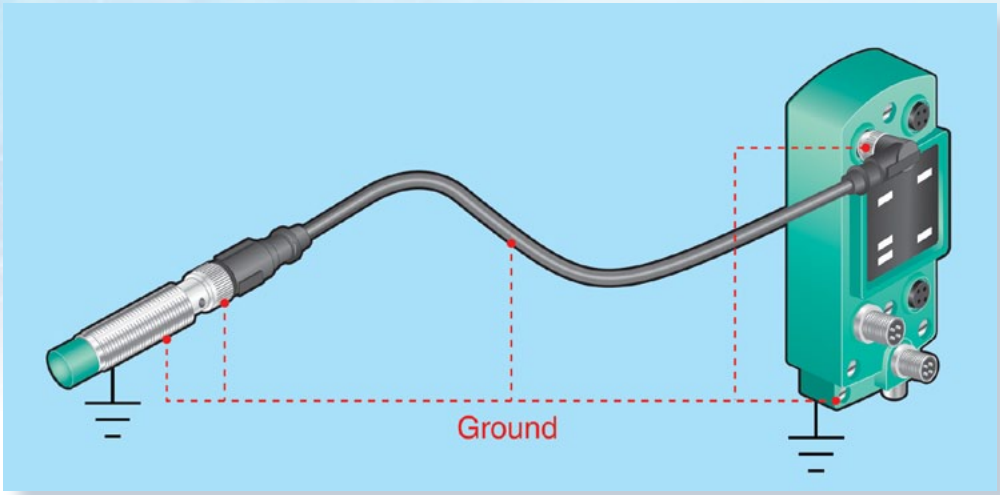
Devices must be grounded properly. Many hardware manufacturers spend a considerable amount of time and effort ensuring that grounding lugs and grounding terminals are built into their products. Use them. And don't try to save a few pennies using a 24-gauge wire to ground the device. Since we are talking about networks, it is quite likely that the PLC is located

relatively far from the data source. If so, it is a good idea to make sure that the entire machine is grounded to the same potential. When that is not the case, a shielded network cable may be selected to bring those machine sections to the same electrical potential, but this type of cable was not intended to do the job of a heavy solid or braided wire cable that was designed to provide a low-resistance path from a device to an earth ground.

Instead, disjointed machine sections must be connected by heavy-duty grounding straps and connected to a solid earth ground connection. When a shielded cable is brought into a metal junction box, immediately split the shield off and connect it to the box at the location where the cable enters. This method ensures that noise riding on the shield will not be brought near the equipment in the junction box but will be diverted to ground right away.

Proper cable routing

A typical machine has many different electrical consumers, and some of those, for instance motors and drives, tend to generate higher levels of electromagnetic (EMC) noise. One of the most common mistakes is to route the motor cables in close proximity to network cables. Don't do it. The rule of thumb is to separate power and controls by 4 in. to 20 in., and this is one of those cases where more really is better.



Proper hardware selection

Step one of a successful network implementation is to select hardware that is well designed. This includes the network infrastructure as well as all other components. Getting back to the drives example, an installation that uses a drive with less electromagnetic emissions will inherently be less problematic than one using a drive that significantly pollutes the spectrum.

Shielded cable? Don't be misled

Many engineers want to go the extra mile and specify shielded cordsets. The only problem is that most shielded cordsets are useless! For a shielded cordset to work, the shield must somehow be connected to the machine ground. Unfortunately, in typical shielded cordsets, the shield simply extends along the length of the cable but does not connect to the connector or coupling nuts. The only advantage of this kind of cordset is that it is mechanically stronger. Any external noise "riding along the shield" will not be diverted to ground and away from the signal wires. Instead, the noise signal will have the opportunity to jump right on the signal leads at the connector.

Keep cables short

Any cable can act like an antenna. Keep it short. Also, do not help noise get onto your signals by looping long sections of unnecessary cable along the machine. This turns the cable into a transformer, making it easier for unwanted signals to couple into the line.

Free help

When the signal cable is placed inside of an open wire duct, push it into the corner. That way, both the bottom and side of the duct help shield the cable from external noise.

Ferrites

In situations where the noise comes in the form of high-energy pulses, ferrites are a good idea. For best performance, the network cable should be looped around the ferrite several times. Be sure to do this at each end of the cable also. Better yet, ferrites should be used on those cables that create the noise in the first place. Your PC monitor's power cord has such a ferrite built in for a good reason.

When not to shield

While Ethernet cable should definitively be shielded and grounded properly, this is not necessarily the case for the AS-Interface network working in conjunction with Ethernet. This network is designed to be used with unshielded cable and, very importantly, neither of the two leads should be grounded. While shielding is possible and possibly useful in the worst electromagnetically polluted environments, using shielded cable will result in a 30% reduction of possible segment length.

Helge Hornis, PhD, manager, Intelligent Systems Group, Pepperl+Fuchs. www.pepperl-fuchs.us
Edited by Mark T. Hoske, content manager, Control Engineering, CFE Media, mhoske@cfemedia.com. http://controleng.com/networks

Automation Networks:

Physical Layer Consolidation; Ethernet Protocol Discord

While the world of "automation networks" is getting simpler, this statement needs further explanation and amendment. It is true that Ethernet gets most of the attention and most professionals agree that it will be the technology of the future, but that does not mean we will have to worry about only one Ethernet-based networking technology.

As soon as Ethernet gained a level of acceptance, the battle shifted. Major PLC manufacturers each developed their own flavor of an "open" Ethernet protocol, effectively agreeing on a cable but not much more. Profinet does not talk to EtherNet/IP, and neither talks to EtherCAT. Unfortunately for the user, not all that much has been gained, but there has been some forward progress.

- Since PCs come with Ethernet ports, configuring PLCs that use these Ethernet-based networks has gotten easier. It is not necessary to have a dedicated hardware adapter converting RS-232 to the network of choice.
- Most Ethernet devices support some sort of setup and/or diagnostics via a web page. This is nice, as web browsers can be turned into visualization and diagnostics tools.
- Chances are (but this is not guaranteed) that the physical network infrastructure (cable, switches, and connectors) can be used for any flavor of Ethernet solution. This is helpful for machine builders who find themselves developing for multiple PLCs on the market.
- The installation rules for Ethernet-based solutions are independent of the protocol. This helps because good installation practices for Profinet will also be good installation practices for EtherNet/IP.
- Ethernet protocols securely transmit data from source to sink.

This advice also applies to AS-Interface, the widely used low-level I/O network "under" Ethernet. More specifically, assuming a bit error rate of 10-4 (that is, on average 1 in 10,000 data bits is corrupted by an external influence), an AS-Interface system running 24 hours a day, 365 days a year will have one undetected error in roughly 2,300 years, clearly a level that can be neglected.

Optimizing Ethernet for Industrial Implementation

When selecting and installing industrial Ethernet, consider this advice from IMS Research

John Morse, senior market analyst, automation and control, IMS Research, answered questions regarding industrial Ethernet implementation. IMSResearch.com

What are key considerations when optimizing an industrial Ethernet implementation?

Availability of skill set—If a user is switching from a fieldbus to Ethernet, an understanding of the modus operandi of Ethernet is essential, particularly regarding the addressing mechanism. Some fieldbuses are very easy to implement, and the Ethernet switch can be quite a change. Also, it is very easy to get blasé about Ethernet when it is used in a commercial environment where it has become plug-and-play for many users. There are more considerations when it is used in industrial automation.

Infrastructure—Is the cabling up to the job? This is particularly important if gigabit Ethernet is being employed.

Is nondeterminism an issue?

This used to be a big challenge but is less so in recent times due to the common use of switches to isolate sensitive parts of the network and the fact that many applications are unfazed by a small delay in node-to-node response times. Also, few networks are so busy that it's a problem.

Why use Ethernet instead of another industrial network?

Four reasons: **1)** Compatibility with the existing IT system enables seamless integration of data throughout the enterprise. **2)** Common use of infrastructure network components can ease implementation. This is more relevant to enterprises that do not need industrially hardened products. In some cases, there are cost savings to be had as the price of components goes down and as demand goes up. **3)** Speed helps. Even 10/100 Mbps Ethernet is fast! **4)** Ethernet is fashionable right now.

What Ethernet protocol do you need and why?

There are two main types of Ethernet. General protocols, such as Ethernet TCP/IP, Profinet, and EtherNet/IP, and those designed to meet high-speed, deterministic and low-jitter application, such as EtherCAT and SERCOS III [also CC-Link IE and Profinet IRT]. Around 50% of industrial applications work fine with the standard Ethernet TCP/IP.

If determinism is an issue, then an industrial variant must be considered. Reasons will include high-speed production (bottling plants are typical) and motion control applications where synchronization of motors/servos is critical. Where there are safety critical issues to consider, such as e-stops, the network must be able to react fast and reliably.

Can multiple protocols be used on the same Ethernet physical layer?

Theoretically, the answer is always yes if the protocol uses layers 1 and 2 of the OSI model. However, there are combinations that are not recommended, and it is best for users to check with the standard authority for the protocol before committing to a particular technology.

Should you use fiber or copper?

Typically, fiber optics are used for backbone infrastructure with copper drop-downs. Naturally, fiber optic cable is immune to EMC but more expensive and harder to terminate reliably. Few companies appear to be using fiber optic cable for other applications apart from those needing to transport data over a long distance. This is more typical in process industries where the sites are larger.

Edited by Mark T. Hoske, content manager, Control Engineering, CFE Media. mhoske@cfemedia.com.

Are There Too Many Industrial Networking Protocols?

Simplify your industrial networking with Ethernet-based communications

Bernie Anger (GE) and Carl Henning (PINA) discuss networking with Peter Welander.

The idea that Ethernet deployments are growing in industrial networks isn't exactly news, but one group is saying that its industrial Ethernet protocol is ready to replace many other networking approaches, and perhaps all of them. Profinet International North America (PINA) recently sponsored a conference in cooperation with Siemens Industry and General Electric Intelligent Platforms to advance the notion that Ethernet in general, and Profinet specifically, can replace most if not all other shop-floor networking protocols. Siemens and GE both say they are doing that very thing today.

The contention is that companies can realize substantial savings and simplify maintenance if they make the transition to Profinet at all levels, from individual field devices and sensors, right up to the enterprise. There are some qualifications of course. At present, this sort of approach is much more suited to discrete manufacturing than a process plant. An auto assembly context is more practical than a refinery for a number of reasons, both hardware- and software-related

The Internet is quickly becoming the standard for modern networking. And its capabilities are being rapidly enhanced by the cloud. As Bernie Anger, general manager of control and communication systems for GE Intelligent Platforms, pointed out, Skype has proven that it is possible to have secure point-to-point communication via the cloud and without any infrastructure. His suggestion that by 2020 there will be 75 billion devices connected to the Internet means that some of those will undoubtedly be in your plant.

The video is a conversation with Bernie Anger and Carl Henning, deputy director, PINA, about some of the practical implications of this idea. Whether you use Profinet or some other flavor of industrial Ethernet protocol, the message is clear. The basic nature of networking is changing, and it is a major improvement.

Peter Welander, pwelander@cfemedia.com

www.allthingsprofinet.com
www.ge-ip.com
www.sea.siemens.com

White Paper

Ten Things to Remember About Industrial Ethernet

I. Security issues can bring down your network

A Wi-Fi-enabled computer can connect to multiple networks at the same time. Your employees can give a hacker a pathway into your internal network simply by powering up a laptop. Imagine the mess an eco-terrorist could make if he didn't like the look of your smokestack. Even your well-intentioned employees can bring a network down, simply by blundering around in areas they shouldn't. Don't take chances with network security.

Most wireless systems employ industry-standard wired equivalent privacy (WEP). A hacker can get around it within a few hours. Look into more powerful standards like Extensible Authentication Protocol and Tunneled Extensible Authentication Protocol.

Never assume that your industrial Ethernet products have built-in security features. At the very least, you should use inspection-type firewalls (such as packet filters) to control any access that is based on the IP source address, destination address, and port number.

Don't just talk about changing your passwords on a regular basis. Do it. And don't make them easy to guess.

Consumer plug and play devices can flood your network with traffic in a "broadcast storm" as they try to self-configure or advertise their presence to every other node on the network. Faulty devices can vomit zillions of "runts," or abnormally short Ethernet frames. Using switches instead of hubs will take care of those problems.

Duplicate IP addresses can deactivate devices that otherwise appear to be perfectly functional.

II. Failing to document your installation will cause trouble in the future

Document your installation. When devices need to be replaced, make it happen quickly. Things you need to know and document for every device:

- Replacement part numbers
- IP addresses
- Subnet masks
- Gateway addresses
- Menu settings of devices like serial servers, data collectors, routers and configurable switches
- Functions like DHCP enabled/disabled, static vs. dynamic IP addresses

III. It pays off to map out a plan for assigning and re-assigning IP addresses

There is no standardized way to set IP addresses in automation, but don't just wing it. Have a plan in place.

- Whether you use DHCP or set IP addresses manually, IP assignments should be semi-permanent.
- Understand the client software IP address requirements as they relate to the hardware devices in a client/server application. Note that in a PLC-style control system, the PLC is a client and all of the I/O devices are servers, which is the exact opposite of the arrangement in an office LAN.
- Documentation should clearly indicate the mechanism by which the IP address of a replacement device should be set.
- You should cooperate with your IT department in choosing IP addresses so that conflicts do not arise in the future.

Figure 1

IV. Industrial-grade installations are cheaper in the long run

You get what you pay for in this world. If you've duct-taped a $20 office store Ethernet hub into your panel and plugged the DC adapter into an outlet strip, you're going to pay for it when your network goes down.

Ruggedize your communications with industrial-grade hardware (see Fig. 1) and let the doom-beasties go eat somebody else.

- Use DIN rail mounting, not duct tape
- Use low-voltage AC/DC connections instead of AC
- Look for industrial-grade temperature specs and industrial grade physical construction
- Deploy fault interrupt relays
- Look for advanced functions like port management and features that facilitate trouble-shooting, like port mirroring
- Back yourself up with live technical support and sound advice from real people

V. It is useful to segment your network

A business LAN and a control network have very different roles, and so it only makes sense to increase your system-wide level of security by limiting their interaction. Separate them with a firewall

or, at minimum, a bridge or router. Additionally, your industrial Ethernet network can be looked at as two separate entities: a control-level industrial network and an I/O-level industrial network. These can be protected with additional security boundaries. Ideally, each manufacturing cell would be isolated and protected.

VI. You can network-enable legacy devices

It is far too soon to consider abandoning your legacy serial equipment. In fact, the serial communications protocol remains so useful that the number of deployed serial devices is expected to keep growing. Connect your legacy serial devices to Ethernet with serial servers (see Fig. 2) and let them keep doing their jobs. B&B offers a more detailed application guide for this subject. You can get it free at www.bb-elec.com/serialserver

VII. Laying cable correctly is worth the trouble

Install shielded twisted pair (STP) wire anywhere physical protection or local codes require the use of conduit. Attach the STP shield to ground at only one end of the cable. (Connecting at both ends creates ground loops.) If you are required to terminate the shield at both ends, wire a metal oxide varistor (MOV) shunt in parallel with a one megohm resistor and 0.01- to 0.1-mF capacitor. Check cables with a cable tester, not just with an ohmmeter. A tester quickly identifies continuity problems such as shorts, open wires, reversed pairs, crossed pairs and shield integrity. Metal cable trays should be conductive from end to end. Avoid proximity to power lines and sources of electrical transients. High-voltage lines should intersect the cable at a 90° angle. Your conduit should maintain at least a 10 cm distance from 120 VAC, 15 cm from 220 VAC, and 20 cm from 440 VAC. If you don't use conduit, double those distances.

Figure 2

VIII. Industrial-grade connectors prevent problems

RJ-45 "telephone connectors" don't stand up to industrial applications. Their contacts have a small surface area and vibration can wear away the thin layer of gold that covers the underlying nickel, making the connection susceptible to corrosion and oxidation. A simple yank on the cable can also damage a connection. They're not a great choice for your robotic welder when downtime costs $15,000 per minute. Fortunately there are alternatives. IP65 or IP67 cables keep out liquids, maximize the contact surface area, and improve the sturdiness of the design. All of them facilitate feeding Ethernet cables through panels.

IX. It is important to understand your industrial automation protocols and compatibility concerns before you issue purchase orders

There are numerous open standards for representing industrial data on Ethernet, like Modbus/TCP, Ethernet/IP, Foundation Fieldbus and Profinet. And some vendors use proprietary standards. The fieldbus wars are not over yet. But it's possible to define structures that make them interoperable. Don't commit to anything until you've done your homework.

X. Mixing Wi-Fi, Hi-Fi and process control requires advanced planning

Position your Wi-Fi antennas so that they cover all of the required space. Walk around with a signal meter and make sure that they do. At the same time, do your best to restrict transmission to desired areas only. You can use directional antennas to restrict radiation in undesirable directions. It's one thing to do data acquisition with wireless, but quite another to run I/O from your PLC. Keep the control stuff on physical cables wherever possible.

Contact Information

URL: www.bb-elec.com

To place an order: orders@bb-elec.com

For tech support: support@bb-elec.com

International Office:
707 Dayton Road
PO Box 1040 Ottawa, IL 61350 USA
Phone: 815-433-5100; **Fax:** 815-433-5104

European Office:
Westlink Commercial Park
Oranmore Co. Galway, Ireland
Phone: +353 91 792444: **Fax:** +353 91 792445