Planning Pays Off **WHEN IMPLEMENTING ETHERNET**

Experts offer tips for building and implementing an effective industrial Ethernet network.

By Terry Costlow, Contributing Editor

When Danny Vujovic co-founded Tekkra Systems Inc. in 2005, selecting a network for the packaging equipment was a straightforward decision. Ethernet was the only option that made sense. Tekkra uses EtherNet/IP, an ODVA protocol developed by Rockwell Automation Inc., in its shrink bundling equipment and end-of-line packaging systems. After the basic benefit of Ethernet, increased connectivity with business-level systems, remote diagnostics is one of the biggest benefits for the Romeoville, Ill.-based supplier.

"EtherNet/IP's remote diagnostic capabilities allow us to provide 24/7 customer support," Vujovic says of the protocol from ODVA (formerly known as the Open DeviceNet Vendors Association). Networking the controllers, drives and human-machine interface (HMI) lets customers monitor machines and control the manufacturing process by communicating with other machines on the line, he explains.

That's an increasingly common occurrence, but networking specialists all warn companies such as Tekkra and its customers that only the decision is easy. Installing Ethernet on the factory floor is not a simple plug-and-play process. "The biggest difference is the planning involved with an Ethernet network; you have to have the appropriate topology with switch placement for devices in the right places. Generally, there is more planning on the front end," says Chris Vitale, senior product manager with automation-components supplier Turck Inc.'s network division in Plymouth, Minn.

But that planning involves many different facets. When teams build networks, they have to examine many facets such as redundancy and whether the cost of managed switches has a payoff. They also have to pay far more attention to security issues now that factories are accessible from the outside world.

OUTSIDE LOOKING IN

Though improved communications between the front office and the plant floor is a key driver behind the move to Ethernet, reduced downtime is generally a bigger benefit for

"The biggest difference is the planning involved with an Ethernet network; you have to have the appropriate topology with switch placement for devices in the right places."

those who work on the factory floor. Better diagnostics tools, including remote access, make it much easier to find problems and get downed networks up and running.

When network problems arise, the openness of Ethernet and transmission control protocol/Internet protocol (TCP/IP) pays off big time. Technicians located anywhere can easily tap into systems to find out what's wrong and initiate fixes. It's no longer a problem when the company's expert is at a facility halfway around the globe.

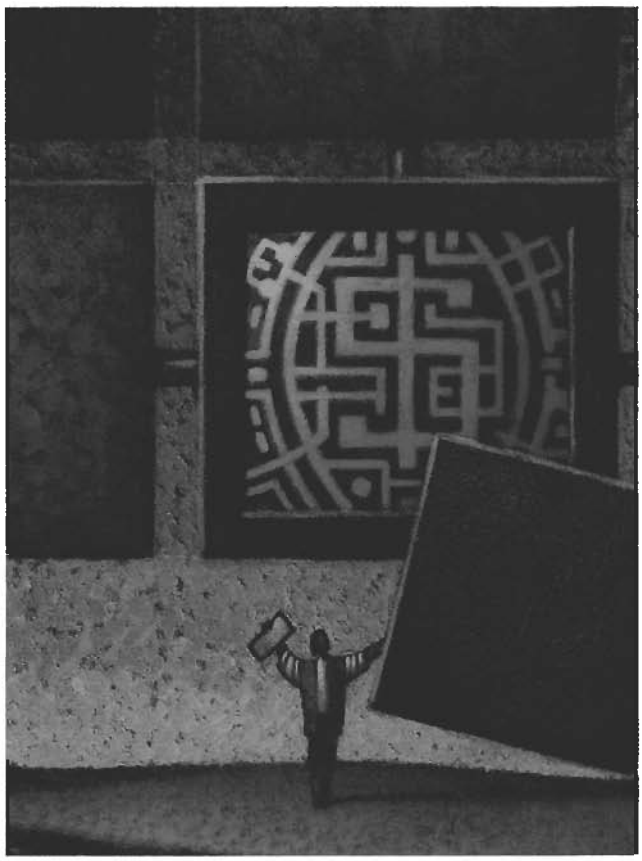
"By routing the devices through individual IP addresses, a user can access diagnostic data all the way down to a field device from anywhere in the world," Vitale says. Those users can often see as much information, often including historical data that preceded a failure, as an operator who's on site.

In this area, the capabilities developed for information technology (IT) can be adapted without a lot of changes. Many component providers feel that the issues involved with remote access are very straightforward. "The main issue is gaining a safe entrance to that remote network, and having a fast enough connection," says Ken Austin, Ethernet product marketing lead specialist for Phoenix Contact, an automation-components company with U.S. headquarters in Harrisburg, Pa.

A key aspect of remote access is to let the technicians who work on the machines every day access them when they're not in the facility. But a growing number of equipment manufacturers are using these capabilities to monitor their machines to

make sure they continue to run at near-optimal levels. That type of accessibility lets them alert owners when they need to take care of their equipment.

"Remote access can let the equipment manufacturer access machines at the facility to do diagnostics, doing things like monitoring operating time and alerting maintenance personnel when it's time for preventive maintenance," says Mike Hannah, NetLinx product business manager for Rockwell Automation, in Mayfield Heights, Ohio. However, he notes that users will always require some sort of restrictions so outsiders don't have too much insight into plant operations.



REMOTE VIDEO

Remote access is providing insight of another sort to companies that want to give operators a broader view of what's going on in their facilities. "We're seeing more interest in other types of activity, things like sending video over networks," says Paul Wacker, product manager for Industrial Communications at vendor Advantech Corp., in Cincinnati. "It's mostly supervisory in large plants where equipment runs unattended. Someone might be able to see a jam before it gets so bad they need to dispatch maintenance personnel." He notes that video can also be used in conjunction with light curtains. When the curtain is broken, video cameras can provide information to remote managers.

The ability to run remote diagnostics carries over to the human-machine interface. The HMI lets remote operators pull

WIRELESS MOVES FORWARD

The freedom that comes when cabling disappears has captured the imagination of industrial engineers. Over the past couple of years, market growth for wireless networks has soared, as untethered nodes pop up in all sorts of new applications.

Wireless technologies were viewed warily early in the decade, but that's waned as initial applications proved that the noisy electrical environment didn't cause signal loss. After that roadblock was removed, wireless networks have been gaining momentum like the proverbial snowball rolling down a hill.

Some companies say that even in this down economy, wireless is growing at rates of 50 percent or more. Wireless networks give designers the freedom to install nodes and move them around without figuring out cable routing schemes.

"We are seeing a lot of Wi-Fi (for Wireless Fidelity) used in plant floors, for example, on autonomous guided vehicles that move about a factory and can't have wires attached to them, but still need to be able to communicate to a central control location," says Ariana Drivdahl, product marketing manager for Industrial Wireless at components vendor Moxa Americas Inc., of Brea, Calif.

The networks are moving well beyond vehicles. "We're starting to see more wireless in applications where wires can get cut or broken and where wired networks can't meet temperature requirements," says Brad Hegrat, principal consultant for network and security at vendor Rockwell Automation Inc., in Milwaukee.

Wi-Fi is a dominant architecture for this expansion. It leverages the advances made in commercial Ethernet, so industrial users are assured that costs will drop and technology will advance.

Recent technical changes underscore the rapid advances. Earlier this year, the Institute for Electrical and Electronics Engineers approved IEEE 802.11n-2009, which increases the maximum data rate from 54 megabits (Mbits)/second to 600 Mbits/second. This may translate into a user throughput of 110 Mbits/second.

Perhaps more important for the many industrial applications in which speed isn't critical is Wi-Fi's evolution in data security. Wireless networks offer more potential security openings than wired schemes, so industrial users are excited about recent improvements here.

Wi-Fi Protected Access 2 (WPA2) provides an upgrade over basic WPA encryption, making it much more difficult for outsiders to establish a wireless path into the plant floor network. Stronger encryption techniques will make it extremely difficult for hackers and others to break in. "WPA2 sets truly difficult barriers for people who worry about authenticity," says Eddie Lee, senior marketing manager for Moxa.

Moving to the latest data protection technologies will help plant managers stay one step ahead of outsiders who have malicious intent. "When you deploy wireless, you should constantly change the keys over a set time interval, requiring devices to reauthenticate themselves," Hegrat says.

As with conventional networks, users have to look beyond the basic technologies to address all aspects of security. Employee training is a central aspect of security.

"One of things you can do that helps a lot is to use the latest encryption standards," says Paul Wacker, product manager for Industrial Communications at vendor Advantech Corp., Cincinnati. "You also have to remember the human side, even with wired networks, that's a big part of security."

Disgruntled employees are among the most likely culprits when humans hijack networks. Making sure that they can't do damage is a key element in a security plan. One basic technique is to avoid universal passwords that allow operators into areas where they don't normally work. They lack accountability and can be used even after an employee is terminated.

"When you deploy wireless, you should constantly change the keys over a set time interval, requiring devices to reauthenticate themselves."

Though Wi-Fi is becoming the de facto standard for wireless, it's nowhere near the only approach. Alternative standards and proprietary schemes are both succeeding during this early stage of the wireless movement.

For example, automation-components supplier Banner Engineering Corp., of Minneapolis, uses a proprietary 900 megahertz (MHz) network, saying that it has twice the distance of standards such as Wi-Fi, ZigBee or Bluetooth. It's used for applications that just send a few bytes of information, then go into sleep modes.

"We install small, wireless nodes that send only a few words of data to tell the state of an input," says Bob Gardner, senior product manager for wireless at Banner. In some ways, this wireless net works like a fieldbus, gathering data that is then sent up to an Ethernet backbone. "There's one place in the plant where Ethernet pulls that data in," Gardner says.

"By routing the devices through individual IP addresses, a user can access diagnostic data all the way down to a field device from anywhere in the world."

up data to see where networking problems occurred. For this type of diagnostics, the use of managed switches is a critical requirement. "There's a lot of information in managed switches that can be pulled up in the HMI," Wacker says. "You can see if there's a fault in a switch or whether there are issues with power supplies, to name a couple."

Many companies believe that one of the best ways to improve diagnostic capabilities is to employ managed switches. They cost more, but features such as Simple Network Management Protocol (SNMP) bring substantial benefits.

"Unmanaged switches are generally one third the cost of managed switches, but the reason to pay is that with SNMP, you have the ability to narrow down and find problems like traffic jams, seeing exactly where they are. If you save money by going to unmanaged switches, you'll just see that something is bogging down the network. Then you have to find out where it is," says Eddie Lee, senior marketing manager for components supplier Moxa Americas Inc., of Brea, Calif.

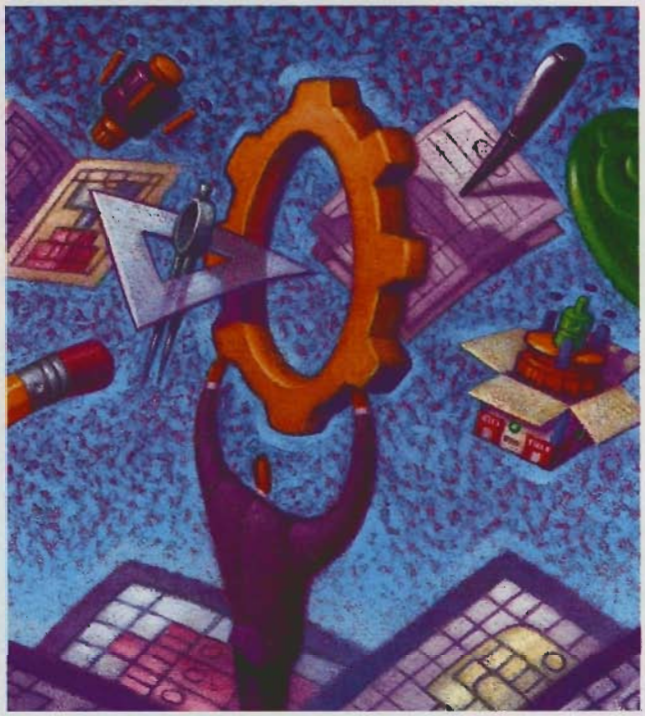
In mission-critical applications, many network managers are doubling up on key components. These fail-safe systems ensure that critical network components will be available even while faulty components are being replaced. "Redundant power supplies are particularly important for infrastructure products. Media redundancy can also be important if somebody disconnects or breaks a cable," Wacker says. However, he notes that developers can't use redundant systems unless they use intelligent switches. "Duplication is really important, but to do it, you need managed switches," he says.

The nuances of managing redundant components doesn't stop at employing managed switches. Constant communications over two separate cables raises the potential for confusion, particularly if duplicate data packets arrive at slightly different times. Special programs and protocols are required to switch from one network link to another.

"The implementation of redundant paths between network devices, along with a mechanism such as Rapid Spanning Tree Protocol that ensures only one active path between two network devices, provides the ability to create a self-healing network from initial network commissioning," says Phoenix Contact's Austin. The Rapid Spanning Tree Protocol helps networks recover connectivity after failures.

KEEP 'EM OUT

Security has become a critical issue for engineers who are building industrial networks. Using Ethernet and TCP/IP opens doors for the same sort of attacks that plague home and office users. Industrial networks are being hit by more and more assaults. "The number and the sophistication of attacks are increasing. It's important for the control side to ensure they are taking responsibility in keeping their control networks secure and protected, independent of what IT may or may not be doing," says Dan Schaffer, Automation Networking and Security marketing specialist for Phoenix Contact.



As these attacks rise, more companies are realizing that these networks are no longer isolated and therefore unlikely to have security breaches. But doing something about that remains a difficult task. There hasn't been a need for security technologies that protect industrial assets, so getting financial managers to allocate funds can be difficult. But many proponents say that spending on network security is just as important as buying sprinkler systems that can protect against fires. In either case, safeguards cost money that's considered well spent when it's needed.

"In tough economic times, you have to take a long-term, big picture view," Schaffer says. "The cost in real dollars adds up in a hurry when you fall victim to either an intentional attack or just suffer downtime due to an internal problem that bleeds over from the corporate (aka information technology or IT) side of a network."

Installing firewalls is a critical first step. Limiting access is also one of the key differences between the plant floor and the front office. Many networking specialists advise clients to regulate connectivity in factories. "In industrial control, you use the principle of least access, only allowing an asset or user access to do what they need. If I don't have reason to access a PLC (programmable logic controller), I shouldn't have access to it. That's a lot different than in the office, where every node communicates with every other node," says Brad Hegrat, principal consultant for network and security at Rockwell Automation, in Milwaukee.

Dedicating access so only certain nodes can talk to each other will go a long way in providing security. But when viruses or hackers get past firewalls and bypass other safeguards, network managers have to ensure that they're stopped before serious damage is done.

"The concept of 'defense in depth' is also important to protect control networks," Schaffer says. "In short, it is the practice of layering security, so even if an attack is successful in, say, compromising the router/firewall connecting a site to the Internet, the attacker is thwarted from gaining access or causing damage to other facets of the network such as PLCs and HMIs."

LINK TO THE PAST

When engineers build greenfield systems, they can install Ethernet cables everywhere. Plans for wireless networks and the expansion of wired networks make future growth easier. But for most network developers, that level of freedom isn't available. Most have to deal with legacy networks and old, difficult-to-change cabling runs are a reality in most facilities.

Ethernet provides some powerful options for those who must link Ethernet backbones to established fieldbuses. One of the foremost is that it can carry signals from many different systems, making it simpler to link older equipment to the high-speed network. "You can run a lot of protocols over the same set of wires, so Ethernet's great for backward compatibility. You can take a device that's 15 years old, plug it in and it runs," Wacker says.

Most of these legacy networks will be serial fieldbuses. Reducing the number of these networks is one of the first steps most engineers will want to take. Another is to link the remaining fieldbuses to Ethernet. "In many facilities, users will have multiple isolated serial networks. That defeats the benefit of going to Ethernet," Lee says. "When you have separate serial and Ethernet networks, using gateways to convert protocols to Ethernet is a huge step in the right direction."

"You can run a lot of protocols over the same set of wires, so Ethernet's great for backward compatibility. You can take a device that's 15 years old, plug it in and it runs."

Installing these gateways is a fairly straightforward task. However, that doesn't mean that it can be overlooked or left until the final phase of a networking overhaul. "Dealing with closed, proprietary systems can be difficult. You need to set up gateways and write code to convert files," says Rockwell Automation's Hannah. "Setting up gateways and writing applications code to convert fieldbus data to Ethernet is not a roadblock, but it does take time and money to solve the problem."

The use of fieldbuses is declining as Ethernet takes over, but fieldbuses aren't headed for the endangered species list. Simple fieldbuses such as DeviceNet, Profibus, and AS-interface remain viable solutions for components that don't generate much data.

"Ethernet is moving down, but it will be a while before it gets to actuators and low level devices.," Hannah says. "But you probably won't ever see actuators and things like proximity switches on Ethernet; it's just not cost effective."