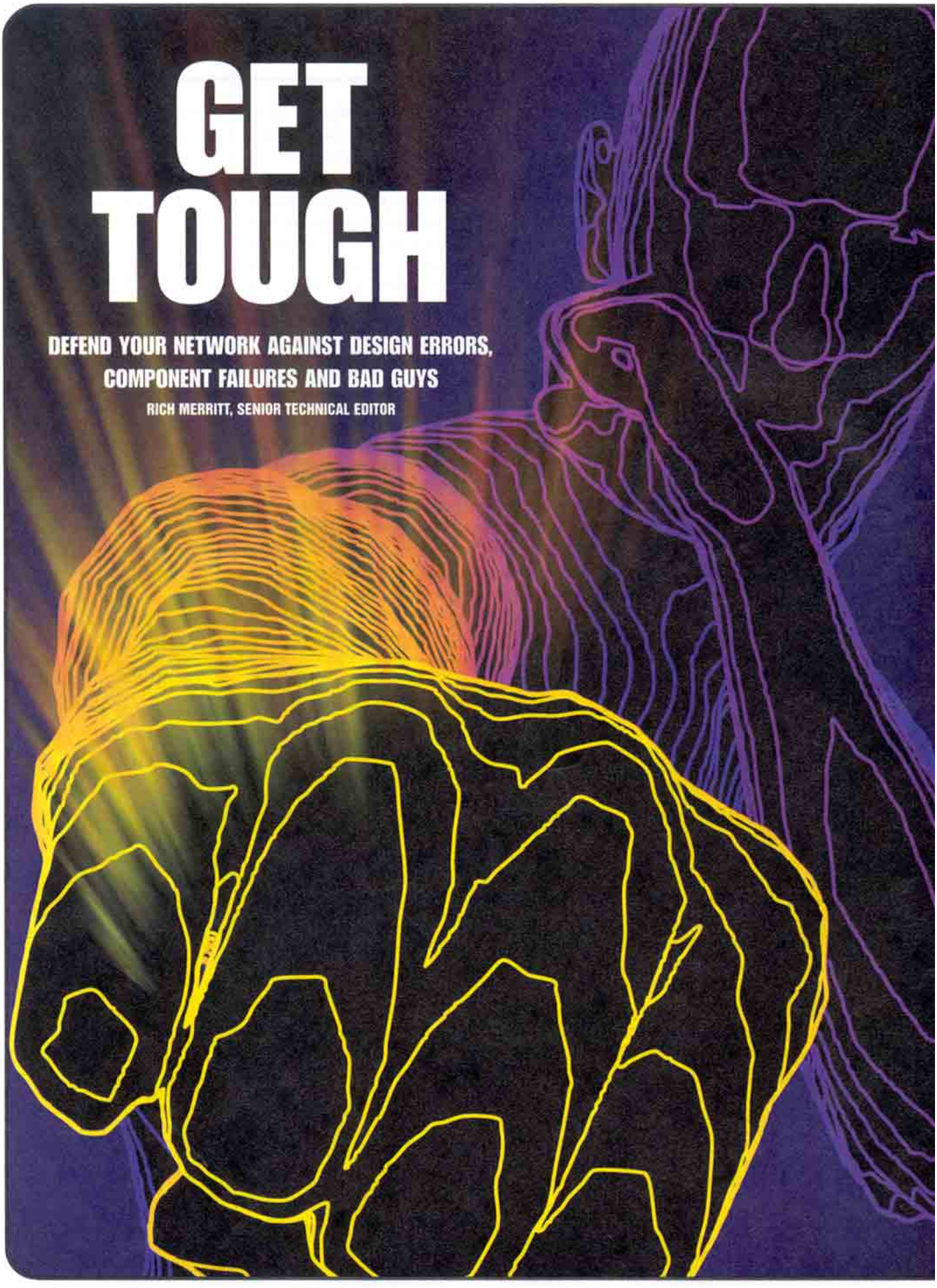
GET TOUGH

DEFEND YOUR NETWORK AGAINST DESIGN ERRORS, COMPONENT FAILURES AND BAD GUYS

RICH MERRITT, SENIOR TECHNICAL EDITOR



WHAT is your definition of a robust industrial network? How about a network that is reliable, immune to industrial noise and environmental issues, secure, and keeps working no matter what?

This article details some of the best practices that lead to that robust network. We'll ignore the controversy and competition among networks, and not suggest any one network is better than another. When properly designed and installed, all industrial networks are robust.

One lesson to take to heart is that you just can't be too careful, and you can't cheap out with an industrial network. Take installation, for example. Don't cut corners. "We may be overly conservative in our grounding methods, but I've never had a grounding issue on a network or in my instruments." says Cliff Speedy, controls engineer at C&I Engineering, Louisville, Ky. "We usually stick to isolated grounds that travel to our instrument grounding bar, which, in turn, is isolated and connects to a reliable grounding source at one point." Over-engineered, some might say, but Speedy's networks are robust. Many are not.

"Twenty-eight percent of all networks serviced by our industrial network services group have marginal or intermittent media problems due to installation issues," says Mike Bush, program manger for the Automation Control and Information Group at Rockwell Automation (www.rockwellautomation.com).

You can't overspend on your network, either—not if you want it to keep running. "In a sample of 776 ControlNet nodes checked, there were 390 connector problems and 54 cabling problems," says Bush. "Many times, it is a result of attempting to save a few cents on the cost of these critical components."

Then there is the problem of network security. Some people advise control engineers to confer with their colleagues in IT, and take advantage of their security. Scott Saunders, director of strategic marketing at Moore Industries-Intl. (www.miinet.com) scoffs at the very idea. "Little of the experience IT groups have dealing with security layers and virus protection is shared with process control network personnel," he says. "The lack of cooperation that sometimes exists between the two departments can be the worst enemy to overall network security."

That isn't always the case. "We, fortunately, have a very good relationship with our IT people, and use them extensively to support our control system," says Ed Bullerdiek, control group leader at Marathon Ashland Petroleum in Detroit. "It is working very well. Yes, there are educational issues on both sides, but they can be worked through." Bullerdiek thinks the idea that IT and controls personnel cannot work together is counterproductive. "The idea is to allow the controls engineers to focus on their specialty—making the process run better—and allow the IT support personnel focus on their specialty, which is keeping a system running," states Bullerdiek. "There is enough work to keep us all very busy."

NETWORK HARDWARE SELECTION

Setting up the physical connections is the first step in establishing a robust industrial network. In many cases, a network has to operate in unfriendly, electrically noisy and sometimes hazardous environments (Figure 1). Follow good wiring practices and use the proper hardware and you can eliminate many problems right away.

"Cables, connectors, terminations and grounding are possibly the most important issues a customer must deal with in an installation," says Gary Slivka, product manager at Rockwell Automation Industrial Network Services (www.rockwellautomation.com). "The network physical layer is the foundation of any network installation. Start with a bad foundation, and any network-connected product will struggle to communicate, resulting in an under-performing network solution."

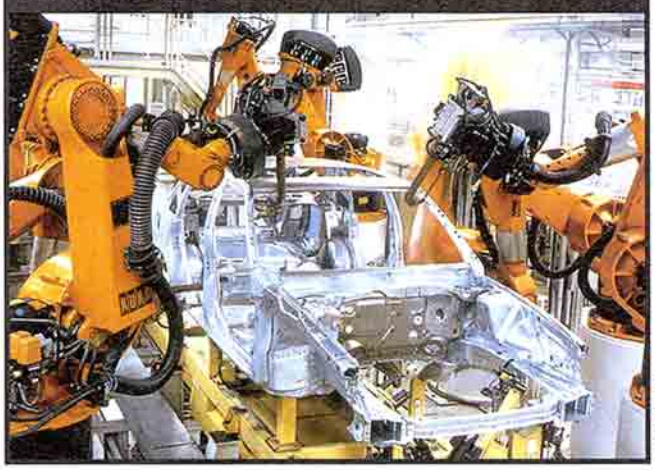
Let's start with cable. Mike Fahrion, marketing director of B&B Electronics (www.bb-elec.com), is not a system integrator, but he has advised hundreds of end users and SIs on the best ways to put in networks. He doesn't quibble: "The best is fiberoptics, and second best is shielded, properly grounded cable." Yes, indeed, but which cables? There are dozens of choices.

"There are a number of different cables for indoor and outdoor use designed specifically for industrial environments," says Melanie Spare, automation marketing manager at Siemens Energy & Automation (www.siemens.com). "Fiberoptic cables are completely resistant to any electromagnetic interference and ideally suited for future cabling developments. Another major advantage for using fiberoptics is the increased ability to achieve longer distances between access points within your network."

Most engineers agree that fiber is best. "One of the most popular and now cost-effective ways to avoid all of the common pitfalls of industrial networking is to use single-mode or multi-mode fiber instead of unshielded twisted pair (UTP) or shielded twisted pair (STP) cable," says Scott Saunders, director of strategic marketing, at Moore Industries-Intl. (www.miinet. com). "Fiber is impervious to induced noise, RF interference, lightning or voltage surges and common-mode noise."

But fiber cable is expensive, isn't it? "In the past, fiber was triple the cost of UTP per foot," says Saunders. "Today, fiber use is prevalent, causing prices to fall to where you almost cannot afford to choose UTP over fiber in new applications."

FIG. 1: NOISY ROBOTS



Lumberg USA

Industrial networks often have to work in the presence of electrical noise from robot welders, motors, drives and high voltages. Good wiring practices and proper hardware can eliminate many noise problems right away.

For copper cables, the consensus is that Category 5 and Category 5E-rated cable will work, although they are designed primarily for office environments. For industrial, you want the latest industrial cable, which is Category 6.

As explained by the Category 6 Consortium (www.tiaonline.org/standards/category6), the general difference between Category 5e and Category 6 is in the transmission performance and extension of the available bandwidth from 100 MHz for Category 5e to 200 MHz for Category 6. This includes better insertion loss, near-end crosstalk (NEXT), return loss and equal level far-end crosstalk (ELFEXT). These improvements provide a higher signal-to-noise ratio for higher reliability than current applications and higher data rates for future applications.

The additional performance parameters in Cat 6 provide a sort of "forgiveness factor" for things that happen within a cabling infrastructure over its lifetime, thus ensuring that bandwidth remains available.

Both Cat 6 and fiber cable are relatively expensive. Are they worth it? "A Panduit study showed an average Ethernet network crashes 20 times per year," says Bush. "Seventy percent of the time this is due to cabling, with approximately 36% of the downtime events costing more than $10,000."

Some say RJ-45 connectors are a good choice for connectors. "Fewer choices are in the best interest of customers," says Slivka. "That is why a single RJ-45 connector, a single encapsulated RJ-45 connector, and a single M12-4 connector have been defined in the EtherNet/IP specification."

There can be significant cost-savings thanks to quick and secure assembly systems for copper cables. "This means that the existing RJ-45 standard cabling technology can be used in an industrial environment, thereby enabling structured cabling by means of patch cables, patch fields, installation cables and connection plugs and sockets," adds Spare.

Then again, maybe not. "You don't have to spend much time investigating industrial Ethernet to discover that RJ-45 'telephone connectors' aren't viewed with a great deal of respect," Fahrion says. "The design lacks even the most minimal environmental protec-

TABLE I: IP RATINGS SEAL COMPONENT FATE

First Number	Protection Level (Dust/Foreign Object)	Second Number	Protection Level (Water)
0	No Protection	0	No Protection
1	Protected against solid foreign objects of 50 mm Ø and ›	1	Protected against vertically falling water drops
2	Protected against solid foreign objects of 12.5 mm Ø and ›	2	Protected against vertically falling water drops when enclosure tilted up 15°
3	Protected against solid foreign objects of 2.5 mm Ø and ›	3	Protected against spraying water
4	Protected against solid foreign objects of 1.0 mm Ø and ›	4	Protected against splashing water
5	Dust Protected	5	Protected against water jets
6	Dust Tight	6	Protected against powerful water jets
		7	Protected against the effects of temporary immersion in water
		8	Protected against the effects of continuous immersion in water

IEC IP ratings determine how well a component withstands dust, foreign objects and water. A product rated IP67 would be "dust tight" and could remain completely sealed and protected from the penetration of water when immersed for 30 minutes at a depth of one meter.

tion and can be damaged easily with a good yank on the cable." The surface area of the contacts is small, so if the thin layer of gold over nickel is worn away by vibration, it can be susceptible to corrosion and oxidation. "Not a great choice for your robotic welder, especially if downtime costs $15,000 per minute," adds Fahrion. "Limit RJ-45 use to inside the cabinet."

A simple way to choose a connector might be to remember that the criteria used to choose the cable is a good starting point. "The connectors at the end of the cables must work in the same environment and face the same challenges as the cable," advises Larry Eget, mechanical engineer for Lumberg (www.lumbergusa.com).

PROTECT THE EQUIPMENT

Once you have all that nice new cable, and the network interfaces and connectors are ready to be installed, it's time to think about environmental protection. No matter how good the components are, without protection they can be destroyed by the elements.

Most North Americans are familiar with NEMA standards, but IP ratings from the IEC are becoming important as well. Table I describes the "Ingress Protection" ratings of the IEC IP classification system.

If you have a particularly nasty environment, you may want to go an extra step and epoxy or "pot" your connectors. "Most people think of epoxy as an adhesive or sealant," says Karsten Loehken, networking product specialist for Lumberg, "Epoxy, as a potting material for encapsulating electronic components in a junction box, does not have a peer as effective. Research has shown epoxy can serve as a protective insulation for PC boards and wiring inside distribution and junction boxes."

Once a junction box has been potted with the epoxy compound, it chemically sets and turns into a solid plastic. Some manufacturers, Lumberg among them, use epoxy in every distribution box they make. An end user, machine builder or system integrator can achieve an IP67 or IP68 rating by using epoxy to seal a backplate on a distribution box. Be careful, though. Loehken warns that any moisture in the environment when that box is being sealed can condense and eventually cause corrosion.

Fahrion advises using optical isolators. "If you have an inherently non-isolated network, such as those using an RS-485 physical layer, add isolation at every node," he says. "For serial networks this is usually done with optical isolator products. The cost is generally $30-$150 per node. This practice makes it hard to screw up a network from a grounding perspective."

Ruggedness can be further enhanced by installing surge suppression at key points such as building penetrations or at central wiring closets. "Remember that the surge suppression point needs to have a high-quality ground available, adds Fahrion."

The longer the wiring run, the more trouble you can get into with ground loops, Fahrion notes. "Even the inherent 1,500 V of isolation found in Ethernet can be inadequate on long runs," he warns. "Runs longer than several hundred feet require fiber instead of copper. With fiber we have enough isolation to satisfy the toughest environments."

In non-ring networks in many plants, a mix of hardware is best," says Speedy. "Local industrial switches employing a copper infrastructure dispersed throughout the plant—each of which is connected to a central switch via fiber—is often the best solution. Most of the communication is kept within the local network and the copper media is kept short. You minimize the risk of lost data by not relying on a single trunk-style connection."

LET'S GET REDUNDANT

Even the best, most expensive hardware fails eventually, gets run over by a forklift, or takes a lightning strike. When that happens, a network might go down—unless it is redundant.

Ken Ludwig, president of Mid America Consultants, a system integrator in Overland Park, Kan., had an even tougher problem: He ran into some very smart people who wanted to destroy his network, so the network design had to withstand tampering and wanton destruction.

What's tougher than a maddened fork lift driver? How about a bunch of prisoners who want to escape? Ludwig installed a PLC-based security and monitoring system at a large detention facility that, he says, must remain nameless for obvious reasons. It has 31 Allen-Bradley PLCs, all linked by a redundant network. To prevent prisoners from defeating the network, a network with a dual-redundant fiberoptic loop backbone and a copper Ethernet network (Figure 2) was installed.

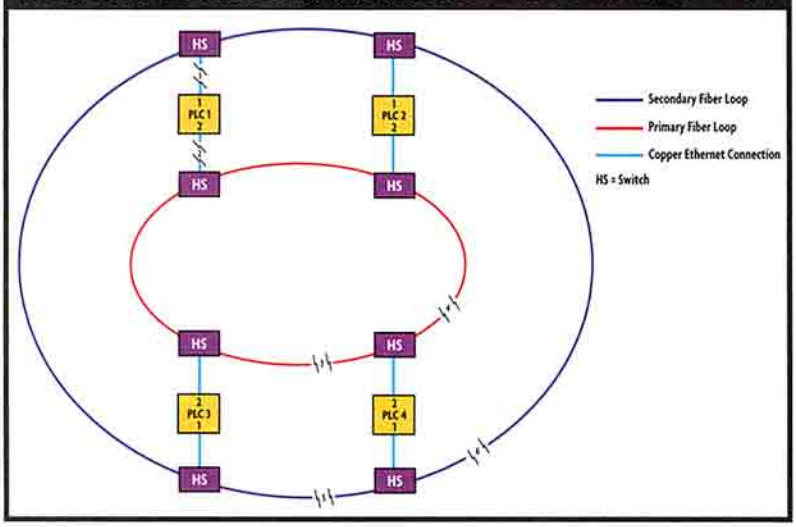
This system is as redundant as possible. "It takes four fiber breaks on the backbone or two copper Ethernet cable breaks between the switches and the PLC to isolate any PLC," says Ludwig.

Each set of switches and a PLC are in the same cabinet, in a locked room, so it really would take an equipment failure to isolate it, rather than something an inmate might do. "The fiber is routed in two different paths, so access to a fiber bank would not take out both networks simultaneously," he explains.

The switches, supplied by Hirschmann, are set up with one as a master and the remainder in default condition. "Although it looks like a loop on paper, it really is a bus, where the master is monitoring who is on the network," he explains. "If it ever cannot see, it closes a switch internally, and sends data backward down the bus to try and reach everyone. It works very well."

Speedy says he used a redundant system in a refinery. "We used two switches, two fiber sets, and two communication cards both in the controller and in the HMI computer," he says. "The key to it was Triconex's

FIG. 2: HOW TO SECURE THE BIG HOUSE



This prison network is about as redundant as can be. To isolate PLC1, a fork lift would have to take out both of the copper connections. To isolate PLC4, a saboteur would have to take a pair of shears to four different fiberoptic connections on two fiber networks.

driver for Wonderware software, but it worked very smoothly. I was able to alarm the loss of one network by monitoring an internal tag for each connection. It was a nice setup."

Saunders points out that redundancy has been around for a long time, and is easy to do from a hardware point of view.

"My experience is that everyone wants redundancy, but only the battle-scarred few are willing to pay for it," notes Fahrion. "The designer needs to understand the cost of failure in order to decide to invest in network redundancy." This may need to be documented into a business case for management in order to make the investment.

Redundancy had best be designed in from the beginning of a project, because it's tough to add it on later "Redundancy must be designed into the cabling system," Fahrion advises. "Wire your network in a ring instead of home-run. That ring—along with Ethernet switches that support redundancy—will give you two data paths, so no single cabling or switch failure will take down the network. For more protection, dual redundant rings can be connected. And don't forget to address power redundancy and the end devices."

Historically, redundancy always has been vendor supplied, often proprietary and very expensive. But times have changed. Now, not only are open redundant solutions available off the shelf from virtually every control equipment and industrial vendor, but self-healing systems are available, too.

"One of the advantages of using industrial Ethernet is that there are established IEEE redundancy standards," says Larry Komarek, automation product manager at Phoenix Contact (www. phoenixcon.com). "The Spanning Tree (STP) and Rapid Spanning Tree (RSTP) redundancy approaches are standard in commercial managed switches and now are becoming available in industrial managed switches. These standards not only provide cable-break recovery, they also create alternate communications paths in the case of power down or failure of the managed switches."

Some of the big control vendors are switching over from proprietary redundant systems. Foxboro/Invensys, for example, uses RSTP, which is "the big brother of STP," says Kevin Burak, consulting network engineer at Invensys Process Systems (www.invensys.com). "RSTP allows Ethernet networks to have redundant data paths without creating broadcast loops in the network. When a break or

failure occurs, the RSTP heals the network in less than a second. With the switches Foxboro now uses in its I/A Series mesh network, the network heals itself in less than one-quarter of a second."

If you want to take advantage of the STP and RSTP self-healing capabilities, you may have to work with a vendor, or with your IT department, because the technique requires network programming skills. Be careful, though. "Proprietary redundancy schemes are offered on the market with several 100 msec communication path recovery times, but they are not 'redundancy compatible' with commercial switches," warns Komarek.

MORE ON SECURITY ISSUES

The final step in making your network robust involves keeping the bad guys out of your network. This wasn't a problem until recently. "In the past, proprietary data and remote I/O networks were inherently isolated from the outside world," explains Komarek. "Except for malicious cutting of cables, it was difficult for outsiders to do any damage. Accessing data on the network required PLC programming in languages only control engineers knew. The network was controlled by a single specialized scanner that had no public access."

All that has changed. Ethernet is creeping into all levels of industrial networks, and opening up the once-cryptic world of industrial equipment to public view. Now, anything with an Ethernet port is vulnerable to viruses, hackers, industrial spies, disgruntled employees and meddlers.

The simplest and easiest way to keep outsiders from getting into a hardwired network is, as Speedy advises, "Don't connect to outside sources." In other words, no Internet access, no e-mail, and no connections to the IT department.

"Any outside connections should be left unplugged unless the system integrator, your IT department or an outside equipment vendor needs legitimate access," he adds. In such a case, make the physical connection, let the outside agency have the necessary access, and then disconnect it when it is all over.

Scott Saunders agrees. "The recent trend is to totally sever all connections

WHAT ABOUT WIRELESS?

"Wireless technology is everywhere," says Scott Saunders, director of strategic marketing at Moore Industries-Intl. (www.miinet.com). "From Bluetooth, to ZigBee to 802.11a/b/g, wireless is here to stay. However, the question remains whether it is secure and reliable enough for the industrial environment. While wireless approaches based on the 802.11 standard offer tremendous throughput, distance limitations, obstructions and the ability to overcome background noise are real problems in industrial applications."

Because of security problems with wireless, you may have to limit coverage or slow the transmission speed. "Wireless systems can use FHSS—frequency-hopping spread-spectrum—technology," advises Saunders. "This offers better interference rejection and security by hopping its RF packets in a random pattern. Only the nodes that are in this network know what frequencies to hop to and when." The downside of this technology is its throughput. "Technologies based on the 802.11 standard push data through at speeds of over 100 Mbps while most proprietary FHSS technologies typically top out about 250 Kbps," says Saunders. "So, for now, you have a choice: more speed or less security."

Security becomes a problem when a wireless network can be penetrated from outside the plant. "Securing a wireless network requires careful attention to both network design and security," says Kevin Burak, consulting network engineer at Invensys Process Systems (www.invensys.com). Burak recommends these guidelines when designing and setting up a wireless network:

- **Survey the RF coverage area**
- **Identify any RF interference potentials**
- **Limit coverage area to the facility**
- **Use directional antennas as required**
- **Use only commercial-grade equipment**
- **Select equipment that is compliant with 802.11 and 802.1x standards.**

NETWORK WIRING TIPS

If physical protection or local codes require conduit, use STP wire.

Isolate the STP shield from the conduit—high voltages may be present on the conduit.

Attach the STP shield to ground at only one end of the cable. Connecting at both ends creates ground loops with substantial current flow and induces noise.

If you are required to terminate the shield at both ends, wire a metal oxide varistor (MOV) shunt in parallel with a 1-Mohm resistor and 0.01-0.1 mF capacitor. This severely limits ground current except when extreme voltages are present.

Check cables with a cable tester, not just with an ohmmeter. A tester identifies continuity problems such as shorts, open wires, reversed pairs, crossed pairs, shield integrity, and miswiring of cables.

If your cable trays are metal, they 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.

Maintain at least a 10-cm distance from 120 VAC, 15 cm from 220 VAC, and 20 cm from 440 VAC, if you use conduit. If you don't use conduit, double those distances.

Source: The Ten Commandments of Industrial Ethernet, B&B Electronics.

between the public Internet and the control network," he explains. "Some corporations have taken their security measures a step further by completely separating the front office network from the process control network (PCN). When a front office network and the PCN are tied together, layers of protection instituted by IT personnel may include firewalls, NAT routers, gateways and proxy servers. However, even if layers of cyber security are in place, many companies still lack the physical security layers and policies to make their networks formidable."

Rakaczky says develop a security plan that includes the best available standards-based tools and technology such as firewalls, network-based intrusion prevention/detection, host-based intrusion prevention/detection, and anti-virus software.

But be careful about updating antivirus definition files to a DCS LAN. "Our IT personnel warn us that there is a possibility that new virus updates could interfere with the DCS software," says Bullerdiek. "A staged update approach is recommended, and do the staging at widely spaced intervals. If you have good security, the chance of picking up a virus is very small, but you will be getting new antivirus definition files regularly. I would recommend doing no more than a third of the network each week as a way to balance the risks. The use of memory sticks, ZIP drives, etc., also should be strictly controlled. Some would say they should be absolutely forbidden on a live network."

Rockwell's Bush agrees. The best way to keep out the bad guys is to limit access to the factory floor network to those people with a legitimate need, and only allow network traffic that is really required. "One important step toward limiting access is to create an 'inner defense perimeter' to logically separate the enterprise intranet from the factory floor network," he advises. "This creates an internal barrier that can be used to enforce the security rules around who can get access to the factory network."

Factory access security rules can be more restrictive than those between the Internet and the intranet, he says, because the kinds of data needed (and the users that need it) are usually well defined and limited to a smaller number of protocols and users. "In fact, traditional IT security technology such as firewalls, VPNs, routers, and so on, that are used to protect the enterprise network also can be can be employed at this barrier to filter unnecessary network traffic from unauthorized users. This lowers the probability of a worm, virus or bad guy invading the factory network." ●