

Industrial Networking for the Rest of Us

As open digital networks continue to transform process automation and information architectures, the need to understand networking technology has added yet another layer of complexity to the already imposing knowledge base required of today's process automation professional.

Indeed, engineers and technicians well-versed in instrumentation and control techniques often find themselves in new and unfamiliar situations, working with new and unfamiliar tools. For example, when first con-

switches—is necessary to terminate a segment properly. If a device coupler is disconnected from the segment accidentally or for maintenance, the change is detected automatically, terminating the segment at the proper coupler and allowing communications to continue.

At the control network level, MTL and industrial network security consultant Eric Byres of Byres Security are bringing easy-to-implement security to plant-floor networks with the joint development of the Tofino Security Solution—a no-



The greatest industrial network innovations today are not in the networks, but in making them easier and more foolproof to implement.

figuring a firewall or running multiple instruments on a fieldbus segment, I expect more than a few of you yearned for more comfortable, isolated days of milliamps, multimeters and home-run wiring. With all the compelling benefits of integration and transparency have come potential liabilities born of complexity and connectivity to the outside world.

Still, networking technology and its applications continue to advance, and, perhaps signifying the ultimate maturation of any technology, the greatest innovations today are not in the networks *per se*, but in making them easier and more foolproof to implement. Two examples, both new technologies introduced at October's ISA Expo in Houston, illustrate my point.

First, at the field network level, MooreHawke's humble-at-first-glance Trunkguard device couplers employ several clever innovations designed to ease commissioning headaches, as well as ensure that the failure of a single instrument won't bring down an entire fieldbus network segment.

Rather than limiting current flow to a short-circuited instrument, the Trunkguard "folds back" current flow to a trickle level. This prevents other instruments on the same segment from being starved of power and a power supply overload that would knock out the entire segment, according to Scott Saunders, vice president sales and marketing for MooreHawke parent, Moore Industries.

Trunkguard also includes a nifty—and patented—automatic termination feature that eliminates communication problems caused by too many or too few segment terminations. In essence, the device coupler senses whether it is the last fieldbus junction device in the segment and terminates if it is. No installer action—such as setting DIP

configuration security appliance that requires no installation expertise. Field technicians simply attach power to Tofino and walk away, transforming vulnerable control devices into highly secure fortresses, Byres says.

Despite our best efforts to isolate our control systems, the bad guys—and bugs—still get in. "Traditional firewalls are too complex for most security professionals to configure correctly and are even harder to set up on the plant floor. Once a virus or hacker gets past the control system firewall, the typical PLC or DCS is an easy target—as control devices and protocols offer no authentication, integrity or confidentiality mechanisms," Byres adds.

He likens Tofino to a combination personal firewall and intrusion detection system for operator stations, PLC, RTU and distributed control systems. "Plug a Tofino onto the control network in front of a device, and it learns what type of device it needs to protect; looks up the device's vulnerabilities in a central database; then tunes itself to protect that specific device. It even understands SCADA and process control protocols so it can act as a barrier to unauthorized access without obstructing valid control commands," he says. "It's time we accepted the fact that the staff operating and maintaining our critical control systems are, by necessity, highly trained control systems specialists and not information technology or security specialists. An electrician can't afford to worry about creating access control lists for firewalls or configuring encryption certificates."

I think we all knew that already. But it's nice to see someone actually doing something about it. **G**

Keith Larson,
VP Content, Putman Media