INDUSTRIAL NETWORKING
Q1 • 2009
A SUPPLEMENT TO PUTMAN MEDIA PUBLICATIONS

Users Get Out of Their COTS

CONSTRUCTED IN 1999, MY CURRENT PLACE of employment provided my first experience with a control system based almost entirely on Ethernet. Every controller, workstation, historian and engineering interface was interconnected via commercial off-the-shelf (COTS) Ethernet hubs. About two years after we started up, our control systems supplier was supporting projects with tens of thousands of tags, and we switched from hubs to the then-recommended Ethernet switch of the 3Com SuperStack variety.

While far from the consumer products sold at big-box stores, the 3Com products were nonetheless created and optimized to serve an office business network, not an industrial process-plant control system. The fact that this market was huge compared to control systems applications was obvious from the cost; the new switches went on a credit card. My supplier's recommended switch has changed yet again, but the 8-year-old SuperStack switches have been invisible for their lack of issues. Thankfully, I have had to learn little about switches; we just plug our Cat. 5E cables' RJ45 connectors into them and away they go. Like all such devices, there's a browser-based interface for managing the switches, whose IP address, username and password I have long forgotten. They are, knock on wood, so trouble-free, why would I consider an industrial hardened switch or other network hardware?

One of the first challenges for COTS is when we venture outside the control house. Many use bulky "wall wart" power supplies which need an indoor AC plug. Temperature specs are an issue, and you will search a while for switches that aren't designed for 19-in. rack mounting, which are a challenge to install in a typical field enclosure. Somehow, RJ45 connections—the ones that resemble your phone cable's wall jack/plug—just seem a bit flimsy when I'm terminating in a field junction box.

The assembly-line guys and gals have been dealing with this for a while, and now you even can buy an IP67, submersible connection for your Cat. 5/6 cables, like Hirschmann's Octopus line of industrial Ethernet switches. Not only does this give us a rugged, secure—a la minifast or eurofast—water- and oil-resistant termination for a network cable, it might become a handy differentiator between you and your business-network IS comrades—as in, "Here is where your domain ends and mine begins. Now, go back up our Outlook server."

> "WHILE PROPRIETARY NETWORKS WERE EXPENSIVE, MANY OF OUR END USERS WOULD WELCOME A RETURN TO THE OBSCURITY AND SECURITY THEY PROVIDED."

When our stuff looks like theirs, it's easier for our domain to get lumped into IS. For a few percent more, you can buy switches, routers, access points, cables and a variety of other network components that are built-for-purpose, for industrial process control applications.

Security has become a major concern, as well as a puzzle and a hardship. "While proprietary networks were expensive, many of our end users would welcome a return to the obscurity and security they provided", says Duncan Schleiss, vice president of the process systems marketing division at Emerson Process Management (www.emerson.com), "so we are introducing COTS switches that become built-for-purpose with the application of proprietary software and firmware, what we call 'proprietary off-the-shelf.'"

For utilities that access their substation devices via IP, RuggedCom introduced Gauntlet, a NERC CIP-compliant solution providing a security perimeter for protection from cyber attacks. For more generic industrial applications, there are routers and firewalls that isolate control infrastructure from the business network. MTL offers Tofino, a built-for-purpose firewall specifically designed for shielding PLC and DCS controllers from a threat that has penetrated the PCN.

DCS and PLC proprietary hardware, as in controllers, I/O modules and power supplies, have gone from pampered, clean, air-conditioned and humidity-controlled rack rooms to being hardened for extreme environments and hazardous locations. Many are innately qualified for Class I, Div. 2; no Z purge is needed. But the same generation started employing COTS equipment—network switches, hubs and Windows OS boxes—that's more akin to the DCS of the 1980s, at least in terms of how harsh its environment can be. Today's product offerings are erasing this disparity. For a relatively small premium relative to the security and peace of mind they afford, users should be considering today's line of industrially hardened network devices for their process control network applications. ●

JOHN REZABEK
jrezabek@ispcorp.com

John Rezabek is a process control specialist at ISP in Lima, Ohio.