

It had to happen eventually. Driven by potential efficiencies and savings, the evolution from point-to-point hardwiring to twisted-pair fieldbuses and onward to Ethernet, Internet and wireless keeps pushing inexorably outward to seek links and integrate with other networks. At the same time, progressively more sophisticated components, starting with relays and solenoids, followed by PLCs and board-level PCs, and on to Ethernet gateways and switches, continually reshapes plant-floor networks to become more similar to their corporate/environmental/information technology (IT)-governed counterparts.

However, there are just a few more wrinkles to work out.

There are two typical scenarios that demonstrate how plant-floor and corporate-IT networks are becoming more integrated. First, more

plant-floor components of all types are being built with Internet Protocol (IP) addresses and other capabilities for linking to other networks, which put them under the jurisdiction of corporate IT departments and managers. Second, some corporate/physical backbones, especially Ethernet-enabled networks, occasionally are extending a few lines beyond their usual deployment, and reaching down to monitor some production functions, rather than replicating another Ethernet network just for the plant floor.

Both of these examples show how formerly separate networks are overlapping, and taking the first steps to overall integration. However, to gain the benefits and minimize the risks of network unification and simplification, users must teach their plant-floor engineers and IT staffs to cooperate, implement some essential security infrastructures, and train these staffs to use and maintain them.

"Before 9/11, security meant I was concerned about keeping valuable tools from walking out of the plant," says Bill Lessig, plant manager at Honeywell Specialty Materials' (www.honeywell.com/sites/sm) 1,900-acre facility in Geismar, La., which recently integrated its process control and physical security systems. "Now, my security concerns have shifted to thinking about threats from external sources, assuring business continuity, minimizing impacts in the event of an attack, and making sure the surrounding community is safe."

As your network links grow, your problems grow. "Everyone is running into these same issues," says Bob Huba, DeltaV System Security product manager at Emerson Process Management (www.emersonprocess.com). "The tendency is to think of requests for links to plant networks and their data as just another IT job, but there's often a lack of knowledge between the corporate local area network (LAN) and physical control of manufacturing assets. IT departments

INTEGRATED SECURITY MUST-HAVES

Primary methods for ensuring effective integrated network security should include:

1. Implementing well-tested and maintained firewalls.
2. Deploying Microsoft Windows security patches as soon as they're available, but also checking that they won't have adverse effects.
3. Installing up-to-date anti-virus software.
4. Making sure Windows PCs are configured with high-security models, and locking down PCs when not in use.
5. Settling on security policies and training staff to practice them, such as not bringing in software programs from outside the facility on ripstops or datasticks, and then running them on internal PCs.

Source: Honeywell Process Solutions

COME TOGETHER

By Jim Montague, executive editor

Integration of Plant-Floor, Building, Physical Security, and Enterprise Networks Means More Chances for Unauthorized Access and More Need for Intelligent Security, Cooperation, and Training

like to lay their procedures onto plants, but they need to grasp the differences between the process control system and the business level. Each side is listening and learning the other's issues, but it's still a little painful."

Huba reports one of Emerson's chemical plant customers recently outsourced its IT management internationally, and then found its process controllers couldn't talk to its network devices through its HMI when their firewall was disabled remotely. He says several misconfigured switches were slowing the network, but it took a week to get through the IT firm's management layers to secure the required passwords and permissions. Huba adds that another client had a network router that kept failing and refusing to pass

on separate PCs to decrease. We've ended up with peer-to-peer networks that can talk to each other like they do on the plant-floor, and we now have whole buildings that are programmable and driven by software. The true benefit of this is that we can instruct these systems, for example, to lower temperature 2 °C in occupied area at times when electrical costs are twice normal."

In fact, Shaoguan Iron and Steel Group recently implemented a LonWorks network to more accurately measure and manage energy consumption in real-time at its 10-square-kilometer plant, and reduced its operating costs 10%. Now, data from the plant's energy and control devices is integrated with its manufacturing execution system (MES) to help it identify best-case use scenarios for energy

"WE USUALLY MEET TWICE EACH MONTH TO TALK ABOUT SECURITY AND HOW TO MARRY DIFFERENT PLANT AND BUSINESS-LEVEL APPLICATIONS. IF WE HAD AN ADVERSARIAL RELATIONSHIP WITH IT, WE'D NEVER HAVE BEEN ABLE TO DO WHAT WE'VE DONE."

data, and that an investigation revealed that a remote IT person was reconfiguring it repeatedly to meet corporate standards from which the router was supposed to be exempt.

JOB DESCRIPTIONS MERGING

"In energy management, for instance, most facilities previously had monolithic systems separated by job title for power, HVAC, lighting, elevators, security, and life/fire safety, and each had its own PCs and interfaces," says Barry Haaser, senior director of Echelon's (www.echelon.com) LonWorks infrastructure business. "Software changed these industries, and allowed device functions to increase and reliance

consumption and production. Located in Guangdong, Shaoguan produces 5 million tons of steel per year.

"In China, energy can be a third of a steel plant's overall operating costs," says Jianmel Huang, Shaoguan's IT director. "Echelon's technology gave us the ability to create an infrastructure that helps us quickly deploy a scalable system, and achieve our energy and operating goals."

Ironically, while plant-floor networks typically provide application data to the overall enterprise, sometimes the corporate network can directly aid the plant process, too. Jason Urso, Honeywell Process Solution's product marketing manager, adds that video surveillance has long been a part of the physical security infrastructure at many

facilities, but network integration often is giving video a new dual role in aiding process control.

"Because physical security devices are already in the process control setting, these cameras also can be used to check for leaks, vibration damage, and other adverse situations," says Urso. "Data sharing technology also enables users to examine streaming video with algorithms that can note differences such as changes in thermography."

GOSPEL ACCORDING TO GEISMAR

To protect chemical plants and refineries from potential attacks and other incidents, Honeywell Process Solutions is offering other companies the program it recently used to integrate security and process control at its Geismar specialty materials plant, near New Orleans. Honeywell developed and implemented a multi-layered security system that integrates its Experion PKS process control

system and its Electronic Building Integrator (EBI) cyber, electronic and physical site security systems over its common distributed server architecture, and these links reportedly allow faster, more efficient responses to any adverse events. Developed and implemented over 16 months and at a cost of \$3 million, this multi-layered security system reportedly takes a holistic approach, and integrates process control, automation and security systems to reduce risk and increase safety preparedness.

The Geismar plant is located on the Mississippi river (Figure 1), and the site is occupied by Honeywell and four other companies. Honeywell employs approximately 275 people at the site, with another 85 contractors on site at any given time. Counting the other companies' staffs, headcount at the site is more than 1,000 people. As host, Honeywell is responsible for the perimeter security of the entire site, as well as the security of its own facility. Honeywell produces several

chemical products at Geismar, including hydrofluoric acid, fluorocarbon refrigerants and Alcon resin.

"The goal at Geismar, like other chemical facilities, was to enhance safety and security to match the increased risk levels of the plant," says Lessig. "As a chemical manufacturer and as a process control, security and building controls supplier, Honeywell was in a unique position to take a look at securing the site in an innovative way."

The program's current capabilities and benefits include:

- Identify and control who enters and exits the facility
 - Track movements of building occupants and assets
 - Control access to restricted areas
 - Track and locate equipment, products, and other resources
 - Track the location of personnel on site in the event of an incident
 - Integrate control and security systems for greater speed and efficiency
 - Protect process automation networks and systems from cyber threats
 - Integrate vital waterway and dock monitoring through a radar system
 - Respond proactively to alarms and events
 - Share data to generate cost savings
- "Having the security system totally integrated with process control is what makes this project best in class" adds Lessig. "If there's ever an incident on site, everyone (security and process employees) knows about the incident in real time. We're now able to get the right information out to the right people quickly, and go into action immediately. This reduces risk, enhancing not only security, but safety."

Urso adds that Geismar will combine its wireless components and a third-party ultrawideband (UWB) radio frequency identification (RFID) technology to pinpoint precise locations of individuals at the plant by the end of 2007. The facility's current ID card swipe system only documents last-known locations.

"The biggest trend and challenge now is linking process control with business systems, so users can have a fully linked supply chain," says Urso. "This is where two worlds that



10, 16, 18-port
Managed Switches
Gigabit Available!

Remote Access
Ethernet Modem

Real-time 5 mS
Ring Switches

Slim Line
Managed &
Unmanaged
Switches

And much more...

Complete Line of Industrial Ethernet Switches

SIXNET



- Full range of industrial certifications
- 1,000,000 hours of uptime (MTBF)
- -40 to +75°C operating temperature
- Free upgrades & long term support
- Fiber optic, IP67, POE Switches...

New!



Free CD at www.managedswitch.com

FIGURE 1: BIG MUDDY MONITORING



A radar antenna and cameras monitor the Mississippi river near Honeywell Specialty Materials' dock in Geismar, La., as part of the 1,900-acre facility's layered security program.

used to be in isolation now need to securely exchange information. This can help a refinery reconfigure itself sooner and with less labor to, for example, better handle a ship full of a certain type of crude oil, and allow it to better respond to market dynamics."

FIRE-UP FIREWALLS

Despite the apparent ease and advantages of simply opening connections between plant-floor and corporate networks, experienced users warn that these links must only occur through well-defined, thoroughly tested, and maintained firewalls, demilitarized zones (DMZs), or virtual private networks (VPNs). However, as network integration causes potential connections to multiply, it becomes harder to enforce these security directives, even though they're needed more than ever. Likewise, performing a thorough network inventory, data blueprint, and risk assessment becomes an even more crucial starting point.

Brad Hegrat, Rockwell Automation's (www.rockwellautomation.com) senior network and security engineer, suggests that users employ:

- Stateful packet inspection (SPI) firewalls and/or deep packet inspection (DPI) firewalls that check if data is bound for the correct destination address, and that it comes from the proper source address.
- Packet-filtered firewalls, which also allow

or deny communication based on IP addresses, but are quicker than SPI and DPI methods.

- Application gateway or proxy firewalls, which sever connections at the proxy level, and then use that proxy to serve the data when asked. These devices are used for corporate web traffic, and they're the most secure, but also the slowest.

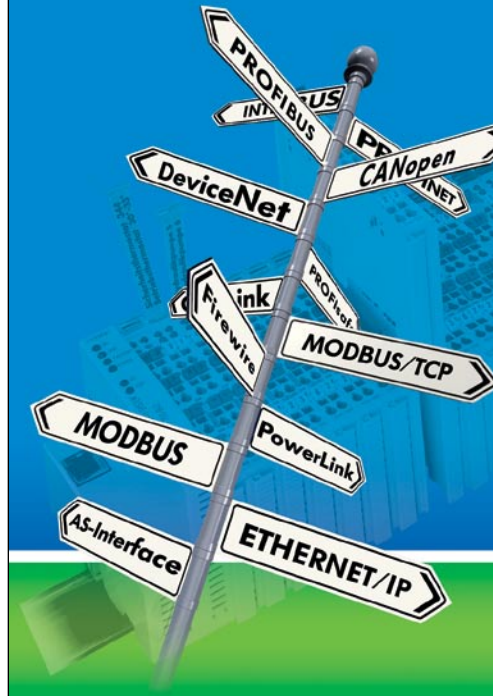
Hegrat adds that firewalls are more secure because they filter all data through one point, but routers and switches are less secure because they usually have multiple network connections. "One of our customers that makes heavy equipment in the Midwest had a virtual local area network (VLAN) with several access points, and last summer the Zotob worm virus found a hole in it," says Hegrat. "This event brought down production for seven hours at dozen of plants, and cost millions of dollars in lost production time." They had to scrub this virus the old-fashioned way and manually restore thousands of devices across the U.S.

"Today, intelligent firewalls can monitor network traffic, respond to network-based events like this by logically disconnecting themselves, and separating corporate/external networks from production," says Hegrat.

To further help users safely integrate control and corporate networks, Bennet Levine, Contemporary Controls' (www.ccontrols.com) R&D manager, advises them to implement:

All Signs Point to...

...the WAGO-I/O-SYSTEM



Fieldbus I/O requirements pulling you in different directions? Choose the fieldbus independent WAGO-I/O-SYSTEM for all your I/O needs.

The System

- Over 25 bus-couplers supporting over 16 fieldbus protocols
- More than 200 analog, digital, and special function I/O modules
- Granular 1, 2, 4, or 8 channel modules - buy only the I/O you need
- Modular, DIN rail mount rack-less design - easily add and remove I/O

The Benefits

- Easily connect to any PLC CPU for local or distributed I/O applications
- More cost effective and flexible than PLC expansion racks and PLC I/O
- Reduce inventory and component cost with one I/O hardware platform
- Reduce cabinet space - modules less than 1/2" wide and bus-couplers approximately 2" wide

For more information on becoming fieldbus independent, contact WAGO at 1-800-DIN-RAIL (346-7245) or info.us@wago.com

www.wago.us/fieldbus.htm

WAGO[®]
INNOVATIVE CONNECTIONS

- Rate limiting to predetermine an adjustable ceiling for the maximum bandwidth on the ports on their network devices.
- Port locking that only allows certain media access control (MAC) addresses to be carried through on specific ports. This enables blocking


of all but the one or two PCs that the user wants the network to be able to access.

- Overlapped VLANs that isolate corporate and plant-floor networks by allowing only one device to sit on each side, and then sharing data through it. This is

similar to a DMZ strategy.

"Ethernet requires a little more awareness because it's too flexible to some extent," says Levine. "If you're not careful, you easily can access an office network from the plant or vice-versa, and potentially flood the other with unwanted data." To prevent these problems, Contemporary Controls supplies EIS8-100T and UL 864-rated Ethernet switches to segregate and direct network traffic.

In fact, system integrator ATS Automation (www.atsinc.org) recently used EIS8-100T



**Belden... The Critical Link
In Your Industrial Infrastructure.**

Manufacturing productivity increasingly depends upon "seamless" data communications and automation systems — even in the harshest environments. And seamless means Belden.

Belden has developed the world's most comprehensive line of industrial cabling solutions, always achieving maximum system performance. And maximum uptime.

Take a look at this brief overview of Belden's IndustrialTuff® line:

- DataTuff® twisted pair and TrayOptic® optical fiber Industrial Ethernet cables
- A wide range of cables for applications addressing numerous industrial protocols — including Belden's ControlBus®, Blue Hose®, DataBus®, DeviceBus® and RS-485 cables

- Variable frequency drive (VFD) cables for AC motor drives
 - Belden Infinity® flexible automation cables for robotic and continuous motion applications
 - A broad selection of PLTC and TC instrumentation and control cables
- IndustrialTuff products are manufactured in ISO 9001:2000 quality-certified facilities. Shouldn't you link up with the best?

Call **1.800.BELDEN.1**

Or go to Belden's Web site for more information, at www.belden.com

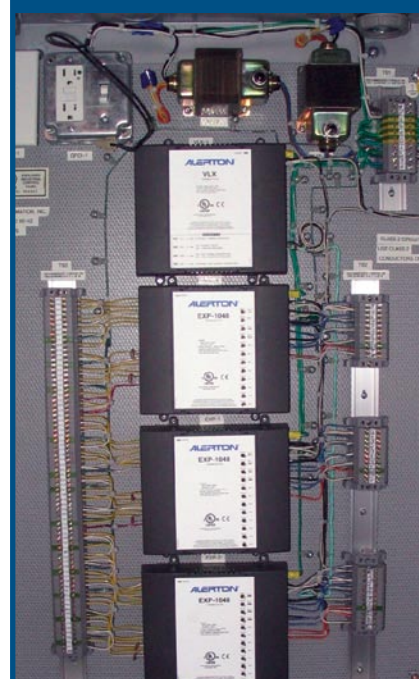


BELDEN
SENDING ALL THE RIGHT SIGNALS

©2006, Belden Inc.



FIGURE 2: SWITCHES COMBINE CONTROL



Two Ethernet switches are physically connected to an Alerton BACnet/Ethernet smoke control network to jointly run day-to-day HVAC, alarm-based smoke handling, and other equipment at the 42-story WaMu Bank and Seattle Art Museum.

switches to help implement an integrated Alerton distributed digital control (DDC) system at the new, combined 42-story Washington Mutual (WaMu) Bank and Seattle Art Museum. ATS senior sales engineer Pete Segall says this application shows how plant and corporate networks can be successfully integrated because it combines:

- HVAC and smoke control;
- Automatic transfer switches, emergency

generators, and power monitoring for WaMu via Modbus;

- Variable-frequency drives (VFDs) and lighting controls via BACnet Ethernet integration; and

- EST fire alarms via a field server driver.

Segall reports that two EIS8-100T switches helped ATS develop an integrated control that could jointly monitor and control HVAC, smoke, and other combined smoke-and-HVAC equipment both daily and on an alarm-event basis. "Pure smoke control systems don't function on a day-to-day basis, but HVAC and combined systems do," adds Segall.

The two Ethernet switches were physically connected to the Alerton BACnet/Ethernet

smoke control network via Cat 5 cabling, so precise, required DDC logic routines could be carried out (Figure 2). One switch is located in the central fire control room, and the other is in a telecom room on WaMu's second floor. In addition, one switch is used as a gateway between the non-smoke control Global DDC logic boards and the building management system's computer and user interface.

"Ten years ago, this kind of integration would have been extremely difficult because there were no open protocols, and we would have had to write proprietary system drivers to translate between the fire, control and security protocols," says Segall. "Open

NETWORK SECURITY IN MULTIPLE ZONES AND SUB-ZONES

In its "Process Control Network—Reference Architecture" whitepaper, Invensys Process Systems (www.invensys.com) recommends segmenting process control networks into four major security zones, including Internet, data center, plant network, and control network, as well as several supplementary sub-zones as needed. Each zone is separated by a firewall. Secure network design dictates that the perimeter firewall comes from a different manufacturer to provide maximum resistance to penetration. This one firewall might be a pair of high availability units in a fail-over mode. For networks that require real-time or near real-time communications to the process control network, it's recommended that at a minimum this device be a high-availability or redundant unit.

The network is divided into the following major zones and sub-zones:

Field I/O—Communications in this zone typically are direct hardwired communications between the I/O devices and their controllers. Security is accomplished by physical security means.

Controls Network—This zone has the highest level of security and carries process control device communications. Traffic on this network segment must be limited to only the process control network traffic as it is very sensitive to the volume of traffic and protocols used.

Plant Network—Carries general business network traffic such as messaging, ERP, file

and print sharing, and Internet browsing, etc. This zone might span multiple locations across a wide area network. Traffic from this zone may not directly access the Control Network Zone.

Data Center—This could be one or multiple zones that exist at the corporate data center.

Internet—This zone consists of the unprotected public Internet.

Sub-Zones—Added sub-zones may be implemented to provide an extra level of control. These commonly are implemented as DMZs on the firewall. Typical uses of these sub-zones are:

- **Data Acquisition and Interface**—This sub-zone marks the interface for all communications in or out of the process control network. It contains servers or workstations that gather data from the controls network devices, and makes it available to the plant network.
- **Service and Support**—This sub-zone is used by support agencies when servicing the controls network. This connection point should be treated no differently than any other connections to the outside world, using strong authentication, encryption or secure VPN access. Modems used should incorporate encryption and dial-back capability. Devices introduced to the network should be using updated anti-virus software. It's also common for the perimeter firewall to have several DMZs defined.

Control Cabinet Extensions...

...with the
WAGO-I/O-IP 67/68



The 757 Series, IP-67/68 sensor/actuator junction boxes, safely extend your control cabinet functions out into the field and local to the machine or process:

- Halogen-Free PUR cable for extreme flexing and increased safety (no emission of toxic or corrosive fumes) applications
- Unique spacer eases installation by creating a clean, modular mounting manifold
- 100% potted to ensure system integrity
- Built-in LED's for power and signal status
- Available with M23 connector or pre-cabled, as well as 4, 6, or 8 port configurations
- 4 or 5 poles per port for the connection of one or two sensors per port (M12)
- Marking tag holder for every port provides clear circuit identification

Now with M8 Connectors!

For a free brochure or application support, contact WAGO today at 1-800 DIN Rail (346-7245) or info.us@wago.com
www.wago.us/IP67.htm

WAGO[®]
INNOVATIVE CONNECTIONS

protocols such as BACnet and Modbus make all of this easier, and having a single point of connection between the several hundred Ethernet devices in our dedicated HVAC and fire network and WaMu's overall corporate network gives us secure flexibility."

COOPERATION CULTURE

Whatever technical methods are used to integrate industrial and business networks, everyone agrees none will be secure without plant and IT cooperation, jointly developed security policies, and training.

Jay Hardison, plant superintendent for Colorado Springs Utilities (CSU), says the utility has been using EtherNet/IP for its corporate backbone, and Profibus and DeviceNet for its plant-floor water/wastewater treatment plants for several years, and recently added Rockwell Software Maintenance Automation Control Center (RSMACC). RSMACC adds required security and offers supplemental authentication, auditing, archiving, and verification.

Hardison explains that CSU is integrating its networks into an overall historical database, which it will use to drive its Maximo work management system and

Squeeze More out of your Network Budget

N-TRON® Now Offers Affordable, Entry-Level Industrial Ethernet Switches

Same Reliable N-TRON Quality at a Lower Price

- \$119 OEM Price for 104TX Four Port Unmanaged Switch
- \$139 OEM Price for 105TX Five Port Unmanaged Switch
- -40°C to 80°C Operating Temp
- > 2 Million Hours MTBF
- Supports Full or Half Duplex Operation with up to 1.0Gb/s Maximum Throughput
- Redundant Power Inputs (10-30 VDC)
- ESD Protection Diodes on all Ports
- Surge Protection Diodes on all Power Inputs

N-TRON
THE INDUSTRIAL NETWORK COMPANY

Visit us on the web @ www.n-tron.com, or call (251) 342-2164



N-TRON now offers affordable, compact, entry-level, industrial Ethernet switches. These unmanaged four or five port copper Ethernet switches are ideal candidates for network expansion and are designed for use in mission critical data acquisition, control, and Ethernet I/O applications. Housed in a rugged steel DIN-Rail mount enclosure, the compact size provides a smaller footprint allowing multiple switches to fit in tight spaces. The 104TX and 105TX carry an impressive operating temperature rating of -40°C to 80°C. With over two million hours MTBF these hearty little switches are built to last thereby increasing the economic value.



FIGURE 3: SPRINGS IN COLORADO



ROCKWELL AUTOMATION

Colorado Springs Utilities' Northern Water Reclamation facility combines EtherNet/IP, Profibus, DeviceNet, and maintenance automation software at its water/wastewater treatment plant.

preventive, run-time-based maintenance program. He adds that subsequent reading and diagnostics will let CSU run its plant on a more unmanned basis using a VPN, and increase capacity to handle the 3,000 taps it's added annually for the past several years without adding manpower.

"We're able to do this because we have a good working relationship and a common vision with our IT department," says Hardison. "Our IT people participate on the plant-floor, learn about our controls, and even go to control conferences. Meanwhile, they've educated us about Ethernet, switches, routers, and firewalls. We usually meet twice each month to talk about security and how to marry different plant and business-level applications. If we had an adversarial relationship with IT, we'd never have been able to do what we've done." ●