SPECIAL REPORT

CONTROL

PROMOTING EXCELLENCE IN PROCESS AUTOMATION CONTROLGLOBAL.COM

State of Technology Report
PLCs, PCs and PACs

With its high visibility, sophistication and connections to historians, advanced control and business systems, the distributed control system (DCS) tends to get all the glory in process control applications. But in plants both with and without a DCS, much of the logic execution, local HMI support and I/O communications are carried out by plant-floor programmable logic controllers (PLCs), process automation controllers (PACs) and controllers based on commercial personal computer (PC) architectures and operating systems.

All three forms of controllers have shrunk in size while gaining enormous computing power, software flexibility and industrial strength, and now can capably perform the hardware functions of any but the largest DCS. Here, we present our past year's articles describing innovative applications of PLCs, PACs and PCs. For an overview of our previous controller coverage, access the 2015 version of this report at http://info.controlglobal.com/soty-150617-lp.

PutmanMedia®

CONTENTS

Advertiser Index

Advantech Control Industrial PC

Providing Computing, Connectivity and Control for Smart Factories

ADVANTECH

Enabling an Intelligent Planet

Advantech's APAX-5580 is a powerful control industrial PC with an Intel® Core™ i7/i3/Celeron processor. It features flexible I/O expansion, network capability through various interfaces, real-time I/O control, and supports dual power input/UPS module for maximum uptime.

High Performance Computing

Features latest Intel Core i7/i3/Celeron CPUs with open operating system support including Microsoft Windows Embedded and Embedded Linux

Boundless Connectivity

Built-in Serial, USB, Ethernet, WiFi, and Fieldbus

Robust Control

Includes real-time distributed bus technology, hot-swappable I/O modules, open software support including CODESYS IEC 61131-3

APAX-5580
High powered Control Industrial PC with Intel Core i7/i3/Celeron processors

APAX-5000
Full Range of I/O modules including AI/AO, DI/DO, T/C, RTD, Relay, and Counter

APAX-5435
Wide variety of communication interfaces including fieldbus, wireless, and I/O

CODESYS SoftLogic Control Software

www.advantech.com

PLCs and PACs can solve the protocol translation problem

Using PLCs or PACs and Ethernet as gateways to digital communication protocols can be a low-cost alternative

By Dan Hebert

Most process plants use many different digital communication protocols, so conversion is required. A DCS can often perform protocol conversion, but generally at a very high cost. A better alternative in many cases is using PLCs or PACs as protocol conversion gateways, and then connecting the PLC or PAC to the DCS via Ethernet. For plants controlled by one or more PLCs or PACs instead of by a DCS, the PLC or PAC becomes the gateway by default.

“One use of our plug-in communication modules is to migrate an old DCS to the new Rockwell Automation PlantPAx,” says Ken Roslan, vice president of global marketing for ProSoft Technology. “This allows continued use of the old DCS I/O and a phased migration, minimizing risk and downtime.”

In a related example, the United Space Alliance (USA) assembly and refurbishment facility at NASA’s Kennedy Space Center in Florida used ProSoft’s Modbus communication modules and Rockwell Automation’s ControlLogix platform to control the batch-mixing process for the insulation used on the space shuttle.

A ControlLogix PAC and an Allen-Bradley SLC-500 controlled each of two mixers. USA tried using 4-20 mA feedback between the controllers and the flow meters, but found they were unable to obtain the needed level of accuracy and precision. “We contacted

“A better alternative in many cases is using PLCs or PACs as protocol conversion gateways.”

Micro Motion and they pointed us to ProSoft’s Modbus communication modules, which integrate directly into the ControlLogix and SLC-500 platforms,” explains Dan Dermody, control systems engineer at USA.

“We tested them out and quickly discovered they provided the accuracy and precision we needed. The module collects flow data and feeds it directly into the ControlLogix data tables,” Dermody continues. “This type of flow control system maintains all the process parameters, so nothing goes out of specification during mixing.”

In wastewater plants, Profibus is a much used protocol. The Changi Water Reclamation Plant in Singapore selected Profibus DP V1 as its communication protocol, requiring conversion to talk to Schneider Electric PLCs.

“A better alternative in many cases is using PLCs or PACs as protocol conversion gateways.”

The plant uses 160 ProSoft Profibus DP V1 Quantum modules to communicate between the PLC and a long list of field devices including magnetic flowmeters, thermal mass flowmeters, pressure and differential pressure level transmitters, radar/ultrasonic transmitters, dissolved oxygen analyzers, temperature transmitters and electric actuators.

Plants often need to convert from Profibus DP to Profibus PA. “In many applications, Profibus DP is advantageous to span long distances, and it also allows creation of fiber redundant rings for increased reliability,” notes Andres Suazo Wildt, the serial and process fieldbus product specialist at Phoenix Contact. To connect to Profibus PA, Profibus DP/PA couplers are available from Phoenix Contact.

IO-Link is a popular low-cost, point-to-point communication protocol often supplied with many types of sensors. “Unfortunately most PLC I/O cards available today do not yet support IO-Link,” points out Dr. Helge Hornis, the intelligent sys-

"In many applications, Profibus DP is advantageous to span long distances, and it also allows creation of fiber redundant rings for increased reliability."

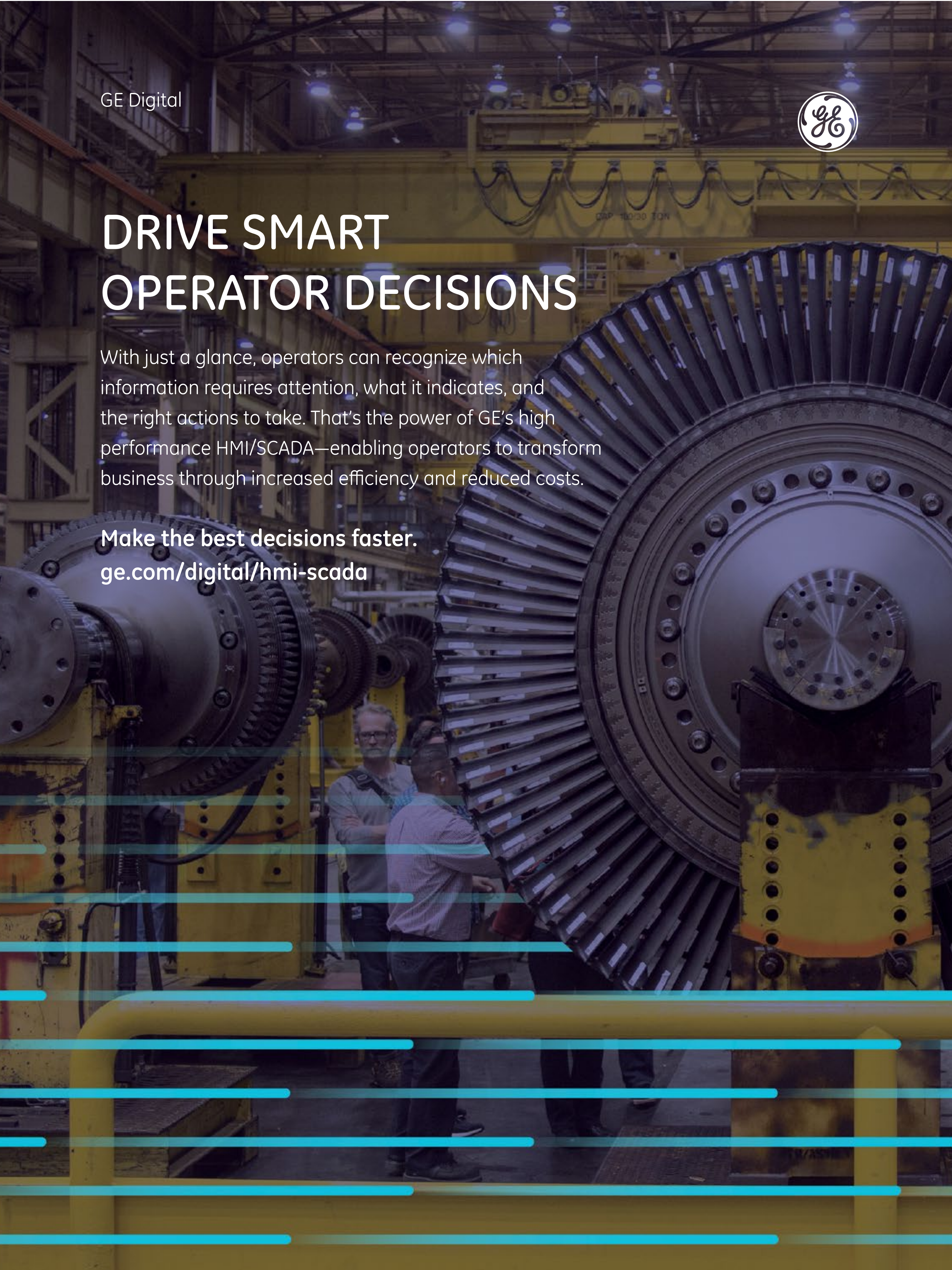
tems group manager at Pepperl+Fuchs. The Pepperl+Fuchs solution is its SmartBridge, connected between the PLC's I/O card and IO-Link sensors to intercept IO-Link data and send it to the app. Using a smartphone or tablet running iOS or Android, the SmartBridge establishes a wireless interface to the mobile device.

In cases where the I/O card is IO-Link-enabled, SmartBridge listens to the communication and sends a copy of the sensor data to the mobile device. When a conventional I/O card is used, SmartBridge assumes the role of the IO-Link master and separates the diagnostics data from the switch state, with all diagnostics-related information visualized on the app, while the sensor switch state is passed on to the I/O cards.

Turck provides a specialized PLC communication device called an Ethernet spanner/scanner module. "Our Ethernet spanner/scanner module provides an easy way to link multiple subnets together for data exchange, even ones speaking different protocols," says Chris Vitale, the senior product manager for networks at Turck.

"The device reduces the need for multiple PLC origination points, greatly reducing costs. By linking subnets with a spanner/scanner, networks can be less complex because the device allows Ethernet IP addresses to be reused. The Ethernet spanner/scanner specifically acts as an I/O connection aggregator, reducing the number of connections to the PLC, simplifying installation and lowering system costs," adds Vitale.

Dan Hebert is senior technical editor for *Control* and *Control Design*. Email him at dhebert@putman.net.



Four ways to collect process plant data

PCs with HMI software can work as plant's sole data collection tool

By Dan Hebert

Big data from process plants originates at the sensor level, often with a healthy dose of manually entered information. There are four ways for you to collect, store and analyze this data: electronic data recorders, PLCs, HMIs and data historians.

Processes requiring I/O that can connect to sensors, local operator interfaces and data storage are best served by an electronic data recorder. "In many applications, a local operator must keep watch over a batch process, and periodically annotate the acknowledgement of an alarm event with a text comment," says Steve Byrom, product manager for data acquisition, Yokogawa.

"In FDA program areas, the recording system must support compliance with regulation 21 CFR Part 11, requiring user log-in before granting access to the system. The latest, multi-point, touch-panel recording systems allow users to rapidly log in, acknowledge alarms, enter descriptive text data, and apply electronic signatures by touching screen icons and typing text on-screen. Trend history can be reviewed with a swipe to any area of interest in the saved data records, and data is saved in real time to secure, non-volatile flash memory," says Byrom.

"With enough processing power and storage space, PCs with HMI software often can function as a plant's sole data collection tool."

Many process plants purchase packaged units such as compressors, often with their own PLC-based control system. Modern PLCs can store significant amounts of data locally, and transmit or transfer this data to higher-level computing systems in a variety of ways.

Jeff Payne, product manager for PLCs, I/O and PC-based controls at AutomationDirect, explains. "Many modern PLCs and PACs have built-in data acquisition, data storage and networking capabilities. This allows data to be collected and stored locally and also transmitted to other systems. This can be done by simply connecting an Ethernet port to a network. If no connection is available, data can be pulled from a removable mass storage device such as a USB pen drive."

Next in sophistication is PC-based HMI software, particularly when coupled with an SQL database installed on the same machine. With a PC with sufficient power and storage space, these platforms often can function as a plant's sole data collection tool.

"The most common method of data collection is PC-based HMI software like our InduSoft Web Studio," claims Richard Clark, an engineer with InduSoft. Process variables and batch information can be trended and stored in a local proprietary or a SQL database. Sometimes the amount and volume of data needing to be stored is beyond the scope and capability of the HMI or SCADA system, and an external, dedicated plant historian must be connected to the PC.

Take the case of an application for a water treatment plant in Alaska, where a historian was required due to the sheer volume of data and other factors. Working with Dowland-Bach (www.dowlandbach.com), a local Rockwell system integrator, the plant upgraded its control system to improve reporting, data storage capabilities and maintenance efficiencies by installing FactoryTalk Historian software from Rockwell Automation.

Before installing the new system, it took operators six hours to generate one report — a task that needed to be repeated five times per month, at an annual cost of $18,000. Report generation was also frustrating and error-prone, as operators had to manually scroll through each day's one-minute samples to locate high-turbidity points.

The facility is now producing highly accurate 24-hour data trend reports with minimal effort. With the historian software, reports take minutes. Regulatory compliance requires seven years of data on the system, which overworked the original databases and caused breakdowns costing $20,000 annually in maintenance costs alone. Using the historian software, the plant easily stores 25 years of data, eliminating unplanned maintenance and downtime due to failures.

Dan Hebert is senior technical editor for *Control* and *Control Design*. Email him at dhebert@putman.net.

Expand your potential with the experience of Modicon.

Since inventing the PLC in 1968, the Modicon™ family of PLCs has defined technology that enables and connects your machines and processes. We know that the only way to meet the future demands of automation is to provide products that exceed your expectations now. The Modicon product range provides the flexibility and versatility to help you achieve benchmark machine and process performance.

modicon.com

Life Is On | Schneider Electric

Creative ways to cut costs in hazardous areas

For remote operator interface applications in hazardous environments, a thin client is the most economical solution

By Dan Hebert

Installing a display monitor or a PC in a hazardous area used to be a very expensive proposition, but new technologies are easing implementation. Thin clients can be used for the operator interface tasks of displaying information and entering commands, often via a touchscreen. They don't require much processing power, don't consume much energy and don't generate a lot of heat. This makes it possible for manufacturers to provide thin clients in sealed enclosures suitable for installation in Class I, Div. 2 applications.

A major international oil company has a facility near San Francisco Bay where oil from tankers is transferred to storage tank farms. The company wanted to place six industrial workstations in the field near the transfer points for easy operator access, and connect these workstations back to a control room 500 feet away through a series of industrial switches.

The solution was to link the thin-client workstations back to the Honeywell DCS in the control room. "This installation is in a Class I, Div. 2 outdoor environment with year-round outdoor use and no purge system is needed," relates Louis Szabo, business development manager for the HMI and purge business unit at Pepperl+Fuchs.

"Our certified VisuNet IND OIT workstations met the required price point and hazardous requirements. A 22-in. touchscreen was selected for compatibility with the HMI widescreen graphics already developed for the control room," adds Szabo.

Although a thin-client architecture works well for extending operator interface capabilities from protected areas, such as control rooms to hazardous areas, other applications are more suited to solutions that simply extend the distance from the PC to the display monitor—often by miles.

In these situations, a KVM extender is often the best choice, as it requires very little in the way of design, just the installation of KVM hardware at the source and destination. A chemical company in the Houston area used this technology to install two workstations in a Class I, Div. 2 area, and link them to a remote Siemens PCS 7 control system.

The workstations are under a roof in an open-air environment, and the requirements were for two Class I, Div. 2-certified workstations, each with a wide-screen, glove-friendly touch display, a keyboard and a trackball. All the components needed to be housed in a stainless steel enclosure and pedestal to meet NEMA 4X requirements. The client didn't want to use a purge system, so all of these components had to be rated for use in Class I, Div. 2, including a fiber-optic KVM receiver.

A fiber-optic KVM extender was installed at the control room miles away from the workstations. The solution was built by Pepperl+Fuchs SEC group, and certified under UL's 698A NNNY panel program to meet the primary customer's concerns about the hazardous-area mounting of a certified system, exposure to both hazardous and potentially corrosive environments and temperatures over 115 °F.

For remote operator interface applications in hazardous environments, a thin client is the most economical solution, followed by a KVM extender. The most expensive is to install a PC, often with peripherals such as a printer, but in some applications that's what's needed.

A good solution in these cases is to use non-rated components installed in a purged enclosure. Depending on the type of purge system, this can allow non-rated components installed in standard NEMA 12 enclosures to be used in hazardous environments up to Class I, Div. 1.

"Purging and pressurization systems may be integrated or mounted separately, and the application can include any variety of exposed or remote devices such as pushbuttons, keyboards and barcode scanners," says Mike Baucom, CEO, Bebco Industries. "Depending on the application, the devices can be protected by safety barriers within the pressurized enclosure to render them intrinsically safe."

Dan Hebert is senior technical editor for *Control* and *Control Design*. Email him at dhebert@putman.net.

How PLCs of critical facilities are protected from cyber attacks

Béla Lipták and our Ask the Experts panel say engaged employees are the best protection. Employees are the weakest link in industrial security, so they need to be trained, tested and engaged to protect their systems

This column is moderated by Béla Lipták, automation and safety consultant and editor of the Instrument and Automation Engineers' Handbook (IAEH). If you have an automation-related question for this column, write to liptakbela@aol.com.

QUESTIONS

What is being done to protect the malware-vulnerable programmable memory of the PLCs of critical facilities? Anything?

It is possible to program a PLC memory and then program a lockdown so the memory becomes write-once rather than write-always, and thus would be immune to malware attacks.

Because, for example, nuclear power plants, hydroelectric dams and pipeline systems are essentially steady-state in operation, then a write-once memory would have to be differently programmed to effect a change in the operation of the machinery controlled by the PLC. Thus, a technician from the control room would take the new memory down to the PLC.

The PLC could, for security, have a locked, hinged cover over its memory socket. There would be a programmed shutdown of the PLC's controlled machinery and the first memory would be removed, to be taken back to the control room for storage for possible future use. The new memory would be inserted into the socket, checksummed for identity by the control room operator, and the machinery would be restarted, now operated by the new memory in the PLC.

Alan Morris, morris.ward@verizon.net

ANSWERS

Protections must be twofold:

1. Protect the physical access port for programming. This means placing the PLC in a locked cabinet or location, with control over who can access the programming port. This doesn't prevent all errors, for example, the programming PC may itself be compromised, as with the Stuxnet attack. If you are worried about that level of threat (considered the highest level of threat), then only allow dedicated PCs to be used for programming.

2: Protect the network access to the PLC. Most programming packages have network access, and many PLCs allow network access to change values in programmable memory (through OPC, OPC-UA, ProfiNet, DeviceNet, etc.). To protect against outside network access (assuming you have taken the steps to protect the programming and HMI devices), you must set up a layered defense on zones and conduits. (See ISA/IEC 64223, Requirements for IACS Security Management.) Only allow direct access to the PLC from a secure zone. The security rules on the conduits should not allow direct access to the PLC, but should go through a proxy that checks that the access is valid and within limits. There are also physical devices that you can place on the PLC network port that act as an individualized firewall for the PLC. However, remember that sophisticated threats will appear as valid commands, so the primary protection is to use only approved devices within a zone, setup a DMZ between your externally available business network and your control networks, use the best practices for patch management, and setup a canary system in the zone to check if it is compromised.

You can lock the code using a password on many PLCs (Simatic S7, Rockwell, etc.). However, this can be bypassed if the password is known. You can even uncode the program code so it can't be read and reverse engineered. It sounds to me like you need a non-networked PLC, or one that only publishes information and does not allow any writes at all. The other elements would require a very specific PLC and additional hardware.

If you use the same protection on everything, then on average you are providing either too much protection or too little. To determine what to protect, you should inventory the systems to determine what needs to be protected, inventory the data to determine what needs to be protected, and determine the value of the process, product or information (actual "accountable" value).

Lastly, remember that engaged employees are the best protection. Employees are the weakest link in industrial security, so they need to be trained, tested and engaged to protect their systems.

Dennis Brandl

DnBrandl@BRLConsulting.com

I call this gross overkill. I suppose that the NRC might ask for something like this, but I say, just don't connect to the Internet. From what event is this cumbersome procedure protecting?

Many PLCs no longer have removable program memory boards. What then?

I know of nothing being done to protect real PLCs from malware or any other security attack. These PLCs do not use commercial operating systems and attack from Internet sources is extremely unlikely. Rarely are real PLCs connected to the Internet in any way. However, there are two situations in which such an attack is possible for PLCs:

1. PLCs may be implemented on industrial PCs using commercial PLC software to implement IEC 61131-3 programming languages. These PC/PLCs may be connected to the Internet and are subject to malware attack, but can be protected using conventional PC antimalware, antivirus software, and the use of firewall protection from any unauthorized access via the plant network.
2. As was proven by the Stuxnet attack on the centrifuge controllers at the uranium enrichment process in Iran, malware was installed at the Siemens PLC manufacturing plant by covert means without Internet connection. Deep knowledge of the Siemens software was required to create and install this malware as well as covert access to the Siemens plant in Karlsruhe, Germany.

Dick Caro

RCaro@Caro.us

The material listed below is recommended for further reading concerning both the attack mechanisms and the potential safeguards. These recommendations were made by Alex (Alejandro) Varga, Dennis Brandl, Hiten A. Dalal and myself:

1. Creating a weapon of mass disruption: Attacking Programmable Logic Controllers
2. On dynamic malware payloads aimed at Programmable Logic Controllers
3. GE's approach to cybersecurity
4. Process Explorer + VirusTotal (to check all processes with 50+ AV's)
5. If you cannot afford an Einstein to protect the network, try a canary
6. How can you activate the protection level with a password in the HW Config for an S7 CPU?
7. Bedrock Automation offers a very secure controller (but also very expensive), designed from the ground up to be secure.

Béla Lipták

liptakbela@aol.com

Process automation, controls boost production at yogurt plant

PC-based controls provide dcs capabilities, but they can also be implemented and reconfigured more easily than dedicated, hardwired, less software-based systems

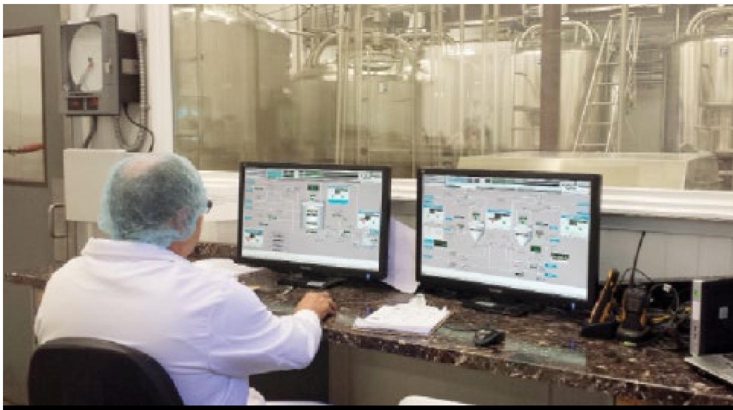
By Jim Montague, executive editor, *Control*

Sometimes success can be as challenging as failure. For example, too much demand can be as scary as no demand at all, especially when you're lacking production capacity. This is where process automation —lately in the form of PC-based control — can do its best work.

For instance, after discovering Paul and Grant Mathewson's Australian-style yogurt in Noosa, Queensland, Koel Thomae convinced the brothers to bring their family recipe to the U.S., and start Noosa Finest Yoghurt at Morning Fresh Dairy in Bellvue, Colo. Launched in 2010, the new company's full-fat product was originally intended for local Colorado consumers, but demand snowballed so fast that Noosa decided in 2012 to build a new, 25,000-square-foot plant just 50 meters from its original facility, so it could expand distribution to all 50 states. However, it also had to move quickly from producing its artisanal yogurt manually to automating production to keep up with its skyrocketing demand.

Along with measuring and metering ingredients by hand, Noosa's operators had been manually monitoring and documenting critical processes, setting up valve-transfer paths, dialing in mixer and pump speeds, and adjusting temperature control valves. Unfortunately, when problems occurred, they had to spend hours troubleshooting, and often could only speculate on the cause because they couldn't backtrack their data and pinpoint the difficulty.

"We had no expectation our product would take off so quickly, but when we picked up some large retail customers, we had to expand quickly to fulfill orders," says Wade Groetsch, Noosa's COO. "The only way we could increase capacity was to automate. We also saw demand increasing well into the future, so to meet production goals, we needed a system that would monitor the process, collect data and allow for easy future expansion. And we needed to track data for our quality assurance and for different regulatory reports required by the FDA."



CULTURE CONTROL
Figure 1: Noosa Finest Yoghurt migrated from manual to automated controls and increased production 300% with no added staff or resources, and reduced lost batches by 96% by adopting the PlantPAx process automation system at its expanded plant in Bellvue, Colo.

FILL MORE CUPS

To ramp up production and process controls, Noosa worked with Malisko Engineering Inc., a system integrator in St. Louis, Mo., and Denver, Colo., and member of Rockwell Automation's PartnerNetwork program. In just six months, they jointly designed and implemented an automated control system for yogurt production, clean-in-place tasks and utilities, and integrated Rockwell's PlantPAx process automation system, which includes a predefined process system library to enable Noosa's components to work together. This library consists of software-based, HMI process-object templates with PLC add-on instructions for many process-related functions and control tasks. Using an EtherNet/IP backbone to deliver real-time data throughout Noosa's plant, Malisko's team deployed PlantPAx servers on a VMware virtualized host and deployed thin-client HMIs in the plant floor. (Figure 1). Also, Microsoft's Active Directory domain controller was installed for user security, and it uses Cisco's VPN firewall for secure, 24/7 access and troubleshooting from anywhere with Internet access.

"The PlantPAx system-sizing tools coupled with the predefined library of process objects enables us to deploy projects more rapidly," says Dan Malyszko, operations director at Malisko. "The rich functionality of the library's HMI device faceplates allows users to configure and troubleshoot more efficiently, reducing the need to dive into complex PLC code for routine maintenance operations. Users can save approximately 30% on upfront integration costs by using software libraries such as those in the PlantPAx system."

Noosa reports its new automation system is easy to set up and operate, and allows operators to capture material tracking information, such as raw milk/cream receiving information, critical temperatures at specific process points, ingredient amounts, batch cycle times and CIP tracking, more easily. Information can now be retrieved to investigate process excursions, which saves troubleshooting time and expense, and eliminates much former guesswork.

This improved visibility into its production process has made Noosa's operations and overall yogurt process much more efficient. In fact, since opening its new facility, the company has increased production capacity by 300% without adding more staff. Likewise, when it started in 2010, Noosa's equipment could only fill one cup of yogurt at a time, but now its two automated lines can fill about 100 cups per minute.

"Our new facility allows us to produce more yogurt, but also produce it more consistently," adds Groetsch. "Our manual process had many inconsistencies and many times resulted in lost batches of yogurt. With the PlantPAx system, we've decreased lost batches by 95%."

Finally, because demand for its yogurt is continuing to accelerate, Noosa is presently working on another plant expansion, which it expects to finish by the end of 2014. Aided by the scalability of PlantPAx, this new plant will have a redundant, fault-tolerant server architecture. "As new equipment and process units are needed to support demand, Noosa can add more I/O, PAC controllers and servers without adversely affecting the base characterized architecture of the PlantPAx system," says Malyszko.

CAREFUL CARBONATION

Along with aiding the migration from manual to automated processes, PC-based solutions let users maintain much tighter control and tolerances in their applications.

For example, Allied Petro Chemical (www.alliedpetrochem.com) produces petroleum-based distillates at its facility in Alvin, Texas, just south of Houston. The facility has two main sections, including the refining side with two vacuum-distillation towers that separate petroleum distillates to produce naphtha, kerosene, diesel and residual fuel oil, and the additive side that has three reactor units where high-molecular-weight alkylates are sulfonated to produce Allied's SA-320, SA-470 and SA-490 additives. Following initial production, these additives are neutralized and carbonated to create neutral- and over-base calcium sulfonate products. However, sulfonation is a rapid, highly exothermic reaction, so its reaction mass must be continually cooled, and the amount of sulfur trioxide added must be precisely controlled to avoid side reactions and unwanted carbon from forming.

Previously, Allied controlled its refining process manually, but this was labor-intensive,

AUTOMATING AGRICULTURE
Figure 2: Repete developed its FLX solution with KEPServerEX software and an OPC server, which allow its conveyors, motors, grinders, mixers and other devices to communicate and work with unfamiliar PLCs in international applications.

increased potential for errors, and made it difficult to expand the firm's operations and business. Consequently, Joey Kessel, Allied's manager, researched several process control solutions, and selected Opto 22's (www.opto22.com) Snap PAC hardware and software mainly because control points could be easily mapped and changed in its PAC Control programming software. Specifically, Allied installed Snap PAC S- and R-Series controllers, I/O processors, I/O modules, PAC display software and a plant-wide Ethernet network.

Kessel reports that changing distillation from manual to automatic control delivered several benefits. "It's now easier to achieve and maintain the quality of the final distillate products," he says. "Instrumentation added to the control system makes extensive process data available for production and regulatory purposes, while new equipment monitoring and logging capabilities allow preventive maintenance that keeps downtime to a minimum. Having the new control system in place reduced the number of personnel needed to operate the plant by half. Operators are needed at the plant 24 hours a day, so this resulted in significant savings. This also gives staff time to fine-tune production processes, maintain equipment and scale up production."

CONTACTING, COORDINATING CONTROLLERS

Beyond enabling quicker reconfiguration and tighter performance, PC-based controls often can use more closely integrated network connections to achieve more efficient operations — and even help users break into new industries and markets.

For instance, Repete Corp. (http://repete.com) in Sussex, Wis., has been building and integrating automation and controls for agricultural milling applications for almost 50 years. These include process-specific controls and plant-wide automation systems for manufacturing fertilizer, mixing animal feed, batching and pelletizing pet food, and processing seed and other products (Figure 2). The company traditionally uses Rockwell Automation's PLCs and data servers, but when it recently began working with users outside the U.S., it encountered some less familiar PLCs and communication protocols, such as those from Siemens and Mitsubishi. It needed a way to interoperate with any control protocol, as well as prevent downtime that can cost $50,000 to $200,000 per hour, so two years ago it launched its FLX software, which interoperates with different controllers with help from Kepware Technologies' (www.kepware.com) KEPServerEX that uses an OPC server and supports more than 150 communication protocols.

"Our goal has been to become hardware agnostic, so our conveyors, motors, valves, pellet lines, grinders, mixers and other equipment can plug-and-play with different controllers, and allow us to deliver 100% tested solutions," says Wade Leverett, Repete's president. "Over the years, PC-based controls have outstripped PLCs, and these PC tools enable us to do regression testing at the push of a button and simulate solutions before we go to a customer's site."

Mike Peters, Repete's operations director, explains that FLX and its OPC server let Repete's devices communicate with different controls more easily, convert ladder logic instructions with fewer adjustments and handle customers' change requests much more quickly. FLX also helps operators schedule production runs by taking raw material and other input data, and then creating a unique plan for executing product formulas with users' available equipment and controls—much like enterprise resource planning software takes in orders. Finally, FLX also allows remote monitoring, diagnostics and control, so Repete can troubleshoot and service clients' systems without having to be on-site. Consequently, the company is presently building an average of six major integration systems per month, and its ability to communicate with almost any PLC is even enabling it to expand beyond its core focus on food production to serve new industries, such as recycling in Asia and cargo-handling in Europe.

"Every job is a custom job, and we still create many unique solutions, but FLX's software plug-ins enable us to pull components from our equipment library far more often and implement them faster with less programming and the right controls. Our software and OPC server also link seamlessly with other ERP and management executions systems," says Peters. "As a result, automation system installations that used to take five or six weeks to put together can now be done in just two or three weeks. In fact, we can simulate a full mill in one business day, and this means a lot less errors and time on-site than with traditional controls."

Jim Montague is the Executive Editor at *Control* and *Control Design*. Jim has spent the last 13 years as an editor and brings a wealth of automation and controls knowledge to the position. For the past eight years, Jim worked at Reed Business Information as News Editor for *Control Engineering* magazine. Jim has a BA in English from Carleton College in Northfield, Minnesota, and lives in Skokie, Illinois.