CONTROL ENGINEERING

DCS Migration:
Breaking the Last Bonds of Old Technology

CONTROL ENGINEERING

UNIFIED CONTROL MIGRATION

Lush green forests sweep grandly from the mountains to the ocean in the coastal states of Espirito Santo and Bahia, Brazil, about 450 kilometers north of Rio de Janeiro. What's unusual about these forests is that they're part of nearly 611,000 acres of eucalyptus plantations owned and managed by Aracruz Celulose, one of the world's leading producers of market pulp, which is shipped around the world to paper producers who make tissue, fine printing, writing, and specialty paper products.

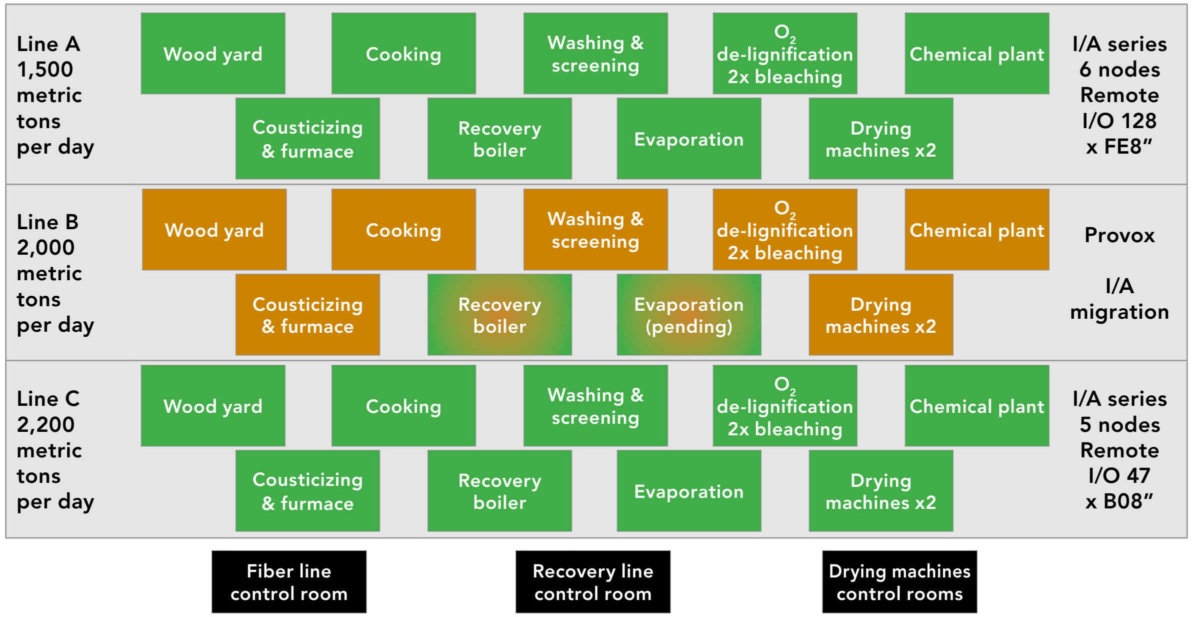
Maria Eunice Casulli,
Invensys Operations Management

The Aracruz pulp mill has grown to be the world's largest producer of bleached eucalyptus pulp and operates the world's largest single pulp production facility, producing more than 2 million tons of pulp per year. To support and grow that level of product, Aracruz has taken measured steps to bring all of its operations under a consistent process control and optimization strategy. Recent commissioning of its new Fiberline C marks a significant milestone in the mill's transition to a fully integrated production enterprise, in which all production lines are controlled from functional control points, and advanced process control is used to optimize everything from digesting to drying.

Aracruz built Fiberline C using modern, integrated control technology that eventually will run all mill processes. Its first line, Fiberline A, has been upgraded with these controls, as have the boiler and evaporation units of Fiberline B. Fiberline C is believed to be the world's first pulp operation designed and built with advanced process control (APC) and optimization technology.

The mill's progress to this stage is part of an ongoing process of capacity expansion and system upgrades, which started with pulp production via Fiberline A in 1976. At that time, Fiberline A was producing 400,000 tons of bleached pulp per year, under control of Foxboro PCI 100 pneumatic instrumentation. In 1988, Aracruz built Fiberline B, which expanded annual production by 600,000 tons, using Provox DCS.

ARACRUZ MILL DCS CONFIGURATIONS



Line A 1,500 metric tons per day: Wood yard; Cooking; Washing & screening; O_2 de-lignification 2x bleaching; Chemical plant; Causticizing & furmace; Recovery boiler; Evaporation; Drying machines x2 — I/A series 6 nodes Remote I/O 128 x FE8”

Line B 2,000 metric tons per day: Wood yard; Cooking; Washing & screening; O_2 de-lignification 2x bleaching; Chemical plant; Causticizing & furmace; Recovery boiler; Evaporation (pending); Drying machines x2 — Provox I/A migration

Line C 2,200 metric tons per day: Wood yard; Cooking; Washing & screening; O_2 de-lignification 2x bleaching; Chemical plant; Causticizing & furmace; Recovery boiler; Evaporation; Drying machines x2 — I/A series 5 nodes Remote I/O 47 x B08”

Fiber line control room — Recovery line control room — Drying machines control rooms

*FE8 = Field Enclosure 8 is an environmentally hardened enclosure that can be mounted in the field and has slots for 8 I/O modules.
**B05 = custom Brazilian protected cabinet with I/O modules and terminals in back-to-back enclosures.

In 1995, Aracruz modernized lines A and B, eliminating production bottlenecks while expanding capacity to 1.2 million tons per year. At Fiberline A, the original pneumatic control systems were replaced with the Invensys' Foxboro I/A Series. This control system was configured in a six-node local area network (LAN) with multiple application processors, user workstations, and an interface to programmable logic controllers (PLCs). As many as 125 field enclosures provided the I/O interfacing to more than 1,500 field instruments, using FoxCom communications protocol. In addition, InTouch human-machine interface software from Invensys' Wonderware was installed to create new process visualization screens for operator control of wood yard operations.

Unified Strategy

Because Fiberline A controls architecture was deemed effective, in 2000 Aracruz management used it as the basis for construction of Fiberline C and upgrades on other lines. The goal was to allow each line to operate independently and provide a unified control strategy and view into operations for better management of overall plant productivity.

This graphic shows details of processes linked to a DCS on the three lines prior to Line B migration.

Basic production processes are similar in all three lines. Logs arrive daily by truck or barge from the plantations. As needed, the wood is loaded into debarkers and chippers that feed each line. Chips are conveyed into stainless steel pulp digesters, where they are cooked with caustic liquors to form the pulp. Brown pulp stock is washed and screened before being bleached white and fed into drying machines. At the end of each drying machine, the “pulp blankets” are cut into rectangular sheets and baled for shipping. Wrapped bales are then transported by truck to a nearby port for shipping.

Different vendors supplied equipment for each step (see DCS configuration graphic), but all processes are integrated into a common control strategy managed under the I/A Series control system.

Flexible I/O Modules

I/A Series automation packages on Fiberline C consist of five network nodes with UNIX servers and Microsoft Windows NT workstation processors.

A Trident triple modular redundant safety shutdown system from Invensys’ Triconex business unit protects the oxygen reactor. Foxboro field instruments—including pressure, temperature, magnetic flow, mass flow, pH, and conductivity devices—interface with the system by means of the FoxCom protocol, using remote I/O racks located close to the process. Motor controls are connected via intelligent MCCs to as many as 25 Micro I/A Series nodes via Profibus networks, without using PLCs.

“The final step in upgrading the plant was completely changing the layout of three control rooms for the Fiberlines, recovery line, and drying machines to consolidate Lines A, B, and C,” says Renato Gueron, project manager. “This was necessary because Line A had Foxboro CRT consoles and monitors, while Line B had competitive CRT consoles and monitors, which meant that there would be no space to add Line C operating stations. They now all operate under one master control system.”Workstations with thin-profile LCD screens have now been installed in all three control rooms.

Retrofitting

Retrofitting controls on Fiberline B was simplified because of Invensys’ plug-in migration strategy, by which other processors and I/O cards have been exchanged with Foxboro I/A Series replacements of the same form factor, incorporating updated electronics circuitry. These I/O modules are functionally identical to ordinary I/A Series modules, but are repackaged to plug into most legacy I/O racks, enabling the switchover without moving any field wiring, minimizing production downtime.

At Fiberline B, the “plug-in” method has been used to replace the Provox systems that controlled boiler and evaporation units.

This approach helped bring the new line on-stream faster—and under budget—and it provides a path for future growth in production capacity, making it easier for all three fiberlines to use the same regulatory controls to support the advanced process control and optimization already underway for Fiberline C.

Author Information
Maria Eunice Casulli, Invensys Operations Management

END

SECURING LEGACY CONTROL SYSTEMS

Very few of the process control platforms operating today were installed with any cyber security protection built in. Most predate wide deployment of the internet. Can these systems be protected against today's threats?

Peter Welander, Control Engineering

Cyber security issues have taken center stage over the last few years, and their visibility seems to increase almost on a daily basis. New IT and industrial control system platforms are incorporating vastly improved security functions, but the problem for industry is that huge numbers of control systems predate these cyber security efforts, and many even predate large-scale deployment of

the Internet. Connections to those systems from the outside provide the means for hackers to get in and do all sorts of damage, unless barriers are put in place to keep them out. The question is, can old systems be adequately protected?

"Traditionally, a control system was purchased, engineered, configured, implemented, and pretty much forgotten about for the next 20 or so years," says Ernie Rakaczky, principal security architect for Invensys Process Systems. "In many ways that's still the mindset of the control community, but a lot has happened in the last five or 10 years. Many of those early systems had no capability to be connected to anything else. They were designed to do one thing in life: they open and close a valve or they measure a level, so the cyber world really doesn't play a role."

The problem is, the world didn't stay that way. With the growth of information technology in general, the desire to extract information and to provide connectivity to outside users grew too. Rakaczky adds, "At one point, a traditional control system was 100% focused on controlling a process. Now it's probably 50% control and 50% information exchange. When that started to happen, and we started to move data off the control platform to a historian or plant network or enterprise network, it was time to start adding some best practices, being more cautious, and putting some functionality in to protect yourselves."

Safe To Connect?

Some experts take the position that the only truly safe connection is no connection. "In almost all cases, proprietary systems had proprietary networks," says Kevin Staggs, CISSP, engineering fellow, global security architect, Honeywell Process Solutions. "Adding any connectivity puts them at a significant risk, because they're not even designed to protect themselves, and there is nothing to allow them to be protected. For those old systems, you must absolutely understand and know where those connection points are, and know what technology is used for those connection points. In a lot of cases those points will be historians."

But if maintaining an air gap is your main line of defense, the isolation needs to be absolute to be effective. "People tend to believe that isolated networks are secure, and put all their eggs in one basket, believing that because it's isolated it's secure," says Todd Stauffer, manager of process automation systems for Siemens Energy & Automation. "But there are many scenarios where people have an isolated network, but somebody brought in a memory stick from outside, or temporarily connected a laptop, or temporarily connected a network, and really messed up that isolated network. Unless you have the practices in place to make sure people don't bring memory sticks, CDs, or DVDs into an isolated area, then you need to have security on this isolated network or you're going to be very vulnerable when that does happen."

Understanding Multiple Generations

Old control platforms cover a long time span, with some still running that date back to the earliest DCS deployments. For all practical purposes, they can be divided into two broad categories: Proprietary networks and Microsoft Windows-based architecture.

Some that operate older systems comfort themselves believing that even if a hacker does break in, he or she simply will not know what to do with that obsolete technology. But is that really a protection strategy? John Cusimano, senior consultant for Exida likens that strategy to skating on thin ice. "If someone gets into one of the older systems, and they have knowledge of the system in terms of what the command structure is, I think it would be quite easy to violate it," he advises. "The distinction is that the intruder has to have a higher skill set to be able to violate an older system. But once you have access to it, you could probably execute any command you wanted."

The problem is that the population of potential qualified hackers has probably grown a great deal in the last year or so. Ken Pappas, security strategist for intrusion prevention system provider Top Layer warns, "The fear today, because the economy is what it is with companies laying off people in the thousands, they're now dealing with disgruntled employees that already have inside knowledge as to how these systems work. So if you put one-plus-one together, these people know how to get in the network, and they know what to do when they're in there, so they can cause a lot more havoc than the average hacker who just knows how to break into a network. It's not that the hackers got smarter, it's that we have a new class of hackers in post-workers."

Some users believe that once Windows moved into the plant in the 1990s, that it helped provide a more secure environment. Cusimano says this is not the case, but he "worries mostly about the systems that came out roughly 15 years ago, when Windows was first getting introduced into the control system world. There are systems still out there running Windows NT-based HMIs. That was the generation where systems were first starting to go open, but used those older versions of Windows where security was pretty much nonexistent. That's a generation in particular that needs to be looked at."

Staggs agrees, and advises, "Older Windows systems should not be connected to the business network. They absolutely must be compartmentalized, and you must understand what traffic has to flow from them into the business network. You must have a very tightly configured firewall, and if you can, you should flow that information through a more modern server. You can protect the more modern server, and it serves as a bastion device. Most of the time it's a historian, so get those upgraded and make them the most modern technology."

Old in this context means any Windows generation that is no longer supported. Windows 2000 is on extended support through June 30, 2010. Anything earlier than that falls into the unprotected category and will have no more security updates.

What Can You Do?

"Security by obscurity doesn't apply in the modern, interconnected situation," warns Sean McGurk, director of the control systems security program (CSSP) for the U.S. Department of Homeland Security (DHS). "We've done analysis of vulnerabilities at facilities for years now, and the vast majority of those vulnerabilities, about 46% of them, are in the DMZ (demilitarized zone) between the process control network and the business network. That's an unacceptably high ratio when you think that's the area where connectivity is most important. You need to look at ways to lock down those communication channels."

True enough, but easier said than done. Protecting something that was never intended to be protected or that has passed out of manufacturer support is not easy. Todd Nicholson, chief marketing officer for Industrial Defender explains, "The challenge with this environment is that everybody certainly has a need for a secure perimeter, especially if you're connecting to the outside world, but the legacy nature of this environment—hardware, software, operating systems—is challenged because these environments cannot utilize modern security technology like anti-virus at the plant system level without dramatically impacting performance and availability. You have a very fragile environment, and you have to think about that when laying out your defense strategy."

Nevertheless, there are strategies. Going into extensive detail is beyond the scope of this article, however there are resources to help start the process in the sidebar. Most strategies begin by analyzing your current architecture in detail, and cataloging all software running on your control networks. Finding all the outside connections is another major step, and is often an eye-opening experience for companies that have lost track over the years. Staggs advises beginning with your historians and upgrading those, but don't stop there in your search for connections. He suggests, "To find potential connection points, you should be looking for OPC, serial gateways, modems, safety system connectivity, Modbus serial or IP, and even Foundation Fieldbus or Profibus."

Time To Migrate

Are cyber security concerns enough to drive a migration? Ultimately, the answer may be to migrate to a newer platform that has a higher level of protection. Of course that's no small task, particularly during an economic downturn. "I think most of the engineers that are actually running the system understand the risk, but whether they can quantify the risk and give it as a reason to migrate is another issue," says Ken Keiser, migration marketing manager for Siemens Energy & Automation.

"I don't know if they can articulate it to management. It's easier to say, 'It doesn't work any more and it will affect production,' rather than try to articulate that it's a security issue—although they do realize that risk," Keiser says. "It helps that people tend to want to upgrade one of the most vulnerable parts of the system first, and that's the HMI. It's easier to connect to a controller from the top down, rather than trying to attach leads to a remote instrument and send it the other way."

J.T. Keating, vice president of marketing for CoreTrace, sees migration as too slow an approach. He advises, "While cyber-security concerns are definitely an appropriate rationale for upgrading older systems, it's usually unrealistic to contemplate replacing these systems, at least in any practical timeframe. Security means now, replacing means next year. Since these are often critical systems, replacing them must be a carefully crafted process, and in 2009, fiduciary requirements often mean making do with what you have, instead of ripping and replacing what could amount to large sections of infrastructure. Across the energy sector the sentiment is to 'make do with less.' Hardly the ideal for increasing the security posture of these critical systems, but that is the reality."

Will federal regulation force a large scale change? What about all the new NERC (National Electric Reliability Corporation) requirements? McGurk points out that 80% of critical infrastructure is in the private sector, and even NERC only covers a relatively small portion of the larger energy industry. He acknowledges a sad reality, "Frankly, there's been the mindset for quite a while to find ways to avoid compliance as opposed to recognizing the need for security."

The Human Element

So far the discussion has largely been about technical solutions. But there are human elements as well. Keeping a system secure requires that your people participate in the process. One people-related problem common with older systems is a lack of documentation. After a system has been in place for a decade or more, like other parts of the process, there may not be current documentation that reflects what is actually operating. It's common to find vulnerabilities resulting from undocumented system changes.

Nicholson observes, "Not only in the plant environment but in enterprise IT, change management is a very large challenge. For example, when you open up a port to allow access for someone from the outside, how do you effectively track and monitor the changes to the system? Someone might forget about having a port open here or there that exposes the system."

Matt Luallen, co-founder of Encari and Control Engineering cyber security blogger, stresses the importance of procedures when dealing with problems. He says, "Effective information security programs must consist of sufficient and effective procedures for handling incidents." These include event identification, containment, root cause identification, eradication, recurrence prevention, defined call trees, tie-ins into change management documentation to identify approved and unapproved changes, and the appropriate escalation and reporting procedures, he says.

"We typically see modifications to control system software and hardware go undocumented, unnoticed, and subsequently not centrally approved," continues Luallen. "This in its own right is a security violation; however, this is a scenario that is not easily solved solely through the use of technology. In most cases, the PLCs, RTUs, relays and other control system hardware and software do not have a capability to ensure an approval process for control modifications."

Procedures are important, but people have to understand their role in keeping the plant safe. The DHS reports that social engineering is one of the biggest attack vectors. McGurk laments, "How often do we see vulnerabilities and exploits that are conducted as a result of poor operational practices because people don't understand the need for security."

Marty Edwards, Idaho National Laboratory DHS CSSP manager, outlines the kind of cultural change that needs to happen: "One of the biggest challenges we have in security—whether it's in control systems, or IT, or physical security—is creating that security culture, and you can do that regardless of the vintage of the equipment that you have. It's your personnel. It's your training. It's the culture that they operate in."

From a safety perspective, industrial and processing areas have had that culture for some time, says Edwards. "You don't do anything in a plant without thinking about what the safety ramifications are," he says. "We must instill that same culture, so that before I do anything, I think about the security ramifications. Should I post a network drawing at a user group conference that contains all the most intimate details of our control system? That's a change that everybody can make immediately, and it costs a lot less than replacing equipment."

Author Information
Peter Welander is the process industries editor.
Reach him at PWelander@cfemedia.com.

DHS Recommended Resources

Marty Edwards, Idaho National Laboratory DHS CSSP manager, offers a few recommendations for helpful resources. His first suggestion is to begin at the main Control Systems Security Program Website: www.us-cert.gov/control_systems.

He also suggests the following two specific publications relevant to legacy systems:

Recommended Practice For Patch Management Of Control Systems

"A key component in protecting a nation's critical infrastructure and key resources is the security of control systems. The term industrial control system refers to supervisory control and data acquisition, process control, distributed control, and any other systems that control, monitor, and manage the nation's critical infrastructure. Critical Infrastructure and Key Resources (CIKRs) consist of electric power generators, transmission systems, transportation systems, dam and water systems, communication systems, chemical and petroleum systems, and other critical systems that cannot tolerate sudden interruptions in service. Simply stated, a control system gathers information and then performs a function based on its established parameters and the information it receives. The patch management of industrial control systems software used in CIKRs is inconsistent at best and nonexistent at worst. Patches are important to resolve security vulnerabilities and functional issues. This report recommends patch management practices for consideration and deployment by industrial control systems asset owners."

http://www.us-cert.gov/control_systems/practices/documents/PatchManagementRecommendedPractice_Final.pdf

Securing Control System Modems

"This recommended practice provides guidance on the analysis of methodologies for evaluating security risks associated with modems and their use in an organization. This document also offers useful methods for creating a defense-in-depth architecture that protects the system components that use modems for connectivity. It is assumed that the reader of this document has a basic understanding of vulnerabilities associated with modem and modem communications, as this information is available from other sources."

http://www.us-cert.gov/control_systems/practices/documents/SecuringModems.pdf

Author Information
Peter Welander is the process industries editor.
Reach him at PWelander@cfemedia.com.

END

UPGRADING CONTROL: MIGRATION OR EVOLUTION?

At a recent automation supplier user group, a speaker cited an interesting statistic. He said that 50% of the DCS (distributed control system) platforms running process plants today are at least 20 years old. Knowing that, it isn't hard to understand why control system upgrades are on many peoples' minds as companies face growing cost and competitive pressures.

Peter Welander, Control Engineering

Should you be looking at replacing your control system simply because it's in the half that's more than 20 years old? Not necessarily, any more than you might want to think about trading in your 1987 car. Your aging DCS may regulate your process perfectly well, but like an old car, it can become maintenance-intensive and certainly lacks some of the capabilities of newer designs. Even if you decide those new capabilities aren't all that important, eventually parts become harder to find, and keeping the system going gets costly.

While age-related problems are certainly a compelling argument for upgrading a system, functionality issues can also enter into the discussion. Even newer systems may not have some of the functions that could create value for your business.

There are two main drivers for control system upgrades: obsolescence and functionality needs.

The first and most powerful driver that pushes change is obsolescence. When a platform is failing and the original provider no longer supports it, the risks of leaving it in place become too high. Obtaining replacement hardware eventually becomes problematic, leaving users to depend on parts recyclers and eBay. If part of a system goes down and there are no replacements, a whole process unit can grind to a halt.

Still, some plant managers have to learn the hard way. "It's very difficult to build a business case based only on obsolescence," says Mike Vernak, manager for Rockwell Automation's legacy DCS migration program. "Plant managers tell their plant engineers all the time, 'If your system's working and we're not experiencing any downtime, I can't justify a capital expenditure based on obsolescence.' Of course, if you are experiencing downtime, the ROI is easy to calculate. But it's hard to calculate it based on no downtime."

While unreliable performance is the most obvious problem, moving toward obsolescence can have more subtle effects, including knowledge erosion. "Companies are finding it difficult to maintain technical expertise for these 20- or 25-year-old legacy systems," Vernak adds. "The OEMs especially don't have expertise, either because of attrition or retirements. Kids coming out of colleges today that are 22 or 24 years old have absolutely no idea about that technology. I hear things like, 'That system is older than I am. They didn't teach me this in college.' They don't have a clue how to work on it. It's also expensive to maintain for training. I've seen companies that have multiple disparate DCS and PLC systems in a single plant. I can't imagine how much cost that must be every year for the plant manager to maintain multiple folks for multiple control systems."

The second driver that pulls change is functionality. A platform does not have to be all that old to lack specific functions that might be very helpful. For example, a system that does not have the I/O capability to handle HART diagnostics will probably not be able to support an asset management program. Others may not have the connectivity to support growing integration with enterprise level systems.

John Murray, ABB global business development manager for control systems evolution, says his group did a survey on what motivates companies to upgrade control platforms. "It surprised us that a very significant number, over 50%, said improving operator performance or maintenance practices were reasons that they were considering upgrades. We see that a lot today, as people recognize that's where they have to get the step improvement in their business. The term is overused but it's really about operational excellence. Solutions like asset management, information management, and data mining can really give you a competitive advantage if used properly. What we call a traditional control system has to be enhanced with these capabilities," he says.

Vernak agrees with that assessment and adds: "Most customers are migrating not because of obsolescence, but because of lack of performance from their systems. It doesn't necessarily mean it isn't controlling the process. It means that they aren't able to get data that they need out of the system to be able to make better decisions.

"Because of the proprietary nature of the system, it's hard to get data out or to be selective with the data they can get. These systems do not interface well with modern IT systems, with modern historians, etc. Many aren't capable of connecting to expert systems that allow them to do advanced process control easily or cost effectively. It's a lack of functionality."

Older systems were designed to function in greater isolation, so cyber security is often rudimentary or nonexistent. "A lot of people think, wrongly, that legacy systems are safe because they're legacy systems," says Ken Keiser, Siemens migration marketing manager. "When it was first installed, that system might have been completely isolated. But as time goes on, maybe someone put in a modem line somewhere, or a link to an intermediate historian and that historian happens to be on the Internet where they didn't think about the intermediate connection. You never know how something is connected after a 20-year period of time."

Justifying Your Needs

The first step in any upgrade project is figuring out what you need, in as specific terms as possible. Some answers may be very obvious but others that are equally important may require some probing. One of the downsides of remaining with an old system is that you don't realize how technology has progressed. The result is that you may not think to ask for some types of functions because you don't know that they are even available.

"Everybody wants to improve profit," says Murray. "But you have to work with customers to determine how they want to achieve that. The better a customer understands what problem he wants to solve, very specifically, we will come up with a much better solution. Whether it's a new feature, new capability, or just adding controllers to provide better availability, once they understand that, they get a real sense of what those improvements are going to be. Then they can quantify that financially in terms of benefits they'll derive or cost reductions, and that helps the cost justification process.

"If you have some grandiose target or scheme, then you're really scratching for 'how do I justify these expenditures?' It's important to drill down into the details for everybody's sake to understand the problem and get the best solution."

No plan is complete without a financial justification. Some situations will be very clear and direct. Replacing an old system that is waiting to fail and cannot be repaired should not be difficult to sell to management, particularly if its failure will halt production.

The difficult part may be convincing those responsible that the failure could be imminent. More subtle changes can be challenging. Your ability to place a value on an upgrade that adds some new functionality could depend on the extent to which you are personally convinced.

Marjorie Ochsner, senior product manager, DCS platform migrations, for Honeywell Process Solutions, offers some useful questions to ask yourself early in the process:

- What's your cost of doing nothing, and what are the expected benefits of doing the migration?
- How much is that unplanned shutdown costing you?
- What is your actual cost of maintenance for this older system?
- How much are you paying for that replacement hardware at the parts recycler or eBay?
- What is the cost of inadequate response?

Then there's the positive side: What are the added benefits of a new system? What's the value of renewed operator effectiveness? Are there advanced control strategies that you can bring in? What is the value of bringing in those HART signals from the field? "We look at the answers to those questions and have a very detailed analysis that we help our customers with," says Ochsner.

How Drastic A Change?

Control platform upgrades can range from small incremental changes to full rip-and-replace projects. Typically, the older the system, the more drastic the change. Older platforms were more integrated and not designed with open architecture which makes changing one part of the system more difficult. More modern approaches tend to be modular, allowing for evolutionary improvements.

Frequently companies begin with the HMI, and it's more than just about graphics. The HMI is the main connection point for the data pipeline, providing an interface to higher level systems and a mechanism for more advanced control strategies.

"The HMI is the component in a DCS that is made obsolete first, due to internal or external forces," says Siemens' Keiser. "When customers approach us, they are coming because they have a specific problem with the control system. It may be a problem in the controller, but more likely it is a problem viewing the data in the controller, so it's really an HMI problem."

Keiser says an HMI is not all that difficult or expensive to replace, so it's a relatively easy migration to make for a first step. "You have a new look and feel, but the same exact equipment beneath it. As far as the process is concerned, it has not changed, the process control has not changed, so all of that equipment, knowledge and know-how is the same," he says.

In some cases, a migration may involve a newer system from the same supplier, assuming that company still exists in a recognizable form. Other times it may be a more drastic change, moving to a completely different platform.

"When you get to the point that a system can't meet your business needs, a more radical solution may be the only answer," says Mark Bitto, ABB global business development manager, control systems evolution. "But even there, you should still look at what kind of investments you can protect. Can I leave the wiring in place? Can I leave the terminations in place? What costs can I eliminate best through whatever solution I have?"

A full change is traumatic in many respects, and companies should not take it lightly.

"There has to be a very critical reason why customers don't want to proceed down an incremental migration path," says Keiser. "They're saying, 'We're done with this vendor. We need to see what's out there.' In one case I can think of, the customer was considering a stepwise migration, but the more they looked at, they realized they had to take the big step. Smaller companies are more likely to do that. Some huge chemical company might not, preferring a lower-risk approach."

No Time To Shut Down

Still, the extent of a change may be limited by production requirements for a plant. Full rip-and-replace projects invariably involve some downtime, whether it's planned or not. A more incremental change can reduce this risk.

"Shutting down a process is often more expensive than keeping it going while you're doing the upgrade," Honeywell's Ochsner suggests. "So most of the time owners do it incrementally on a unit-by-unit or controller-by-controller basis, laying the foundation with the networking and everything else so that they make a fairly smooth cut-over.

"It helps to do things from the top of the architecture on down, replacing the HMI first, then the networking, then the controllers," she adds.

Planning, Executing Changes

Once you have decided to proceed down a specific path, it's time to lay out the details. "The first step is always planning," advises Oschsner. "You've got to know what you have, upfront."

The first thing Honeywell looks at is the state of documentation, "which, sadly, is not usually in the greatest shape," says Oschsner. "We want accurate and complete documentation upfront, even to the point of knowing what model numbers of controllers and I/O you have in the field."

Graham Bennett of Invensys Operations Management has been involved with many projects and offers his suggestion for sharing responsibilities with the customer.

"We compile a work activities breakdown as a standard procedure," Bennett says. "It lists pre-migration, migration, and post-migration items. We have action items that leave no stone unturned. Everybody has items and we follow it to the letter. One of the things is to confirm functionality of any third-party protocol."

The ultimate benefits of a well-thought-out and well-executed upgrade project can be huge. Improvements of control capabilities, data mining, operator interface, feedstock utilization, product quality, and many other areas are all possible. But all of them depend on an intimate knowledge of your process, combined with effective analysis and planning.

Mining/Chemicals Case History: Uniting Disparate Systems

Teck Cominco is a large mining, metals, and chemical company based in Vancouver, Canada. Its Trail facility in central British Columbia, includes one of the world's largest fully integrated zinc and lead smelting and refining complexes, including the Waneta hydroelectric dam and transmission system. Trail's metallurgical operations produce refined zinc and lead along with a variety of specialty metals, chemicals, and fertilizer products. The Waneta dam provides power for the facility, local customers, and the U.S.

Rob Zwick is superintendent of process control, and he has been involved in an effort to move the entire facility to one common platform. As he describes it, "We have five major plants. We ended up with five platforms: ABB, Fisher Provox, Honeywell TDC 2000, Foxboro, and a PLC/Wonderware. One of the things we've been working toward is consolidating on Foxboro [I/A Series control system from Invensys Process Systems] as a common platform as best we can.

"We have migrated away from the Honeywell. We're migrating away from the Fisher Provox, and by the end of this year, the Foxboro system will handle about 75% of our I/O," Zwick says. "All our plants are coming to an identical platform with Foxboro hardware and software."

Maintenance and training problems were a major driver toward convergence. Parts availability for the oldest platforms had been pushing a change, as the company cannot risk unscheduled downtime. Of course the pressure to maintain uninterrupted production has not made the migration efforts any easier.

"We're on our fourth migration now," Zwick notes. "Our operations certainly run 24/7, and all the plants are inextricably linked, so we have to coordinate shutdowns between plants very carefully. We do have regular maintenance shutdowns for a couple hours here or there on a monthly basis, and we look for those to do the migration."

Making The Decision

During the evaluation phase, Zwick and his colleagues considered many possibilities and came to some interesting conclusions. "Thinking about the platforms that I've been exposed to, the functionality is really becoming hard to distinguish," he reflects. "So, to justify a choice on technical advantage of one DCS over another is actually getting pretty difficult."

All companies have been working at improving and modernizing their hardware and software, Zwick says. "Foxboro has a good installed base with mining and metals in Canada, whereas others don't. Others have done better in oil and gas. It strikes me that differences are more historical than any advantages of features in a particular industry sector," he says.

Legacy Connections

One of the things that has helped facilitate the changeovers has been special Foxboro I/O cards that provide an interface between the old and new system. Graham Bennett, migration consultant for Invensys Process Systems describes the approach:

"We retain all the field wiring up to and including the marshalling cabinets, and then the interface cabling between the marshalling cabinets and the actual I/O of the legacy vendor. We take the connection off and replace the card one-for-one using a new card made to the form factor of the legacy vendor," he says.

"Having the one-for-one lineup, there isn't any configuration change needed, and every point on the I/O from the field lines up with the original card layout," Bennett adds.

Zwick is getting ready for his next major move. "It's a big one," he says. "We'll have a 12-hour window, but it's 4,000 I/O points, so we'll need all of it. Downtime on this plant is $100,000 per hour," he says.

Utilities Case History: Choosing The Right Tool

Colorado Springs Utilities is a municipally owned utility group providing electric power, gas, water, and wastewater services to residences and businesses. The electric power division operates a small fleet of coal-fired units, several hydroelectric plants, and is a co-owner of a gas-fired combined cycle turbine plant. Additionally it operates the 54 MW George Birdsall plant, with a gas-fired conventional boiler for 12-hour emergency and peaking capacity.

The Birdsall plant was built in the mid-1950s and still has its original boiler and turbine. Consequently, it lacks the efficiency of newer plants and no longer operates as base-loaded capacity for cost reasons. However, with growing power demand in the area, its operating time is increasing each year. Brent Richardson is plant manager, and recently brought the facility through a control system migration.

The plant had been running with a Rosemount RS3 DCS since about 1991, but Richardson reported that they decided to look for an alternative when he received word that the platform was into its final decade of OEM support. Given that Birdsall is not a very large plant with fewer than 150 I/O points and straightforward control strategy, Richardson and his colleagues decided to explore a variety of options.

"We were familiar and comfortable with DCS, for its power and speed," says Richardson. "We first set out to look at DCS platforms, including Delta V. Our Ray Nixon generating plant has an ABB system, so we considered that. We also looked at our water department. It is doing all its process control with Allen-Bradley ControLogix PLCs. Once we looked at the power and speed of the new PLC based system, we found that it was actually about 10 times faster than what we were controlling the units with right now."

The idea of sharing the same system as the water department had considerable appeal, and serves as a prototype for retrofits that are anticipated at the hydroelectric plants within the next four years.

"There were numerous systems that could have done the job," Richardson adds. "We want a system that can control our entire fleet, including the hydro plants. The PLC system gives us what we need here, and will integrate with all our other facilities. As soon as I put in my system, I had the whole intelligence of the water department on the ControLogix platform, since they were standardized on it. I can use their resources, including five or six trained I&C technicians and even spare parts. I'm no longer stuck on a standalone platform. Having those resources available brought huge value to us."

Author Information
Peter Welander is the process industries editor. Reach him at PWelander@cfemedia.com.

END