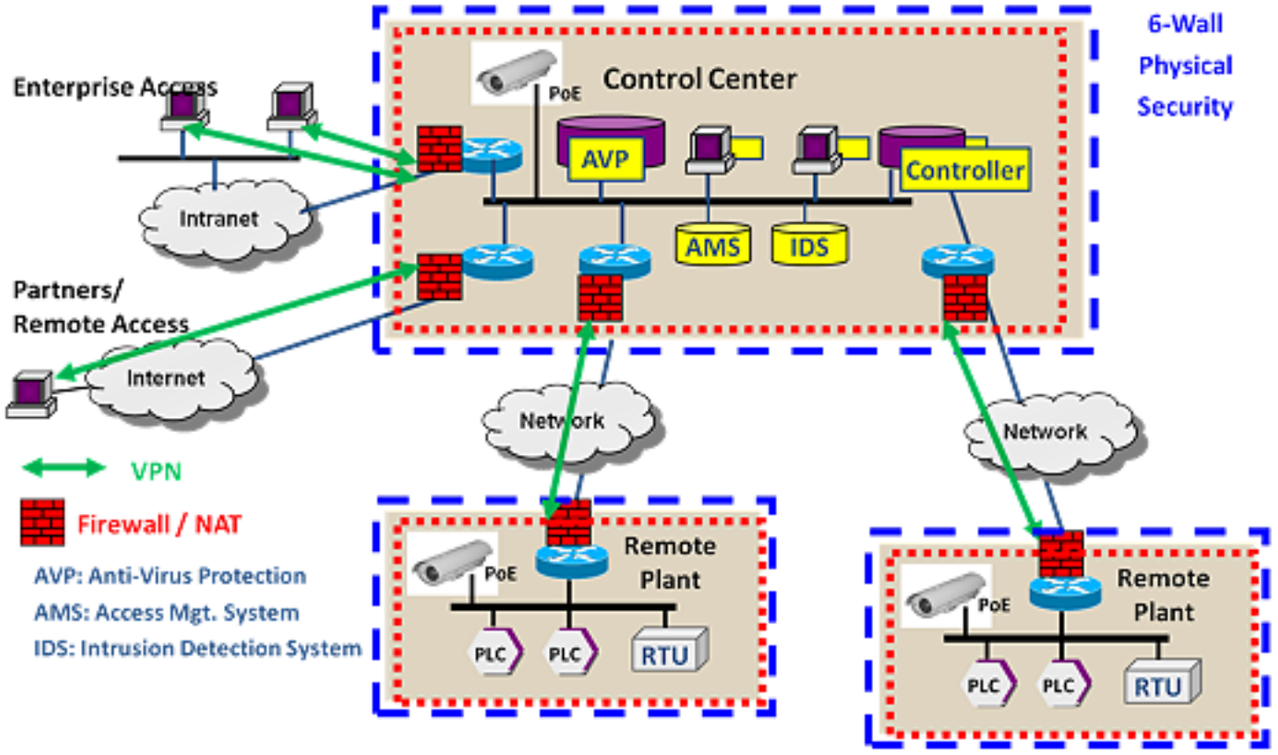
Cyber Security

Table of Content

GarrettCom®: Industrial Networking at its Best™.

GarrettCom is an industry leader in providing networking and cyber security solutions for challenging industrial environments, including power utility substations, video surveillance, transportation, industrial automation, and mobile networking applications in trains, tanks and other environments subject to shock and vibration. The Magnum line of Ethernet switches and routers provides a comprehensive industrial network architecture encompassing a switched Ethernet core, distributed edge devices for both Ethernet and Serial protocols, and secured connections to various WAN services. GarrettCom offers one of the broadest selections of hardened switches and routers, with associated cyber security networking and solutions software to industrial facilities around the world. The company's product line is noted for its configurability and ease-of-use GUI-based management software. GarrettCom also offers the widest breadth of PoE switches in the industry, designed to network even the most remote video security and access control products.

GarrettCom is led by Frank Madren, President since 1992, with more than 30 years experience in the computing and networking technology industry. Executive Vice President and CTO Lee House brings more than 20 years experience in engineering management, product design, engineering and R&D in telecommunications and networking companies. Vice President of Sales Burt Hadlock brings over 25 years of technology sales and management, most recently in the cyber security industry. The illustration below illustrates GarrettCom's Defence in Depth networking topology for industrial communications.
For more information see www.GarrettCom.com.



Control Engineering Cyber Security Bloggers Puzzle Over Recent Industrial Control System Security Assessment Survey Results.

01/01/2010

Matthew E. Luallen, CCIE, CISSP, GIAC, and Steven E. Hamburg, PE Encari

Nearly 200 responses were received to Control Engineering 's Industrial Control Systems Cyber Security Assessment Survey that commenced in November 2009. While some trends from the responses were expected, others were quite surprising. This article will provide our analysis of the responses, starting with simple observations and concluding with analysis of less expected responses and trends.

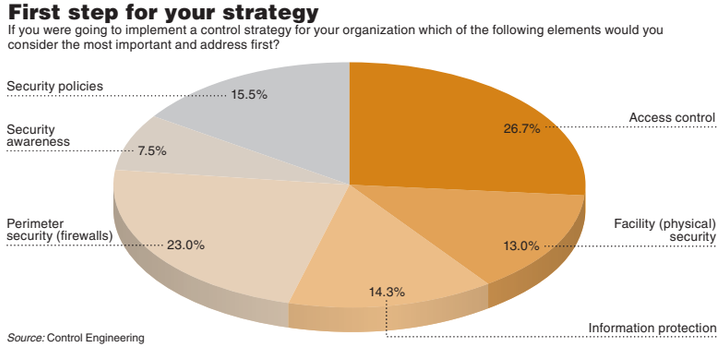
The first surprise was that 24% indicated they do not believe there are any threats and risks associated with their information control system that could affect their business operations. This seems very puzzling since most organizations operate with the understanding that there is no such thing as 100% security. In an environment where industrial control systems are becoming more dependent upon increased connectivity, including the Internet and remote control capabilities, we expected nearly a 100% response acknowledging the presence of such risks. The most prevalent cyber security concerns expressed by nearly 20% of respondents acknowledging the presence of disconcerting risks were viruses and malicious software.

Another very surprising observation is only 53% indicated they are an "organization involved in an industry where you are compelled to implement specific information control system protections." That leaves 47% that are not compelled to implement specific information control system protections. For the same reasons mentioned above regarding perceived risk, we expected a much higher number of responses indicating an urgency to implement specific information control system protections.

Answers provide a mixed bag, but some basic security concepts seem to be soaking in.

It was also surprising to see that only 50% indicate that their organization has an operating computer emergency response team to detect cyber security breach attempts and successful cyber security breaches. We find this odd in an environment where the number of cyber security threats facing industrial control systems is extremely high and has been growing dramatically in recent years. Another unexpected trend is 22% indicated they have never performed any type of vulnerability assessment. Encari recommends that organizations perform vulnerability assessments at least annually, which is reinforced by approximately 65% who indicated that they have conducted a vulnerability assessment within the past year. This has been accepted as a best practice since the cyber security threat landscape and infrastructure environments continuously change. In addition, the most prevalent industry change recently has been increased cyber capabilities and connectivity thereby necessitating such assessments. If sufficient in scope and effectively executed, they can yield strong insight into an organization's industrial control systems cyber security posture.

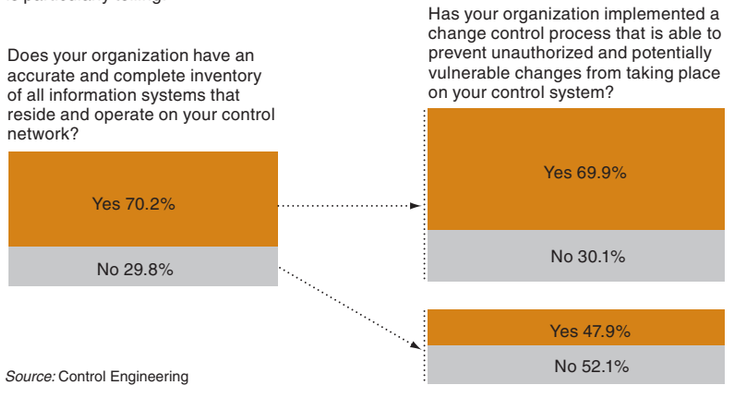
Along this same line, we weren't surprised to see that only 46% indicate that they have contracted the services of an external firm to conduct some form of a vulnerability assessment. The reality is that an organization's internal assessment capabilities can rarely match the skills of cyber security consulting firms whose core competency is performing



such assessments. When planned with an effective project scope, an assessment can be financially viable and provide profound insights into organizations' cyber security postures. Well-performed assessments reduce overall operating costs similar to preventive medicine or Taguchi's model of building quality (and security) in to the design. Organizations that maintain internal capabilities should consider contracting a consulting firm at least every two years, while organizations that do not have an internal capability should consider contracting a consulting firm annually.

Comparing critical answers

Sometimes the answer to a followup question is particularly telling:



Source: Control Engineering

Protecting Information

We were pleased to see that 75% indicate that their organization either has already implemented or is deploying an information protection program. While not specified in the responses, we have a high degree of confidence that a majority of the respondents are currently implementing information protection programs. Further, based upon what we have encountered in numerous organizations, we suspect that many of the information protection programs implemented are likely insufficient. This skepticism stems from the difficulty of implementing such programs for industrial control systems and general corporate information. Statistical evidence from the Privacy Rights Clearinghouse bears this out. Organizations generate a plethora of information that exists in many forms, including digital, hard copies, and verbally. In order to establish an effective and sufficient information protection program, it must address and apply protective controls for all sensitive information usage scenarios. For example, how does the program protect sensitive information:

- Sent via email;
- Stored on USB thumb drives and technician laptop computers;
- Faxed to a vendor;
- Printed by a network printer;
- Residing in a database; and
- Communicated verbally?

Some answers show contradictions. Almost half the people who say they have no system inventory still claim a change control process.

How do you ensure that all information subject to the information protection program is labeled with its appropriate classification (e.g., "confidential," or "secret")? We have worked with many organizations that have established sufficiently comprehensive information protection programs but have struggled with implementation.

Security First Steps

Given that we have encountered many organizations that have experienced challenges with maintaining an accurate and complete inventory of all information systems that reside and operate on control networks, we were surprised to see that 70% indicate the contrary. However, later in this article there are trends we noticed that may challenge the thought processes applied toward the responses.

It was interesting to see a somewhat uniform distribution of responses regarding the issues organizations would address first regarding the implementation of a control strategy (see pie chart graphic):

- 27% access control;
- 23% perimeter security (e.g., firewalls);
- 16% security policies;
- 14% information protection);
- 13% facility (i.e., physical) security; and
- 7% security awareness.

Since many cyber security incidents historically have resulted from human error, malicious and disgruntled employees, users with authorized cyber access, and lack of security awareness, we hoped to see a greater number of responses pertaining to security awareness. Unfortunately, it has been common to encounter organizations neglecting security awareness as a part within its overall industrial control systems security programs.

Other Key Results

Several other notable findings of the survey:

- Of respondents indicating concerns regarding potential inappropriate information disclosure, 31% have not implemented an information protection program.
- Of respondents indicating concern regarding potential exposure to viruses and malicious software, 29% are operating in the absence of

a monitoring capability to detect security breach attempts and successful security breaches.

- Of respondents indicating concerns regarding risk associated with cyber security threats, 48% are operating without a computer emergency response team, and 19% have never performed a vulnerability assessment.

- Of respondents indicating they have an accurate and complete inventory of all information systems that reside and operate on their control networks, 30% are currently operating with no change control process that is able to prevent unauthorized and potentially vulnerable changes from taking place on their control system.

- Of respondents indicating they have monitoring capability to detect security breach attempts and successful security breaches, 70% say they also have an emergency response team. Less than 5% have the emergency response team but no monitoring capability.

Comparing critical answers

Sometimes the answer to a followup question is particularly telling:

Source: Control Engineering

Responses are split on monitoring capability, but those that do tend to have the next logical stages in place as well.

The various combinations of responses noted in these points indicate a lack of maturity of the responders' industrial control system cyber security programs. This is an indication that these organizations are likely addressing cyber security concerns in isolation versus in the context of a holistic cyber security strategy. For example:

- How can you effectively address concerns regarding potential virus and malicious software exposure without monitoring capability?
- Why would you operate without a computer emergency response team, or why would you not perform a vulnerability assessment if you were concerned about risks associated with cyber security threats?

- How can you claim to have an accurate and complete inventory of all information systems that reside and operate on control networks without a change control process?

Today's reality is that we have a long way to go to understand and sufficiently protect our digital world to ensure continuing safety of the electronically controlled physical world. We are at a crossroads in time that requires us to push harder for resources to fix the problem and ensure that those resources are properly aligned with the most appropriate solutions. Every environment is different but the ultimate goal is the same: safe and reliable control of an efficient system. Now it is your goal individually, your company organically, and your industry collectively, to identify the appropriate path forward — a path that will continue our prosperity safely. We hope that our ongoing articles focusing on applying security defense-in-depth to industrial control systems will help achieve this ultimate goal.

Author Information
Consultants Matt Luallen and Steve Hamburg are co-founders of Encari and write the Industrial Cyber Security blog for Control Engineering.

What Do Process Control System Owners Worry About? Here Are Some Cyber Security Concerns Sent In By Readers In A Recent Survey.

12/22/2009

Peter Welander

In the January issue of Control Engineering , there will be an article that examines the results of a recent industrial cyber security survey. One question asked, "Does your organization believe there are threats and risks associated with your information control system that could affect your business? If Yes, what specific risks do you suspect / know exist?" Respondents had the opportunity to write in remarks. Looking at those, the results are very widely scattered, but there are a few that appear with some consistency.

- Typical network troubles, such as viruses, Trojans, spam, worms, spyware, phishing, and other malware are mentioned frequently.

- Internal attacks, either inadvertent or deliberate. The term "disgruntled (ex-)employee" came up a number of times.

- Transfer of malware or proprietary data via a thumb drive or a careless contractor's computer.

- Loss or theft of proprietary information. For example: "Company records, instrumentation values, and status are all at risk." "Loss of intellectual property." "Data safety comes to be a big issue. Many business plans will lose their value if the information is revealed before it's implemented."

- Problems that could disrupt or shut down control systems. For example: "We are not worried about starting, stopping equipment, or changing set points, just unknowingly overloading networks and/or stopping processors." "An intruder could flood the control network with messages such that the control system bogs down." "Spam is a threat as it clogs the information'superhighway.'" "Outside attacks meant only to snoop a network can stop a processor."

While most responses were brief and general, there were some that were more detailed and specific:

"Significant vulnerabilities within the open systems world based on Microsoft technologies have presented countless risks to the control systems user. This, coupled with a flood of wireless products from vendors that do not seem to place a high priority on cyber security, present today's control system user with enormous risks of an attack on their key plant assets. This is further compounded by vendors' unwillingness to openly document their own vulnerabilities and how to utilize proven countermeasures to minimize your exposure to these risks."

"1. Virus, worms, hackers. 2. Internal or external unauthorized modification or deletion of data. 3. Unauthorized viewing/theft of information. 4. Environment damage or harm to humans. 5. Interruption of normal operation of control system or safety system. 6. Loss or theft of product."

"Internal data or file damage by employees for malicious reasons. If there is a way to get at it, they will. Access to online programming software by unauthorized personnel could cause a machine motion function to occur, causing injury or death to other employees."

"We need remote access to our systems via the Internet. We know that that creates a risk. We need trained people to help us reduce this risk. There are very few people that understand control systems and their networks and the internet along with network security skills."

"Weaknesses in existing operating systems and applications coming from Microsoft are inherent in the architecture and can never be corrected until the architecture is altered in ways that will likely render it incompatible with its application base. Other operating systems fare only somewhat better as they adopt the very same weaknesses to retain interoperability between embedded and server systems."

"1. Possible access to control network. 2. Possible open access at various points in system. 3. Not enough or secure enough firewalls between corporate network and control network 4. Bad password management. 5. Possible back doors through phone modems."

It's clear from the results that many users have a realistic concept of the threats facing industrial control systems. Still, 23.6% of the respondents answered "no" to the question, "Does your organization believe there are threats and risks associated with your information control system that could affect your business?" The fact that so many don't believe there is a risk may, in some ways, be one of the biggest risks in itself.

Read Cyber security for legacy control systems.

Read the Control Engineering industrial cyber security blog.

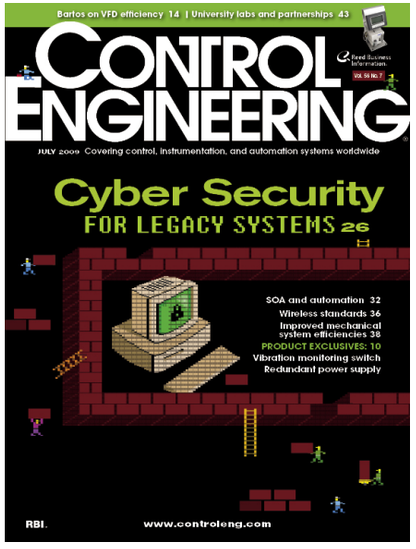
-Peter Welander, process industries editor, PWelander@cfemedia.com
Control Engineering Process & Advanced Control Monthly eNewsletter
Register here to select your choice of free eNewsletters.

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?

07/01/2009

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 replac-

07/01/2009

ing 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 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."

www.csrp.inl.gov/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."

www.csrp.inl.gov/Documents/SecuringModems.pdf

A Plan Lets Everyone Respond Properly to a Control System Security Breach, Whether it's a Failure of a Critical Cyber Component or an Intentional Break-In.

Kevin Staggs, Honeywell Process Solutions

12/01/2009

Today's modern industrial control systems are built on open system platforms and technologies. This means that what was once proprietary and closed is now more accessible—and therefore more vulnerable to intrusion. While we frequently hear reports about cyber security breaches in financial and consumer systems, we are now just starting to hear about such incidents reported on control systems. Many of these are the result of malicious activity, and others are the result of unintended consequences that result from a change made somewhere in the system, or an inappropriate use of the system.

It is best to be prepared and have an incident response plan in place. The purpose of the plan is to better prepare your organization for responding when there is suspicion of an incident to one of your control systems. This plan will allow you to properly respond to any type of cyber security incident—whether it is a failure of a critical cyber component, malicious software executing on your system or an intentional break-in to one of your control systems.

Components Of The Plan

An early part of the plan will be to describe the various types of incidents that may occur on your systems. These will range from simple failures such as a hard disk or CPU failure, infection of your system with a worm or virus, unintended consequences from changes made to the system, or a deliberate attack on the system from an insider or outsider.

The plan will describe who to call when such an incident occurs. The plan will include procedures for the responders to follow to determine the type of attack and how best to respond. The plan should also include procedures that will allow the process or plant to continue to operate while personnel are responding to the cyber security incident.

The plan should include definitions for additional responses where necessary. For example, if the security incident is the result of a virus or worm being introduced into the system, include actions that can be taken to delete the virus or worm, as well as procedures for how to prevent the incident from occurring again. This will require that an investigation be performed in order to determine how the virus or worm was introduced into the system.

Define Forensics

The plan should also define what forensics are to be performed if the incident is intentional, and how to maintain the chain of custody of evidence gathered as part of the investigation. There are times when outside help is needed to resolve the problem, or to report the problem properly to comply with regulations. Therefore, reporting procedures and regulations should be documented in the plan as well. In many cases, the control system vendor has expertise in this area that can be very useful in creating the plan.

There are many more aspects to putting together a cyber security incident response plan for your industrial control systems. A good approach to use in creating the plan is to work with your IT organization as well as your vendors. Both will already have plans in place, and they will be able to assist in the creation of a plan for your industrial control systems. It is critical, as well, to get management support for the creation of the plan.

Once the plan is developed, all members of the organization will need to be trained on their role with respect to the incident response plan. Some may only need to know who to call, while others will require detailed training on how to respond.

One final note: Ensure the plan works. The execution of the plan should be practiced and updated with lessons learned. With a good cyber security incident response plan in place and understood, an organization can minimize the impact of an incident on its industrial control system.

References

www.security.honeywell.com/industrial/solutions/cyber/index.html

Author Information

Kevin Staggs is an Engineering Fellow with Honeywell Process Solutions and a member of the company's global architecture team. This article is an excerpt from a Control Engineering podcast.

GarrettCom®: Cyber Security For Industrial Applications

Howard Linton, Director of Technical Services, GarrettCom Inc.

With the recent proliferation of cyber attacks, it has become increasingly clear that no business or industry is safe from attack. It is well documented that cyber security threats continue to rise. While these threats once seemed to be mostly limited to attempts to access financial data, recent data indicates that cyber attacks now cut across all business sectors. Security vendor Symantec recently revealed that 75% of enterprises on a global basis witnessed some form of cyber attack during 2009.

As the threat becomes more apparent for industrial applications, what can factory operations and IT management do to prepare for and fend off attacks resulting from unauthorized network access, cyber theft, and cyber attacks where malicious invaders destroy or corrupt important monitoring and/or control data? It also pays to look at the ways that cyber security and physical security can merge into an integrated security solution targeted using IP. An integrated solution strategy can make sure that only authorized employees have access to sensitive equipment and information, as well as monitor the actions of employees who may be security threats either through intention or human error.

In their excellent article posted December 1, 2009, in Control Engineering, bloggers Matt Luallen and Steve Hamburg state, "While many industrial control systems are becoming commercially available with various integrated cyber security controls, the reality is these systems are still susceptible to many types of threats. Consequently, they should not be deployed in isolation, at least from a cyber security perspective. The question that system owners and implementers raise is, 'How do we maximize the assurance that our industrial control systems will be sufficiently resilient against cyber attacks once deployed?' The answer is defense-in-depth."

Defense in Depth offers a powerful approach to industrial cyber and physical security – and its basic tenets go back at least as far in history as the famous Sun Tzu's "Art of War": use a layered defense that provides multiple and varied defense strategies against any attack vector rather than relying on a single line of defense.

Network Security using Defense in Depth

Defense in Depth is a layered security approach that uses several forms of network security to protect against intrusion from physical and cyber-borne attacks. The layers are setup to work in parallel, one technology overlapping, in many cases, with another; together they form a significant safeguard against attack.

Traditional examples of layering technologies include

- Firewalls and DMZs (Demilitarized Zones)
- VPNs (Virtual Private Networks)
- VLANs (Virtual Local Area Network)
- Secure Access Manager and Authentication Systems
- Centralized Logging and Auditing
- Video Surveillance Technologies and Physical Access Control

Additional information on Defense in Depth may be found in two publications from the National Institute of Standards and Technology: "Recommended Security Controls for Federal Information Systems—Special Publication 800-53" and "Guide to Industrial Control Systems Security—Special Publication 800-82".

General Industrial Network Topology

Here is a simplified look at a general-purpose industrial network, where the key network components include

- Main industrial campus and/or facility control center
- One or more remote locations
- Enterprise access portal
- Partners and remote access portal
- Multiple public and private transit networks (intranet, internet, etc.)

With multiple access points and multiple network hops (private and public), the following diagram illustrates a network that is wide open to abuse from cyber or physical attacks. This paper features a number of simple steps that can be taken to better secure this type of network using a Defense in Depth approach.

Firewall/NAT

Firewall functionality is usually an option available on routers that are installed in the network. A firewall is typically located at the entry points to the core network and to all remote facilities, where it acts like a gate to protect and ensure that nothing private goes out and nothing malicious comes in. A firewall's value is its ability to regulate the flow of traffic between computer networks of different trust levels, thus it inspects network traffic passing through it, and denies or permits passage based on a set of rules.

Typical examples are the Internet, which is a zone with no trust, and an internal network which is a zone of higher trust. A zone with an intermediate trust level, situated between the Internet and a trusted internal network, is often referred to as a "perimeter network" or Demilitarized

Zone (DMZ). Modern firewalls target packet information for Layers 3 and 4 (transport and link layer) and are often called 'Stateful' firewalls: they provide an additional level of security by examining the state of the connection as well as the packet itself.

A firewall can be an excellent choice as the only cyber perimeter protection for a site or as a player in a more complex network environment.

In addition to the basic firewall functions, a second layer of abstraction involves hiding inside IP addresses from the outside world by invoking a network address translation (NAT) functionality. In this case, the hosts protected behind a firewall commonly have addresses in the "private address range". Originally, the NAT function was developed to address the limited number of IPv4 routable addresses, however its facility for hiding the addresses of protected devices has become an increasingly important defense against network reconnaissance.

VPNs

Once the firewall has filtered out unwanted or unauthorized traffic, the next step is to make sure that the connections going outside of the firewall are protected. Secure access should be used whenever control messaging, protection messaging, configuration sessions, SCADA traffic, or other secure data will traverse networks where security could be compromised. Interception, or worse, unauthorized introduction of mischief into such traffic, could severely impact critical infrastructure operation with potentially disastrous results. For many applications, ensuring authenticity and security of networked connections is critical.

Of the various technologies used for secure access, VPNs include the most widely used and most broadly applicable set of standard protocols for creating secure connections across networks that can conceivably be compromised. Secure VPN protocols include L2TP, IPsec, SSL/TLS VPN (with SSL/TLS) or PPTP (with MPPE).

A virtual private network, or VPN, is a network that is layered onto a more general network using specific protocols or methods to ensure "private" transmission of data. VPN sessions can be established using various techniques and then tunneled across the transport network in an encapsulated, typically encrypted and secure, format, making it "invisible" for all practical purposes. The level of security obtained in a VPN network depends on the protocols used, the methods of authentication used in establishing the connection, and the presence and strength of any encryption algorithm used.

The term VPN can be used to describe many different network configurations and protocols. Non-secure VPNs can be used to transport, prioritize and allocate bandwidth for various customers over a multi-purpose transport network. Secure VPNs, however, use transport and session negotiation protocols, as well as authentication and cryptography, to create secure connections over "exposed" (public, semi-public or otherwise accessible) communications paths.

The most common use for secure VPNs is to establish remote access sessions between a VPN device, or endpoint, on one end of the "exposed" network, and another VPN device on the other end (for example across the internet). VPN sessions can be established as end-point to end-point sessions to create a secure path between two devices or applications or to establish a secure tunnel between two locations that can be used by many devices or end points. These alternatives are configurable in rich VPN solution implementations.

Virtual LANs

Virtual LANs or VLANs can add another layer of defense. VLANS make it possible to segregate the different traffic flows (such as VoIP, video, management, and control applications) into separate broadcast/multicast domains. Not only does this segregation keep the applications more secure by limiting where the applications reside, but it can also provide damage control. If one of the applications is compromised, the VLANs will keep the other applications isolated and safe.

Secure Access Manager (SAM)

Secure Access Management systems are another mechanism in the arsenal of protecting the network and sub-systems. SAMs enforce "Triple A" security (authentication, authorization and accounting) by ensuring that only specifically authorized people are able to electronically access the control system components or other devices that are part of the network. Further, a SAM also makes sure that any actions or changes that are made are comprehensively logged for later retrieval and analysis. An insider attack can be malicious in nature or simply a careless act carried out by an employee that is "just trying to get the job done" and, in so doing, circumvents security. The Secure Access Manager shortcuts these types of threats by enforcing security policies.
When a remote or local operator tries to connect to a system, the user is transparently connected to an Access Management System (AMS) server. An AMS server obtains credentials from the end user and then can interrogate other security systems such as Microsoft's Active Directory or two-factor authentication systems, such as RSA SecurID servers, as well as gather information from its own profile data base. It can the authenticate (or disallow access to) the user, as well as determine whether or not to authorize target devices the user was trying to access. Once authorization is successful, the user is connected through the various secure active firewalls and VPN tunnels to the actual devices.

Centralized Logging and Auditing

Key to all of the systems providing layered security is the ability for all network components to enter comprehensive logging and reporting information into a common repository. Recording and tracking "when, where, what" in a central system supports real-time detection and correlation of security threats. When something looks wrong, the information is immediately transmitted as an alert to IT departments and personnel so that they can shut down services and/or modify security policies. The information is also useful for detecting incident trends and other forensics. Protocols such as SNMP, SNTP for time synchronization as well as Syslog provide simple tools to support forensic research.

Secure Network Management

Another aspect of securing the network is to ensure that the networking components themselves are secure. Secure Network Management requires each network element to implement secure management interfaces requiring rigorous authentication/authorization, as well as both local logging and remote event notification regarding status, configuration changes and network security events. Many of the traditional access methods, such as HTTP and TELNET, have open security and passwords in plain text; they should be replaced by more secure methods, such as SSH/SSL(HTTPS) for console access, SNMPv3, secure FTP, and Syslog remote logging.

Video Surveillance Technologies and Physical Access

Physical security normally means building "six wall" physical barriers around the facility. However, in most cases, someone has to enter the building at some time, so methods such as electronic card readers can be used to authenticate a person against data in a server running Radius or another type of authentication application. Physical access can be logged manually as well as by electronic logs. Video cameras and pixel-based systems that focus on certain parts of the video frame and send an alert if there is movement detected are powerful new security tools. Additionally, the use of PoE (Power over Ethernet), which supports both network access and power to remote monitoring devices, makes digital video security and access control easier and less expense to deploy than older analog-based systems.

Another component of physical security is protecting access to the networking equipment itself. A secure system can be compromised if it is possible to maliciously or inadvertently plug an unauthorized device into an Ethernet switch or router, or into a terminal server. Technologies such as VLAN, static MAC security, and 802.1x can provide Ethernet port security, while static Serial-IP and filters, serial-port SSL and serial-port VLANs can provide serial-port security. Firewall technology and/or SSL can be extended within a local site to ensure end-to-end connection security.

Defense in Depth in Action

To really understand Defense in Depth, it is important to see how some companies have developed layered cyber security strategies. Companies of all sizes are evaluating options and requirements when addressing various levels of security access from field hardware (IEDs) to human machine interfaces, workstations and SCADA systems. Access to the industrial communications network, remote vendor access and support, and key databases and historical records are all areas where Defense in Depth decisions need to be made.

Each industrial facility will address its own needs in its own way, and most agree that a cyber security program is an incremental process.

Many industrial facilities are watching what is happening in the power utility industry because of stringent NERC mandates. The experience of one utility company is instructive. As a rural electric power cooperative, "Ridgemont Utility" does not yet fall under NERC mandates, but a security audit several years ago convinced them it was time to take security more seriously. Their Defense in Depth strategy followed the thinking below.

The first decision was to develop and maintain two separate networks – one corporate and one on the SCADA side. This limits the ability of incursions in either network to affect the other. The corporate network is concerned with standard business operations including contracts, accounting and filing systems. The SCADA network, on the other hand, uses secure measures to protect the control of the system – and access into the control system. In fact, the SCADA system is designed in a way that allows security personnel to isolate the SCADA network in a very short period of time without impacting its ability to run operations.

The philosophy of running separate networks for separate functions goes even deeper in the operating philosophy of the company. Firewalls are in place at every remote location and at every site where Ridgemont's networks come into contact with the outside world. Firewall equipment in a clustered environment with hot-standby firewalls for failover protection guards gateways between networks, and is backed by redundant switching behind firewalls and redundant links. VLANs, which are run over point-to-point VPNs between firewalls, as well as different logical and physical networks for different functionalities, make it difficult for intruders to penetrate the system, even while authorized users can move easily among networks to get what they need. Even links running across leased circuits between outposts and the main office use point-to-point VPNs.

Ridgemont, which is in transition between serial and IP-based communications, use serial tunneling devices to run certain SCADA operations through the network, utilizing routers designed to support serial and IP in the same box.

Another philosophy is to block every port that is not necessary within a network. Realizing that many network switches and other IEDs come with all ports available for access and default passwords in place, the co-op shuts down all ports and removes all default passwords so that security is built from the bottom up. The operations manager would rather have access blocked by a firewall after a port had been connected to a new piece of equipment, and fix it, than take the easy approach and leave everything open and available for potential attack. To foil intruders, Ridgemont uses NAT functionality to change port numbers from their default programming to make it more difficult for unauthorized access.

Ridgemont has defined policies that determine what user will have access to which net, and which specific resources on that net. When outside access to a network is necessary, it is passed through a connection using SSL and both per-port and per-user authorization. The authentication process uses Active Directory, and is performed on the local level, not from a central location.

Everything that can be password protected is – often down to a different password for each piece of equipment. As mentioned earlier, a first order of business for Ridgemont when installing any piece of equipment is to discover and change default passwords. There is no standardization on passwords, which are randomly generated and require a minimum of eight digits, including at least one special character, number and letter per password. With thousands of pieces of equipment within the system, password management is difficult, but deemed essential. IP addresses are removed from equipment to protect the network in case of physical breach.

A Syslog server and SNMP management allow Ridgemont to track who is logging into the IP-based equipment—and when (legacy serial connectivity does not afford that luxury, and is being replaced). A next order of business is installing secure access software that will enable management to know what has been changed as well as who and when.

WiFi is carefully isolated on a separate network that links directly to the cable company. Access is offered as a convenience for sales people, customer representatives, repair crews and other outside visitors. Internally, employees need to access the internet through VPN appliances using SSL. Ridgemont ensures that firmware and software are kept up to date and have deployed the latest security patches.

Recommended security practices generally recommend using outside security experts as well as internal teams. An affiliate utility, which is under NERC mandates, helps Ridgemont with the details of its security system. Like most fields, expertise and daily exposure provide a level of sophistication not possible when security is only “part of the job’.

Ridgemont’s operations manager notes that maintaining security can be very difficult. “You do due diligence; you do the best you can.” But, a key component to any security system is alert and educated employees.

“We talk about security at staff meetings and employee meetings. We remind people to leave their PCs at home and not plug them into the co-op network – ‘don’t bypass everything we have done!’. We have a good employee base and not a lot of turnover, and that makes our job easier,” he says.

Conclusion

Introducing a number of simple security elements into an industrial network will significantly reduce the risk of physical or cyber attacks. The resulting network topology should look very much like this:

The clock is ticking. IT groups and operations managers in industrial networking applications must come to the realization that it is a matter of when, not if, a physical or cyber attack will occur in their industry – and possibly their plant.

Fortunately there are readily available, off-the-shelf, industrial-strength networking equipment, and cost-effective tools, systems, and partners to work with to deploy Defense in Depth protection for any type of industrial network. Defense in Depth is not a one-time goal but a continual process of assessing network vulnerabilities, updating security policies and adding emerging technologies in a continues cycle in order to protect valuable cyber and physical assets.