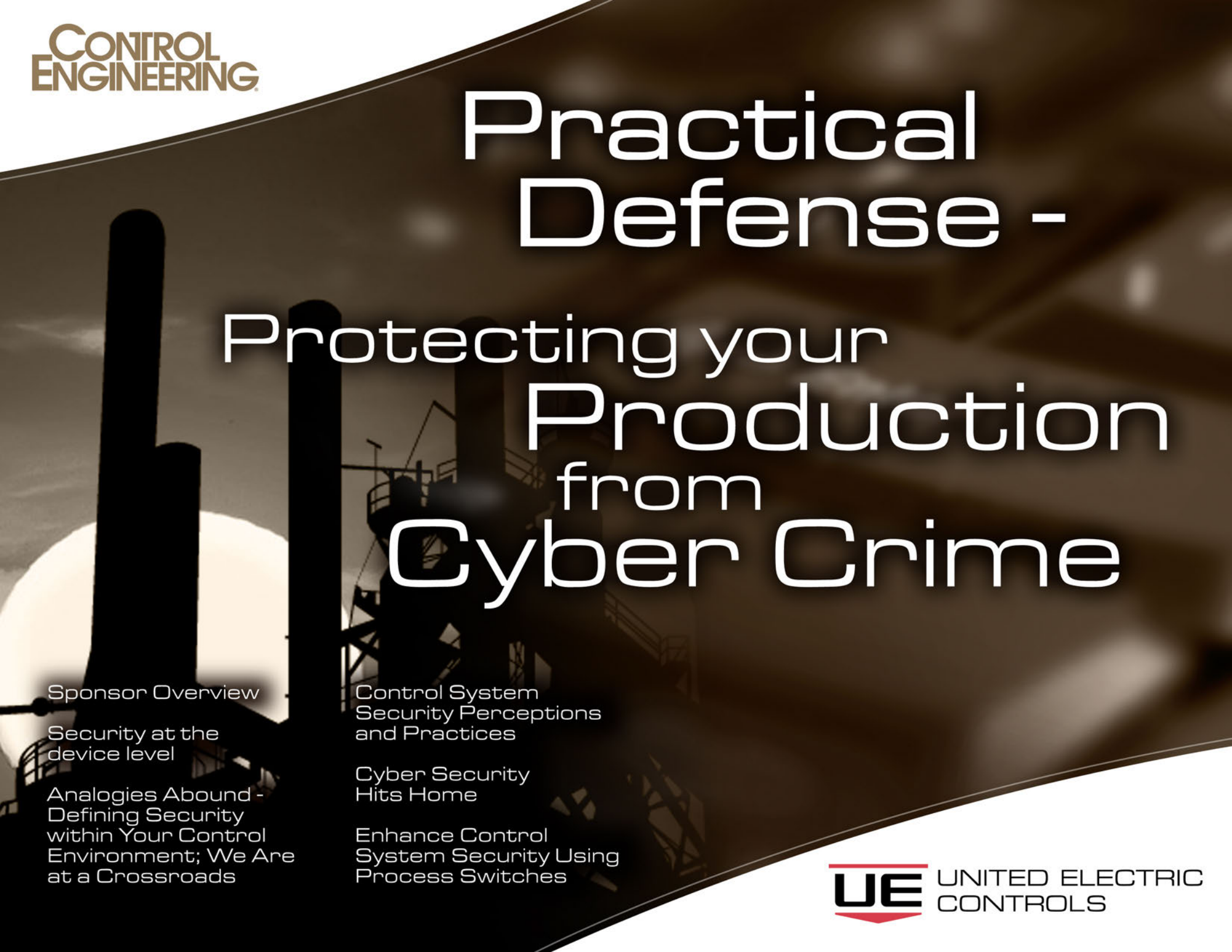


CONTROL ENGINEERING

Practical Defense - Protecting your Production from Cyber Crime

Sponsor Overview

Security at the device level

Analogies Abound - Defining Security within Your Control Environment; We Are at a Crossroads

Control System Security Perceptions and Practices

Cyber Security Hits Home

Enhance Control System Security Using Process Switches

UE UNITED ELECTRIC CONTROLS

Sponsor Overview

United Electric Controls, a privately held corporation headquartered in Watertown, Massachusetts, USA, is a manufacturer of durable and reliable pressure and temperature switches and sensors used in industrial applications throughout the world. UE products provide a critical and independent layer of Plant Safety instrumentation that protects equipment, processes and personnel in a wide variety of challenging environments and operating conditions.

Our reputation for dependable pressure and temperature solutions is a result of innovative design, superior manufacturing techniques, and a corporate focus on uncompromising quality and service to our customers.

Innovative Design

- **Solid-state One Series electronic switch for plant safety applications**
- **Cost-effective solutions to meet and exceed customer requirements**
- **Rugged construction for the most challenging environments**

Rapid Delivery

- **Lean manufacturing for maximum productivity**
- **Practitioner of continuous improvement and elimination of waste**
- **One-piece-flow for optimum manufacturing efficiency**

Uncompromising Quality

- **ISO 9001:2000 certified**
- **Customer-first approach through service, delivery and value**
- **Wide selection of products that meet global agency certification**

Three Manufacturing Divisions

- **United Electric Controls**
- **Applied Sensor Technologies**
- **Precision Sensors**

Environmental Stewardship

- **Energy management**
- **Recycling**
- **Non-toxic manufacturing**

Security at the Device Level

Matthew Luallen

Cyber security is war. You have to defend your systems from all sorts of outside attackers, and if one that's skilled and determined gets you in his sights, defending yourself may be tougher than you think. In traditional warfare, as an invading army moves into a new territory, logistics become more difficult the farther the army moves from its home bases and resistance usually stiffens. The opposite is true in most cyber defenses. Once an attacker breaks through a hardened perimeter, moving around inside is usually pretty easy. That's why defense in depth with incident detection, response, and attribution is so important.

Field devices, meaning individual sensors, transmitters, actuators, motor controllers, and the like, are considered the bottom of industrial networks. However, they can still be the target of cyber attacks if you have a sophisticated attacker. Some recent incidents with water utilities attributed to failed sensors or a bad pump resulted in releases of large amounts of water or even destroyed a pump. Some see these as clear cyber attacks.

If your technicians can configure a field device through the control system, dedicated handheld tools, or by plugging in a laptop to the network, an attacker can do the same thing if he follows the right path. If configuration information is accessible, a device can be changed or simply turned off. If enough strategic devices are manipulated in a production unit, all sorts of bad things could result.

Making this happen requires intimate knowledge of your systems as the hacker has to know two things: which devices to get at, and how to get at them. An insider will know this information, but someone outside your plant probably does not. With lots of time, patience, and maybe some luck, a hacker might be able to follow enough trails and eventually find what he's looking for, but this is a very tedious process if you have a few thousand I/O tags.

A more practical alternative might be to get some help from an insider. If the hacker can identify one or several individuals in the plant who work in the strategic area, he might try to break into those individuals' e-mail accounts. If a technician uses his or her personal Gmail account to discuss work-related topics, that is probably the easiest attack vector. The hacker may also follow the technician home and break in via the home wireless

network. Reading some e-mails or using e-mail as the path to get into the company network can yield a bounty of information that could help the hacker focus his efforts.

If the PLC or I/O section of the control system attached to the strategic devices is not sufficiently protected, it will be little trouble for the attacker to do whatever he wants with those sensors. Even if there is defense in depth, there have to be approved pathways for the desired information to move up and down. If the hacker can sift through enough data and follow those conduits through the defenses, the defenses won't be very effective. Some security analysts believe the people who deployed Stuxnet used another malware program to gather information on the targeted systems to help find the best ways to get to the desired devices.

In many respects, the best defense against this sort of attack is maintaining tight internal practices. A common factor in most of these situations is that people are part of the attack vector. Getting company data by breaking into personal e-mail accounts, employees uploading malware via phishing attacks, and sloppy practices with passwords often figure into the analysis after incidents surface. When a hacker gets no help from inside, the job is much tougher.

Matt Luallen is founder of Cybati, a cyber security training and consulting organization,

Analogies Abound - Defining Security within Your Control Environment; We Are at a Crossroads

Matthew Luallen & Steve Hamburg

Have you had difficulties in expressing risk within your organization, or have your colleagues provided guidance that is challenging to fully understand? This is quite common in every discipline and specifically appears to be more pervasive in any vertical where the numbers of acronyms outnumber the number of support personnel. Many of us are aware of how far reaching control systems are within our lives; however, simultaneously the world marches onward with many not aware of how much the physical world is now controlled by cyber assets.

Where are control networks today? SCADA networks exist covering far-reaching physically geographic areas, such as fresh water and waste water delivery, electricity generation and delivery, heavy and light rail, transportation control, natural gas, and oil pipelines. Distributed control systems provide automated solutions for oil refineries, electricity generation, manufacturing, and agriculture. There are even more localized control systems within aircraft, semi-trucks, and even your automobile. These networks have become increasingly automated over the past two decades and increasingly interconnected over the past five years. This interconnectedness provides richness of data to aid in business decisions, performance enhancements, and increased productivity. The connectivity provides for both distributed and centralized real time control of multiple physical assets with built-in safeguards to reduce the probability of system failures.

It is truly amazing – what feats we have accomplished in such short time during both the industrial and now the technological revolution.

Sadly, in present day, these feats come with a price: increased risk due to the lack of our historical physical security controls providing the expected security to which we are accustomed. The reality is that on the Internet, the highly sought after “good part of town” does not exist; each of us in this virtual world is literally the speed of light away from each other’s digital doorstep. This is a paradigm shift from our current thought processes associated with our “security.” The physical security controls of the past lack in providing the visibility or necessary response associated with this virtual world. Furthermore, the natural human senses of sight, sound, smell, taste, and touch do not directly apply to this virtual world. Literally, we need to educate ourselves with a sixth sense to understand the risks we are undertaking with our technological advances and appropriate solutions to reduce them to levels deemed comfortable by our society.

How do we move forward in today’s world? How can we define our logical security in such a way that provides the same level of security as we have physically?

Analogy #1
(Physical) Someone is constantly attempting to pick your door lock or break down your door.
(Logical) Your home network is continuously scanned from around the world in an attempt to find the vulnerability in your outer walls.
(Comments) If our physical doorstep was attacked as often as our logical doorstep, each of us would attempt to find another place to live.

Analogy #2
(Physical) You arrive home to find someone sleeping on your couch that is not anyone you know.
(Logical) A new service or port has been enabled on your cyber asset (e.g. HMI, PLC, Relay, Workstation)
(Comments) The tools necessary to truly understand our digital environment at the same level as our physical world are too complex and often misunderstood. Recently at a conference attended by Encari, the concept of "Cyber Archaeologist" was coined. We are highly abstracted from the physical world in which we live and the logical world that automates it.

Analogy #3
(Physical) You find a needle lying next to your car in the parking lot and inject yourself.
(Logical) You find a USB flash drive lying next to your car in the parking lot and plug it into your computer.
(Comments) No comments necessary: just don't do it! Don't take candy, drugs, i.e., anything from strangers.

Analogy #4
(Physical) You purchase an automobile with a flawed accelerator or braking mechanism and have it repaired via a recall notification.
(Logical) You purchase a control system with vulnerable code and have it patched by the vendor (both appear to take the same amount of time)
(Comments) In this most recent example for the control system in automobiles, it is setting precedence that the manufacturer is responsible for software flaws (Toyota Prius braking system).
Use our perspective as an opportunity to provide your own analogies; it is invaluable that we as an industry and more broadly as a global society can convey what is happening within cyber security. We are at a crossroads.

Control Engineering cyber security bloggers puzzle over recent industrial control system security assessment survey results.

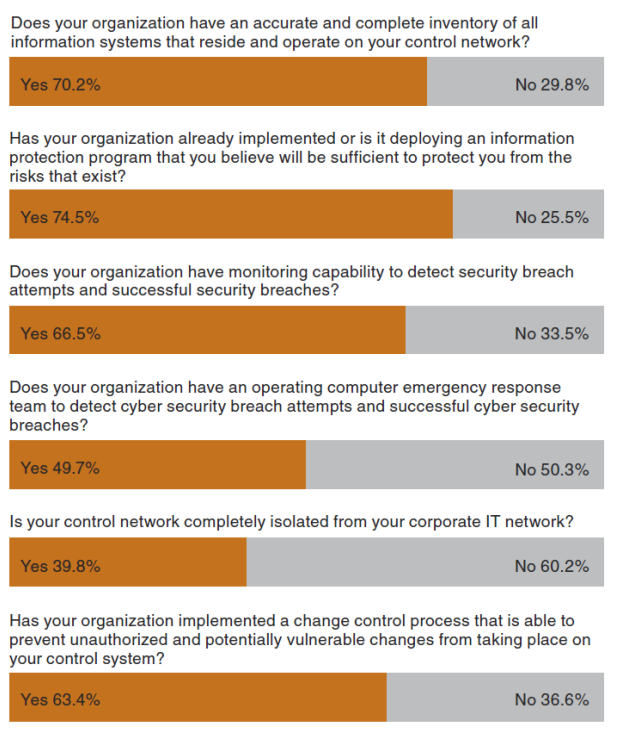
Matthew E. Luallen, CCIE, CISSP, GIAC, and Steven E. Hamburg, PE Encari

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.

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



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

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.

Users seem divided as to the most important element of a security solution. Some may be based on internal experiences and incidents.

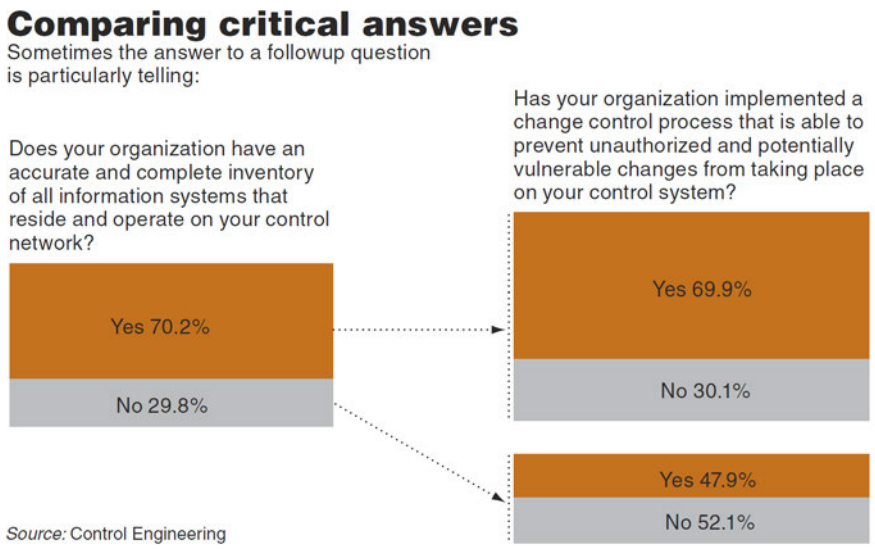
Protecting information

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 confi-

dence 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;**
- **Communicated verbally?**
- **Printed by a network printer;**
- **Residing in a database; and**
- **Faxed to a vendor;**



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

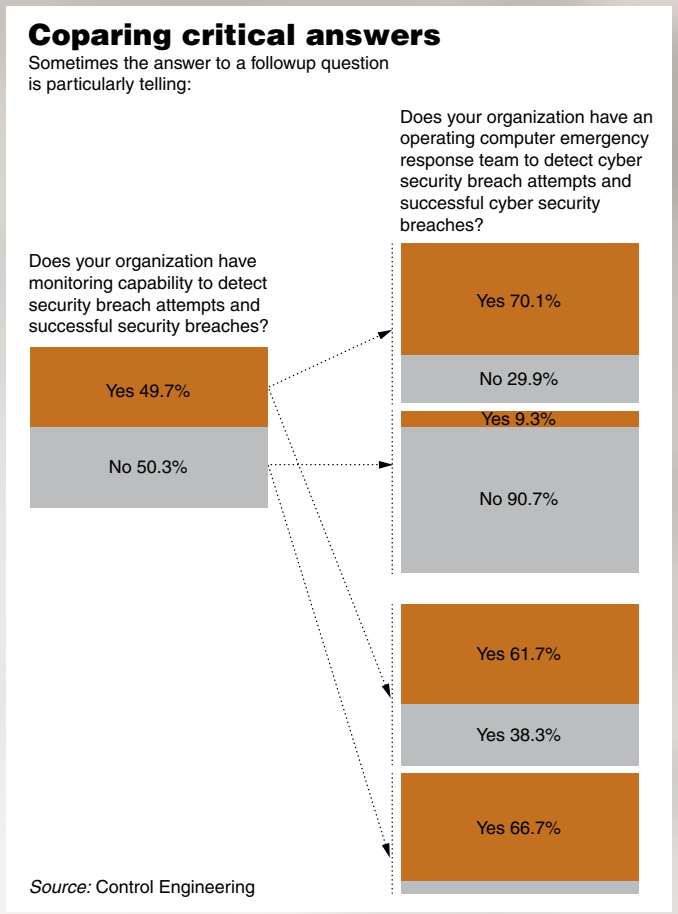
Several other notable findings of the survey:

- 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 re side 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.

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 po tential 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 vulnerabil ity assessment if you were concerned about risks associ ated with cyber security threats?
- How can you claim to have an accurate and complete in ventory 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.



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

Author Information

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

Cyber Security Hits Home

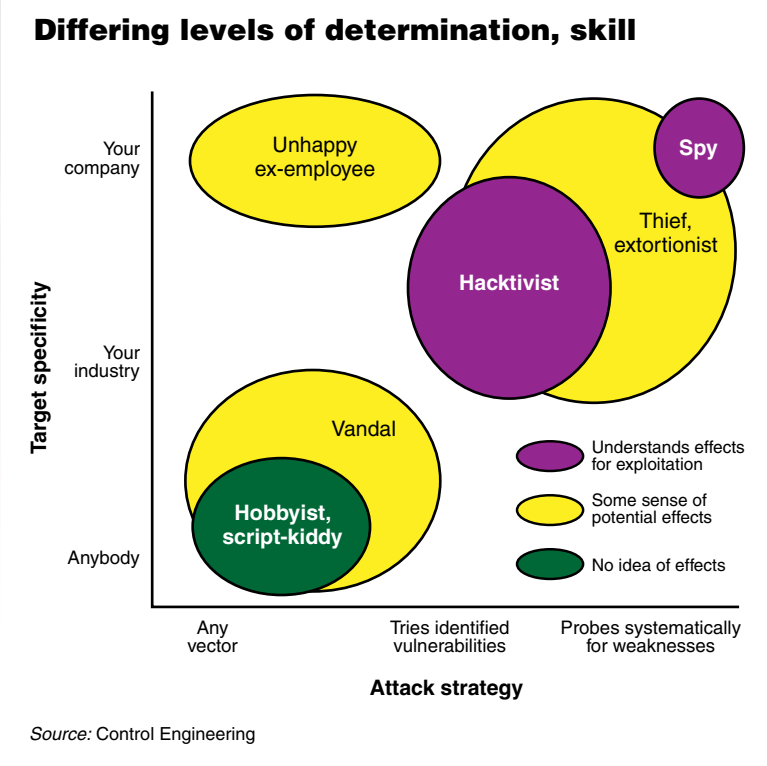
With the coming of the new year, cyber security activity at power plants and larger electric utilities has taken a major step. NERC CIP (National Electric Reliability Corporation, critical infrastructure protection) regulations are coming into force that require producers and distributors of bulk power to take specific security precautions to ensure uninterrupted delivery.

Peter Welander, Control Engineering

With the coming of the new year, cyber security activity at power plants and larger electric utilities has taken a major step. NERC CIP (National Electric Reliability Corporation, critical infrastructure protection) regulations are coming into force that require producers and distributors of bulk power to take specific security precautions to ensure uninterrupted delivery. These requirements have teeth in the form of substantial fines that can be charged against offenders.

Many that are not in the utility industry are watching the situation with the expectation that deployment of similar regulations will spread to other verticals sooner rather than later. Over the last year or two, industrial cyber security issues have been developing with greater intensity. One event was a report about a year ago from the CIA that an overseas utility had been compromised successfully by cyber attackers in an extortion scheme. The nature of serious hacking (see graphic) has expanded from being simply an amusement to criminal, terrorist, or even state-sponsored espionage. Such escalation demands an appropriate and dynamic defensive response.

Implementation of the NERC CIP regulations has been compared to the confusion surrounding Sarbanes-Oxley (SOX) after its passage in 2002. Eric Casteel, manager of SCADA and security business development for Emerson's power & water division recognizes the similarities. "When SOX compliance came out, there was very little guidance and interpretations varied widely," he says. "We're seeing the same kind of thing with the NERC CIP standard. Some customers are taking the high road and want to adopt best practices to get an 'A' for their audit. Others just want to pass with a 'C.' Some plants try to say, 'We're not a critical asset.' If they don't have black start facilities and they're not a significant megawatt generator, they might have a case. But when you look at the overall security of the grid, you're only as strong as your weakest component. At some point, regulators will come back and say, every power generating, transmission, and distribution provider must implement these regardless of whether it's a critical asset or not."



Source: Control Engineering

Hackers can have a wide variety of skills and motives to break into your systems. These characterizations are general, but suggest what might be out there. Hobbyists aren't too difficult to fend off with a little effort, but a skilled and motivated terrorist or criminal is a different story.

Where to start?

If you're with an electric utility or other industry, how do you begin to implement basic cyber security practices for your DCS (distributed control system), SCADA (supervisory control and data acquisition), or other industrial control network? Such a project should begin with an assessment of where you are today, specifically taking inventory of all the devices on your networks, what they're connected to, and what software is running on them. This is the first step in finding out how hackers can get into your systems from the outside, and setting up appropriate barriers.

"Users usually have a very poor feel for their actual system architecture and connectivity," says Todd Stauffer, process automation systems marketing manager for Siemens Energy and Automation. "A lot of things get connected directly or indirectly to control networks that people responsible for the process have little control of. One of the first things that folks should do is establish what their real system architecture is, and it will likely be significantly different than what they think they have. As a rule, people will almost always find connections they didn't realize were there."

David Rehbein, senior data management solutions consultant for Emerson Process Management, spent many years evaluating networks while working for Microsoft. He agrees that making an assessment is a critical first step. "Those system inventories can sniff every IP address on your network, and things often pop up that nobody even knew were out there. Somebody came in and put something on the network and forgot to tell IT, and all of a sudden you have a rogue client or server on your system. If you don't know it's there, you don't know if it is getting patched at the right levels. You don't know if it's secure. You don't know if it's running virus check software."

Understanding your connections

Control systems that exist as islands are easy to protect, however few of these still exist. When management wants to know what's going on in the plant, the easiest way to get information is to look into the control system. This means a link with the corporate network which is undoubtedly connected to the Internet. If this connection is not well protected, this is a primary point of access. The larger the extent of integration, the larger number of potential entry points. This is called the attack surface area.

Rehbein recalls a project he was involved with while at Microsoft: "We finished our first assessment in a day because it was a very unsophisticated site. They didn't have a connection between their plant floor network and anything else. You had to get into their building even to get access to it. Compare that to somebody who wants to share inventory or current production levels with customers or the corporate IT department in Switzerland. That requires direct Internet connection, which provides a door for anybody to come into your system." Business demands for connectivity are putting more pressure on operators and control systems, and that opens potential attack vectors. Shawn Gold, global program manager for open systems services for Honeywell Process Solutions, worries about companies losing their ability to handle problems internally. Increasing dependence on outside support means adding entry points. "You have risks associated with any connections to the outside world," he warns. "But you have a greater demand, especially in today's economy, to allow more connections for outside services and resources to help you out. You may have documented all those connections, and that's a good thing, but there are potentially undocumented connections that take place, or ad hoc connections that take place to manage through emergencies. These can create security risks, so you need to be aware of what you're going to have to do in the case of an emergency and what you have to do to protect yourself while you're working through those difficult times."

Monitoring software

In addition to connections, you need to know what software resides on your networks. This is critical for two major reasons: some software has vulnerabilities that can be exploited by hackers, and poorly written programs can cause problems internally.

"Every time you add software, you increase the attack surface," advises Kevin Staggs, global security architect for Honeywell Process Solutions. "You might bring in some piece of unnecessary software that causes a conflict on the system with some other piece of necessary control software and then causes the system to fail, and you have a loss-of-view incident. Sometimes software isn't written as well as it should be and causes a memory leak. One anti-virus system patch we found had a memory leak in it, and a control system using that program would run for about 35 days before it ran out of memory. When that happens you have a terrible slowdown or warnings on the display, and the operators don't know what to do about those."

Staggs adds that those problematic programs can have similar consequences to malware introduced by a hacker. If programs are not thoroughly vetted by your control system vendor, they can cause conflicts that may not be apparent immediately. He suggests, “It’s a matter of having very good change management procedures in place, and when you do execute a change, make sure you check baseline performance before, check again immediately after, and watch it for a period of time. You can detect problems if you use that level of rigor.”

When you know what is on your networks, you will know if you have to deal with a specific problem that comes to light. Siemens’ Stauffer warns of situations where white hat organizations publish vulnerabilities they’ve found in common software platforms in an effort to force vendors to fix them. “They aren’t realizing that they’re getting the system all out of whack,” he says. “People are forced to do things that they aren’t ready to do when holes in legacy systems are posted on the Internet for everybody to see. That’s enough to tell a hacker what to shoot for with a given system. Security by obscurity? Forget that. The weaknesses of your system are posted on the Web.”

Consult your vendor

One of the easiest steps you can take is to consult the supplier(s) who built your systems originally. Most companies can provide instructions, case studies, best practices, and other advice based on collected experience. There are many more aspects of cyber security that are not practical to discuss here. Personnel policies, management buy-in, physical security, defense in-depth, and so on, all influence strategy. Many organizations and companies have produced resources on cyber security for industrial systems. The sidebars attached to this article are an excellent place to begin your research. Always keep in mind that there are no ultimate answers, and there is no absolute security. The best you can hope for is to have levels of protection that are stronger than your attackers.

Author Information

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

Resources for your cyber security implementation

Many resources are at our disposal for properly “securing” process control systems. Securing process control systems entails appropriate defense-in-depth controls, such as gaining management support, performing assessments, identifying risk factors, selecting remediation solutions, gaining management support and effectively integrating the appropriate technology, procedures and security awareness and training program after you have gained management support. And don’t forget gaining management support.

There are many options available to provide education regarding the process; however, the best starting point would be to review and gain a thorough understanding of the following:

1. NERC CIP (North American Electric Reliability Corporation, critical infrastructure protection): These are important cyber security standards affecting organizations in the bulk electric system. They also pertain to other process control-enabled verticals, such as aviation, railroads, wastewater treatment, natural gas, refinery, chemical, and manufacturing as they are also considered internationally as critical infrastructures. NERC CIP is the first cyber security standard that can impose sanctions, which can include fines up to $1 million per day for encountered instances of non-compliant findings. Other verticals with SCADA and DCS systems are reviewing this since it is identified as a larger critical infrastructure protection standard.

2. Idaho National Laboratory National SCADA Test Bed and DHS Control System Security Program: This program provides many details regarding security awareness, security assessments and secure architecture. It is also massive in scope and can prove to be difficult to navigate.

3. NIST SP 800-82 (National Institute of Standards and Technologies Special Publication): This new document provides guidance on securing industrial control systems. The final version is forthcoming after the third and final public comment period, which expired on November 30, 2008.

4. ISA 99: This standard provides specifics for establishing and operating a control system security program. Part 4 of the standard is to provide additional clarification about what sets apart control systems security from traditional IT security.

5. Traditional IT solutions such as Control Objectives for Information and related Technology (CObIT), ISO 27005 and ISO 17799: Many frameworks for IT control and security exist that can support foundational work within industrial control system environments. Traditional IT business systems and process control systems are interconnected for efficiencies and cost reductions; therefore, it is appropriate to couple specific IT and process control operations synergistically. The critical question is what defines appropriate demarcation points between jointly and uniquely operated systems? Finding the answer is a challenge, which will be specific to the organization and industry.

Many organizations have produced standards specific to SCADA systems, including: ISA, ISO, IEC, API, AGA, ChemITC, DHS CSSP, PCSF, CIGRE, NSTB, IEEE, EPRI, I3P, NERC, and NIST. In an effort to assist all critical infrastructures in addressing prevalent security challenges, Control Engineering will continue to provide clarity regarding these standards in a practical and applied manner via its cyber security blog.

A key reference on defense in depth

One document considered a classic in the industrial cyber security arsenal is "Control Systems Cyber Security: Defense in Depth Strategies, May 2006," by David Kuipers and Mark Fabro. Fabro is president and chief security scientist at Lofty Perch, and has worked extensively with the U.S. DHS and INL (Idaho National Labs). He has this to say about developing that paper:

"As the DHS Control Systems Security Program (CSSP) works so closely with private sector, one of the major ideas explored was how to build effective cyber security into large scale systems that were previously isolated. The issues of convergence, combined with the age and operational nuance inherent in some of the 'for purpose' technologies made contemporary cyber security solutions unfeasible. Asset owners and operators had shown that some measures, such as IDS (intrusion detection system) and firewalls, can be used effectively with no impact to operations. A solution was needed that provided asset owners direction to leverage proven security practices in a manner that was not going to break their systems but was going to reduce cyber risk. "The defense in depth model uses the concept that appropriate levels of security can be applied at different levels in the control architecture, such that the aggregate of all the security elements creates an extensive security defense posture. The approach in creating the practice guide was to educate readers about some of the more common vulnerabilities that can exist within control system environments, and how the appropriate deployment of security solutions can help mitigate those vulnerabilities. The goal was to leverage all of the feedback CSSP had collected from stakeholders, provide insight into how to address their needs, and create guidance that could be reviewed by the community of interest. In the end, the product was something that was vetted and reviewed by the very stakeholders that were looking for guidance, and the impact has been very positive. Now we have a recommended practice that provides insight into several proven methods that can secure control system architectures, and have it done in such a way that the balance between security and performance is maintained."

Enhance Control System Security Using Process Switches

In today's world of standardized communications, no man is an island and neither is any process control system. Networking is about to expand greatly, thanks to the increasing adoption of integrated devices, the internet, and a proliferation of open operating systems. Increasing attacks that exploit weaknesses in the network may not be far behind. Real world examples have shown that control systems can be hacked, sometimes with deadly results.

This white paper looks at how open Microsoft technology used in virtually all contemporary control systems, such as distributed control systems (DCS) and supervisory control and data acquisition (SCADA), can mean less security. The paper explores why current solutions may not be up to the task of protection. It also shows how simple, yet reliable electro-mechanical switch-based protection can improve cyber defenses by complementing traditional techniques with another layer of protection independent of centralized control systems.

Better Technology, Less Security

A long running trend is behind the increasing vulnerability of control systems to hacking and other forms of cyber mischief. Centralized control systems are typically tied together through an open network and software that is susceptible to cyber-attack. What's more, the network extends out beyond the plant floor. Indeed, a part of the plant floor network is increasingly reaching around the world, thanks to web-based tools and interfaces.

Networking adds extra capabilities, information sharing, and lowers the cost of commercial off-the-shelf components used in process control systems. Data from a control system can be fed into enterprise management

software, enabling the use of business intelligence techniques to tackle problems and improve overall performance.

However, current networked systems are more vulnerable to attack than yesterday's stand-alone and analog-based setups. This increased susceptibility arises from expanding exposure on two fronts. First, an open standardized network that can be accessed around the world for good can also be manipulated globally for bad. Second, the more complex a network becomes, in terms of connected devices and topology, the more likely it is that some vulnerability will open up, particularly if system updates are not deployed in a timely manner.

Perhaps the best known and most complete example of this in a SCADA setting is the Stuxnet worm, which was discovered in June 2010. Stuxnet infects computers through infected USB flash drives and exploits multiple Microsoft Windows security vulnerabilities. More recently, another worm related to Stuxnet dubbed Duqu was discovered by a Budapest University. Built on the same source code as Stuxnet, Duqu may be one of many malware worms floating in cyberspace ready to attack.

An investigation by the Idaho National Laboratory demonstrated potential physical damage with a 27-ton power generator by sending conflicting instructions governing speed and other characteristics that induced the generator to literally shake apart, destroying it. In a simulation, Sandia National Laboratory engineers showed that turning off a recirculation pump while upping heat could incapacitate an entire oil refinery by simply destroying a critical component.

Current Solutions Need Improvement

Traditional solutions are not as effective as they once were. One aspect of the traditional approach is to patch software to plug vulnerabilities. Doing this prevents an attacker from gaining control of a system through the use of a trick - such as a buffer overflow overloading the software – thereby allowing an attacker free reign.

Yet another approach is to employ firewalls and intrusion detection devices to keep intruders out and prevent the exploitation of weaknesses. Very sensitive and critical control applications are further hardened through network segregation to limit points of contact to the outside world, making the systems more secure. Costly redundant components and controllers can also be used, if control applications are vital enough to warrant the extra expense.

In today's world, unfortunately, all of these tactics can – and do – fail due to the efforts of smart savvy attackers. On the software side, the list of vulnerabilities in Linux, Windows, iOS, Android and other operating systems is long and growing.Despite the valiant efforts of the control system suppliers, attacks can succeed if an unpatched operating system or applications exist inside a trusted area due to lax system upgrades.

In addition, the growth of newer technologies, such as fieldbus networks, industrial wireless networks, and mobile hand-held devices is another potential path for hackers. The new crop of safety instrumented systems (SIS) shift from separated analog systems to digital networking architectures may be susceptible to operating system weaknesses. Wireless networks are new and even with the extraordinary security measures included in the standards, only one entry point out of an infinite amount due to ubiquitous access points through sensors and mobile devices is needed to create havoc.

In total, this situation means that the most secure approach possible – network segregation – is much less effective.

Turning to Tried and True Technology

Clearly, there is a need to add to the defense against cyber-attack. Ideally, the defense would operate in the event of a compromised control system. The solution has to be fast acting, as even small delays can lead to damaged equipment, toxic environmental exposure, loss of life, and long downtimes. It also has to be reliable, working when needed and not triggering at the wrong times. Finally, it has to be hack-proof and support current infrastructure.

Electro-mechanical process switches, a robust and proven technology, meet all of these requirements. At first glance, this is somewhat surprising since the technology is not typically considered for cyber security. However, electro-mechanical switches do not have software or an operating system susceptible to cyber attack. When properly applied, electro-mechanical switches can provide safety functions independent of a central control system. There is no processor involved, which means there is nothing to hack. Electro-mechanical switches are also fast, tripping quickly when milliseconds count. What's more, modern implementations, like United Electric's 100, 120 and 400 Series of pressure and temperature switches, have virtually

no false positives. When these switches trip, it is because a safe operating limit has been exceeded, dangerous conditions exist, or both.

The key to this approach is the placement of switches so that they monitor suitable process parameters. They also must be connected so that they can take the appropriate action. In the event of an out-of-limit process condition, the switches will trip. Since the switches can power relays, they can be wired so as to shut down compressors, pumps, turbines or whatever is needed to correct the situation and limit the damage.

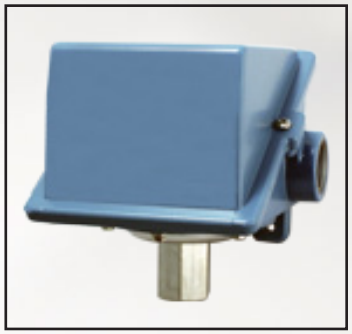
Of course, the choice of what parameters to measure and where to do so will be dictated by the particular process in question. Likewise, what to have a switch act upon will also be process specific. They could, for example, shut off a compressor to keep a vessel from an overpressure situation or they could trip relays to take an entire plant floor offline.

To see the power of this approach, consider that one of the first actions taken in Sandia National Laboratory oil refinery attack simulation was to put the system on manual, thereby overriding automated safeguards. This hack attempt would have failed, though, given an appropriately placed and configured electro-mechanical switch. The switch would have tripped once the temperature exceeded a set point. There would be nothing the attacker could have done.

As an added bonus, switches protect against both deliberate and accidental catastrophes. After all, they do not care why a temperature limit, for example, has been exceeded. The situation could be due to malicious hacking or the failure of a pump circulating coolant. In either case, though, the switch would take the same action and provide an emergency shutdown.

100 Series Pressure & Temperature Switches

120 Series Pressure & Temperature Switches



400 Series Pressure & Temperature Switches

Conclusion

As has been shown, increasing connectivity and automation have brought benefits, such as diagnostics, predictive maintenance, and process optimization to process control. However, by bridging the gap between control systems and the world, these advances have also made automated control systems vulnerable to attack. Traditional solutions may not be adequate to safeguard systems in an environment where multiple, rapidly evolving technologies combine to create many potential weak links.

The solution involves a properly designed safety layer of electro-mechanical process switches to complement traditional software solutions. Switches are fast, reliable, hack-proof, and act independent of the control system. Electro-mechanical switches should be considered as the primary or redundant layer to protect critical equipment in today's dangerous landscape. So, while no control system today may be an island, electro-mechanical switches can, in effect, provide protection from intruders before they can cause damage.

Author Information

Wil Chin
Phone: 617-926-1000 ext.1292
Email: wchin@ueonline.com

UE UNITED ELECTRIC CONTROLS

Leading manufacturer of pressure and temperature switches and transmitters since 1931.
www.ueonline.com