CONTROL
PROMOTING EXCELLENCE IN PROCESS AUTOMATION • CONTROLGLOBAL.COM

SPECIAL REPORT

CYBERSECURITY IN OPERATIONAL TECHNOLOGY

The Industrial Internet promises great opportunity, but to fully realize its potential, the Industrial Internet must be secure. Strategies such as air gapping are ineffective at best, and can provide a false sense of security at worst.

The threats to industrial environments are real and growing, including small-time thrill seeking thugs, nation-state hackers and internal staff or contractors. Research and real-world examples are showing a dramatic rise in attacks. In fact, Security magazine reported in 2014 that nearly 70 percent of critical infrastructure companies have suffered a security breach.

Securing an operational technology (OT) environment is significantly different than securing a traditional information technology (IT) environment. What you're securing is different, and how you secure it is different. IT focuses on digital information protection. OT focuses on people and physical asset protection. To deliver security solutions specific for OT requires an industrial mindset, purpose-built technology and specific OT security expertise.

This Special Report presents the best OT security articles, tips and resources from the pages of *Control* and *Control Design*. We hope you will find it useful in your journey to success and security.

– ***The Editors***

BEGIN

Sponsored by wurldtech
A GE Company

PutmanMedia®

Table of Contents

Process instrumentation (level 1) cybersecurity issues 3

New standards coming for cybersecurity of critical infrastructure 5

Q&A: DHS cybersecurity director on avoiding security vulnerabilities when connecting to the IIoT 7

DHS urges 7 strategies to defend ICS 12

OT Security: Where to Start 13

Process instrumentation (level 1) cybersecurity issues

Cyber vulnerabilities from integration lurk everywhere, from the bottom up

By Joe Weiss

In his presentation at the October 2013 ICS Cyber Security Conference, a DOD researcher called ICS cyber warfare a "race to the bottom." Of course, he wasn't commenting on the morality of cyberwarfare. He was referring to the soft underbelly of ICS: the Level 1 field devices in the lexicon of the Purdue Enterprise Reference Architecture which is a 1990s reference model for enterprise architecture, developed by members of the Industry-Purdue University Consortium for Computer Integrated Manufacturing.

Level 0 — The physical process — The actual physical process.

Level 1 — Intelligent devices — Sensing and manipulating the physical processes. Process sensors, analyzers, actuators and related instrumentation. Time frame: milliseconds to seconds.

Level 2 — Control systems — Supervising, monitoring and controlling the physical processes. Real-time controls and software; DCS, human-machine interface (HMI); supervisory and data acquisition (SCADA) software. Time Frame: minutes

Level 3 — Manufacturing operations systems — Managing production work flow to produce the desired products. Batch management; manufacturing execution/operations management systems (MES/MOMS); laboratory, maintenance and plant performance management systems; data historians and related middleware. Time frame: shifts, hours, minutes, seconds.

Level 4 — Business logistics systems — Managing the business-related activities of the manufacturing operation. Enterprise Resource Planning (ERP – e.g., SAP, Oracle) is the primary system; establishes the basic plant production schedule, material use, shipping and inventory levels. Time frame: months, weeks, days, shifts.

The Level 1 process sensors can, in real time and without operator intervention, monitor physical process parameters (pressure, temperature, flow, voltage, current, chemical composition, radiation, among others) and cause preprogrammed changes to the Level 0 physical processes via Level 1 actuators, drives, motor-operated valves, etc. This is where process safety is paramount.

Many such monitoring and control devices used in industrial applications now use the HART (Highway Addressable Remote Transducer) communications protocol, in either its wired or wireless form. In essence, HART enables the overlay of a digital signal on top of the sensor's traditional 4-20ma serial signal. Security researchers have given HART considerable attention in recent years. In 2014, Russian security researchers identified cyber vulnerabilities in wired-HART systems. In January 2016, Applied Risk researchers identified cyber vulnerability issues with WirelessHART systems.

It is important that we understand the proper message and draw the right conclusions about these security studies. The message and conclusions are certainly not limited to HART or HART-enabled devices and systems. For example, similar vulnerabilities have been, or will be, documented in systems using Foundation Fieldbus, Profibus, and Modbus protocols as these protocols also were designed without adequate concern for cybersecurity. The real lesson relates to the cyber threats from the digital integration of Level 1 equipment, and especially integration with human-machine interfaces in Level 2 and 3 operating systems.

Cyber vulnerabilities from integration lurk everywhere, from the bottom up: the sensors (including the microprocessor that makes the device a transmitter – sensor/transmitter); the sensor/transmitter transmission protocols; the asset management software; and beyond. Daisy-chaining enter-

prise levels has made the entire system exponentially more cyber vulnerable—and dangerous.

Sensor communication systems have evolved from analog to digital to facilitate integration with HMI and other aspects of higher level control systems which use Windows and other commercial operating systems. Sensor/transmitters are now directly connected to the final end devices (drives, valves, actuators, etc) so that real time monitoring and control can be accomplished at the device level and provide the information back to the HMIs. Unfortunately, sensor/transmitters and other field devices have not evolved to match the enhanced cybersecurity risks posed by the digital communication capabilities including the continued lack of authentication. In general, there are no commonly accepted standards for key management in a control system environment. The Applied Risk researchers defeated WirelessHART digital keys and cryptography management by compromising the security manager. There are also insufficient safeguards to protect or validate data integrity at this level. Sensor/transmitters and other Level 1 devices have accordingly become vectors for cyber-physical attacks.

Above the field devices is the Level 2 asset management software. This software can be installed on the control system PC and its operator interface can be used to monitor the data from HART or other digitally-enabled field devices. The asset management software provides the operator with access to both the primary variables, many secondary variables and other information transmitted by the field devices. An operator (or a potential attacker) can check the field device measurement output, calibration logs, and error alerts and can reconfigure the sensor/transmitter or control device. Reconfiguration can include changes to variables, limits, alarm ranges, and so forth, and even reflash and write to Electrically Erasable Programmable Read-Only Memory (EEPROM).

The networking of Level 2 and 1 devices are also subject to compromise. The strategic importance of such vulnerabilities cannot be underestimated. An attacker could manipulate the operation of industrial processes, with consequences generally obvious to all. The attacker could also affect the maintenance of industrial equipment, because asset management software is used for predictive equipment maintenance. As demonstrated by the Aurora vulnerability, it is not always clear how a cyber compromise affecting equipment lifetime could be detected. As with Stuxnet, the input data often would be accepted by the controllers without question if the data remains within an acceptable operating range—either the original range or the attacker's revised range.

Generally speaking, HART security researchers have shown any number of potentially disastrous outcomes, from the compromise of a single device to the use of the compromised device to compromise other devices on the HART highway, or to alter the industrial processes controlled by the asset management software. Of course, an attacker interested in financial manipulation could also use the asset management software as a backdoor into the ERP system. The security researcher that found the wired-HART vulnerability was an ERP security expert focused on gaining unauthorized access to the ERP.

The digital integration of field devices has occurred with the best of intentions: Human, real-time interface with sensor data facilitates the equivalent of "just-in-time" control. (How wonderful to be able to adjust your wind turbines remotely based on the current weather update.) But we can't keep ignoring the cyber vulnerabilities introduced by having remote monitoring and control capabilities.

Do all critical systems need to go "back to the future" with nothing but 4-20ma point-to-point serial? Not necessarily. But we do need to think things through. Do operators and analysts really need control system data within milliseconds? How do you perform risk assessments of systems and devices with almost no security? Should safety and control systems be integrated? Should field device integration approaches such as FDT which standardizes the communication and configuration interface between all field devices and host systems using HART, Fieldbus, Profibus, or Modbus be more secure before it is used in critical control system applications? And so forth.

Control Systems Cybersecurity Expert Joseph M. Weiss is an international authority on cybersecurity, control systems and system security. Weiss writes the Unfettered Blog for ControlGlobal.com, where he weighs in on cybersecurity, science and technology, security emerging threats and more.

New standards coming for cybersecurity of critical infrastructure

Even if you don't see your industry as critical, it stands to benefit from emerging activities to harden networks through standards

By Ian Verhappen, P.Eng.

In response to Executive Order (EO) 13636, NIST released version 1 of "Framework for Improving Critical Infrastructure Cybersecurity" in February 2014. It says the EO defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters," which is certainly potentially a broad swath of industry. Critical infrastructure is commonly assumed to be utilities, emergency responders and similar, but it could and perhaps should include all forms of manufacturing, or at least those related to the energy industry and other hazardous goods.

The EO's Framework model works somewhat like most risk management tools, developing a grid of functions (Core) versus compliance (Tiers) to determine your level of risk and compliance. A number of tools are available to assist with performing the analysis, and Table 2 in Appendix A includes a wide range of references for each of the identified functions and subcategories.

What, you may ask, does all this have to do with wireless?

Many organizations treat wireless differently than wired infrastructure, in many cases going so far as connecting the wireless networks to the control system via the DMZ. This, of course, adds more delay to the signal transit time, while also providing another opportunity to make an error in the configuration. This is despite the fact, as we've discussed in the past, that the field sensor network protocols at least contain inherent security features more rigorous than the consumer products, such as cell phones and tablets that we're starting to use for remote monitoring (and I am confident, in some cases, control).

In addition, much of the critical infrastructure relies on SCADA to connect widely dispersed units such as pump stations, transformer stations, etc., which, because of the distance, uses a wireless backhaul based on protocols such as DNP3 or IEC 61850. Of course, many of the SCADA systems, certainly legacy and large installations, likely use licensed spectrum, which helps with reliability. But as the saying goes, "bits are bits." So if they're being routed via standard protocols and in particular as IP packets, the security risk increases at the ends of the connection because of the same vulnerabilities as for any IP-based protocol.

Despite the importance of SCADA to infrastructure and the fact that the majority of these systems are migrating to IP-based networks, there is a surprising lack of standards to assist with and provide best practices for the design, installation and maintenance of these systems. In response to government requests to pipeline operators, the American Petroleum Institute (API) has developed a small set of standards that begin to address some of the unique requirements related to pipeline SCADA systems. I also understand that these documents will soon be up for review.

I'm also working with some folks at ISA to investigate the need for a complementary set of SCADA-related standards and/or technical reports to improve the integrity of all forms of SCADA systems with particular focus and consideration on the "gaps" not covered by existing documents that address protocol, physical layer, etc. ISA will

be issuing a survey document in early February that will also be posted on the ISA website for approximately one month to confirm sufficient interest (i.e. volunteers), minimal conflict with existing documents (such as API), and, of course, input on scope and purpose.

For those readers interested in participating in the new ISA SCADA standard, please contact me at the email address listed below.

Even though much of the process industry is exempt from the Executive Order and associated Framework document, like many things, best practices should be industry-independent. So, there are a number of useful references and tools available courtesy of U.S. taxpayers to improve the overall integrity of our SCADA and control systems. In this case, "I'm from the government and I'm here to help you" is true, provided you make the effort to determine which parts of the tools provided add value versus unnecessary documentation.

Control contributor Ian Verhappen, P.Eng., is an ISA Fellow, ISA Certified Automation Professional (CAP), and a member of the Automation Hall of Fame. Ian is a recognized authority on Foundation Fieldbus, industrial communications technologies and process analyzer systems. You can reach him at iverhappen@gmail.com.

Q&A: DHS cybersecurity director on avoiding security vulnerabilities when connecting to the IIoT

Marty Edwards, head of the U.S. Industrial Control Systems Cyber Emergency Response Team, speaks about security vulnerabilities when control networks connect to other environments

By Dave Perkon

Fundamental security issues can be introduced when connecting control system environments to other environments such as business networks. Marty Edwards, director of Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) at the U.S. Department of Homeland Security, spoke exclusively with Control Designabout several issues that need to be addressed when deciding to open your network and share data.

ICS-CERT works to reduce industrial control system risks within and across all critical infrastructure sectors by coordinating efforts among federal, state, local and tribal governments, as well as industrial control system owners, operators and vendors.

Edwards brings more than 20 years of experience and a strong control systems industry focus to DHS. Before coming to the ICS-CERT, Edwards was a program manager at Idaho National Laboratory. He has also held a wide variety of roles in the instrumentation and automation fields, including field service, instrument engineering, control systems engineering and project management. Edwards holds a diploma of technology in process control and industrial automation (magna cum laude) from the British Columbia Institute of Technology.

Marty Edwards, director of Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) at the U.S. Department of Homeland Security, spoke exclusively with Control Design about several issues that need to be addressed when deciding to open your network and share data.

Source: U.S. Department of Homeland Security

CD: At Control Design, we appreciate the work you're doing every day. We're definitely serious about cybersecurity, but perhaps, like many of t he machine builders out there, we don't know as much as we should. You said in your letter that incidents are happening daily. What's a typical cybersecurity incident related to industrial control systems?

Edwards: They can be detected through a variety of means, and they can actually span a fairly wide range of incident types. Incidents range from what I call commodity-type malware which could be a Trojan design dealing with banking information that is proliferating around the Internet accidentally getting into an industrial control system and infecting the machines. Or it could range all the way out to a significant, advanced and persistent threat from a nation-state-level actor who is very surgically and specifically targeting that control system for whatever the reason is.

CD: Are they causing any type of damage, or what is the typical result when an intruder compromises the control system environment?

"The control system designers have to weigh the advantages of the connectivity with the disadvantages of the security risk that connectivity brings into the system, and then you have to protect it at an appropriate level."

Edwards: We don't have a lot of cases documented globally where actual damage has occurred. Probably the most widespread incident that's been talked about is Stuxnet, which actually caused damage to process equipment. There's also an incident widely recorded in the open press in Germany of a steel mill that may have had some type of malware impact its steel-making process. But, for the most part, the incidents of the malware don't really cause much harm. It would be more of an annoyance if it were in the sort of commodity malware family. But certainly there could be loss of production involved if you have to take a system off-line to clean it up or if the malware somehow affects the processing or uptime of the control system itself causing it to go off-line, resulting in production loss.

CD: So, the Industrial Internet of Things is coming, whether anyone likes it or not. Some are saying it's not secure, but nothing's going to stop it. For the average machine builder though there are likely some safety issues they should be aware of that perhaps they don't pay as much attention to. Are there things the machine builder and controls designer should be doing to address security issues?

Edwards: Yes, absolutely, and I have a lot of empathy for the control system designers because, before coming into this role in security, I was a control systems engineer working both for vendors and users. My background is in the distributed control system area that did continuous plants, but I certainly have empathy. I think the advice is to very clearly understand what your system or machine is designed to do, and it's, for example, a life-safety type of application, or you're doing some type of engineered controls where you have to prevent entry into an area; you want to make sure that those types of systems are completely 100% air-gapped or isolated from any corporate environment, any engineering type environment, any other networks.

The life-safety types of systems should be completely stand-alone and very rigorously protected from a change control point of view. As you get into other systems that don't have a direct life-safety type of application, such as a process skid in a typical manufacturing plant, there's a lot of impetus to connect those to your corporate environment and to your other control-system environments, and what you have to do is look at the risk of compromise or malfunction of that device versus connectivity from a business perspective. Usually it's not the integrator that can make this decision; it's the asset owner or the owner of the manufacturing plant.

The control system designers have to weigh the advantages of the connectivity with the disadvantages of the security risk that connectivity brings into the system, and then you have to protect it at an appropriate level. I think all too often these systems are shipped with an Ethernet card in the PLC backplane or Ethernet connection right on the processor, and people see that, and they just simply connect it to the corporate network and leave it with the default usernames and passwords. It's wide open, and the default security is often turned off. My wish is for the manufacturers and integrators to just take that first step, the first look, at how the security of this device is being configured for whatever application it's being used.

CD: That's a great suggestion: Get started with cybersecurity, and don't just leave access wide open. There are a lot of wireless connections being made on the plant floor to a smartphone or tablet, for example. Aren't those the same concerns as connecting to a business network?

Edwards: They're certainly very similar concerns. I think that people tend to actually think about the security of wireless implementations a little bit more carefully before they actually roll them out because just the term "wireless" makes them think about security. So it's not unusual for us to see wired installations that have absolutely no security and wireless that have at least some.

Of course, just by involving a wireless signal, now you have to start to think about how far that wireless signal propagates. Does it leave my property? If you're in a manufacturing plant or a small facility, can somebody from outside the chain-link fence either inadvertently or intentionally access the wireless signal, and what security protection do you have in place there?

When it comes to tablets, smartphones and bring-your-own device (BYOD), I would urge companies to always, if they need to use a wireless device for human-machine interface (HMI) or process interface, only do so with corporate-owned devices that are under the control of the corporate security policy. I think that there's a trend in the business IT world to let people bring their own devices to connect to the network, but, for these critical process control applications, it's imperative that the devices be under the security policy of the corporate security folks.

And then you can also use enclaves, or, as we call them, demilitarized zones, to bring all your wireless devices in and then group them together before giving them access to any of the sensitive process control networks. Some pretty rigorous controls should be in place so users have to actually authenticate to the system. They need to prove who they are, with a token or some type of two-factor or multifactor authentication, before they're actually allowed to make changes in a machine or process control environment.

CD: You don't think that is likely with the bring-your-own-device type of scenario?

Edwards: It's just a lot harder to enforce in the bring-your-own device scenario. You don't know what the user has installed on the device already. There may be malware on the device that could compromise your process control environment. The IT world is building the policies, and in general when you look at the process control world we tend to lag behind the IT world by about 10 years, so I think it's a very risky area.

We see a lot of issues in those areas, as well as in remote access. Employees have remote access from their computer systems at home, or vendors are provided remote access into their products for warranty or monitoring purposes. Those implementations need to be very carefully scrutinized from a security perspective.

CD: Are there cybersecurity concerns, not only from a wired perspective, but from a smartphone or wireless perspective, also?

Edwards: I think we see the gambit; we see both. In the wired implementation, we do see a lot of devices that we believe shouldn't be available or accessible from the Internet, and yet they are. A person takes the programmable logic controller and inadvertently or intentionally plugs it into the corporate network, giving it an IT address, not realizing that that action could in fact expose it through whatever the corporate perimeter protections are to the Internet. This allows network search tools to map all the devices that are available. Then, in cases where there are default usernames and passwords, the level of effort isn't very high for an adversary to get in.

CD: It is really no different than plugging in to the front of the controller at that point, if they leave it that open.

Edwards: Exactly, and sometimes we found that these are intentional, in a remote facility, for example, where there is a manufacturing plant and maybe a mile up the road there is an unattended intake for that plant, and it is off your main campus or property. In some cases we have seen implementations where people go down to the local electronics store and buy a DSL router, plug it in and get a phone line pulled in from the phone company; the device is banging off the Internet. Then they just go and check the bytes.

CD: And then a hacker, with a little bit of technical knowledge, can go in there and wreak havoc if they want.

Edwards: Absolutely, so you just have to take a really good look at what you are using the device for and what implications it has if the device malfunctions or incorrectly performs the command set that's inside of it. If the control algorithms get rewritten or overwritten, what implications does it have to the process? Consider personnel safety, machine reliability, equipment damage or rejected product, and then put the proper security envelope around that.

CD: That's great advice. I have seen a hydroelectric application in a tropical location that had a wide open network. They connected a main control room and nine remote sites via phone lines and Ethernet. It was wide open. With little work, an adversary could shut power off to a good percentage of the population. It is a concern.

Edwards: The cost of protecting those types of installations has calmed down dramatically. You can buy relatively inexpensive end-to-end VPN solutions where you could encrypt all of the communications between the various facilities and take away a lot of the network exposure. It really doesn't come up when the integrator is laying it out.

The integrator often doesn't go in with a security mindset. In an IT installation, if you are a business that had a corporate headquarters and you had six field offices in different states, no networking or communications engineer would think of running those types of communications open over the Internet anymore. You would never run your email or financial billing across open networks, so why do we think that's OK in the machine and process control world?

CD: So that leads us to a lot of the device and control hardware suppliers who see the value of production, machine and device data. They're kind of the ones leading the charge for the Industrial Internet of Things. At NI-Week this past August, IBM's Greg Gorman said that cybersecurity is just an engineering problem waiting to be solved. If that's true, why not make finding the solution a top priority from a hardware standpoint?

Edwards: This is one of the big challenges for not only the Industrial-Internet-of-Things community, but for other communities and sectors such as building automation. I was at a large building automation conference several months ago, and, while walking the floor, I could see air conditioners and all kinds of heating, ventilating, and air-conditioning devices with little antennas. They're all sending their data up to some post system. I saw what I think somebody referred to as the lick-and-stick sensor. It's a temperature transmitter that you peel off of a small cardboard card and stick it on the side of a pipe. It's wireless. For power, it'll harvest thermal energy from the pipe that it's attached to, and it'll transmit a signal. When you start looking at the computing power that it takes to implement basic encryption inside of these devices, you get into a very cost-prohibitive type of function. I was talking to one manufacturer, who I won't name, that manufacturers thermostats for commercial and residential use. The manufacturer said their price point was such that they couldn't afford to put in $0.50 for the encryption technology because it would price them out of the competitive market.

So as we get into this smaller, cheaper, more commodity-based sensor market, the industry is really going to have a hard time adopting these edge sensors in a secure fashion. The end devices do not yet have the horsepower needed for security and since they're a throwaway and disposable type device, nobody really fixes those kinds of things. You just throw it away and put a new one in. If that's the case, the security configuration will have to be almost default, out of the box, an always-on type of implementation to work. You really can't expect the end user to manipulate them in anyway.

CD: So plan for the minimal in many of the edge devices?

Edwards: Right. In those types of installations, my first advice would be to know if they're all wireless. If so, have them on their own private wireless network. If there is encryption or wireless security available, use it or the best possible security available on all of the devices. Then, prior to bringing those networks into your main machine or process control network, bring them in through some type of perimeter processing. Have walls with some very

strict rules in place that control the inflow and egress of network traffic and continuously monitor those networks.

CD: How many or few are monitoring the networks?

Edwards: Another one of the big takeaways that we've seen during assessments of industrial facilities is that, although they may have their control system engineers that look after all the equipment, nobody's really monitoring any of the systems for security alerts or weaknesses. So, even if you do have some type of intrusion-detection system that's in place, that's monitoring the perimeter of your control network, typically it's only ancillary duties that the engineer looks at that console to see. "Oh, what was this? We had five login attempts last night from somewhere that we don't recognize."

We need to get it ingrained into the operational doctrine that monitoring the security of these devices and networks has just as much importance as keeping the networks running themselves.

CD: It's certainly good to collect the security data, but you have to look at the data once it's collected and make some decisions on it.

Edwards: You have to take the first step, which is to collect the data. All too often in this area we find that people have turned off login capabilities in the security area, even on the human-machine interface. For example, if you want to login with a username and password, a lot of the devices are not logging who logged in and at what time, so you can't extract that information. The next part after you've collected the data is to assign real human capital and personnel to analyze the data on some sort of regular routine and basis. Look for anomalies; if you don't have somebody looking at it, it's of limited value.

CD: So, the security protection can be questionable if you don't do the right thing and be proactive. I've recently seen a controller with cybersecurity layered and embedded in the controller, connections and interconnections. Do you see that happening in industry that can afford to pay more to have cybersecurity technology built-in?

Edwards: The vendor community has been discussing this for some years. The message back up to the security folks is that the end users are not demanding this. It isn't something that they're willing to pay for right out of the box. Hopefully that is shifting and people are willing to pay a premium for a product that's secure right out of the box. I think it's inevitable that the community moves that way. I'm just somewhat disappointed that we haven't seen a lot faster change in that area.

It's difficult because you have interoperability issues with legacy devices. If I come out with a PLC or some sort of control device that has great whiz-bang encryption right at the controller level, how does it interact or operate with the rest of my legacy equipment that's 20-plus years old and doesn't have the same features. It's a complex problem that takes a systematic approach over several years. You actually have to think about how you're going to implement it, what it changes you're going to make to your overall system and how you're going to phase it in and then maintain it over the lifecycle of that asset.

CD: Do you see any new or current past or future Ethernet protocols, industrial protocols, for that matter, having a greater impact on cybersecurity, good or bad perhaps?

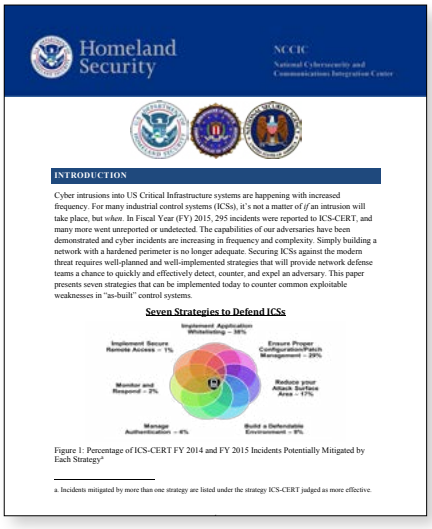
Edwards: Not really. I can't say that I believe that this challenge is protocol-specific or is of more concern with one protocol over another. We've seen issues and vulnerabilities in serial communications; we've seen issues and vulnerabilities with IP Ethernet type of implementations and even proprietary protocols over proprietary networks. Security has to be looked at from a system-of-systems approach. You have to look holistically across your entire installation and design security in from the ground up, whether that means putting the appropriate defensive layers in place around the less-than-secure devices or it means lobbying your vendors to provide you with hardened devices in certain high-risk areas of your process. It's important to group all of those things together.

DHS urges 7 strategies to defend ICS

Department says 295 incidents were reported in 2015, and many more went unreported or undetected

The U.S. Dept. of Homeland Security (DHS) report, "Seven Strategies to Effectively Defend Industrial Control Systems (ICSs)," provides procedures that can be implemented immediately to counter common exploitable weaknesses in control systems.

"In fiscal year 2015, 295 incidents were reported to the Industrial Control Systems Cyber Emergency Response Team, and many more went unreported or undetected," states the report, which was Drafted by the National Cybersecurity and Communications Integration Center (NCCIC). "Securing ICSs against the modern threat requires well-planned and well-implemented strategies that will provide network defense teams a chance to quickly and effectively detect, counter, and expel an adversary."



Homeland Security

NCCIC
National Cybersecurity and Communications Integration Center

INTRODUCTION

Cyber intrusions into US Critical Infrastructure systems are happening with increased frequency. For many industrial control systems (ICSs), it's not a matter of *if* an intrusion will take place, but *when*. In Fiscal Year (FY) 2015, 295 incidents were reported to ICS-CERT, and many more went unreported or undetected. The capabilities of our adversaries have been demonstrated and cyber incidents are increasing in frequency and complexity. Simply building a network with a hardened perimeter is no longer adequate. Securing ICSs against the modern threat requires well-planned and well-implemented strategies that will provide network defense teams a chance to quickly and effectively detect, counter, and expel an adversary. This paper presents seven strategies that can be implemented today to counter common exploitable weaknesses in "as-built" control systems.

Seven Strategies to Defend ICSs

Figure 1: Percentage of ICS-CERT FY 2014 and FY 2015 Incidents Potentially Mitigated by Each Strategy[a]

a. Incidents mitigated by more than one strategy are listed under the strategy ICS-CERT judged as more effective.

Tot that end, the DHS/NCCIC report outlines 7 strategies:

- Implement application whitelisting to detect and prevent execution of malware;
- Ensure proper configuration and patch management centered on safe implementation of trusted patches;
- Reduce attack surface areas by isolating ICS networks from untrusted networks, especially the Internet, locking down unused ports, turning off unused services, and only allowing real-time connectivity to external networks if there's a defined business requirement or control function;
- Build a defensible environment by segmenting networks into logical enclaves, and restricting host-to-host communications paths, while letting normal system communications continue;
- Manage authentication by implementing multi-factor authentication where possible, and reducing privileges to only those needed for a user's duties;
- Monitor and respond by checking Internet protocol (IP) traffic on IC boundaries and within the control network, and using host-based product to detect malicious software and attempted attacks;
- Implement secure remote access by finding obscure access vectors, even "hidden back doors" created by system operators, removing them wherever possible, especially modems that are fundamentally insecure, and limiting any access points that remain.

The report provides more information and real-life examples of each threat and preventive measure. You can access the complete report here.

OT Security: Where to start

Uncover existing weaknesses, map out potential future risks and recommend mitigation strategies with a cybersecurity assessment

Security requires taking a proactive stance to maintain health and prevent bad stuff from happening. In the industrial sector, a great place to start is with an overall site security assessment and health check that can uncover existing weaknesses, map out potential future risks, and recommend mitigation strategies.

In a 2014 ARC study, The Future of Industrial Cyber Security, it recommends organizations "focus on cures, not remedies." (In this case, ARC seems to be saying a remedy treats a disease while a cure eradicates it.) As the study reveals, many existing control systems were developed prior to online security being as grave a concern as it is today. And while the need for compensatory controls and frequent patching (remedies) hasn't gone by the wayside, ARC advises companies to invest more time and energy into developing new strategies that can cure (to the maximum extent possible) the underlying issues.

This is why security hygiene needs to be an organizational priority—and it requires the right game plan. First, emergencies need handling and weaknesses need uncovering. Next comes a treatment plan for any issues found and then it's a matter of ongoing care and prevention. With a security assessment, companies can establish a baseline understanding of their existing security posture and begin to develop an effective long-term strategy for maintaining overall system health and hygiene.

Keep it clean: industrial strength security health

A typical assessment entails:

- Information gathering and documentation relating to an organization's people, architecture, and technology
- Review and analysis of documents detailing network configuration, topology, policies, and other relevant aspects unique to an organization
- Onsite interviews and inspection with subject matter experts for additional technical and contextual understanding not apparent from documentation reviews alone
- Onsite technical testing to assess and evaluate the cyber security posture of assets
- Offline data analysis and application of best practices methodology to assess risks
- Risk assessment to identify sources of vulnerabilities, determine security posture, prioritize potential risks, and provide remediation roadmap
- Findings report to include recommended mitigations based on prioritized risks

Benefits of an assessment include:

- In-depth visibility: Discovery of current security posture via a comprehensive report and workbook that maps out the potential risks for each system analyzed
- Actionable results: Immediate security risk remediation as well as long-term financial planning and resource justification with analysis based on leading expertise in the operational technology security field
- Enhanced security: Best practices methodologies identify key risks and dictate necessary strategies for overall improved security posture

Next, install security solutions purpose-built for industrial and process control environments. Solutions should have a modular platform designed for scale to accommodate complex ICS and SCADA systems and provide full network visibility, control, and protection. And it should interoperate with traditional or next-gen firewalls to provide the right design for your IT–OT security transition zone to best protect your processes and control systems, all without the need for network re-engineering or downtime.

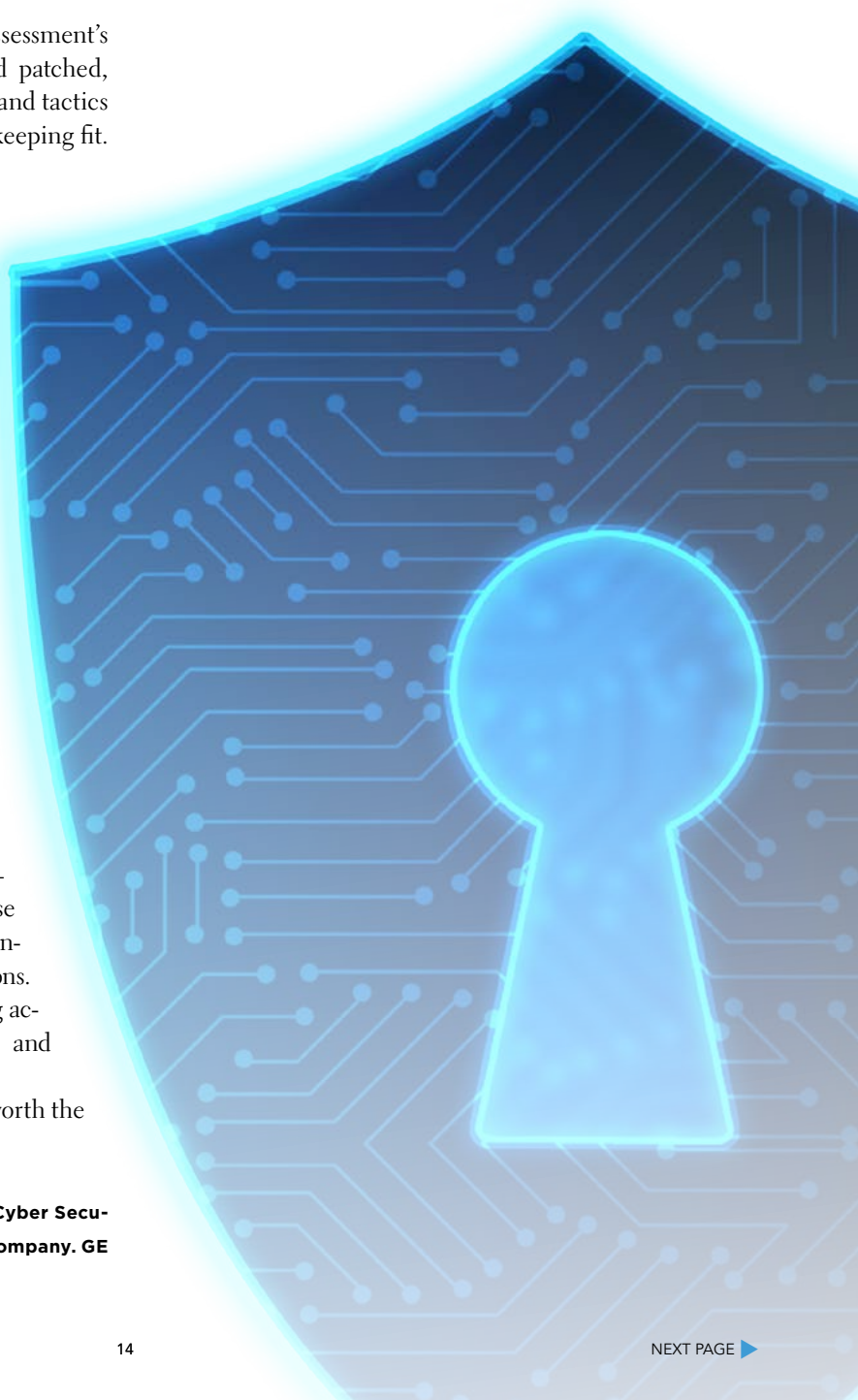
Finally, industrial customers should expect device manufacturers to certify that their products have passed stringent security assessment throughout the product development lifecycle.

Security first

Security cannot be an after thought. Once an assessment's been completed, with vulnerabilities found and patched, companies can also look to implement new rules and tactics and continue to build upon their game plans for keeping fit.

These may include:

- Decreasing the use of commercial off-the-shelf systems that are easier to hack (the cost savings often aren't worth the risk)
- Forbidding use of personal devices in control rooms
- Requiring changes to default passwords on equipment
- Blocking off USB ports (Do you want a USB drive to be the downfall of your operation?)
- Enforcing rules where they already exist
- Implementing stricter pre-employment screening requirements
- Conducting property inventories and audits (on desktops, laptops, removable media, security tokens, access cards)
- Enhancing access controls for privileged users



Moreover, organizations should offer cybersecurity training programs that encourage dialogue—between engineers, contractors, everyone—to raise awareness of cyber security risks, including the dangers of setting up unauthorized Internet connections. Risk is everywhere, but can be reduced by enabling accountability, implementing least privilege access, and regulating sensitive control and data access.

Keeping up security hygiene isn't easy, but it's worth the time, effort, and justified expense to be safe.

This article is excerpted from An Executive Guide to Cyber Security for Operational Technology, by Wurldtech, a GE Company. GE is the sponsor of this Special Report.

Wurldtech, a GE Company

The Industrial Internet brings great promise for operational productivity and data-driven efficiency. But increased connectivity, technology complexity and the Internet of Things are also driving increased threats. In today's environment, industrial organizations have to manage risk associated with external threats, like state-sponsored cyber espionage, as well as internal threats, such as configuration errors that might cause an unplanned outage.

Wurldtech helps indust rial operators and device manufacturers mitigate operational technology (OT) threats and vulnerabilities. We provide products and services that help customers design, test, certify, and secure their internet-connected devices, ICS and other critical controls, as well as their site operations.

Wurldtech began with an industrial mindset. We know what it means to operate and protect a process control strategy. Our technology is purpose-built for protecting industrial processes. Through years of development with deep industry insights, our products can demonstrate unprecedented visibility and protection of critical infrastructure.

Our talented staff of OT cyber practitioners are skilled in applying security technology and processes to a wide variety of industries. Fortune 500 customers rely on Wurldtech to protect their brand reputation in oil & gas, transportation, utilities, healthcare and many other industries. Wurldtech can help customers reduce their attack surface, while developing a robust plan for long-term OT resilience.

Learn more at www.wurldtech.com

wurldtech
A GE Company