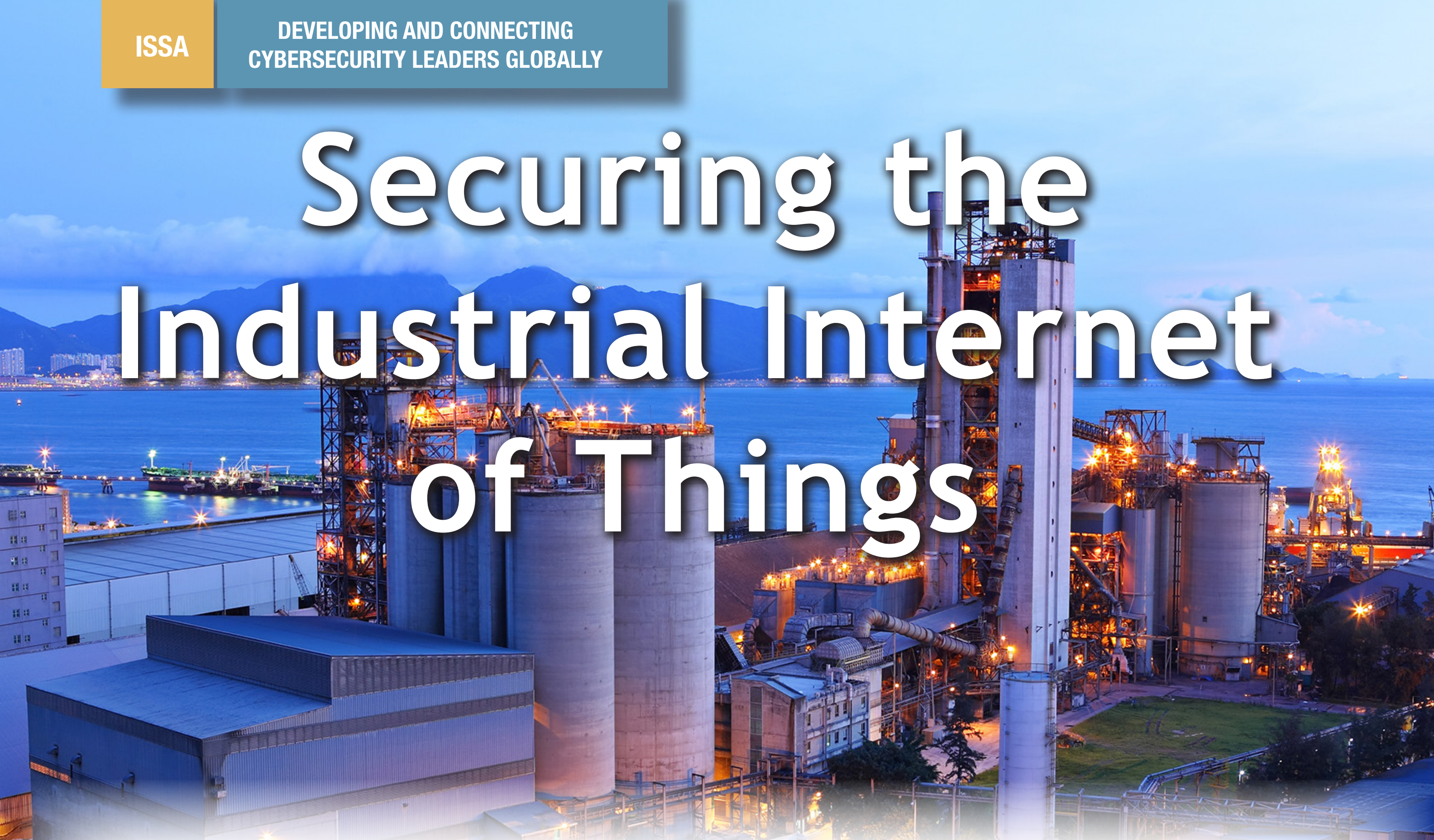


Securing the Industrial Internet of Things

By David Meltzer – ISSA member, Metro Atlanta Chapter

This article discusses security aspects of the Industrial Internet of Things—the explosion of IP-connected devices used in such areas as control systems, manufacturing, utilities, and transportation.

Abstract

This article discusses security aspects of the Industrial Internet of Things—the explosion of IP-connected devices used in such areas as control systems, manufacturing, utilities, and transportation. The industrial Internet of things, like Internet of things as a whole, is rapidly growing and evolving, but comes from a very different historical context. Industrial systems have different attack vectors and threats associated with them, and although many standard IT security concepts can be applied, special consideration needs to be given to the unique requirements and constraints in these environments.

I have spent most of my career in information security focused on IT security. The first time someone asked me about securing the "OT" or "ICS" side, I didn't know what either of those terms meant. It was explained to me that OT (operational technology) and ICS (industrial control systems) both referred to the control networks—the PLC, DCS, HMI, and things like that. I didn't know what a single one of those acronyms meant either! It took me a long time to fully understand this environment. I had to learn the systems involved—that list of new acronyms and what they all did—but more so the unique requirements and challenges faced in securing these systems. Through that process, I have come to appreciate this new world of security and why it's such a critical area of growth and risk today.

While the biggest buzz around the explosion of new IP-connected devices has been around the broader Internet of things (IoT), the piece comprising the industrial Internet of things (IIoT) is still substantial—a $2 trillion opportunity by 2020.[1] The World Economic Forum put out a report in January 2015 on the industrial Internet of things that identified the chief risk and challenge as security and data privacy.[2] With those two data points the light bulb went off in my head: with an explosion in the number of these industrial connected devices and security the #1 challenge—this sounds like something our industry can help with!

What are we trying to secure?

It was easy to ignore industrial systems in the past because they had traits that made them mostly immune to the kinds

1 Simona Jankowski, "*The Sectors Where the Internet of Things Really Matters*," Harvard Business Review, October 22, 2014 - https://hbr.org/2014/10/the-sectors-where-the-internet-of-things-really-matters/.

2 World Economic Forum, "*Industrial Internet of Things: Unleashing the Potential of Connected Products and Services*," January 2015 - http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf.

of threats IT networks faced. The systems were not connected to the IT network—in fact they did not even speak IP. In the earlier days, they were not even on a network at all, but rather connected through serial communications. Once networking was adopted, a complete air-gap still existed between the IT and OT networks, and the latter used proprietary protocols that no attackers understood. You might remember this is the same network evolution we saw on the IT side, and we know where it ended there—with every device interconnected and communicating over standard protocols.

The same evolution has been happening with industrial devices, with a distinction being made between the use of industrial Ethernet as the growing standard, and fieldbus technologies as the legacy incumbent. Still, with very long life cycles in industries such as manufacturing this is a slow evolution, and understanding the security considerations of these legacy protocols and systems will be important for many years to come.[3]

Security concerns apply at both the network and system level. At the network level, it is critical to understand what protocols are being used and for what purposes. Some of the most commonly used industrial protocols, operating at different layers of the stack, include Modbus, DNP3, IEC 61850, Ethernet/IP, and PROFINET. While some protocols are still proprietary to a particular industrial automation vendor, most are now publicly documented. There are freely available implementations of Modbus,[4] DNP3,[5] and other industrial protocols, and industry groups such as ODVA provide public support for protocols including Ethernet/IP[6].

3 Lydon, Bill, "*Industrial Ethernet Growing but Fieldbus Remains Dominant*," Automation.com, November 11, 2013 - http://www.automation.com/automation-news/article/industrial-ethernet-growing-but-fieldbus-remains-dominant.

4 Modbus.org, "*Modbus Technical Resources*," - http://www.modbus.org/tech.php.

5 DNP3 Project - https://code.google.com/p/dnp3/.

6 ODVA - https://www.odva.org/.

Industrial Control Systems Terminology

DCS: Distributed Control System – computer that automates processes, more often used for continuous and large-scale process control than a PLC

DNP3: Distributed network protocol – an industrial communication protocol used most commonly in the utilities sector

Ethernet/IP: A popular industrial Ethernet standard

Fieldbus: Networking technologies commonly used in industrial networks before/instead of Ethernet

HMI: Human Machine Interface – interface an operator uses to monitor and control a system

Modbus: A serial communication protocol used in industrial systems; it also has been adapted to be used over standard TCP and UDP

PLC: Programmable Logic Controller – computer that automates processes

Profinet: A popular industrial Ethernet standard

Sensor: A device that gathers information from the environment

At the system level, there are a handful of industrial automation vendors that produce the majority of all systems deployed and needing to be secured. The vendors vary depending on what industry and geography is involved, but Siemens, ABB, Emerson, Rockwell, and General Electric are all leaders in this space.[7] These are the PLC (programmable logic controllers), DCS (distributed control systems), HMI (human machine interface), and sensors, to name a few, that make up the millions of industrial devices. Although there are software packages running on standard Windows and UNIX systems in some environments, they make up a small fraction of total

7 Pinto, Jim, "*Top-50 Automation Companies*," Automation Media, November, 2013 - http://www.automationmedia.com/JimPinto.asp?ID= 41.

deployments. The large majority of devices are small, embedded systems, running real-time operating systems, communicating using the protocols previously discussed, and being used for a very specific part of an operational process.

What are the risks?

ICS-CERT has been monitoring and sharing intelligence about industrial control system threats since 2010, and in that time has published just over 800 advisories relating to current security issues, vulnerabilities, and exploits.[8] Although not an insignificant number, that is less than three percent of the number of total vulnerabilities published in that time period.[9] While everyone in security knows about the Stuxnet attack, there have been numerous reports of other attacks against industrial systems. ICS-CERT responded to 245 incidents in fiscal year 2014, but many more incidents occur that go unreported.[10] In reviewing these incidents, one of the most unfortunate trends that was found was that the access vectors for attack could not be determined because the systems compromised lacked detection and monitoring capabilities. Dragonfly, like Stuxnet, is another sophisticated attack that has been heavily scrutinized by security experts.[11] A recent cyberattack against a German steel mill also received widespread press.[12]

One of the fundamental tenets of industrial security is to reverse the "C-I-A" priority of confidentiality, integrity, and availability because in industrial systems *availability* is always the top priority. However, there is a new letter I'd put even ahead of that: "S" for *safety*. Cyberattacks crossing into the physical world of industrial systems means that not only may physical systems go down, but a sophisticated attack could further cross the line into actually taking human life. Thankfully, that is a line we haven't seen crossed yet, but the evidence and research is mounting that the risk here is real.

There are multiple examples of accidents that have resulted in the loss of life coming from human or computer errors in working with industrial control systems.[13] Fatalities have occurred from unintentional errors in such ICS events as a gasoline pipeline rupture in Bellingham, Washington, a fire in DC Metro, and a Northeast blackout.[14] [15] In IT security we typically would not consider such things to be security events and I don't think that will change for ICS security, but they do fit the definition of an overall "cyber incident." What we do see here is that there are malicious actors out there actively exploiting ICS systems, and these same ICS environments have shown that the impact of events can cause the loss of human life. Connecting those dots is inevitable at some point.

Examining the risk from a network perspective is a good place to start. Dozens of vulnerabilities have been published against industrial protocols such as DNP3,[16] but even network architecture alone can be a significant source of risk. If an entire industrial network was built without considering security to begin with, it likely lacks all the fundamental network security controls that we take for granted on IT networks, from network segmentation to firewalls to deep packet inspection. These types of networks may be very difficult to retrofit with a more modern secure design, due to the highly customized nature of the environments, the long life cycles, and extreme focus on availability. But there is an upside to modern secure architectures, too: building a more secure network is also building a more resilient network, and that means better availability.

The system level is the next place to look at risks. A denial of service may be the easiest attack vector for many industrial systems today, but the ability to modify the programming of a logic controller is what a sophisticated attacker may be after. Just as networks may lack secure designs, older industrial systems may lack the most fundamental system controls appropriate for an embedded environment such as authentication, authorization, logging, and change management.[17] The industrial automation vendors have largely incorporated all these basic security controls into the industrial automation solutions produced today, but there is still a long lifespan

8 ICS-CERT Advisories - https://ics-cert.us-cert.gov/advisories.

9 Common Vulnerabilities and Exposures, Mitre - https://cve.mitre.org/.

10 ICS-CERT Monitor, National Cybersecurity and Communications Integration Center, Department of Homeland Security, February 2015 - https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf.

11 Langill, Joel, "*Defending Against the Dragonfly Cyber Security Attacks*," Belden, December 2014 - http://info.belden.com/abcd-cyber-security-dragonfly-bc-lp.

12 Zetter, K., "*A Cyberattack Has Caused Physical Damage For the Second Time Ever," Wired*, January 2015 - http://www.wired.com/2015/01/german-steel-mill-hack-destruction/.

13 Weiss, Joseph, *"Another ICS Cyber incident with a fatality,"* Unfettered Blog, February 17, 2015 - http://www.controlglobal.com/blogs/unfettered/another-ics-cyber-incident-with-a-fatality/.

14 Weiss, J. 2010. *Protecting Industrial Control Systems from Electronic Threats*. Momentum Press.

15 Minkel, J.R., 2008. *"The 2003 Northeast Blackout – 5 Years Later," Scientific American*, August 13, 2008 - *https://www.scientificamerican.com/article/2003-blackout-five-years-later/*.

16 Peterson, D., "*Why Crain / Sistrunk Vulns Are A Big Deal*," Digital Bond, October, 2013 - http://www.digitalbond.com/blog/2013/10/16/why-crain-sistrunk-vulns-are-a-big-deal/.

17 Peterson, D. "*PLCs: Insecure By Design v. Vulnerabilities*," Digital Bond, August 2011 - http://www.digitalbond.com/blog/2011/08/02/plcs-insecure-by-design-v-vulnerabilities/.

for many of the older systems still in production. Even with a modern deployment, those basic security controls are still quite a ways behind the advanced threat detection capabilities we look for to detect attacks against IT endpoints.

What are the solutions?

"While security solutions have been designed to deal with these security issues in typical IT systems, special precautions must be taken when introducing these same solutions to ICS environments. In some cases, new security solutions are needed that are tailored to the ICS environment." – NIST SP800-82 R2, *Guide to Industrial Control Systems Security*[18]

No one has to reinvent the wheel in order to secure an industrial environment. NIST SP800-82 R2, *Guide to Industrial Control Systems Security* is an excellent, detailed guide on how to approach this. It anchors its guidance in the well-established NIST SP 800-53 and provides a supplement to how the same controls used in IT environments do apply, do not apply, or may be tailored to apply to industrial systems. While reading the entire 247-page document may be a bit overwhelming, reading the 18 pages of Section 2 is an excellent next step in further educating yourself about ICS security.

Another common standard to familiarize yourself with for industrial environments is ISA/IEC 62443 (formerly ISA99) - *Security for Industrial Automation and Control Systems.*[19] This consists of 13 different standards and reports that cover different areas of security. Many of these are still under development, but even the in-progress drafts contain useful guidance in this area and have been years in the works. For example, ISA/IEC 62443 3-2 is in a working draft now and defines grouping assets into zones and conduits—the idea being that effectively segmenting and controlling the paths of communication between devices can limit the ability of attackers to compromise systems, and further mitigate the ability to propagate attacks across a network.[20] Network segmentation is not a new concept to anyone dealing with IT security, but being able to tie back these fundamental concepts of security to standards that have been developed specifically for ICS can definitely help in convincing the OT side of the house that these concepts will work for them too.

From a practical perspective, there are two very distinct ways to think about security solutions. First, designing security into a new industrial deployment. This is, of course, the best way to build security—baking it into the design is always more effective than the alternative. The downside is that some environments may be 20 years away from a completely new design, so this is not always possible.

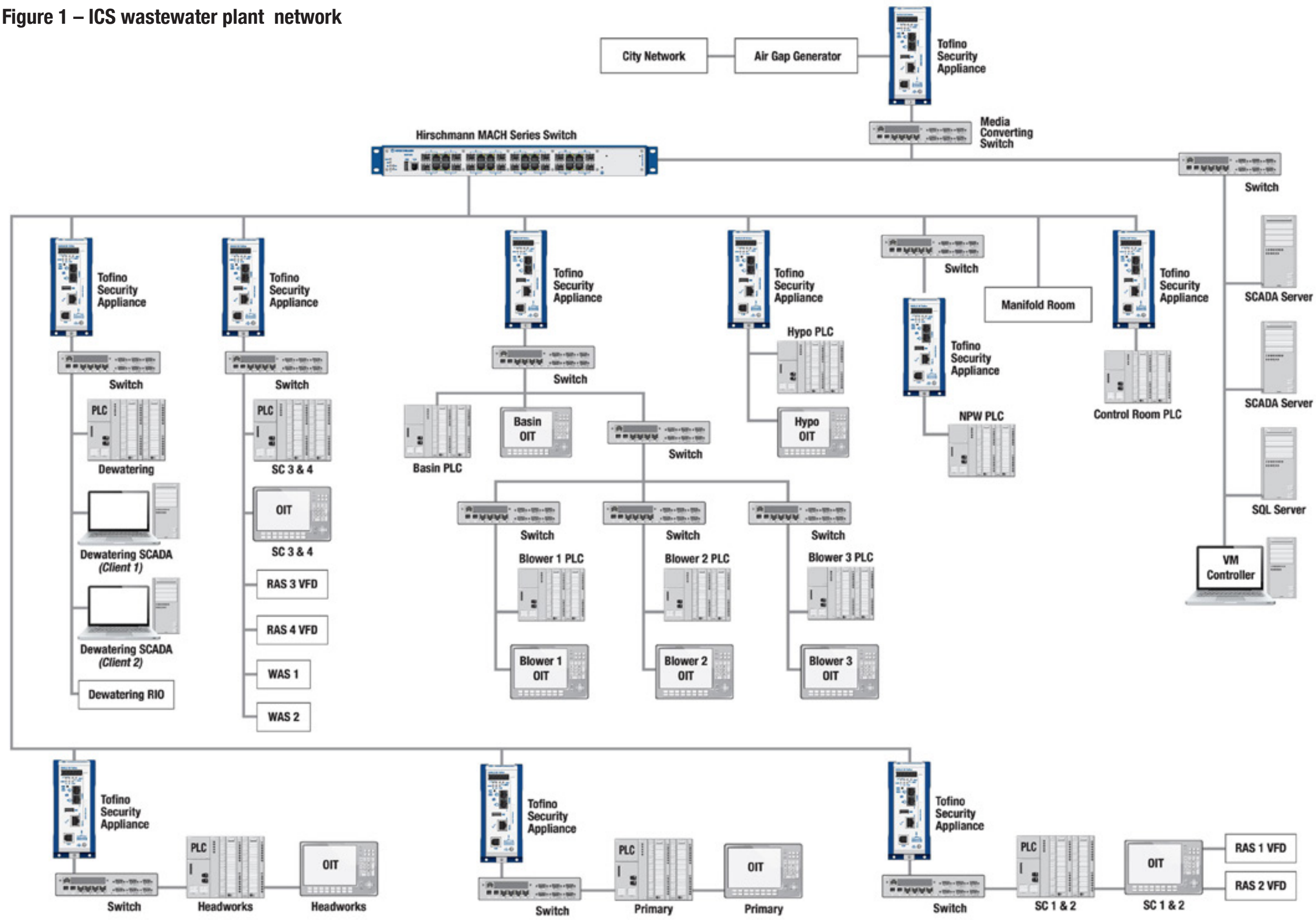
Retrofitting security into an existing environment is the second approach. Being completely non-invasive is absolutely critical for success here. Even disruptions or delays of milliseconds can be unacceptable in some environments, and since availability is the primary concern, doing no harm has to be top of mind. Not only is it important from a security perspective, but its unlikely you will even get a solution deployed unless you can convince those managing the OT environment with overwhelming evidence that the security additions will not cause any disruptions. At the network layer, this means ensuring that normal traffic passes without delay, and any changes to the network can be carefully modeled, tested, and used without interfering with normal operation. Industrial-specific firewalls, gateways, and deep packet inspection devices have been built and are growing in market share. Devices rarely seen in IT environments such as one-way communication devices (data diodes), remote access devices that work over cellular networks, and protocol translating gateways that can speak many of the industrial protocols are a few examples.

18 Stouffer, K., Lightman, S., Pilliterri, V., Abrams, M., Hahn A., "*NIST Special Publication 800-82 Revision 2 Final Public Draft: Guide to Industrial Control Systems (ICS) Security*," NIST, February 2015 - http://csrc.nist.gov/publications/drafts/800-82r2/sp800_82_r2_second_draft.pdf.

19 Byres, E. "*Using ISA/IEC 62443 Standards to Improve Control System Security*," Tofino Security - May 2014 - https://www.tofinosecurity.com/sites/default/files/common/white-papers/Using-ISA_IEC-62443-Standards-WP-v1.2 (May 2014).pdf.

20 ISA-62443-3-2 (IEC 62443-3-2), Security for Industrial Automation and Control Systems - Security Risk Assessment and System Design – August 2014 - http://isa99.isa.org/ISA99 Wiki/WP-3-2.aspx.

Figure 1 – ICS wastewater plant network



At the system level, many traditional security controls need to be re-examined. Any active scanning of a system is going to be met with a great deal of resistance, and for good reason—a scan may easily inadvertently create delays or denials of service. It is important that any use of tools that touch systems go through extensive validation before they ever meet the production environment, which is in many ways the opposite of an IT security approach where scanning the environment to find out what's out there is often one of the earliest steps in an assessment.

While active scanning may be out, proprietary industrial automation vendor systems are not conducive to agent-based architectures either. How about reverse engineering the proprietary protocols the vendors use and talk to the systems over those? That approach has been used by security vendors in the IT space for years, but it only takes one small misunderstanding of a protocol to create an availability problem, so that is also not a great answer.

Let's look at some simple architectures that can improve security from the status quo today. Figure 1 shows a ICS wastewater network from a mid-sized US city that treats 13 million gallons of wastewater each day.[21] The city had upgraded its SCADA network to industrial Ethernet and recognized the risks inherent in connecting industrial controls to the city IT networks. Instead of a flat, open network, something that is very common in ICS environments and allows issues, intentional or unintentional, to easily propagate across the network, the city technicians learned about the ISA/IEC 62443 standards and chose to implement the zone/conduit model it described to provide between network-layer security.

This architecture provides network segmentation, with individual industrial network gateway appliances providing blocking of unnecessary traffic between zones, deep packet inspection capabilities that understands the industrial protocols used in these environments, and monitoring capabilities for the network. Implementing a good network architecture is always a good place to start with securing an environment and in the ICS environment the standards, technology, and expertise all exist to do that successfully.

Where are we headed?

There is still a need for new technologies to be developed in the realm of industrial security. Industrial devices need to be built with security requirements in mind. Although automation vendors have already made some progress in this area, much work remains to be done. Endpoint security also needs better technology solutions to effectively address industrial devices.

21 MacKenzie, H. *"PLC Security for Water / Wastewater Systems,"* March 19, 2014 - http://www.belden.com/blog/industrialsecurity/PLC-Security-for-Water-Wastewater-Systems_511213.cfm.

SECUREWORLD

See Globally. Defend Locally.

Distilling the gobal complexities of cybersecurity down to your city, your network, your shot at a decent night's sleep

2015 Conferences:

Register for a conference near you with these discount codes: **ISSA, ISSASWP, ISSAEO and save up to $200**

For our complete schedule, visit www.secureworldexpo.com

Portland - June 17
Detroit - September 16 & 17
St. Louis - September 22 & 23
Cincinnati - October 6
Denver - October 15
Dallas - October 28 & 29
Bay Area - November 4
Seattle - November 11 & 12

EARN CPE CREDITS

Featured Keynotes:

Carl Herberger
Vice President of Security Solutions, Radware

Colonel Cedric Leighton
USAF (ret.) and CEO, Cedric Leighton Associates

Christopher Pierson
General Counsel & Chief Security Officer, EVP Viewpost

Demetrios Lazarikos
IT Security Researcher and Strategist

James Beeson
CISO
GE Capital Americas

Larry Ponemon
Chairman and Founder of the Ponemon Institute

The 2015 SecureWorld Expo conference theme is the Secret Service. We partnered with one of our country's most valuable organizations to bring you stories about the electronic crimes task force.

SecureWorld Digital:

SECUREWORLD DIGITAL

Connecting you to larger forums, articles and gatherings to shape the conversation. Visit us today at www.secureworldexpo.com to sign up for exclusive web conferences and subscribe to the SecureWorld Post.

Web Conferences:

WebConferences

SecureWorld Post:

SECUREWORLD™ POST
Shaping The Conversation

www.secureworldexpo.com

Security vendors and industrial automation vendors need to cooperate to leverage the existing data collection and analysis systems already in place for process management and expose a security interface to these systems, rather than be forced to choose from the alternative approaches I outlined in the previous section. For example, a security assessment tool could query the API of a supervisory system to gather inventory, configuration, and change information about a PLC. Approaching an industrial environment in that way would avoid having to directly touch any of the most fragile systems in the environment, and that would make for faster, easier deployments of security technology. I hope to see more such cross-vendor cooperation happening in the future, which should ease the concern and risk of security solutions being deployed.

Although technology does need to improve, the biggest barrier to security in industrial control systems is similar to that in IT—resources and budget. The utilities sector in North America has been required to spend around security by the expanding security requirements in North American Electric Reliability Corporation – Critical Infrastructure Protection (NERC CIP), and some of the areas of most attention around NERC CIP include system security management, electronic security perimeters, and security management controls.[22] Although compliance and security are not the same thing, many worthwhile security projects get funded by compliance mandates, and that trend is continuing with NERC. For other industries the call to action may be less urgent without compliance deadlines looming.

Will it take a string of front-page news incidents for companies to start taking these threats seriously? Perhaps that is part of the problem. Unlike personal information breaches, where laws and regulations have forced disclosure of incidents, attacks against private-sector ICS environments are unlikely to fall under any such incidents. It is very easy for such attacks to be ignored, and with ineffective monitoring where little information about the attack could be gathered to begin with, what exactly has been learned to be shared anyhow? Although public disclosure is not necessarily a helpful solution here, improved sharing of threat intelligence amongst peers and in member organizations such as Information Sharing and Analysis Centers (ISAC) will help better inform our industry about these threats and prepare us to act.

Addressing security concerns and building more secure industrial environments will help drive and accelerate the growth of the industrial Internet of things. IT security professionals will play a large role in that, and incorporating industrial security into our world view will give all of us a more complete, holistic view of the threat landscape, helping us better evaluate the overall risks to organizations and create better solutions.

22 Top Five NERC CIP Audit Fails – From the 2013 NERC CIP Reliability Coordinator Compliance Analysis Report, Tripwire, April 2014 - http://www.tripwire.com/register/top-5-nerc-cip-audit-fails/

References

—Macaulay, T. and Singer, B. 2011. *Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS.* Auerbach Publications, CRC Press.

—Langner, R. 2011. *Robust Control System Networks.* Momentum Press.

—Weiss, J. 2010. *Protecting Industrial Control Systems from Electronic Threats.* Momentum Press.

About the Author

David Meltzer is the chief research officer at Tripwire. He has been involved in information security for more than 20 years as a security researcher, entrepreneur, and executive. He may be reached at dmeltzer@tripwire.com.