Mighty Guides®

OT ExpertsShare Their Strategies

Securing Critical Infrastructure in the Power Industry

Sponsored by PAS®

Kaspersky Lab's discovery of Stuxnet in 2010 turned the industrial world on its head. As the first known instance of malicious code specifically designed to seek out and interfere with industrial operations, Stuxnet was a serious wakeup call for OT operators, especially those in much of the world's critical infrastructure. So how has the OT/ICS community responded to the new reality of OT cyber risk?

With generous support from PAS, we asked 7 OT security professionals the following question:

What are the top three pieces of advice you would give a CISO to make the plant OT/ICS environment more secure from cyber attacks?

For OT and IT security people, this is something of a loaded question, largely because OT cybersecurity is still very much a work in progress. For instance, although many contributors stressed the importance of knowing your environment, that in itself is a big challenge that varies from industry to industry and plant to plant. "Asset knowledge" also means different things to different people.

The essays in this eBook provide a wealth of information and present an inside look at an aspect of cybersecurity that is still not well understood. I am certain that anyone responsible for critical industrial operations will benefit from the advice and experiences of those who have contributed to this eBook.

All the best,
David Rogelberg
Publisher,
Mighty Guides, Inc.

Mighty Guides®

Mighty Guides make you stronger.

These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of advice in this guide sits right next to the contributor's name, biography, and links so that you can learn more about their work. This background information gives you the proper context for each expert's independent perspective.

Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.

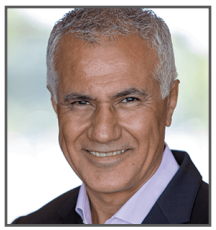
FOREWORD BY EDDIE HABIBI

Digitalization and Industrie 4.0 initiatives require tight integration between the complex, heterogeneous, and highly complex Industrial Control Systems (ICS) and the enterprise IT. However, the very components that enable digitalization—sensors, connectivity and smart applications—also increase risk. Digitalization enhances efficiency, improves safety, and optimizes production, but it also creates more opportunities for bad actors to penetrate operational technology (OT) environments and to wreak havoc.

To secure industrial facilities and ensure safe, reliable production, OT and IT security—traditionally two separate disciplines with different priorities—must come together to share cybersecurity and risk management best practices.

In this eBook, experts on the front lines of OT cybersecurity risk mitigation share their strategies for making control systems more secure. The firsthand experience collected here comes from experts across a diverse range of industries – including oil and gas, chemicals and refining, and power generation. Their essays illustrate the importance of understanding similarities and differences between IT and OT environments. They also share proven experience on adapting IT security controls and best practices to OT environments.

Apply the valuable insights provided in this guide within your own company to protect the endpoints that matter most in your company's industrial facilities—the proprietary industrial control system (ICS) assets responsible for safe and reliable production.



Regards,
Eddie Habibi
Founder & CEO, PAS Global, LLC

Founded in 1993, PAS is a leading provider of software solutions for ICS cybersecurity, process safety, and asset reliability to the energy, process, and power industries worldwide. PAS solutions include industrial control system cybersecurity, automation asset management, IPL assurance, alarm management, high performance HMI™, boundary management, and control loop performance optimization. PAS solutions are installed in over 1,380 facilities worldwide in more than 70 countries. PAS was recently named the #1 Global Provider of Safety Lifecycle Management by ARC Advisory Group including #1 rankings within Chemical, Power Generation, Refining, and Oil & Gas. For more information, visit www.pas.com. Connect with PAS on Twitter @PASGlobal or LinkedIn.

ADVICE FOR CISOs: HOW TO APPROACH OT CYBERSECURITY

In This Section...

IN CRITICAL INFRASTRUCTURE, SAFETY COMES FIRST

BRIAN FOSTER

OT Cybersecurity Engineer
Portland General Electric

Brian Foster is an OT/ICS cybersecurity engineer. Having come to security from controls engineering, he possesses a deep understanding of the industrial equipment and processes he is securing. He builds security into OT systems as a function of safety, and uses quantitative math-based risk analysis to provide meaningful measurements to improvements.

LinkedIn

One of the great challenges in securing OT systems in the power generation and distribution industry is the age of system components. “The average lifespan of a typical ICS device is about 30 years,” says Brian Foster, OT/ICS cybersecurity engineer for Portland General Electric. “And, of course, 30-year-old equipment was not built with cybersecurity in mind.”

Although some vendors produce new equipment that is forward-looking when it comes to cybersecurity, many do not. “A few are building products on a well-made, secure PLC platform,” Foster explains. “They’re good about patching in ways that don’t mess up your controls. There’s a shift among ICS product vendors, but it’s definitely not across the board. I think because of the long lifespan of the equipment, vendors are not pushed very hard to come out with newer technology all the time. It just won’t be adopted very quickly.”

> *“Our number one concern is safety, and any security in our networks has to be designed in a way that is safe. We can’t have a machine fail and kill someone.”*

In this environment of critical infrastructure controlled by a large variety of new and older ICS, Foster believes there are three essential actions the person responsible for OT security must do: »

- **Take the time to understand your OT space.** It's essential to know what is in the environment before you can understand what it needs, but Foster points out that every environment is different. "It's never the same from place to place in OT, and there's going to be many different varieties of equipment," he says. Part of understanding your environment is having a comprehensive inventory of control system assets as well as asset configurations and their changes. There are solutions available to help discover and monitor OT assets, but they are different than those used in IT environments.
- **Recognize that safety trumps all other concerns in an OT network.** This is a fundamental cultural difference between OT environments and IT security, and it affects security strategy. For example, the traditional CIA model (confidentiality, integrity, and availability) is not meaningful in an OT network. "Our number one concern is safety, and any security in our networks has to be designed in a way that is safe. We can't have a machine fail and kill someone. That's just not an acceptable outcome. We approach everything with that safety mindset," Foster says. »

> "Passive tools are unlikely to affect anything. With active tools, you run more of a risk. Whether it's passive or active, these tools must be carefully evaluated before anything is put into place."

- **You must have visibility into the network.** This means being able to see data packets that are moving around and executing the many controls in an OT system. For critical networks like those in the power generation and distribution infrastructure, scanning tools are more likely to be passive than active because of the risk of active tools interfering with a process. “Passive tools are unlikely to affect anything,” says Foster. “With active tools, you run more of a risk. Could it cause traffic on your network that causes a control signal to be missed, which is completely unacceptable? Whether it’s passive or active, these tools must be carefully evaluated before anything is put into place.”

How you respond to suspicious activity is very important. In the IT world, it’s common to prevent suspicious packets from reaching their destination. But you can’t do that in critical infrastructure. “If I send a command to open a breaker, that breaker has to open,” Foster notes. “I don’t care if that command is malicious or otherwise, because someone’s life could be on the line. If we’re saying, ‘Cut the power,’ then regardless of where that command comes from, we’re cutting the power. But I want to know that command occurred. Where did it come from? What did the structure look like? Does it look like all the other times we’ve sent out commands to open the breaker? We have to look at a baseline to determine if this is similar or not. We already opened the breaker because that’s the safe thing to do, but we can look at it after the fact to see if that was the correct action.” ■

KEY POINTS

Download the full e-book: Reducing Industrial Risk: 20 Experts Share Strategies for Managing OT Cybersecurity

1 **Securing 30 year-old-equipment which was not built with security in mind is a great challenge in the power generation and distribution industry.**

2 **In the IT world, it’s common to prevent suspicious packets from reaching their destination. You can’t do that in critical infrastructure.**

JOE WEISS

Managing Partner
Applied Control Solutions

Website

LinkedIn

The question most people ask is if process sensors, actuators, and drives can be remotely compromised. The answer is yes. We understand the process risk that comes from compromising Level 0,1 devices. There are methods for separating ICS cybersecurity safety risk from cybersecurity economic risk. This has to be done at Level 0,1 and doing so gives management the ability to make better business decisions.

OT SECURITY REQUIRES A HOLISTIC VIEW OF PLANT RISK

AGUSTIN VALENCIA

OT Cybersecurity Advisor
Iberdrola

Agustin Valencia is an ICS professional who has held leading engineering, operations, and maintenance roles in the thermal and nuclear generation industry. For the past six years, he has focused on applying cybersecurity controls to both new control systems and legacy systems, from new designs and projects from the operator and maintenance engineer's perspective.

LinkedIn

Cybersecurity has always involved people, processes, and technology, and in a homogeneous IT environment, people often think first about the technological aspects of cybersecurity. But in the OT world that is found inside large industrial plants, "Technology must be chosen for the OT environment and adapted to the plant," says Agustin Valencia. That leaves it up to company processes to fill the cybersecurity gaps. "Technology cannot be enough. In the case of OT systems, procedures and awareness can make the workers our best firewall."

> *Technology must be chosen for the OT environment and adapted to the plant.*

Much of the challenge comes from the criticality of industrial processes, combined with a great diversity of new and old control systems. "Many new components integrate with Ethernet communications and with other things such as firewalls and antivirus software," Valencia says. "They can also connect with the rest of IT software technology. But legacy systems do not provide this capability." To monitor and maintain these systems, it's necessary to extract information directly from the assets, but without affecting communications. Some systems can only do this offline, when a process is stopped. But in many OT environments, processes rarely shut down. »

OT SECURITY REQUIRES A HOLISTIC VIEW OF PLANT RISK

Valencia, whose role at Spanish electricity company Iberdrola covers nuclear power plants and other sources of power generation, approaches OT cybersecurity in this way:

- **Look at risk holistically.** You must first look at all the risks to the entire business, and in the case of large industrial plants and critical infrastructure, this is a much broader risk assessment than is typical in the IT world. “In OT, it’s not a matter of just interrupting the service or losing data,” says Valencia. “You must consider the consequences of a failure that causes damage to workers, to the environment, to the community, the extra cost of stopping production, the cost of waste if production systems are altered, or damage to the plant itself if systems are changed.”
- **Classify assets according to risk.** Of course you must have a complete inventory of assets and configuration status in your OT environment so you know what you must protect. But it’s necessary to take that a step further, to classify those assets according to risk. “Once you know the assets and risk, you can also establish their impact and risk profile,” he notes. In this way, you are able to prioritize vulnerability-management strategies and ICS maintenance. »

“In OT, it’s not a matter of interrupting the service or losing data. You must consider the impact of a failure that causes damage to workers, or to the environment, or to the community, the extra cost of stopping production, or the cost of waste if production systems are altered, or damage to the plant itself if systems are changed.”

- **Develop OT-specific policies, procedures, roles, and responsibilities.** It's important to recognize that OT cybersecurity is not just an IT problem. There is too much in the OT world that is unique and different from IT. This means everyone in the plant needs to understand their contribution to OT cybersecurity. "People must know their responsibilities," says Valencia. "When a problem arises in a specific environment, everyone has a duty for detection, information, analysis, isolation, erradication, or restoration. In OT, the cyber part is complementary to the process part, so the organization must train everyone on their role."

In the OT world, many cybersecurity practices are unique to the industry and the plant. For instance, one can't rush into a plant and install the latest patches if there is an incident or a threat. This can trigger failovers that stop a system or process, which cannot be allowed to happen in an OT environment. "Everything must be tested," Valencia stresses. "And you need that holistic approach. If a threat is coming from somebody who can touch my legacy system, perhaps I have to deploy physical security. But if my problem comes from the network, I can implement controls over that piece of hardware to cover that vulnerability in the legacy system." ■

KEY POINTS

Download the full e-book: Reducing Industrial Risk: 20 Experts Share Strategies for Managing OT Cybersecurity

1 **Classify assets according to risk, so you know what you need to protect and can prioritize vulnerability-management strategies and ICS maintenance.**

2 **OT cybersecurity is not just an IT problem. Everyone in the plant needs to understand their roles and responsibilities for OT cybersecurity.**

ROBUST ICS SECURITY REQUIRES A MULTI-LAYERED APPROACH

JAMES SHANK

IT and Cyber Security
Program Manager
PSEG

James Shank has over 20 years of experience in design, development, operations, and maintenance of technology systems and solutions. An expert in contract administration, electromagnetic and radio frequency interference, and personnel management, he oversees a $3.5 million budget and approximately 30 IT professionals. He earned a BS in Electrical and Electronics Engineering from Penn State University and an MBA from Drexel University.

LinkedIn

James Shank is IT and Cybersecurity Program Manager at PSEG, where he manages the ICS security program for a three-unit nuclear facility that must adhere to the regulatory requirements of the Nuclear Regulatory Commission. He feels that robust ICS security requires a multi-pronged approach incorporating strategies such as network monitoring, control of portable and mobile devices, and several layers of defenses. When considering high-level ICS security priorities, he recommends that chief information security officers (CISOs) take these steps to secure the plant OT/ICS environment against cyber attacks:

> *If you have to exchange information in a bidirectional way, you need to carefully evaluate what data you're allowed to transfer in and out.*

- **Examine your ICS environment's network connectivity with the outside world.** "If you have to exchange information in a bidirectional way, you need to carefully evaluate what data you're allowed to transfer in and out," Shank says. This needs to include a detailed understanding of all ICS device configurations in the environment and their communications capabilities. Shank also recommends conducting a detailed security analysis of the devices that are controlling data transfers, assessing their ports and what types of communication you are allowing to flow through your environment. "If I was going to allow any kind of communication back into the ICS network, I'd also make sure I had real-time monitoring in place," he adds.

"That way, I would know exactly what data was coming into that environment." Inbound commands or data must be carefully scrutinized.

- **Control all of the portable media and mobile devices that come into and out of your ICS environment.** High-profile ICS-related exploits such as Stuxnet and BlackEnergy have had an element of portable media or mobile devices associated with them. To guard against similar attacks, Shank advises implementing a robust personal media device (PMD) program that allows only carefully controlled, authorized devices to connect to the network. "For example, you can secure portable media with passwords so that only someone with the password can actually use the device," he says. You can also use application and device whitelisting software to limit what employees can install on or plug into their laptops and mobile devices. This technology is especially crucial in ICS environments, whose legacy assets rarely have the native capability to reject devices that employees may attach to them. »

> "A program that has multiple layers of defense with strong monitoring will give you a better chance of detecting suspicious activity in your environment."

- **Integrate multiple layers of defense with threat intelligence.** It's easy for skilled hackers or insider threats to compromise a single layer of defense. For this reason, it's best to use a multilayered strategy. "A program that has multiple layers of defense with strong monitoring will give you a better chance of detecting suspicious activity in your environment," Shank says. Seek up-to-date intelligence on emerging threats as well as relevant vulnerabilities so that you can continually optimize your defenses against a potential attack.

Maintaining a strong ICS security posture is challenging, but you can go a long way toward succeeding by keeping a close eye on connectivity with the outside world, controlling devices that enter and exit your environment, and adopting a multi-layered defense strategy. If you take these steps and also make an ongoing commitment to keeping your knowledge, skills, and tools up to date, you can better protect your plant against both current and future cybersecurity threats.

KEY POINTS

Download the full e-book: Reducing Industrial Risk: 20 Experts Share Strategies for Managing OT Cybersecurity

1 **To defend your ICS environment against an attack, analyze and assess network communications touching the outside world—particularly inbound transmissions.**

2 **A single layer of defense can easily be defeated, but a multilayered system is much harder to compromise without being detected.**

MIKE ASSANTE

Director of Critical Infrastructure & ICS
SANS

LinkedIn

The majority of ICS reliant operations have troublesome gaps in knowledge of their assets and an incomplete understanding of expected communications. These deficiencies are exacerbated by disjointed tools and limited points to achieve network visibility. Native tools can be leveraged to provide a partial view, but they can't compete with smart coverage and a well-designed capability to identify new assets, first heard communication sessions, and looking deeply into communications between systems.

SECURITY PROFESSIONALS NEED TO WIN THE TRUST OF OT ENGINEERS

EVERARDO TRUJILLO

Manager, Cybersecurity Operations
Sempra Energy Utilities

Everardo Trujillo has over 20 years of experience and expertise in threat intelligence, vulnerability management, application security, security engineering and architecture, security assessments and security operations, and developing and executing cybersecurity strategy. He also serves as a mentor for high school students who participate in CyberPatriot, educating the next generation of cybersecurity professionals.

Twitter I LinkedIn

Unlike typical OT security managers who often have control engineering backgrounds, Everardo Trujillo began his career in IT systems and worked as an IT security architect. This has given him an edge in considering cyber risks and vulnerabilities in the OT environment.

For example, some electrical power grids have controls that rely on measuring time to perform their functions, such as the system that detects a broken or failing power-transmission line. If a storm causes a power line to break, controls are able to shut off power to that line before it hits the ground. From an OT operator's perspective, this is an important and necessary safety function. "There are controls that rely on position timing, syncrophasors that depend on time measurements to the nanosecond. A common practice is to use GPS clocks," Trujillo says. But drawing on his IT background, he points out a potential vulnerability here. "GPS clocks can be spoofed. They can suffer an attack called time drifting, which is a very slow attack," he says. That kind of incident can seriously impact the function of time-sensitive controls causing them to fail. »

> *Typically, IT and OT folks are not aligned, because they come from different environments.*

SECURITY PROFESSIONALS NEED TO WIN THE TRUST OF OT ENGINEERS

In this case, security architects worked with OT engineers and a national lab to build a time-resilient system to protect against this kind of attack. This is a good example of the importance of IT working closely with OT to identify and remediate vulnerabilities.

To build an OT cybersecurity practice, Trujillo says there are several things an organization must do:

- **Security people need to gain the trust of OT engineers.** "Typically, IT and OT folks are not aligned, because they come from different environments," says Trujillo. "I wouldn't let my software developer from IT go into the OT environment and change things, because he/she wouldn't understand that environment. And the OT engineers focus to make things safe, but they're not aware of some of the cyber threats out there." Trujillo says that OT cybersecurity initiatives often start in IT because IT has more experience dealing with cyber threats. To be successful, the first thing security professionals must do is sit down with OT engineers/personnel and learn from them. Gaining that trust is essential. "Now that we have the support of the OT folks, we come up with ideas for improved security, and they provide us with devices to test. They helped us build our lab. We have people from OT come over and learn about what we're doing, and it becomes a collaborative effort where they come in and share great ideas." »

> "We install a monitoring tool so we can see things from a cybersecurity perspective. Suddenly OT engineers have the ability to see a change in their network that they didn't expect. They say, 'That shouldn't happen.' Now they are informed of these events and are able to take action."

SECURITY PROFESSIONALS NEED TO WIN THE TRUST OF OT ENGINEERS

- **Get a clear understanding of the assets in the environment.** This not only helps security professionals gain a clearer idea of what they must protect, but it helps OT engineers too, and it can help win their trust. There are solutions specifically designed for OT environments that identify assets and collect asset data. These solutions can provide a level of visibility the OT engineers have never had before. “We install a monitoring tool so we can see things from a cybersecurity perspective,” Trujillo explains. “Suddenly OT engineers have the ability to see a change in their network that they didn’t expect. They say, ‘That shouldn’t happen.’ Now they are informed of these events and are able to take action.”
- **Manage your control system vendors.** Vendors know the inner workings of their ICS, and OT engineers depend on that knowledge. Vendors come into the plant to do the installation and configuration, or they subcontract that to a third party. “That’s something we brought up to the OT folks. How does this company vet the contractors they’re hiring? Do they have background checks?” Also, it is difficult to hold ICS vendors to a security standard, in part because they don’t want to be contractually liable for cyber attacks. “We developed a checklist of controls and protocols so we know if they are able to implement those things. We’ve also spun up an R&D team specifically for industrial control systems, and we’ve come up with technologies to help secure these systems,” notes Trujillo.

Download the full e-book: Reducing Industrial Risk: 20 Experts Share Strategies for Managing OT Cybersecurity

KEY POINTS

1 **To be successful, the first thing security people need to do is sit down with OT engineers and learn from them. Gaining that trust is essential.**

2 **Tools that provide visibility into the OT network help security gain a clearer idea of what they must protect, but they help OT engineers as well, and this will help win their trust.**

UNDERSTANDING YOUR SYSTEMS IS KEY TO ICS SECURITY

SCOTT SAUNDERS

Cyber Security Consultant
Company

Scott Saunders has more than 20 years of information-security experience, having worked for the Sacramento Municipal Utility District and the federal Medicaid program for the state of California. Saunders is a Certified Information Security Manager (CISM) and a Certified Information Security Systems Professional (CISSP). He holds a BS in Information Technology-Security and an MS in Information Security Assurance, both from Western Governors University.

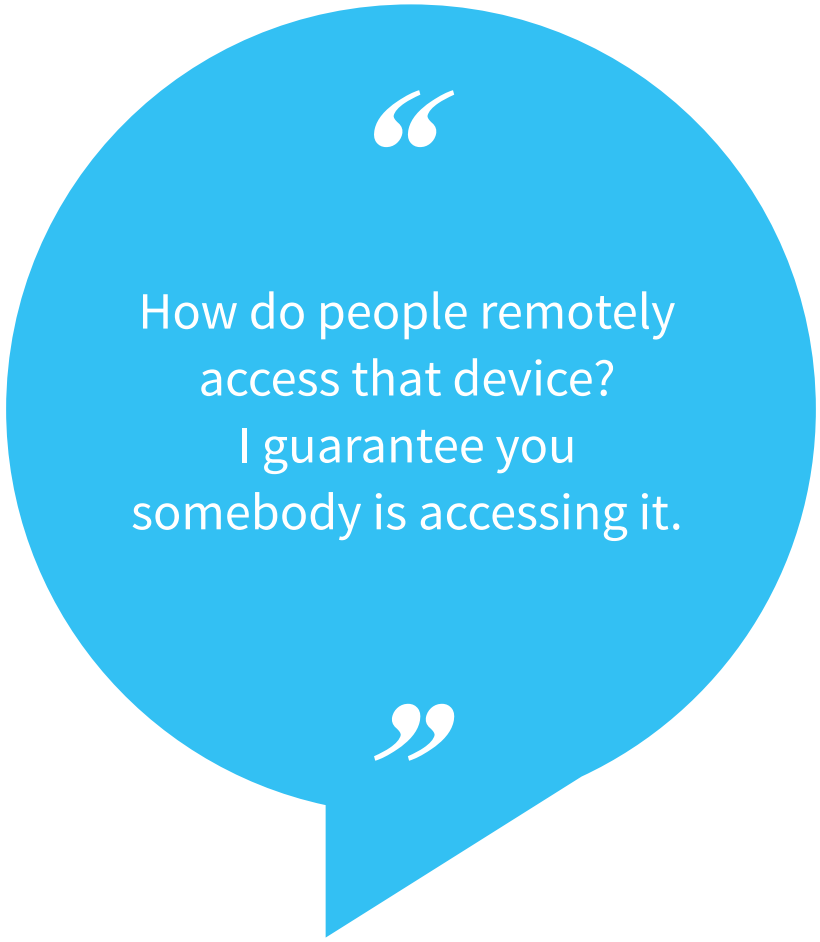
LinkedIn

Having served as cyber security consultant at Exelon for the past three years, Scott Saunders is dedicated to improving security-event monitoring in the OT world across the six Exelon utilities by creating a brand-new, centralized, industrial control system security operations center. When considering high-level ICS security priorities, Scott recommends that professionals keep these tips in mind:

- **Learn about the plant and its systems.** Depending on your plant and its function, your devices might have varying degrees of capability. You'll want to gain a clear, precise understanding of what everything does. "That's always been a huge focus of mine from the very beginning. I want to know what I have and I want to know what it's doing," Saunders says. Once you've done that, then you should look at how you can layer your security controls, determining how they ought to be designed. "You can look at things like segmentation, access controls, network monitoring... all of that goes into what controls might be available to you, as well as how you manage your baseline configurations," he explains. »

> *I want to know what I have and I want to know what it's doing.*

- **Consider how your plant's devices are being accessed.** When you're assessing devices and understanding their function, it's important to evaluate their access controls. "How do people remotely access that device? I guarantee you somebody is accessing it," Saunders elaborates. "In a lot of cases, plants are automated to the point where you don't even have operators there anymore. Instead, you have centralized operation taking place. How is remote access being done? Is there vendor management?" Your team will want to develop a complete picture of precisely how these devices are being accessed and by whom.
- **Take special care to assess indicators from your legacy devices.** Although many plants are automated, there may still be older substations within them that are not automated. It's important to monitor those systems, even if that involves using electro-mechanical feedback from indicators that are focused on physical security rather than cybersecurity. It's a good idea to tell the operator to be on the lookout for certain alarms going off that might indicate that something abnormal is happening on site. That could point to a physical security threat that may be important to respond to from an ICS security perspective. »



Saunders also advises plants to think proactively about preserving institutional knowledge. They often use older devices and technologies, for example, such as serial to IP conversion, as well as newer protocol conversion methods like SEL-3620. “People in the plant know what they have, but they may not have written it down,” he explains. “We need to capture that institutional knowledge. If we don’t start doing that, that’s a risk in our sector because of the age of our workforce.” Accordingly, he recommends that security professionals make sure their understanding of the plant and its systems includes this important knowledge that, if lost, could pose a future risk to the organization.

KEY POINTS

Download the full e-book: Reducing Industrial Risk: 20 Experts Share Strategies for Managing OT Cybersecurity

1 **Security professionals must first acquire a clear understanding of what they have and what it does before designing security controls to match.**

2 **It’s important for plants to preserve institutional knowledge of the OT environment proactively before experienced professionals retire.**

DAVID BATZ

Senior Director,
Cyber & Infrastructure
Security
Edison Electric Institute

Twitter

LinkedIn

We are now seeing adversaries deliberately and purposefully attacking safety instrumented systems. This shows a willingness on the part of an adversary to attack a system that is not actually responsible for production, but rather one that is responsible for keeping a process safe. Defenders need to recognize that adversaries have shown a willingness to attack systems that if compromised, can lead to the loss of human life.

SPENCER WILCOX

Director of Operational Technology Cyber Security
Exelon

Spencer Wilcox is a recognized speaker, and a regular contributor at cybersecurity events. He has judged industry awards and volunteered on the boards of directors for the Cybersecurity Association of Maryland and the Fort Meade Alliance. His specialties include strategic vision, cybersecurity leadership, and cybersecurity risk management. He holds a BS in Information Security from Pierce College and ISMA certification from Georgetown and Northwestern universities.

LinkedIn

Spencer Wilcox is an experienced ICS security leader who provides strategic direction to teams responsible for protecting the grid. He believes that controlling and monitoring network flows is key to improving ICS security. Wilcox suggests three measures chief information security officers (CISOs) can take to make the plant's OT/ICS environment more secure from cyber attacks:

> *Once you've got a baseline, it's really easy to detect if an asset suddenly throws an error or is doing something that it doesn't normally do.*

- **Instead of relying on a device-based strategy, aim for absolute control of your network flows.** "This means not just TCP/IP communications but also protocols like DNP3 and Modbus that may not be visible to your traditional networking gear," he says. Wilcox advises against using VPN tunnels, recommending that users be channeled through a jump server to take their actions on the network. "Having good logging and monitoring of remote access activities through a jump server is very important," he adds. "That way, you can get attribution on who is taking those actions or where that outbound communication is happening or where that inbound communication is originating from."

- **Limit remote access as much as you possibly can.** It's important to limit remote access to the instances and cases in which it is absolutely necessary. In doing so, you will reduce the potential attack surface that a malicious actor could exploit. Although it would be ideal to eliminate remote access altogether, that may not always be realistic. "Every one of your vendors is going to want to have remote access to be able to support their products," Wilcox acknowledges, but it's still best to keep a tight leash on the connections you permit into your ICS environment.
- **Identify security threats moving within and outside your networks.** "It's critically important that you identify security threats moving in and out of your network as well as laterally within your network" Wilcox says. Security professionals can monitor devices to see if they're operating as expected. "Once you've got a baseline, it's really easy to detect if an asset suddenly throws an error or is doing something that it doesn't normally do," he says. In the near future, Wilcox envisions leveraging big data to understand what normal operations look like, accelerating the process of identifying anomalous events in the ICS environment.

> "Changes to the ladder logic result in changes to the way the device is operating."

Aside from these three key points, Wilcox recommends that security professionals also pay attention to the ladder logic that is programmed into their ICS assets. “Changes to the ladder logic result in changes to the way the device is operating,” he says. “So if you were to change ladder logic, you could remove a safety condition.” With that in mind, it’s important to detect when there’s a change on the ladder logic within a device as well as when there’s a change in its firmware. This is not so difficult to accomplish in a small environment, but it becomes more challenging as you scale up. Regardless, you will want to keep this aspect of ICS security on your radar so that you can better protect your infrastructure as it evolves and changes.

KEY POINTS

Download the full e-book: Reducing Industrial Risk: 20 Experts Share Strategies for Managing OT Cybersecurity

1 **It’s important not just to have a comprehensive understanding of the types of communication transpiring on your ICS network but detailed monitoring in place as well.**

2 **Establishing a baseline for what normal behavior looks like will allow you to identify anomalous events in the ICS environment more easily.**

GABRIEL AGBORUCHE

Cybersecurity Specialist
Westinghouse Electric

Gabriel Agboruche is a cybersecurity specialist in the field of nuclear energy who is always looking for a challenge. As an engineer, he enjoys developing simple, easy-to-understand solutions to today's complex problems. As a person, integrity, character development, and commitment are the driving factors that heavily influence all aspects of his life.

LinkedIn

Unlike some OT environments, nuclear power plants are heavily regulated. Nuclear Regulatory Commission (NRC) inspections, which include an evaluation of cybersecurity, typically occur every two years during scheduled outages for plant refueling. This is also when other plant maintenance occurs, such as updating and re-engineering control systems.

But even in this tightly controlled environment there can be devices that introduce vulnerabilities. "When systems are out there in the plant, they often stay there until they fail. One thing we evaluate is the health of those particular assets," says Gabriel Agboruche, who has spent much of his career as a cybersecurity engineer and specialist.

> *Having rogue devices in your OT environment that you don't have control over is a big problem.*

The OT environment in a nuclear power plant is made up of layers of criticality, each one separated from the others by an air gap. One of the challenges in securing these systems while using modern ICS components is preserving those air gaps. Agboruche follows these practices in securing the plant's OT systems:

- **Have a correct, accurate account of all digital assets within your plant.** This includes knowing what you have, understanding how and what those devices control, and working with IT people to understand the data inside those control systems. This is important for safe and secure operation of the plant, and it also helps with NRC inspections. »

"Having rogue devices in your OT environment that you don't have control over is a big problem," Agboruche notes.

- **Assess critical vulnerabilities immediately.** "As soon as we learn of any vulnerabilities or any possible threats that might be coming from anywhere, we have to evaluate our systems to make sure the plant is not at risk," says Agboruche. These might be alerts from control system vendors, or information about a new kind of ICS attack such as Stuxnet. "We don't just hear about things and say we're OK. We need to be able to evaluate our systems to make sure that we're not vulnerable to the same type of attack with the same issues," he comments.
- **Carefully evaluate every piece of equipment that goes into the plant.** This is a continuous process that not only involves looking at new equipment, but it also means evaluating existing systems and comparing those to similar systems in other plants. Agboruche notes that an important part of nuclear power plant cybersecurity is sharing information with other plants. "Sometimes we'll hear from another plant that may have a more mature cybersecurity program. We'll evaluate our systems compared to theirs. We'll do our own evaluation too on the back end, so we have a thorough look at the different vulnerabilities," he says. »

"As soon as we learn of any vulnerabilities or any possible threats that might be coming from anywhere, we have to evaluate our systems to make sure the plant is not vulnerable to those things."

Agboruche points out that there is no way to completely eliminate cyber risk, but people often don't recognize there are risks when you open up your network to certain types of technologies or even vendors. He cites as an example one type of handheld communicator used to wirelessly configure different devices within the plant. It sends and receives proprietary communication protocols. The newest versions of that device now have Bluetooth capabilities. "There's a new vector of interest for somebody who might have malicious intent. Are we comfortable with this? There needs to be an evaluation. If we're comfortable with it, what are we doing to protect against it?"

Agboruche believes that inside an OT operation, data itself is ultimately the most critical asset, but not because of the intrinsic value of the data. "Data is your primary asset because that is what is interacting with the physical world," he says.

Download the full e-book: Reducing Industrial Risk: 20 Experts Share Strategies for Managing OT Cybersecurity

KEY POINTS

1 **People often don't recognize there are risks when you open up your network to certain types of technologies or even vendors.**

2 **Know what you have, all the current configurations of those devices, understand what those devices control, and understand how the data is actually working inside those ICS systems.**

GARY WILLIAMS

Sr. Director, Cybersecurity
Service Offer Leader
Schneider Electric

LinkedIn

It all comes down to this: Cybersecurity has to be part of your operations lifecycle. And in order to do that, you have to make everyone, everywhere, responsible for cybersecurity. We say this again and again, but it's true: Cybersecurity isn't a destination; it's a journey. Security can never be viewed as a one-off project. Attacks on industrial control systems in the era of the IIoT are escalating, and they extend across industries, geographies and broader society. The risk for catastrophe is too great to ignore. New threats, attack techniques, and technologies are continually advancing. That means your people and your security protocols must always be advancing too.