Mighty Guides®

# Lessons Learned:

## Protecting Critical Infrastructure from Cyber Attacks

Sponsored by PAS

# INTRODUCTION

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 5 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.

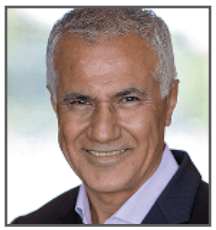
# FOREWORD BY EDDIE HABIBI

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.**

# LESSONS LEARNED: PROTECTING CRITICAL INFRASTRUCTURE FROM CYBER ATTACKS

## In This Section...

# 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

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.**


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

# 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.

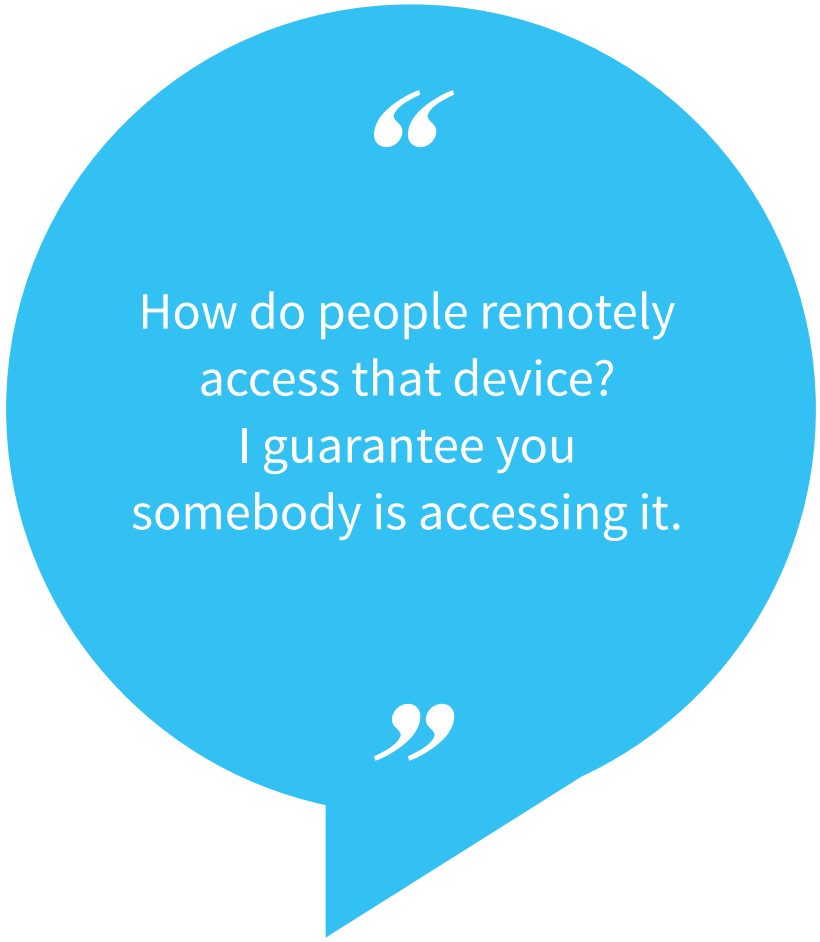
LinkedIn

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. »



# UNDERSTANDING YOUR SYSTEMS IS KEY TO ICS SECURITY

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.**

**RICHARD KNOWLTON**

Chairman
Richard Knowlton Associates

LinkedIn

*It is urgent that OT and IT security—traditionally two separate disciplines with different priorities—come together to share risk management best practices, and to work together to apply it across their functions. In particular, OT security specialists need to start thinking about how they can manage complex, evolving risks. This needs a change in mindset. They must think not just of safety and reliability, but also of what a hacker would go after in my OT estate if I wanted to cause massive damage and disruption.*

# IDENTITY ACCESS, ASSET INVENTORY, AND INCIDENT RESPONSE ARE KEY


**ROBIN FAMILARA**

Senior Network Engineer
CGI


Robin Familara began his career in the Philippines as a customer engineer way back in 1995. When he moved to the United States, he worked for Amazon.com. Then he was hired by CGI as a network engineer and senior consultant for top oil and gas firms. Through the years, he has mastered the art of deploying innovation and creativity to make things happen in even the most critical environment. He has gained clients' trust and enjoyed professional success by promoting safety, security, and compliance.

Twitter I LinkedIn

Robin Familara is responsible for ensuring the safety, operational compliance, and security of industrial control systems for large oil and gas installations. These cover a variety of onshore and offshore production environments with different levels of criticality. Although many of the control systems are modern, some are old enough that they do not have the capability of connecting to a process control domain.

In this kind of environment, Familara recommends that CISOs take three steps to secure their industrial control systems from cyber attacks:

- **Ensure proper identity access.** "Of course you have to begin with identity access," Familara advises. "Right now, everything's connected, even if you scale the systems. You have to protect the identity access or the identity management—that's the first layer."

> *"You have to protect the identity access or the identity management—that's the first layer of your layered defense and defense in-depth security."*

- **Update your asset inventory.** It's important to keep your asset inventory as current and comprehensive as possible. Whereas this was once a manual process, "Now the asset inventory is remotely collected," explains Familara. "That's something that you need to complete because you can't secure a system or a network if you don't know what's in there. All the hosts and all the systems, even the PLC, should be in a portal that you can monitor and manage," he says. »

Despite having modern tools with which to perform this asset inventory, Familara's colleagues still manually check up on some devices in the ICS network. "Our systems engineer still visits certain assets because they have to patch any asset that is standalone," he explains. Once the engineers are at the asset's physical location, they assist with the manual verification in collaboration with an electrical technician. "So they verify the list of systems that are in that asset," Familara says. "We get that information from them and every time there is an addition or a commissioning, we update our asset inventory for that stand alone system." Of course, these inventory updates are made possible due to good communication and mutual agreement between the on-site engineers and system owners.

> "All the hosts and all the systems, even the PLCs, should be in a portal that you can monitor and manage."

- **Make sure the business can fully respond and recover after an attack.** Familara says that it is important to ensure that your company can adequately respond and recover from an incident. To increase the security team's capacity where this is concerned, he advises creating a security scope that encompasses the network's event logs, system logs, and incident response. "Your scope should have this critical data in place to support procedures your team uses to secure the industrial control systems," he adds. »

# IDENTITY ACCESS, ASSET INVENTORY, AND INCIDENT RESPONSE ARE KEY

Familara finds these three strategies valuable in his security practice at top oil and gas firms, where as an ICS cybersecurity and network engineer he supports a global cybersecurity footprint. By proactively managing identity access, network and systems via layered defense and defense in-depth security assurance, taking care to ensure you have an accurate asset inventory, and putting in place procedures to ensure the business responds and recovers from an incident, your company can make significant progress in protecting its ICS environment from a potential attack.


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

## KEY POINTS

1 **Identity access, asset inventory, and procedures for responding to and recovering from an attack are keys to a strong ICS cybersecurity program.**

2 **Good communication between remote network engineers, on-site engineers and system owners makes it easier to update the asset inventory to the most possible accuracy level. Of course, there will always be room for enhancement through optimization and automation.**

**AYO FOLORUNSO AGUNBIADE**

ICS Security Analyst
TransGas

Ayo Folorunso Agunbiade has more than 15 years' experience in technology governance, risk, and compliance, as well as IT and OT cybersecurity. He was a manager at international consulting firm Deloitte for five years. His work has spanned the consulting, banking, and oil and gas sectors, where he has developed and maintained information security compliance and strategies for people, processes, and technology in achieving business goals and objectives.

LinkedIn

Ayo Folorunso Agunbiade is a security analyst for industrial control systems and SCADA security at SaskEnergy in Canada. When considering high-level ICS security priorities, Agunbiade recommends that CISOs take these three steps to protect the plant's OT/ICS environment against cyber attacks:

- **Implement application whitelisting.** "Application Whitelisting (AWL) can detect and prevent attempted execution of malware uploaded by adversaries," Agunbiade says. It helps prevent industrial cyber attacks by denying any applications that are previously approved as non-malicious. Rather than simply blocking malicious code after the fact, AWL only permits trusted and known files to execute. By putting AWL in place and reducing the attack surface, security organizations are sure that the applications operating in their environment are fully vetted and authorized.

> *AWL can detect and prevent attempted execution of malware uploaded by adversaries.*

- **Ensure proper configuration/patch management.** A configuration/patch management program centered on the safe implementation of trusted patches will also reduce the attack surface and help keep control systems more secure. This must include asset discovery and the collection of all critical asset configuration information—essential steps in investigating and prioritizing risk mitigation activities. »

However, patches must be made carefully, especially in critical systems. “I recommend testing all security patches in test environments in partnership with vendors before deploying them into the production environment,” Agunbiade says. Special care must be taken at this stage because deploying patches could lead to further problems that could disrupt the ICS systems or even cause them to become unavailable. It is also worth considering a phased deployment approach, depending on the criticality of the applications or server, when issuing such patches.

- **Analyze attack vectors.** Malicious actors have many opportunities to compromise your systems when there are multiple vectors through which they could potentially gain unauthorized access. For this reason, Agunbiade advises reducing the total attack surface area available to them by analyzing potential attack vectors. “Isolate your ICS networks from any untrusted networks, especially the Internet,” he counsels. “You should also lock down all unused ports and turn off all unused services.” In doing so, you can ensure that potential attackers have fewer points of entry into your ICS environment and that the company has less overall exposure to an attack. »

In addition to this advice, Agunbiade also notes that today's ICS environments enjoy significantly less isolation from the outside world than their predecessors did. As a result, this increased connectivity has made it even more imperative for CISOs to secure their ICS systems. Accordingly, it is important to segment your network, specifically by separating it into logical enclaves and restricting host-to-communications paths. It's also wise to apply firewalls as well as intrusion detection systems, as doing so will limit the damage your firm could encounter in the event of a network perimeter breach. With these recommendations in mind, your plant can meaningfully advance its cybersecurity posture to a position of greater strength.


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

## KEY POINTS

1. **Application whitelisting and proper configuration and patch management reduces the attack surface and helps keep control systems more secure.**

2. **Analyze potential attack vectors to reduce your environment's overall attack surface and make it much more challenging for attackers to compromise your ICS systems.**

**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.*

# FOR BETTER OT SECURITY, CONTROL AND MONITOR YOUR ENVIRONMENT

**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:

- **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." »

> *"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."*

- **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.**