Mighty Guides®

Leveraging IT/OT

Convergence and Developing Effective OT Cybersecurity

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 6 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.

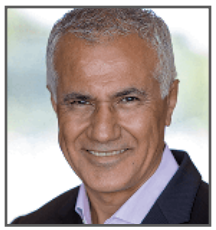
FOREWORD BY EDDIE HABIBI

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.

LEVERAGING IT/OT CONVERGENCE AND DEVELOPING EFFECTIVE OT CYBERSECURITY

In This Section...

RECOMMENDATIONS FOR BUILDING A COMPREHENSIVE ICS CYBERSECURITY PROGRAM

ELEWA ALI

Senior Control System Engineer
SABIC

Elewa Ali is a control system and cybersecurity engineer with more than 13 years of experience in the oil and gas and petrochemicals industries. He is skilled in process control and control systems design, and has in-depth knowledge of ICS-OT cybersecurity. Ali earned his bachelor's degree, with a focus on computer and control, from Zagazig University in Egypt.

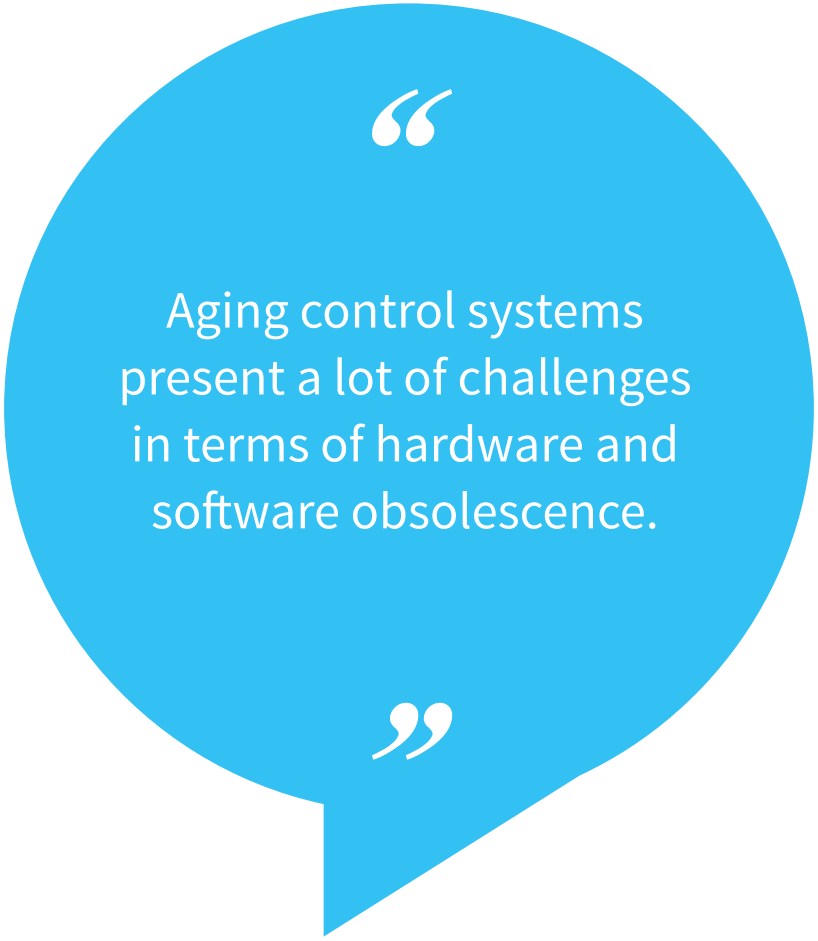
LinkedIn

As a control systems and cybersecurity engineer at a major chemical plan in Saudi Arabia, Elewa Ali is responsible for 500 to 600 digital control systems with a wide range of configurations coming from a number of different vendors. And as is the case in many OT environments, Ali must contend with aging and obsolete systems. When considering high-level ICS security priorities, Ali recommends that that organizations work on building a complete cybersecurity program that includes the following areas of focus:

> *"Standalone machines are very difficult to secure, yet the organization still has to interact with them."*

- **Conduct a comprehensive risk assessment.** Risk assessments play an important role in communicating the business impact of a cybersecurity initiative to executive leadership. "If you have an out-of-date control system in need of an upgrade, you might not be able to upgrade it because of budget constraints," Ali says. In such cases, his firm performs a risk assessment, at the end of which the business decides whether to upgrade. At times, the company may decide that the risk associated with not upgrading that control system is too high. "Upper-level management should make the decision on whether to accept the risk posed by not upgrading the control system," he adds. »

- **Restructure the network to meet today's control system standards.** Ali also recommends restructuring the network to secure control systems. Specifically, he advises placing a firewall between different network layers. "You have to take special protocols that are used in control systems into consideration," he says. "In some cases you need to transfer data between two different layers through these protocols, which today's firewalls don't allow." Ali also advises eliminating as many standalone machines and endpoints as possible. "Standalone machines are very difficult to secure, yet the organization still has to interact with them," he explains. Accordingly, they should be integrated with the whole network, monitored, and included in centralized antivirus, back-up, and patch management procedures.
- **Eliminate all obsolete operating systems and applications.** Obsolescence is another problem that Ali believes organizations must address. "Aging control systems present a lot of challenges in terms of hardware and software obsolescence," he explains. "I advise establishing a complete program that includes procedures and policies, assessments and audits." »



Patch management is also a tricky issue because, as Ali notes, "The control system vendors must verify and approve a patch before deploying it to our machines or our servers." This process can take a few months, which is far too long from a cybersecurity perspective. As a result, his team is applying these patches manually. "And when we say we are doing it manually, that means we are taking too much time to implement it, to deploy it, because we are talking about roughly 500 or 600 machines," he says. With this in mind, Ali suggests that organizations try to find ways to keep their control systems updated in as timely a manner as possible.

Although ICS and OT face complex challenges and competing priorities today, Ali believes a plant can go a long way toward improving its cybersecurity posture by conducting risk assessments, restructuring its network to better secure its control systems, and proactively addressing the growing problem of hardware and software obsolescence. In this way, it will be able to protect its environment more effectively against the threats it faces.

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

KEY POINTS

1. **Risk assessments enable leadership to make informed, high-level business decisions about cybersecurity initiatives.**
2. **Restructuring the network and proactively updating aging hardware and software can help a plant better secure its control systems.**

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 BEGINS WITH PEOPLE, UNDERSTANDING THE ENVIRONMENT, AND SELECTING THE RIGHT CONTROLS

MICHAEL JACOBS

ICS Security Architect
Major Oil and Gas Company

Michael Jacobs has more than 16 years of hands-on security experience in the industrial control systems and information technology fields. Since starting his role at a major global oil, gas, and energy firm in the Middle East, he has renewed his focus on ICS security, after having worked as an enterprise security architect at Fujitsu America. Previously, Jacobs spent the bulk of his career at Network & Security Technologies Inc., where he specialized in network security and the NERC CIP regulations.

Twitter I LinkedIn

Having extensive experience in securing both OT and IT environments, Michael Jacobs has first-hand understanding of how these two realms differ from one another, yet how they increasingly depend on each other. When thinking about the advice he would offer a chief information security officer (CISO) faced with the challenge of securing a plant environment, Jacobs stresses understanding the environment.

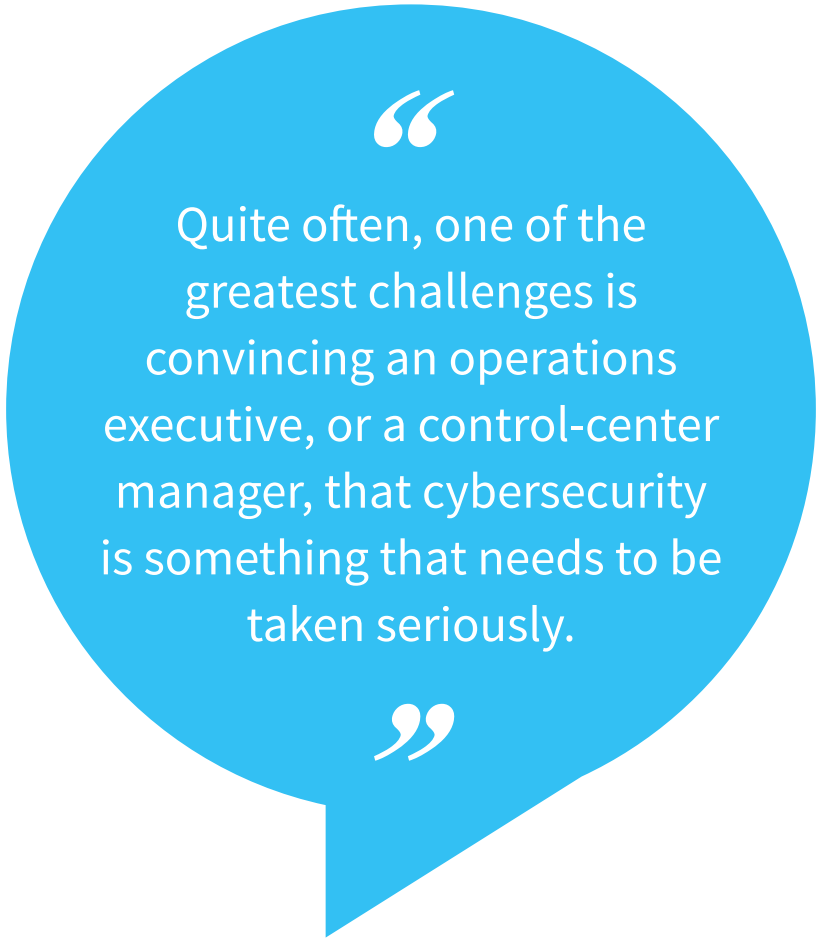
> *Manual identification and correlation [of ICS assets] is possible, but an automated tool makes the task easier and faster.*

"I can't overstate the importance of maintaining an inventory of key ICS assets," says the ICS security architect at a major oil and gas company. "There are many ways to obtain an accurate ICS asset inventory, and in my experience, there isn't a one-size-fits-all approach. A lot depends on the ICS design, the age of the system, the communications technologies in use, etc." Jacobs says a good first step toward building a picture of the asset base, at least in self-contained environments, is a physical walkthrough that involves tracing cables and physically identifying boxes. Once you have that, the network presents an excellent opportunity for asset identification. "You can review network device configurations and states, including routing tables, MAC address tables, ARP tables, firewall rules, etc., that add more definition to the picture, especially for remote devices," Jacobs explains. "Manual identification and correlation is possible, but an automated tool makes the task easier and faster." »

OT SECURITY BEGINS WITH PEOPLE, UNDERSTANDING THE ENVIRONMENT, AND SELECTING THE RIGHT CONTROLS

Once a CISO has a solid understanding of his or her OT/ICS environment, Jacobs recommends:

- **Have a strategy for success that starts with people and communication.** Jacobs recognizes that the CISO's responsibility for protecting key business assets is huge, especially in critical infrastructure, and one's first instinct might be to buy a piece of technology that claims to solve all the problems. But, he says, "To quote someone much smarter than I, 'If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.' In that regard, having a team of talented people who understand both security and OT is paramount."
- **Establish a good working relationship with those responsible for plant operations.** "Quite often, one of the greatest challenges is convincing an operations executive, or a control center manager, that cybersecurity is something that needs to be taken seriously," says Jacobs. "I've had numerous conversations with experts who claim that the OT environment is far too complex for an adversary to successfully perpetuate an attack." Some of the high-visibility attacks in 2016 and 2017 suggest this notion is patently false.



Jacobs suggests having good working relationships and buy-in from the OT staff can go a long way in dispelling this attitude and motivating them to take cybersecurity seriously. "In my opinion, these relationships are just as important as the CISO's relationship with the C-suite."

- **Establish a credible, risk-driven threat model that will guide control selection and implementation. Jacobs says there are plenty of standards to choose from.** "Don't reinvent the wheel, at least not immediately. The trick is selecting and prioritizing controls in a manner that A) address the right threats, B) are implementable within the OT environments, C) actually reduce the risk of an attack, and D) are cost effective," he advises. At the same time, Jacobs emphasizes in regards to security controls, one must "constrain the risks they introduce, which may impact operations, health, safety, and the environment."

Jacobs sees IT and OT coming closer together in ways that make it necessary for processes and technologies used to secure this new infrastructure to constrain the risks they introduce. He also sees how OT might impact IT architectures. "Ironically, I think we're witnessing an era in which IT is moving closer and closer to resembling OT. Take SDN—software defined networking—to its logical conclusion, in which IT and, perhaps someday, OT networks are self-managed and autonomous. Take the architectures being presented: the control plane being separated from the forwarding plane and placed into distributed controllers, making autonomous forwarding decisions on behalf of the network forwarding nodes, based on a logical policy using logical control and feedback channels. Doesn't this start to resemble process automation and control in the OT world?" he points out.

KEY POINTS

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

1 **Begin an asset inventory with a physical walkthrough to trace cables and boxes. Then use the control network and network traffic to identify devices and configurations.**

2 **Prioritize controls in a manner that address the right threats, is implementable within the OT/ICS environment, actually reduces risk of an attack, is cost effective, and minimizes operational and safety risk.**

OT AND IT MUST UNDERSTAND EACH OTHER'S DOMAINS

KAL MIAN

IT Consultant
KALM Consulting

Kal Mian has over 10 years of experience in working with IT systems that directly interface with process controls systems. This includes system designs from new builds and upgrades that deal directly with changing business needs, vendor recommendations, and compliance regulations. Mian has implemented new and evolving security technologies in the oil and gas, midstream, utilities, and telecommunications fields. He advocates a culture of cybersecurity awareness using technology and education to provide an eloquent solution for sustainable future operations.

LinkedIn

As OT systems increasingly connect to IT systems in plant environments, one of the big challenges is filling the knowledge gap between OT and IT operations. "In the OT world, it was always self-managed," says Kal Mian, who has years of experience in the operational side of the oil and gas industry. "There was not a lot of communication in the past, because there was an assumption that business networks were separate from process control networks. Now the interconnections are becoming more commonplace."

> *In the industrial control world, some controls are programmed with proprietary languages. This results in a multitude of third-party vendors and integrators coming in and running the show how they see fit. They often don't follow any system standards. That's a risk.*

To address this knowledge gap and establish a stronger OT security practice, Mian advises taking these steps:

- **Create a culture of cybersecurity awareness among all stakeholders, from users to the executive level.** "As OT and IT become more dependent on each other, you need to have an organization that is culturally aware of cybersecurity," Mian says. He notes that in the OT world, plants have to abide by safety standards first and foremost, but product must flow and processes can't stop. For many plant operators, the old adage "If ain't broke, don't fix it" has long been a guiding principle.

"It was always very reactive," Mian says. "Now we're moving toward a more proactive state of system integration and monitoring. This means you need cybersecurity awareness, you have to have education, and you have to be proactive about threats."

- **Perform a risk assessment that determines where you are now vs. where you need to be, and results in a gap analysis.** This analysis needs to look not only at your current state, but also how you got there. There are many factors that complicate the risk assessment in an OT environment. "In the industrial control world, some controls are programmed with proprietary languages. This results in a multitude of third-party vendors and integrators coming in and running the show how they see fit. They often don't follow any system standards. That's a risk," says Mian. There are other issues too, such as lack of documentation, older systems that predate current regulatory requirements, and IT systems, such as servers in the field, that have not been hardened for an OT environment. "During the risk assessment, get operations people involved and build a consensus about what assets you have, where you are now and the change management processes required to get you where you need to be," he adds. »

"During the risk assessment, get operations people involved and build a consensus about where you are now and the change management processes required to get you where you need to be."

- **Identify and prioritize vulnerabilities.** Some vulnerabilities will be identified in the risk assessment, and some will come from ongoing monitoring of changes in the OT environment. Once vulnerabilities are identified, they must be prioritized. "Prioritize by criticality of the site," says Mian. "Production sites that make the most money should be at the top of the list. Schedule prioritized upgrades around normal maintenance. Make business decisions regarding risk. For example, sometimes it's cost prohibitive to change something. Sometimes systems that aren't critical can be left alone." New solutions are also becoming available that do a better job of assessing and monitoring OT systems. These include aggregators that check your event, systems, and security logs. They can trigger alerts if something is out of the ordinary, but they are designed not to interrupt a process. For instance, they can interrupt the flow of suspicious data and switch a process to manual operation without interfering with the process itself.

A successful OT security strategy depends a lot on OT and IT people gaining a better understanding of each other's domains. "In the past, IT may not have appreciated the work performed by operations. However, now IT better understands there's a lot these people do every day to make systems and processes safe," Mian says.

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

KEY POINTS

1 **Performing a risk assessment is key to establishing a stronger OT security practice.**

2 **Vulnerability identification and prioritization should be done based on the criticality of the site and its systems to the business.**

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.**

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.

OT CYBERSECURITY REQUIRES TOTAL BUSINESS BUY-IN

LUIZ CANCADO

Control Systems IT Lead
Shell

Luiz Cancado specializes in delivering and maintaining technology and cybersecurity for the industry. As well as having held leading roles in implementing and assuring ICS cybersecurity operations, he has extensive experience in engineering and managing projects to integrate ICS and IT—always with cybersecurity in mind. Cancado has worked on many large-scale projects and complex mission-critical operations in industries such as oil and gas, automobile, metals and mining, and steel-making.

Twitter I LinkedIn

Drawing on his experience with both IT and industrial control systems, Luiz Cancado sees a clear convergence of IT and OT technologies. “You see two movements,” he says. “It comes from the bottom up through smarter control devices with more functions, smarter sensors, and wireless instrumentation. And you see it from the top down, from the business side, with new applications that can monitor data from new instrumentation and perform real-time analytics.”

> *You need to have alignment with business and the system owners, plant managers, cycle management—all must understand the risks.*

Cancado says the challenge in integrating IT and OT is not starting the process—because it’s already happening—but to do it securely. To accomplish this, he offers this advice:

- **Business and system owners must understand the ICS risk.** All parties must understand the risks to a control infrastructure that is often poorly documented and may include obsolete hardware from vendors who no longer exist. This is an infrastructure that must support continuous plant operation. “Every single minute, every single hour in which the system is brought down for any reason means that the company is losing money,” says Cancado. “It is a very tough place to work. When presenting the risks to the business, there are a lot of factors that that go into determining risk-mitigation activities. »

You need to have alignment with business and the system owners, plant managers, cycle management—all must understand the risks." Cancado says in the beginning this can be difficult, because you may not have all the controls and skills you need to understand the risks fully.

- **You must build an OT cybersecurity team.** This requires developing a team with highly specialized skills. "There are control and automation systems that were not designed with thought for cybersecurity," Cancado says. "So there is a need for the right variety of technical skills. Few people have those skills, so you need to develop a training program to fill the knowledge and skills gaps." This will involve looking for people who understand IT security and teaching them about control systems, OT protocols, and devices. It will also require teaching OT engineers, who often have an electrical engineering background, the principles of cybersecurity.
- **Understand both your OT and IT environments.** Understanding these environments not only means knowing what is in them, but also understanding how they operate, the vulnerabilities that are unique to each, and also the constraints around vulnerability management and remediation in each environment. »

> "There are great tools to scan and monitor the IT side, but it's different on the OT side. OT monitoring is not as mature."

> "There are great tools to scan and monitor the IT side, but it's different on the OT side. OT monitoring is not as mature," Cancado says. Many businesses rely on ICS system vendors for vulnerability knowledge. Better understanding these vulnerabilities may require working more closely with vendors on cybersecurity. "The OT vulnerability management challenge is in understanding what assets you have and defining the channels to identify and fix vulnerabilities. In the IT world, that's well established. Software vendors release security patches and updates frequently. Many ICS manufactures are not mature enough to operate that way," Cancado explains.

He emphasizes the importance of involving business managers, plant operators, and ICS manufacturers in securing OT systems. "Everything needs to be done in a coordinated way," Cancado says. "It must be well thought out in order not to expose the critical production environment to threats usually found in the IT space." ■

KEY POINTS

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

1 **Understanding OT and IT environments not only means knowing what is in them, but also understanding how they operate together, and how they are different.**

2 **The challenge in integrating IT and OT is not starting the process—because it's already happening—but in doing it securely.**

SID SNITKIN

Vice-President &
GM Enterprise Services
ARC Advisory Group

LinkedIn

Technology developments are rapidly changing the very nature of industrial control systems: new technologies are undermining traditional architecture assumptions; end-to-end business processes are tightly integrating IT and OT applications; programs are being moved to the cloud to enhance value and lower costs. Integration of IT and OT cybersecurity strategies is essential to address the increased risks of these developments.

SECURING OT SYSTEMS REQUIRES SPECIALIZED TOOLS AND APPROACHES

DOUG WYLIE

Director Industrials & Infrastructure Practice
SANS Institute

Doug Wylie directs SANS Institute's industrial and infrastructure practice area. In addition to his 24 years of experience, he is an accomplished writer and speaker, a CISSP, and holds numerous patents. He was recognized by the White House for contributions to the NIST Cybersecurity Framework (CSF) and received the 2013 SANS People Who Made a Difference in Cybersecurity award.

Twitter I Website I LinkedIn

Doug Wylie, director of industrial and infrastructure practice at SANS Institute, recognizes that historically there has been a separation between IT and OT security. "OT security was all about the four walls of the factory, the guards, and the gates," he says. But software-driven industrial controls are changing that. "As the world becomes more digitally connected inside and outside the factory, there is a blending of OT and IT systems. In many respects, security has given those two domains a reason to start interacting," he explains.

> *"In OT environments, you have to use utilities that know where to look, how to look, and can provide that complete view, including considering the operational mode of the system."*

Still, securing an ICS environment represents a very different kind of cybersecurity challenge that requires more specialized tools. Because industrial controls have a far longer life cycle than typical IT systems, there is often a greater variety of devices in the environment. "Over a span of time, it is not unusual for new devices to be added, configurations to change, and for that not to be documented anywhere," Wylie says. "Individuals who made design decisions are no longer part of the maintenance and ongoing operation. You have information loss that has occurred over the years." IT grade utilities designed to identify network components often cannot see many ICS components. "In OT environments, you have to use utilities that know where to look, how to look, and can provide that complete view, including considering the operational mode of the system," he adds. »

SECURING OT SYSTEMS REQUIRES SPECIALIZED TOOLS AND APPROACHES

Another challenge of OT control systems is they typically run all the time. Making control system changes is like changing a tire on a moving vehicle, which makes you think about risk differently. “When an OT system decision is made, it is locked in that period of time,” says Wylie. “This is true for commercial, off-the-shelf operating systems as well as for proprietary systems. They become orphans as these systems age. If the end user isn’t making ongoing investments, then over time the technology moves from being a ‘value add’ that’s generating a return on investment to a risk on investment.”

Given these characteristics of the OT environment, Wylie recommends three approaches to building an ICS cybersecurity strategy:

- **CISOs need to recognize and embrace their leadership role in their organization.** This includes communicating a clear perspective on risks that affect the company, the employees, customers, and the community. “That’s so often lost in some companies that are trying to build a grassroots effort without adequate buy-in from a leadership level,” Wylie notes. ››

> “Over a span of time, it is not unusual for new devices to be added, configurations to change, and for that not to be documented anywhere.”

- **Consider where the first dollars are invested.** "That first dollar concept is important because companies have to make decisions between people, process, products, and technologies that they employ," Wylie explains. "Making those first dollar investments in people helps you make smarter process and technology decisions later on."
- **Recognize that security is not an absolute state.** Decisions made today that help a company reach an acceptable level of risk will need to evolve because new risks emerge, threats change, and companies change, as do people and processes. Wylie says, "Leadership really needs to recognize that the operations side of managing risk through the lifespan of a company involves ongoing investment in people, processes, and technology."

Wylie sees industries beginning to take OT security more seriously by recognizing the importance of OT security leadership and considering more carefully how they invest in security. He also sees more reliance on cloud solutions for OT management. "The ability to analyze the operation and make enhancements requires a very broad perspective and access to lots of data. That's not going to happen on the factory floor," he says. He also emphasizes the critical importance of OT security. "Real stuff happens in the real world, not just this digital world. Everything eventually equates to something moving in a physical world that could have impacts on individuals or communities." ■

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

KEY POINTS

1 **CISOs must embrace their leadership role so they can communicate a clear perspective on risks that affect the company, the employees, customers, and the community.**

2 **Recognize that security is not an absolute state. It must evolve because new risks emerge, threats change, and companies change, as do people and processes.**