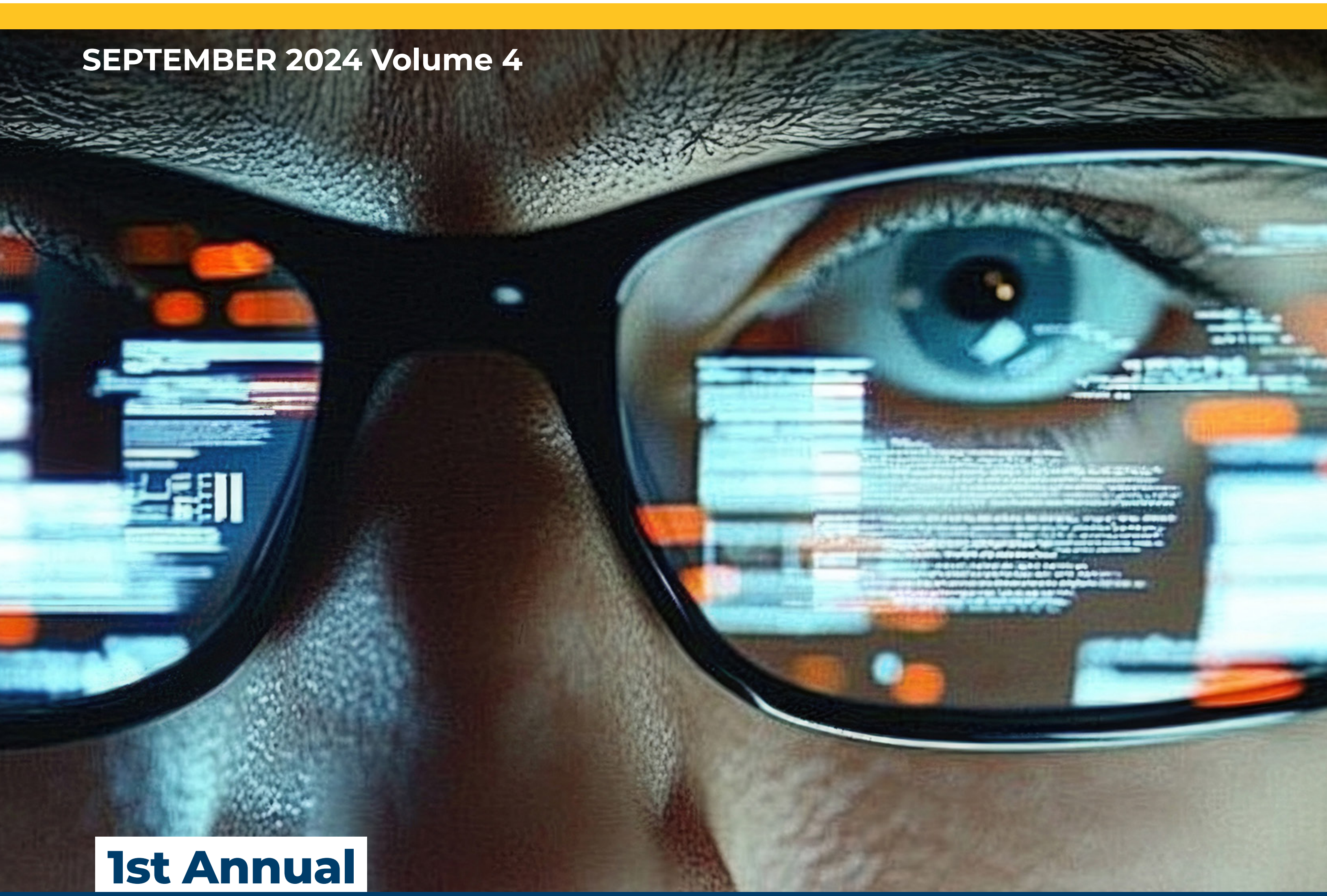
AUTOMATION 2024

SEPTEMBER 2024 Volume 4



1st Annual

OT CYBERSECURITY Trends Report

- Cybersecurity Resiliency Is Vital
- Cybersecurity and Digitalization: A Cautionary Tale
- Understanding the ISA/IEC 62443 Series of Standards
- Adding 'Industrial' to Cybersecurity Education
- OT Cybersecurity Is a Team Effort

AUTOMATION.COM | ISA A subsidiary of the International Society of Automation

Introduction

AUTOMATION 2024 VOLUME 4

1st Annual Industrial Cybersecurity Trends Report

Of 356 cyberattacks recorded in 2023 by ICSSTRIVE.com, 68 caused physical consequences to manufacturing or critical infrastructure facilities. Monetary losses were substantial, amounting to $27 million for Johnson Controls, $49 million for Clorox and up to $450 million for MKS Instruments to name a few.

Protecting operational technology (OT) environments and ensuring their resilience is a complex, multifaceted and specialized endeavor requiring a unique mix of technical knowledge and domain expertise. This first annual OT Cybersecurity Trends issue from Automation.com, a subsidiary of the International Society of Automation, provides a window into the challenges to and available resources for industrial control and automation system cybersecurity.

Jack Smith reveals the importance of the ISA/IEC 62443 series of standards and the many resources available from ISA. Gregory Hale of ISSSource.com discusses how, cyber resilience is vital in the face of inevitable cyberattacks, and industrial digitalization affects safety and security efforts more than ever before. Sean O'Brien reveals how a consensus-based OT security body of knowledge and curriculum materials are training OT cybersecurity specialists. The International Society of Automation has the information and support industrial automation professionals need to rebound from the inevitable. Explore this issue and all the links it contains to see how to best protect your company's OT assets.

Renee Bassett, Chief Editor
Automation.com

About AUTOMATION 2024

The AUTOMATION 2024 ebook series covers Industry 4.0, smart manufacturing, IIoT, cybersecurity, connectivity, machine and process control and more for industrial automation, process control and instrumentation professionals. To subscribe to ebooks and newsletters, visit: www.automation.com/newslettersubscription.

AUTOMATION 2024 is published five times per year (March, May, July, September, and November) by Automation.com, a subsidiary of International Society of Automation (ISA). To advertise, visit: www.automation.com/en-us/advertise.

AUTOMATION.COM

groups/68581

automationdotcom

@automation_com

ISA International Society of Automation
Setting the Standard for Automation™

company/internationalsocietyofautomation

InternationalSocietyOfAutomation

@ISA_Interchange

Renee Bassett, Chief Editor
rbassett@automation.com

Chris Nelson, Advertising Sales Rep
chris@automation.com

Richard T. Simpson, Advertising Sales Rep
rsimpson@automation.com

Gina DiFrancesco, Advertising Sales Rep
GDiFrancesco@automation.com

When we named our industrial application software “Ignition” fifteen years ago, we had no idea just how fitting the name would become...

IGNITING

DIGITAL TRANSFORMATION

Ignition’s industry-leading technology, unlimited licensing model, and army of certified integration partners have ignited a SCADA revolution that has many of the world’s biggest industrial companies transforming their enterprises from the plant floor up.

With plant-floor-proven operational technology, the ability to build a unified namespace, and the power to run on-prem, in the cloud, or both, Ignition is the platform for unlimited digital transformation.

Ignition!®

One Platform, Unlimited Possibilities

Visit inductiveautomation.com/ignition to learn more.

Coca-Cola Morgan Stanley TRUSTED BY NOV Johnson & Johnson

Table of Contents

AUTOMATION 2024 VOLUME 4 OT CYBERSECURITY TRENDS REPORT

3 Introduction

OT CYBERSECURITY INSIGHTS

10 Pairing a Data Diode with Tunnel/ Mirroring for Secure Data Access
By Xavier Mesrobian, Skkynet
There has never been a time when making secure remote connections to industrial data has been more critical.

13 How ISA/IEC 62443 and AI Enhance Security in OT Environments
By Felipe Costa, Moxa
Advancements in network dissection and OT-specific algorithms have improved the security and precision of AI applications.

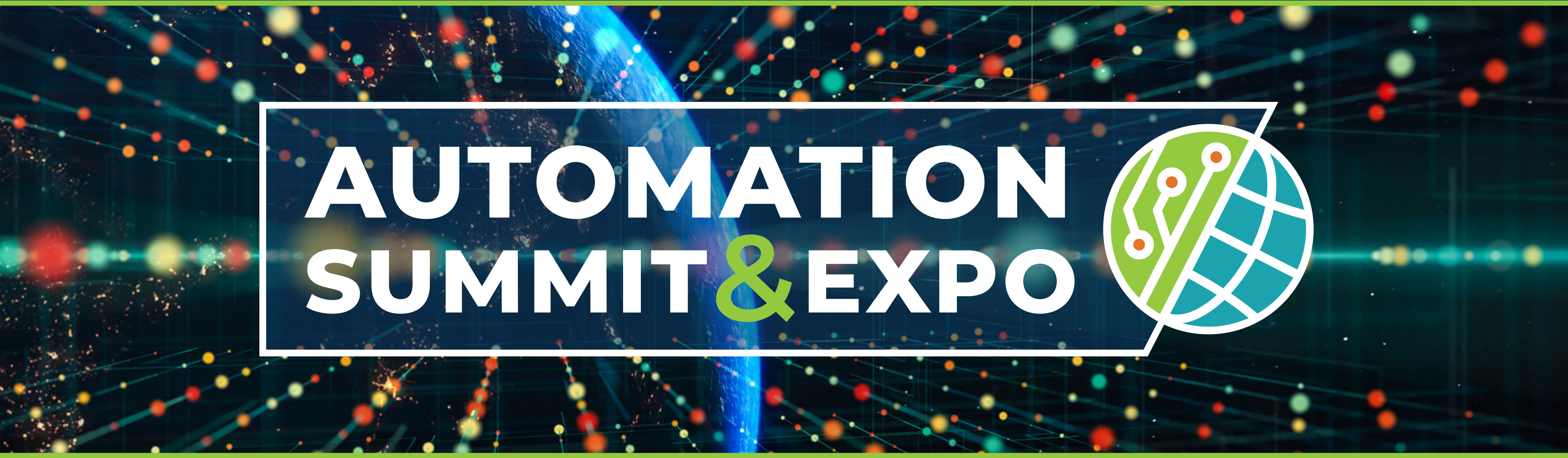
16 Importance of Cybersecurity Experts in OT Environments
By Jose Luis Laguna, Fortinet
This complex and multifaceted discipline requires a combination of technical knowledge and expertise in diverse sub-industries.

SPONSORS

ISA Automation Summit and Expo (ASE)............... 6
ISA GCA 8
1898 & Co 2
Fortinet........ 16
Inductive 4
ISSSource 18
Moxa........ 15
Skkynet........ 12

ISA International Society of Automation
Setting the Standard for Automation™

ase.isa.org



AUTOMATION SUMMIT & EXPO

30 September - 3 October | Charleston, South Carolina, US

The Automation Event of the Year!

Conference sessions on hot topics give you valuable, in-depth insights and knowledge to empower your journey in the automation industry.

Cybersecurity Track
Supply Chain Security, Protection Against Ransomware Attacks, and Safety and Integrity of Automated Systems

Digital Transformation Track
Generative AI, Smart Manufacturing, Cloud Technology and Digital Twins

Career Skills Track
Leadership Skills and Professional Development Within the Automation Industry

The expo brings you face-to-face with vendors from the industrial automation, process control and operational technology (OT) cybersecurity fields.

Industry-leading ISA certificate training courses covering the ISA/IEC 62443 industrial cybersecurity standards will be offered in conjuction with the event.

The ISA Honors and Awards Gala red carpet walk revs up the excitement aboard the USS Yorktown as we recognize the best of ISA.

Register Now

Become a Sponsor

Visit ase.isa.org for a full list of activities and programs included in and held in conjunction with this event.

Table of Contents

FEATURES

19 **While Cyberattacks Are Inevitable, Resilience Is Vital**

By Gregory Hale

Understand consequences, apply basics and use good tools to enhance protection.

30 **Cybersecurity and Digitalization: A Cautionary Tale**

By Gregory Hale

A successful digital enterprise means employing solid cyber principles.

39 **Understanding the ISA/IEC 62443 Series of Standards**

By Jack Smith

This cybersecurity toolset defines requirements and processes for securing industrial automation and control systems.

46 **Adding 'Industrial' to Cybersecurity Education**

By Dr. Sean McBride

Industry, government, and academia embarked on a three-year research project to create a consensus-based OT security body of knowledge.

54 **OT Cybersecurity Is a Team Effort**

By Kara Phelps

Globally relevant standards and conformance programs are important, as is support for automation professionals.

ISA GLOBAL CYBERSECURITY ALLIANCE

Industrial Cybersecurity is a Global Imperative

It's time to join forces. We are stronger together.

Get Engaged!

Johnson Controls
Honeywell
cervello
SecurityRisk ADVISORS

NOZOMI NETWORKS
RA Rockwell Automation
HEXAGON
ACET SOLUTIONS
SIKER

Life Is On Schneider Electric
FORTRESS
Chevron
FORTINET

exida
Radiflow
PURDUE UNIVERSITY Polytechnic Institute
BUREAU VERITAS 1828
NEOM
ISASecure

BR BASEROCK IT SOLUTIONS
DIGITALIMMUNITY STAY PRODUCTIVE, STAY SECURE
tenable
WisePlant Smart, Safe & Secure

TiSafe
EATON Powering Business Worldwide
1898 & CO.
FM Approvals
ac&e

RESILTECH Technologies for Resilience
BYHON
JM Johns Manville A Berkshire Hathaway Company
asp AUTOMATION STRATEGY & PERFORMANCE
INL Idaho National Laboratory
Emerging Technology Apprenticeships

KPMG
Deloitte.
xage SECURITY
OMICRON
senhasegura by MT4 TECHNOLOGY GROUP

COONTEC
txOne networks
xylem Let's Solve Water
ENAXY
Carrier

RED TRIDENT INC
UL Solutions
Idaho State University
[r [redacted]

Inst MC
Peloton CYBER SECURITY
TRANE TECHNOLOGIES
PETRONAS
ENBRIDGE

www.isagca.org

International Society of Automation
Setting the Standard for Automation™

Insider Insights

OT Cybersecurity Trends Report

Pairing a Data Diode with Tunnel/ Mirroring for Secure Data Access

By Xavier Mesrobian, Skkynet

Industrial engineers and corporate executives face a pressing problem. On the one hand, they need access to process data for artificial intelligence (AI) and other applications. On the other hand, cybersecurity exploits targeting industrial systems have been increasing day by day. There has never been a time when making secure remote connections to industrial data has been more critical.

> There has never been a time when making secure remote connections to industrial data has been more critical.

To meet this challenge, many companies are looking into data diode technology. A data diode is a hardware component that enforces one-way data flow. It allows data to pass out of the plant network and prevents any data whatsoever from entering back in. Not one inbound TCP packet can cross a data diode. For applications where even a closed firewall is deemed insufficient, a data diode can provide an extra layer of security.

However, a data diode is not the ideal solution for every remote data access project. Adopting this technology can be challenging, costly, and in some cases, impractical. For example, some remote data connectivity scenarios require bidirectional data flow. What's more, SSL cannot be used with a data diode. For this reason, system designers may benefit by combining data diode and secure tunneling technologies.

Here is an overview of four data-connectivity scenarios.

Client-server. The first scenario is a typical client-server connection, like OPC UA. Although it provides SSL support, a client-server connection requires opening at least one inbound firewall port, exposing the server to an external attack, either directly or through a compromised client. There is no protection against malformed SSL packets—they all get processed. The inherent insecurity of the client-server model makes it an unacceptable choice for remote access to industrial networks.

Tunnel/mirror. A second scenario is tunnel/mirror technology that makes outbound connections through a firewall. This essentially reverses the role of client-server, because in this case, the data source connects outbound to the data user. Tunneling/mirroring can support SSL and it blocks external attacks on the data source. However, because the data flow is bidirectional, and malformed TCP packets are processed, a compromised program on the data user side could attack the data source.

Choosing a tunnel/mirror software package that supports multiple protocols like OPC UA, OPC Classic, MQTT, and Modbus, and provides a unified namespace, gives this option a distinct advantage when you need to integrate legacy systems or diverse data sources.

Tunnel/mirror in data diode mode. A third scenario is a tunnel/mirror implementation running in data diode mode. In addition to making outbound connections and supporting a unified namespace, this approach includes software emulation of a data diode at the data source that discards all incoming TCP control packets and SSL protocol packets. All application data is discarded without being processed, so a compromised data user cannot attack the data source. The only thing exposed to attack is the SSL implementation, if SSL is being used. Since all application data is discarded, data flow over this connection is strictly unidirectional.

Tunnel/mirror with hardware data diode. The fourth scenario is a hardware data diode supported by tunnel/mirror software. The data diode blocks all external attacks, as well as any attacks that may come via a compromised data user because all TCP packets are simply not delivered. This solution can be used with or without a firewall and may also support multiple data protocols. The one drawback to this approach is that SSL is not available when connecting through a hardware data diode. Since all incoming packets are discarded, data flow over this connection is strictly unidirectional.

Which of these four is the best? It depends on your needs. If you are not connecting outside the plant at all, the client-server scenario has worked well for decades and should be sufficient. If you are connecting remotely to a trusted network and need two-way data flow, then tunneling/mirroring would be your best option.

If you are already using tunneling/mirroring, and want to enhance protection on a specific connection, you might consider configuring one or more additional tunnels to run in data diode mode. This would allow you to keep your SSL implementations while enjoying the benefits of a data diode.

And of course, should you truly require a hardware data diode, there are many on the market to choose from. Using one that is compatible with tunnel/mirror software can enhance your connectivity options, especially if you gain multiple protocol support over a unified namespace. Shutting down all incoming data packets should not restrict your choice of the protocol of the data feed you want to access, or the client that receives it.

Xavier Mesrobian is the vice president of sales and marketing at Skkynet, a global leader in industrial data connectivity. With 25+ years in the industry, Skkynet software and services are used in over 27,000 installations.

How ISA/IEC 62443 and AI Enhance Security in OT Environments

By Felipe Costa, Moxa

> Advancements in network dissection and OT-specific algorithms have improved the security and precision of AI applications.

In an increasingly interconnected industrial landscape, cybersecurity is paramount. The ISA/IEC 62443 standard provides a comprehensive framework for securing industrial automation and control systems (IACS) while giving asset owners the flexibility to define which technologies, processes and training best fit their company. It does not enforce specific technologies but rather sets requirements based on the security level. Here we'll explore how integrating artificial intelligence (AI) into intrusion detection systems (IDS) and intrusion prevention systems (IPS) can enhance monitoring, threat intelligence, and response capabilities and how it can be combined with IEC-62443.

The ISA/IEC 62443 series of standards emphasizes creating robust and resilient technologies to counter cyber threats. The standard defines distinct security levels, enabling organizations to tailor security measures based on a comprehensive risk assessment ranging from levels 0 to 4.

Once you have defined the appropriate security level based on a prior risk analysis, you need to deploy a defense-in-depth strategy, as well as monitoring and response mechanisms. Implementing a multi-layered defense approach ensures that security controls are distributed across different layers, minimizing the risk of a single point of failure.

Here, AI can be extremely useful, enhancing perimeter defense and monitoring for malicious patterns attempting lateral movements within the network.

Integrating AI into IDS/IPS systems improves their ability to detect and mitigate sophisticated cyber threats. AI algorithms analyze large datasets to identify patterns and anomalies, significantly improving threat detection accuracy and supporting automated responses. This automation reduces the spread of threats because responses occur immediately, close to the detection point.

Historically, the OT space was resistant to using AI due to issues with IT technology handling OT traffic and misunderstandings about how algorithms work. However, advancements in network dissection and OT-specific algorithms by companies like Moxa have improved the security and precision of AI applications, aligning them with safety requirements.

AI and threat intelligence applications

Combining threat intelligence with AI allows for predictive analysis and establishing a baseline of "good" information patterns, enabling organizations to anticipate and prepare for potential cyber-attacks.

In pre-defined cases, AI-driven systems can automate responses to detected threats, ensuring timely mitigation without human intervention.

The ISA/IEC 62443 standard also emphasizes cybersecurity through structured protocols and training, such as regular employee training, role-based access control and incident response preparedness. It mandates risk assessments, continuous monitoring, and integration with threat intelligence. In this article, we focused on technological aspects, yet it is essential to balance all pillars of cybersecurity.

Conclusion

The ISA/IEC 62443 standard offers a robust framework for securing industrial systems, focusing on technology, people, and processes. Integrating AI-driven IDS/IPS with threat intelligence significantly enhances an organization's security posture, making industrial systems more resilient to cyber threats. As industrial networks grow more complex, adopting these advanced security measures is essential for protecting critical infrastructure.

Felipe Costa is Sr. Product Marketing Manager - Networking & Cybersecurity for Moxa. Felipe is a seasoned cybersecurity director and a certified official instructor in industrial cybersecurity by ISA and EC-Council. He holds more than 30 certifications and a Master of Science in the area. With about 20 years of experience in the industrial sector, he has presented and published articles globally, including at the NASA Artificial Intelligence Congress.

Importance of Cybersecurity Experts in OT Environments

By Jose Luis Laguna, Fortinet

Cybersecurity in operational technology (OT) environments has become a crucial concern in today's growing digital era. As industries digitize, the line between information technology (IT) and OT blurs, enabling more opportunities but also posing greater challenges.

The increase in cyberattacks on OT systems is a known fact that can be further explored in the *2024 State of OT and Cybersecurity Report*. The report found that 73% of organizations have suffered an attack. Specifically, the year-over-year increase of intrusions affecting only OT systems has risen from 17% to 24%.

In addition to this risk landscape, this sector also faces another major challenge: the heterogeneity of the industry due to the diverse sub-industries it encompasses and its complex regulations and rules. Based on these trends, the role of the cybersecurity specialist in OT environments becomes vitally important.

A complex environment to protect

> This complex and multifaceted discipline requires a combination of technical knowledge and expertise in diverse sub-industries.

OT environments cover a wide variety of sub-industries, from energy to manufacturing, passing through oil and gas to transportation and more. All of these rely on cyber-physical systems such as industrial control systems (ICS), supervisory control and data acquisition systems (SCADA) and other devices and technologies that monitor and control physical processes and industrial operations.

Each of these sub-industries has its own specific cybersecurity and automation challenges and needs, thus requiring thorough management.

Cyberattackers also target sub-industries that suit them best, as revealed in the *2024 State of OT and Cybersecurity Report*. One key takeaway is that manufacturing customers are prone to being subjected to staggeringly high ransoms.

From an architectural perspective, the Purdue Reference Model, also known as the Purdue Enterprise Reference Architecture (PERA), is considered the main reference model due to its widespread use in OT environments, as well as its organization of industrial networks into hierarchical levels.

Each sub-industry adapts the model to its specific needs, ensuring that critical systems are protected and that integrations between field operations and enterprise systems are optimized. Furthermore, the evolution of emerging technologies, such as industrial IoT devices (IIoT) and industrial wireless (including industrial 5G), requires an adaptation of the Purdue reference model to each sub-industry every time new technologies are implemented.

Logically, each sub-industry within its operational environments has specific policy and regulatory frameworks designed to address its particular cybersecurity challenges and risks. As the threat landscape evolves, these regulations are also becoming increasingly stringent. Additionally, these norms vary geographically, posing as an added challenge for multinationals operating in different countries as they must adapt their infrastructures to ensure compliance with local regulations.

The subject matter experts

Because different sub-industries have different architectures and regulatory frameworks that vary depending on location of the infrastructure, an OT cybersecurity expert needs not only to understand general cybersecurity principles. They must also possess a deep knowledge of the processes and specific technologies of the sub-industry in which they operate, as well as the policy frameworks that affect them.

Integrating security measures in OT systems is not an easy task due to the critical and continuous process nature of these systems. Moreover, OT cybersecurity is not only about technology but also about people and processes which, of course, vary from one customer to another (even within the same sub-industry). Therefore, OT cybersecurity specialists must work closely with the client's operations engineers and other stakeholders to develop practical and effective security strategies.

As the industrial sector advances in its digital transformation, the demand for OT cybersecurity specialists with experience in different sub-industries will continue to grow. To address the unique challenges of OT cybersecurity, it is essential to rely on experts who understand both the technologies and the specific operational contexts of each sub-industry as well as their regulatory frameworks. This will not only strengthen the security of critical systems, but it will also enable a safer and more efficient operation of the infrastructures that support our broader society.

Jose Luis Laguna has worked for Fortinet for more than 11 years, where he has led the Fortinet engineering team for Spain and Portugal and currently leads the OT solutions architect team for EMEA. He has more than 25 years of experience in engineering and has been systems director and CISO at the Técnicas Reunidas Group specializing in the construction of oil and energy plants.

While Cyberattacks Are Inevitable, Resilience Is Vital

Understand consequences, apply basics and use good tools to enhance protection.

By Gregory Hale

It wasn't that long ago when a series of major companies in the food industry suffered ransomware attacks that forced them to shut down operations.

As in multiple other sectors, the companies were wildly unprepared: living with a false sense of security, thinking they would never suffer any kind of cyberattack, believing they had a built-in sense of resiliency they thought would keep them up and running.

They were wrong.

To that end, the food sector is just one of many that must understand production availability is key in operational technology (OT) environments. Production systems generate enormous amounts of revenue per hour so having one down for days or weeks because of a cyberattack is extremely expensive—not to mention the brand damage, environmental and safety risks involved.

This is exactly where a resilience program can really come into play.

Resilience entails the ability of a system to anticipate, withstand, recover from, and adapt to, cyberattacks and natural or accidental disruptions. Along those lines, organizations must acknowledge the days of the hard-shell security exterior keeping attackers out are long gone. There must be a realistic and comprehensive resilience strategy to control the impacts of an attack.

"We must accept the fact successful attacks are inevitable, but ensure we have the people, processes and technologies in place to avoid catastrophic events," said Mark Carrigan, senior vice president of process safety and OT cybersecurity at Hexagon. "This starts by identifying the most critical assets, understanding the potential consequences of the attack and improving our ability to respond and recover."

Manufacturing, the top target for ransomware attacks, experienced an 18 percent overall increase year over year, according to a report from Zscaler, Inc.

Attack costs rising

Understanding your critical assets is even more important today because the costs of attacks continue to go up. Just look at the numbers from various industry reports.

According to IBM's annual Cost of a Data Breach Report, the industrial sector experienced the costliest increase of any industry, rising by an average of $830,000 per breach over last year.

For 2024, the report found the data breach cost for the industrial sector was $5.56 million compared to the previous year's $4.73 million. Energy also went up to $5.29 million from $4.78 million. Pharmaceuticals also jumped to $5.10 million from $4.82 million.

When it comes to ransomware attacks, manufacturing is the top target, according to a report from cloud security provider Zscaler, Inc.

According to the Zscaler ThreatLabz 2024 Ransomware Report, which analyzed the ransomware threat landscape from April 2023 through April 2024, there was an 18 percent overall increase in ransomware attacks year-over-year, as well as a record-breaking ransom payment of $75 million to the Dark Angels ransomware group,

In terms of specific attacks, MKS Instruments in February 2023 suffered an attack that “affected…production-related systems, and as part of the containment effort, the company has elected to temporarily suspend operations,” according to a report on the incident database, ICSSTRIVE.com. The total cost of that attack to date has been $450 million. The breakdown from that attack was $200 million, which fell on MKS, while one of their suppliers felt a $250 million hit because they couldn’t get product from MKS.

In August 2023, Clorox said damage to the information technology (IT) network “caused widescale disruption of Clorox’s operations.” Total cost of that attack to date is $49 million, according to ICSSTRIVE.

That same year, Johnson Controls was the victim of an attack that cost the company a minimum of $27 million, according to ICSSTRIVE.

Government involvement

When it comes to resiliency, even the U.S. government understands cyberattacks are inescapable, and it shifted its focus toward building resilient systems. That is why it issued a report on resilience created by the President’s Council of Advisors on Science and Technology (PCAST).

Cyber-physical systems are at the core of the critical services that underpin our lives, PCAST said in its report. Cyber-physical systems are increasingly vulnerable to threats from nation-states, terror groups, criminals, a range of natural disasters, as well as accidents and failures.

One case in point PCAST gave when talking about resilience is the 2021 Texas winter power crisis. While the failure of physical systems due to extreme cold led to a skyrocket in demand for electricity to provide heat, the lack of resilience built into the overall system—including its cyber elements—contributed to the catastrophe that left more than 4.5 million homes without power.

"It is refreshing to see the United States Government (USG) finally consider the importance of resilience when looking at the safe, secure, and reliable operation of infrastructure in the eyes of an ever-changing and faster-growing threat landscape," said Joel Langill, founder and managing member of the Industrial Control System Cyber Security Institute (ICSCSI), LLC. "We should understand that security and

Tracking OT Cyber Incidents

There were 356 cyberattacks reported in 2023, of which 68 caused physical consequences to manufacturing or critical infrastructure facilities distributed among more than 500 sites—a 19% increase over the 57 attacks reported in the previous year, according to the 2024 Threat Report issued by ICSSTRIVE. Costs related to cyberattacks were $27 million for Johnson Controls, $49 million for Clorox and up to $450 million for MKS Instruments, to name just a few.

ICSSTRIVE stands for "Industrial Control System Security, Threats, Regulations, Incidents, and Vulnerabilities provided by Experts." ICSSTRIVE.com, a sister site of ISSSource.com, is a database of incidents in the manufacturing sector that started in March 2021. On the site, you can search the more than 1,200 reported incidents in the ICSSTRIVE database by industry sector, country, company, type of attack (like malware or ransomware), or even attack groups.

Other key findings in the 2024 Threat Report include:

- In the period 2019-2023, attacks are almost doubling annually with an average compound annual growth rate of over 90% per year.
- The discrete manufacturing sector was the hardest hit in 2023, followed by transportation and process manufacturing.
- In roughly one-quarter of all attacks since 2010, where public reports included enough detail, threat actors impaired or manipulated operational technology (OT) systems directly. In the remaining attacks, physical consequences were an indirect result of compromising IT systems or other kinds of systems.
- Attack complexity is increasing, including for example the emergence of serious GPS spoofing attacks and an increasing number of supply chain attacks with physical consequences.

The database allows asset owners to research incidents that have occurred in the same industry they operate in. They can learn what has happened to their peers and they can also use it when they become aware of new malware, ransomware, or activity groups. It also helps operators and asset owners understand the magnitude of what kinds of cyberattacks the manufacturing industry is facing and saves time when putting together a justification for a cyber investment.

Find out more from the 2024 Threat Report.

resilience are not the same thing, nor are they mutually exclusive from one another."

Remaining resilient to stay up and running or recovering quickly from an attack is not overly expensive and it is possible for all companies as they most likely have all they need right now to fight off 90 percent of attacks. They just need to apply the basics.

Understand fundamentals

"Cybersecurity in the industrial sector can improve by maintaining strong fundamental practices while integrating advanced tools," said Dewan Chowdhury, chief executive and founder of security provider, malcrawler. "Core practices like network segmentation, regular backups, comprehensive asset inventories, adherence to security frameworks, and secure remote access form a great foundation of a resilient cybersecurity posture.

"Complementing these basics with new technologies such as AI [artificial intelligence] and machine learning can significantly enhance threat detection and response capabilities," he said.

But, he added, don't get caught up in all the bells and whistles of new technologies hitting the market. Understand what you need and apply the proper technologies at the proper time.

"Organizations must avoid the common pitfall of investing in cutting-edge technology that remains unused," Chowdhury said. "Instead, they should focus on integrating these tools into their existing security frameworks to enhance, not replace, fundamental practices. Learning from the past, where many cybersecurity products became obsolete, highlights the importance of staying adaptable and informed about industry trends. By balancing core practices with innovative tools, the industrial sector can build a robust and adaptable cybersecurity defense."

Taking lessons learned from other practices like safety could help build an understanding of resilience.

Learn from safety

"Industrial sectors, especially those with mature process safety cultures, commonly leverage techniques such as peer review or cold eye review (CER) to reduce the likelihood of safety incidents," said Dave Gunter, director of business development at industrial cybersecurity solutions provider Armexa. "Industrial cybersecurity practitioners, in these and other industrial sectors, could achieve additional levels of maturity by adopting similar practices."

"While peer review or CER may seem obvious, in practice, humans often jump to solutions before thoroughly discussing the pros, cons and risks with others before deployment. A diverse team of functional experts brings value to the approach. CER leverages the experiences and skills that you already have within the organization," Gunter said."

For example, Gunter said, senior members of the team typically introduce tried and true fundamental concepts into the discussion. Mid-career practitioners have a clear line of sight as to what works and what doesn't in the current field of operations. Junior team members may ask questions like, "Why do we do it this way?", which may challenge others to consider alternative solutions.

Industrial sectors commonly leverage techniques such as peer review or cold eye review (CER) to reduce the likelihood of safety incidents. Industrial cybersecurity practitioners could achieve additional levels of maturity by adopting similar practices.

"The result is a clear—and hopefully quick—discussion on the concept, the tool or approach, the fundamentals, what-if questions, and a rationalization of why this is occurring and its importance," said Gunter. "I am not suggesting design by committee or disclosing any cyber-sensitive information; however, validating a concept is a key element in quality assurance and testing."

This process can introduce a pragmatic, trust-but-verify (peer review and CER) culture into the OT cybersecurity solution development, explained Gunter. “Industrial OT cybersecurity maturity will benefit from interactions with other professionals, consultants, and service providers to validate technology, trends, skills, work processes, and approaches,” he added.

Over the past 15 years, OT defenses have gotten better and stronger, but there needs to be a constant state of vigilance.

Over the past 15 years, OT defenses have gotten better and stronger, but there needs to be a constant state of vigilance. “Increased focus on OT assets has improved overall cybersecurity,” Carrigan said. “Industry and regulatory bodies realize OT systems are essential to delivering critical services and products and have increased investments to secure these assets.”

In general, Carrigan added, “investments in segmentation, threat detection and remediation, asset management, and basic hygiene have improved our security posture. That said, while we have improved our ability to prevent and detect events, there needs to be more investment to respond and recover.”

OT protection fundamentals

In the spirit of applying fundamental cybersecurity practices for OT, Chowdhury offered a range of practical suggestions.

Network segmentation. Network segmentation protects OT assets effectively. Existing technologies support VLANs to carve out the network, or modern firewalls create zones to separate OT equipment. During a cyber breach, segmentation prevents attackers from accessing other parts of the network, confining them to a specific zone. This confinement facilitates quicker detection and response. Situational awareness in OT networks is simpler compared to corporate IT environments because OT networks are predictable. Attackers on a segmented network trigger multiple alarms when they attempt to access different networks or unusual ports.

Importance of backups. Maintaining backups is essential because every environment experiences downtime. This downtime may result from cyberattacks, human error, or environmental issues. Organizations must ensure they have the latest backups to restore configuration files for OT equipment such as remote terminal units (RTUs), programmable logic controllers (PLCs), computer numerical control (CNC) machines and laser cutters. The effort to maintain backups is minimal, but the rewards are significant. Having up-to-date backups allows OT systems to quickly resume their critical functions after a disruption.

Asset inventory or comprehensive OT configuration management database (CMDB). Quite a few large companies lack a comprehensive understanding of their OT environment. They do not know all the different equipment or their network connections. It is crucial to document all OT equipment, whether connected to the network or air-gapped. At a minimum, collect data on the model, make, industrial purpose, technical point of contact, network connectivity, engineering workstation connections, and human-machine interface (HMI) connections. This data is crucial for understanding the environment and establishing an incident response program. Depending on the CMDB tool used, it can also serve as the central repository for backups.

Implement a security framework. Establishing a cybersecurity program is straightforward with multiple available frameworks. These frameworks help organizations understand what they need to implement for better cybersecurity posture and maturity. The NIST Cybersecurity Framework, for example, is industry-agnostic and allows organizations to map out their cybersecurity program against recommended guidelines. Evaluating an organization against a suitable framework helps identify gaps in the cybersecurity program. The cost is minimal, requiring resources to communicate across the organization to understand the current posture. In addition, the ISA/IEC 62443 series of standards is also a useful tool to help manufacturers and asset owners start and then continue to grow their security programs.

Maintain basic hygiene. Regular software updates, patch management and strong password policies are fundamental. Ensuring these basic hygiene practices are in place can prevent a significant number of attacks.

Secure remote access. During COVID-19, remote access to OT environments surged. Organizations realized cost savings by having vendors remotely troubleshoot and monitor equipment for efficiency and warranty support. However, in the rush to quickly ensure remote access at the time, security professionals delayed implementing precautions until later—and quite a few organizations suffered the consequences. What the industry learned is secure remote access is more important now than it has ever been. Network segmentation helps implement secure remote access programs. With network segmentation, companies can restrict vendors to specific assets and prevent remote access OT devices from interacting with other parts of the network.

Beyond the basics

While applying basic OT cybersecurity practices can alleviate the majority of attacks, Chowdhury said there are also new technologies that can help address sophisticated cyberattacks. “Implementing fundamental actions and leveraging new technologies requires minimal investment, as most companies already have the human and technical resources necessary,” he said.

Useful new technologies include:

- AI and machine learning. AI and machine learning bring significant advances in securing operational technology environments. AI leverages behavioral analysis to detect anomalous activities within OT systems that may indicate a breach. By continuously monitoring equipment and user behavior, AI can identify deviations from normal patterns, alerting security teams to potential threats before they cause significant harm. Machine learning models can predict and respond to emerging threats in real-time within OT environments offering threat intelligence. These

Resilience Best Practices

It is no secret cyberattacks of all types continue to increase as certain industrial sectors remain low-hanging fruit for attackers. The following are some basic best practices to stay ahead of attackers:

- Fight to remain resilient.
- Understand your risk equation.
- Understand the likelihood and the consequence of an attack.
- Train, train, and then train some more; get specific OT training.
- Re-evaluate your system and understand the dynamic nature of cybersecurity.
- Increase visibility.
- Take stock of what you have on your system.
- Understand what is talking to what.
- Create a culture of collaboration.
- Communicate.

models analyze vast amounts of data from sensors and control systems to identify patterns and indicators of compromise, allowing organizations to proactively defend against sophisticated attacks.

- Zero trust architecture. Zero trust architecture enhances security in OT environments by assuming no user or system is inherently trustworthy.
- Identity and access management (IAM). IAM ensures only authorized individuals have access to critical OT systems. By enforcing strict identity verification and access controls, IAM reduces the risk of unauthorized access and potential breaches in the OT environment.
- Micro-segmentation. Micro-segmentation breaks down OT networks into smaller, isolated segments to limit the spread of potential breaches. This approach contains threats within confined areas, preventing them from moving laterally across the OT network.
- Security orchestration, automation and response (SOAR). SOAR technologies streamline and automate security operations in OT environments, enhancing an organization’s ability to respond to incidents swiftly and effectively. By integrating various security tools and processes, SOAR improves the efficiency and coordination of incident response efforts, reducing the impact of cyberattacks on critical OT systems.

Understand consequences

Cybersecurity is all about understanding risk and applying the basic controls and sprinkling in new technologies to keep the bad guys out and keeping the system up and running by eliminating as much unplanned downtime as possible.

“Cybersecurity is a risk game—as long as computers are required to deliver critical products and services, they will have some vulnerability to an attack,” Carrigan said. “Risk is a simple equation: *Risk = Likelihood x Consequence*. Most of our investments have been in reducing the ‘likelihood’ side of the equation. The future of OT cybersecurity will be in reducing the consequences of cyberattacks—specifically, how to minimize the impact of infiltration and restore operations within an acceptable period."

Manufacturers must understand their risk appetite and know what and where their organization's crown jewels are and how to protect them. "Applying the same security practices to all OT assets is not practical—some are more important than others, even within the same company and the same OT network," Carrigan said.

Remaining resilient to a cyber incident—any kind of incident—means manufacturers must apply the basics, sprinkle in some new technologies and plan, test, revise, and then start that process all over again.

Don't live with a false sense of security. Creating and following a resilience plan will keep your organization up and running while remaining productive and profitable.

Final thoughts

In the end, remaining resilient is a program and not just a slogan.

No matter what the status is of any security program, it must keep evolving to get better and better because attackers are not standing pat. Whether it is ransomware, a terrorist, or a hacktivist attack, a threat actor wants to get in, get what they can, and then get out successfully.

A successful resilience program always falls back on applying solid technology, understanding and communicating the process, and having smart workers understand what to do at the right time.

ABOUT THE AUTHOR

Gregory Hale is the editor and founder of Industrial Safety and Security Source, ISSSource, and former chief editor of *InTech* magazine.

Cybersecurity and Digitalization: **A Cautionary Tale**

A successful digital enterprise means employing solid cyber principles.

By Gregory Hale

Digital transformation across the industrial sector has been a work in progress for years, but the push to increase connectivity from the executive suite to HR and accounting to the manufacturing floor is becoming even more acute.

It only makes sense, as digital technologies can drive improved quality control, boost efficiency gains, reduce costs, enable better environmental controls and create a stronger, more quality product. Not only is digitalization changing the stigma of manufacturing being a musty old environment, it is also turning the sector into a glistening new workplace employing state-of-the-art technology that allows organizations to take on any competitor across the globe.

As these benefits allow for improved efficiency, faster decision-making, increased equipment uptime, improved supply chain management, reduced errors, faster turnaround times, and decreased costs, the key ingredient to this digital recipe is cybersecurity.

“Digitalization is rapidly expanding, making cybersecurity an essential backbone for sustaining digital enterprises,” said Dewan Chowdhury, chief executive and founder of cybersecurity provider, malcrawler. “The recent Microsoft-CrowdStrike incident highlighted the potential risks of an unsecured digital environment.”

Manufacturing, the top target for ransomware attacks, experienced an 18 percent overall increase year over year, according to a report from Zscaler, Inc.

The scenario leading to the Microsoft-CrowdStrike incident had the CrowdStrike Falcon sensor delivering artificial intelligence (AI) and machine learning to protect systems by identifying and remediating advanced threats. In February 2024, CrowdStrike introduced a new sensor capability. On 19 July 2024, a Rapid Response Content update went out to certain Microsoft Windows hosts with the new capability first released in February, CrowdStrike officials said. The sensor expected 20 input fields, while the update provided 21 input fields. In this instance, the mismatch resulted in an out-of-bounds memory read, causing a system crash that affected 8.5 million computers globally and cost companies $5.4 billion.

“While this particular issue resulted from an internal error, it raises concerns about the consequences if an attacker deliberately seeks to cause harm,” Chowdhury said. “This situation demonstrates the critical need for integrating people, processes and technology to enhance cybersecurity in the digital age.”

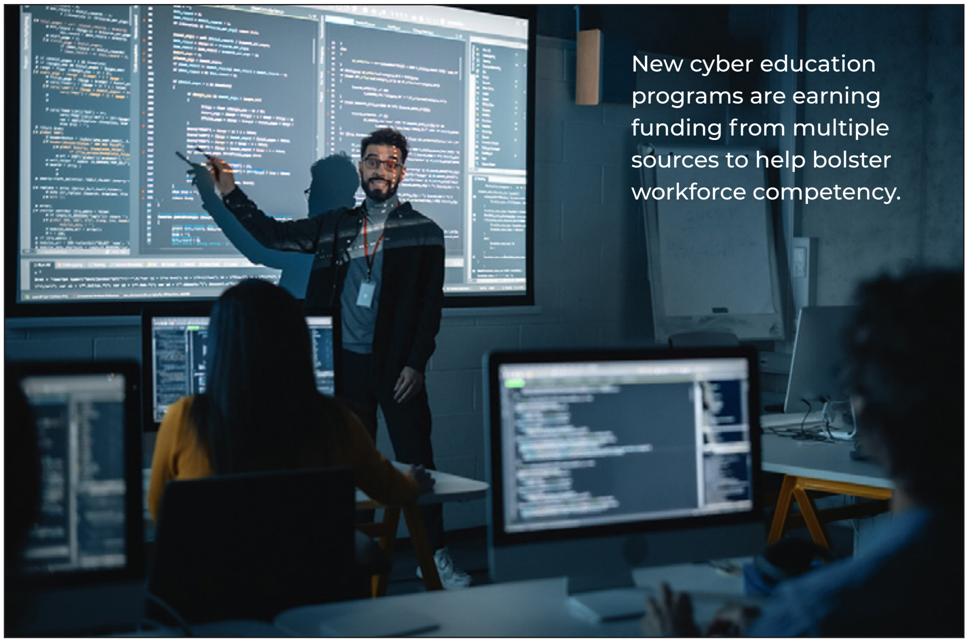
Multiple threats

With increased connectivity in the digital environment, there are more opportunities for threat actors to hit manufacturers with multiple types of attacks including terrorists, hacktivism, supply chain disruption and ransomware.

To that end, one ransomware attack on a German bicycle maker halted production, invoicing and deliveries for three weeks. According to a report in the ICSSTRIVE.com incident repository, disrupted supply chains meant required parts did not arrive so workers could not assemble and deliver the bicycles. As a result of the attack, the company filed for bankruptcy.

While there may have been plenty of reasons why that specific company went out of business, there is no mistaking as the digital environment moves forward with a lack of qualified cybersecurity professionals, elements like artificial intelligence (AI), machine learning, training, education, planning, convergence and even the cloud are coming more into play.

“The age of digitalization, including machine learning and AI is here,” said Mark Carrigan, senior vice president of process safety and OT cybersecurity at Hexagon. “The current and potential benefits these technologies can provide are compelling and will transform how we conduct business.”



New cyber education programs are earning funding from multiple sources to help bolster workforce competency.

With digitalization here to stay, security experts across the board can’t stress enough that having the right people, processes and technologies in place is vital. “Combining skilled personnel, effective processes, and advanced technology is crucial for bolstering cybersecurity,” Chowdhury said. “The shortage of qualified cybersecurity professionals poses a significant challenge. In response, organizations must rely more on artificial intelligence to automate threat detection and response. AI can analyze vast amounts of data quickly, identifying potential threats and mitigating risks, thus compensating for the lack of human resources.”

Creating cyber-skilled workers

The skills gap is a huge issue with an average of 3.4 million industrial cybersecurity open positions globally with more than 410,695 of those jobs in the U.S. alone, according to a report from (ICS)2, an international nonprofit membership association focused on inspiring a safe and secure cyber world.

Cyber education is one aspect continuing to grow to help fill that gap. (See “Adding ‘Industrial’ to Cybersecurity Education elsewhere in this issue.) Indeed, new programs are earning funding from multiple agencies to help bolster the workforce.

Arizona State University’s School of Computing and Augmented Intelligence, part of the Ira A. Fulton Schools of Engineering just earned a two-year, $4.5 million grant from the U.S. Defense Advanced Research Projects Agency (DARPA) to establish an institute that will develop national and global cybersecurity educational standards and curriculums designed to address critical workforce shortages.

The University of Texas at San Antonio (UTSA) created a new college dedicated to AI, cybersecurity, computing, data science, and related disciplines.

A cybersecurity scholarship program is also starting up at the College of Engineering and Computer Science at Florida Atlantic University (FAU) since it received a $2.6 million grant from the National Science Foundation (NSF).

In addition, grants worth approximately $200,000 addressing the nation's shortage of skilled cybersecurity employees will be awarded to 18 education and community organizations in 15 states. These grants are a part of the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) program that awarded cooperative agreements of nearly $3.6 million to build the workforce needed to safeguard enterprises from cybersecurity risks.

According to the U.S. Department of Homeland Security, cybersecurity threats to critical infrastructure are one of the country's greatest strategic risks. Grants and awards have increased due to this. The Internet Crime Report, compiled annually by the Federal Bureau of Investigation, charts growth in cybercrime, noting a record number of complaints in 2023 with $12.5 billion in reported financial losses.

Technologies available to detect and automatically intervene to stop a cyberattack are becoming common in the IT world. They will be further enhanced by leveraging AI techniques. Applying these same technologies in the OT world carries much more risk.

Employee training

Continuous training and education for employees also plays a vital role in maintaining a strong cybersecurity posture.

"A well-informed staff can recognize and respond to potential threats more effectively, reducing the likelihood of breaches caused by human error," Chowdhury said. "As technology evolves, ongoing education ensures that employees remain up to date with the latest security practices and tools."

Part of that ongoing education is evolving from the continuing convergence of information technology (IT) and operational technology (OT) systems and knowledge. "Applying these digital techniques to the OT world, whether to improve productivity, insights, or cybersecurity, will be more difficult than in the IT world," Carrigan said. "The reason is there are key differences between IT and OT that will not change anytime soon."

Carrigan indicated these differences relate to:

- **Flexibility.** IT assets are generally flexible. A single server or PC may conduct a variety of tasks or host multiple applications. OT assets have a specific mission, highly customized to deliver specific tasks to control or monitor operations.
- **Security versus availability.** In general, in the IT world, security takes precedence over availability. Often, on short notice, IT can shut down an asset to install critical security updates. In OT, the opposite is true. These assets must be available 24/7 and often do not update with the most recent security capabilities to avoid unnecessary downtime.
- **New versus old.** In the IT world, assets typically have a relatively short life (three to five years) before an upgrade. In OT it is common to have assets that are more than 20 years old controlling critical infrastructure. The cost to upgrade these assets—in both cash outlays and disruptions to the business—means they have an extended life.
- **Homogeneous versus heterogeneous systems.** In general, IT assets use a limited number of operating systems (Microsoft, Apple OS, Linux, etc.) and protocols to communicate. OT assets end up dominated by vendor-specific operating systems, protocols, and other designs unique and proprietary to each vendor. Integration in the OT world is typically more complicated and customized compared to IT.

Those differences must be considered when applying machine learning or AI to an OT environment, Carrigan said. "As an example, technologies are available to detect and automatically intervene to stop a cyberattack," he explained. "These capabilities are becoming common in the IT world and will be further enhanced by leveraging AI techniques. Applying these same technologies in the OT world carries much more risk—any system that automatically interrupts the actions of an OT system could lead to significant loss of production or equipment damage—the same consequences we are trying to avoid via cyberattacks."

Carrigan added: "The key differences between IT and OT, which will remain for years, means there must be more care when considering machine learning or AI for the OT environment."

New direction

According to the Cisco inaugural 2024 State of Industrial Networking Report, it does appear manufacturers are beginning to design and

People and Process Are Key to Digitalization

With 75 million baby boomers retiring from their manufacturing jobs in such a short time, the industry is facing a large demographic twist. It may seem like the industry will become more reliant on technology, but the tried-and-true cybersecurity triad of people, processes and technology will become even more pronounced in the coming years.

While some in the industry fear digital transformation will eliminate workers, others say people will become the most important asset.

As technology innovation continues to grow and become smarter and more developed, it is also there to support and empower both people and processes. With that in mind, the following are some best practices to ensure a more secure digital environment:

- Gain a strong grasp of basic cybersecurity fundamentals.
- Communicate constantly.
- Secure remote access.
- Network segmentation.
- Constantly back up data.
- Implement a security framework.
- Create a culture of collaboration with purpose-built OT and IT views to help address cybersecurity issues via different views and preferences.
- Understand what is talking to what through continuous and real-time monitoring of asset and network connectivity with immediate alerts on any violation of security policies or anomalies.
- Ensure visibility into ICS assets and networks, employing smart and advanced discovery techniques for complete asset inventory.
- Visualize network topology and connectivity to provide a real-time view.
- Predefine policies incorporating requirements in regulatory standards.
- AI algorithms for auto-defining comprehensive security policies and proactively identifying a variety of threats and vulnerabilities.

deploy their OT environments to improve security, increase efficiency, and provide a platform for innovation. The report mentioned cybersecurity—the backbone of the digital movement—was the biggest reported challenge in running and maintaining industrial networks. Also adding to the problem are the requirements of Industry 4.0, a backlog of legacy systems and assets, an expanding attack surface and an overstretched workforce.

In the report, 89% of respondents said cybersecurity compliance is very important in their operational network. Also, the number one challenge when running industrial infrastructure is mitigating cyber threats.

With the management of enterprise and industrial networks increasingly overlapping, the report also found IT and OT teams need to become more collaborative. Executive leadership can see the benefits of a unified approach but, currently, the two functions remain siloed, impacting efficiency and threatening the overall security posture.

Recognizing the industry does not adjust well to change, but knowing change is inevitable, collaboration is improving and new technologies are evolving to improve security. "Based on what I have observed, the influx of new technology in the cybersecurity industry is truly remarkable, especially with the explosion of artificial intelligence applications," Chowdhury said. "I would not be surprised if roles like tier-one SOC [security operation center] analyst become completely automated by AI soon. It is nearly impossible for a human to efficiently sort through the tens of thousands or even hundreds of thousands of logs generated in a modern infrastructure. Additionally, I have noticed a rise in automated penetration testing tools that allow organizations to continuously test their security controls."

Investing in AI, cloud

Chowdhury believes the cybersecurity industry faces "a significant gap" between the number of available jobs and the qualified professionals needed to fill them. "Although schools are working hard to educate the next generation of cybersecurity experts, the lack of real-world scenario experience remains a significant challenge. This is why I see companies investing heavily in AI to bridge this gap and enhance their cybersecurity defenses."

In more digitalized environments, cloud computing is also becoming a bigger element—something industry wags never thought would happen. "Strategic planning and adopting cloud solutions are essential in modern cybersecurity strategies," Chowdhury said. "The cloud offers scalability and flexibility, which can enhance security measures. However, careful planning is necessary to integrate these technologies effectively, ensuring they complement existing security frameworks. By balancing foundational practices with innovative tools, organizations can build a resilient and adaptable defense against cyber threats coming from an expanded attack surface."

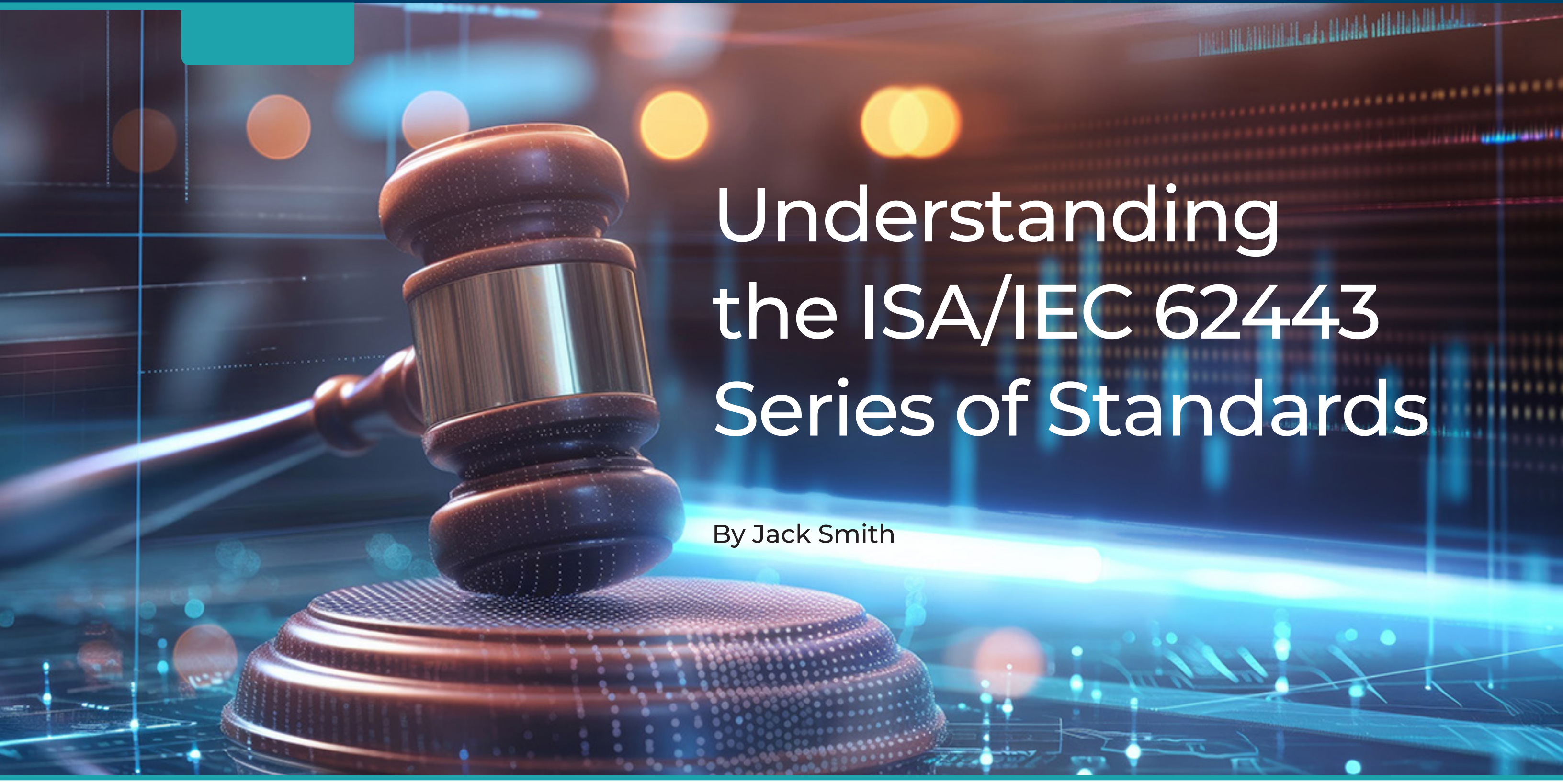
As the threat landscape in the digital world constantly evolves, it is making it increasingly challenging for organizations.

With an expanded attack surface through increased connectivity, it can be a very daunting task to protect a network with all these connections. But with more demand to produce more and more product, understanding what production is doing and how to increase productivity is important.

Digital technology advances are continuing to move forward and the key to avoiding any kind of setback is a strong cybersecurity component acting as the backbone for a manufacturing enterprise.

ABOUT THE AUTHOR

Gregory Hale is the editor and founder of Industrial Safety and Security Source, ISSSource, and former chief editor of *InTech* magazine.



Understanding the ISA/IEC 62443 Series of Standards

By Jack Smith

This cybersecurity toolset defines requirements and processes for securing industrial automation and control systems.

Digital transformation paves the way for businesses to improve efficiency, reduce errors, improve overall equipment effectiveness (OEE) and reduce costs. With the promise of operational technology (OT) advances, comes the need for protecting assets through painstakingly applying cybersecurity principles.

To ensure that businesses are on the same cybersecurity page, a best practice is to adopt and follow established criteria such as the ISA/IEC 62443 series of standards.

The International Society of Automation (ISA) established the ISA99 standards committee in 2002, recognizing the need to secure equipment and operations that comprise U.S. critical infrastructure against cyberattacks. Since then, ISA99 has published a comprehensive family of standards and technical reports purpose-built to address securing automation and control systems.

The ISA/IEC 62443 standards are submitted to the International Electrotechnical Commission (IEC) for global adoption as international standards ISA/IEC 62443. The ISA/IEC 62443 series of standards are endorsed by the United Nations. With use cases from more than 20 different industries, the ISA/IEC 62443 series of standards has demonstrated its utility in all industry verticals that use operational technology systems. In 2021, IEC recognized the series as a horizontal standard, meaning that they have been proven to apply to a broad range of different industries.

The IEC 62443 series of standards addresses cybersecurity for OT in automation and control systems. The series is divided into different sections and describes both technical- and process-related aspects of automation and control system cybersecurity. The series is also known as ISA/IEC 62443 in recognition of the fact that much of the initial development was done by the ISA99 committee of ISA.

Cybersecurity topics are divided by stakeholder category/roles including:

- the operator
- the service providers (system integration and maintenance)
- the component/system manufacturers.

The different roles follow a risk-based approach to prevent and manage security risks in their activities.

The ISA/IEC 62443 series of standards defines requirements and processes for implementing and maintaining electronically secure industrial automation and control systems (IACS). These standards set best practices for security and provide a way to assess the level of

The ISA/IEC 62443 series of standards has demonstrated its utility in all industry verticals that use operational technology systems. In 2021, the IEC recognized the series as a horizontal standard.

security performance. Their approach to the cybersecurity challenge is holistic, bridging the gap between OT and information technology (IT) as well as between process safety and cybersecurity.

900 volunteers contribute

Steve Mustard, president of National Automation Inc. and former ISA president (2021) explained the work that goes into creating and maintaining the standards. “It’s not just a standard, it’s a multiple set of documents,” he said. “The first versions were in 2005, ‘06, ‘07 and ‘08, and they’re being updated now because they get updated every five years. It became an IEC standard and incorporated Part 2-4 from IEC into that set.”

Mustard said there are around 900 volunteers from all over the world on the ISA99 committee. “Some write content, some review content and some vote on content. They’re in different companies. They’re asset owners, vendors, consultants and educators. They all contribute their time freely. Not all of them are members of ISA, but we’d like them to be,” he added.

“We also have a lot of experts from government organizations and non-government organizations,” continued Mustard. “They put a lot of time in, continuously developing different parts of the standard and technical reports, which are documents that help explain some of the detail in the normative versions of the standards and how you execute that. It’s a lot of work.”

Currently, there is certification for products and systems, and then the development lifecycle for vendors. These standards set cybersecurity benchmarks in all industry sectors that use IACS, including building automation, electric power generation and distribution, medical devices, transportation, and process industries such as oil and gas and chemicals.

“Very soon, there will be a site-level assurance program,” explained Mustard. “Parts 2-1 and 3-3 [of ISA/IEC 62443] and many of the other parts of the standard are covering all the requirements in there, much like ISO27001. All the vendors who come along are providing their pieces, but someone has to put them together. The individual projects are great, but it's the whole ecosystem that you have to certify or validate that the risk is being managed."

Ultimately, it's up to the business who owns these systems to make sure the integrators are delivering systems that meet the requirements to the specified level while testing and validating that the services and the maintenance contracts … meet the requirements and manage that risk across the business.

Communicating with others

Chris McLaughlin, chief information security officer (CISO) at Johns Manville and one of the many ISA volunteers who are developing the standard, said, "I'd love for there to be an ISO certification at some point. What's important to us is to be able to demonstrate to physical insurance providers that we have a program that's working. But at the first stages, you're just focused on getting all the pieces."

McLaughlin said insurance companies are asking about cybersecurity. At Johns Manville, he said, "Our physical insurance companies have been doing cyber assessments at each one of our plant locations. Those are our big assets. It would be a big loss if you lost a whole production facility; that's a significant impact, not just a short-term impact. The insurance companies are asking a lot more cyber questions; they're asking for network maps. I don't want to give my insurance provider all those details, so we say: 'We follow these controls. This is how we generally do it, and we have a third party that has audited it.'"

Anna Burrell, an OT cybersecurity consultant with Deloitte, said, "You have to make sure you're [implementing ISA/IEC 62443] across all of your estate. These cyber incidents don't care if it's on a site. It's going to hit a business and it's going to either come into your sites and your OT networks and move up, or it's going to come in the top and move down. So how do you holistically manage all of that risk end to end?"

“ISA/IEC 62443 is a toolset,” explained Burrell. “It’s a standard to give structure and organization in a way that engineers understand. The way you choose to implement those controls works with other policies and standards. It references that it has to work in conjunction with organizational policies and it gives a structure and a common language. It helps people work together to say, ‘How are we going to do this?’”

Burrell said, “You can assure against [62443] because you can check things, but it’s not enforcing how you do things. I think that’s how it’s different and why it applies across industries and sites, projects, and organizations. It’s much wider than necessarily some of the more specific [standards].”

The owner/system integrator relationship

Businesses that own automation assets must ensure system integrators are delivering systems that meet specified requirements. System integrators must be involved in the process. Part 2-4 of the standard helps integrators understand the asset owners’ needs so they can convey the essence of those needs to asset owners, which benefits the owner/integrator relationship.

Mustard expressed that Part 2-4 is very much about requirements for system integrators and maintenance providers. “It provides a comprehensive list of requirements that an asset owner would want from a vendor, system integrator or maintenance provider. They’re dealing with multiple organizations, which, without the standard, have their own set of requirements that are similar but not identical. If they all use the same standard, it makes their life a lot easier in terms of responding to the requirements,” he said.

Consider BP, for example, Mustard continued. When they have contracts for work in system integration or maintenance, they develop their own set of requirements that are BP-specific. If you go to Shell, they have their own. They build requirements based on what they have done in the past. They may not necessarily incorporate all the requirements that ISA/IEC 62443 has. “When you have a project, there’s a lot of requirements about basic cyber hygiene you need to do, and those get overlooked sometimes in contracts,” he said.

"If you use ISA/IEC 62443-2-4 as the basis, you have everything covered so you're not going to forget anything. My recommendation is for asset owners to adopt Part 2-4, and also for the system integrators and maintenance providers to read and understand it and be prepared to respond when asset owners put out a request for services in line with that standard," Mustard explained.

"The integrator delivers solutions that are meeting those requirements," explained Burrell. "But ultimately, it's up to the business who owns these systems to make sure the integrators are delivering systems that meet the requirements to the specified level while testing and validating that the services and the maintenance contracts have been done to meet the requirements and manage that risk across the business."

"The integrators must deliver solutions to meet the requirements, to make sure that the technology can be implemented securely, or the components are certified and meeting those objectives," Burrell continued. "But as an asset owner, you have to put that technology into your organization in the right way, make sure it's meeting your need, and ensure the risk is being managed so that these systems are operating correctly while keeping yourselves safe and production working."

Final thoughts

Training people on ISA/IEC 62443 is an ongoing task. "We find that there's a shortage of talented people in this space," said Andre Ristaino, managing director at ISA. "We've been funding the development of training classes.

Additional Resources on ISA/IEC 62443

More information on the ISA/IEC 62443 series of standards can be found on the ISA website. There you will find links to the following resources.

- Published Standards and Technical Reports
- ISA Cybersecurity Certificate Training Program
- ISA Global Cybersecurity Alliance (ISAGCA) website
- Quick Start Guide to ISA/IEC 62443
- Guide to Security Lifecycles in ISA/IEC 62443
- IACS Taxonomy Glossary
- IACS Principal Roles and Responsibilities
- Overview of ISASecure Certification for ISA/IEC 62443
- IoT Security Maturity Model: 62443 Mappings for Asset Owners and Product Suppliers
- ISASecure website for Supplier and Product Certification

For product suppliers, there's a class called 'IC47.' It covers the standards associated with product development. It's a three- or four-day class, and it also has modules that address requirements for product assessors. We saw that there was a gap with the product assessors at our certification bodies. We're trying to fill that void as well, and we expect to do additional training in the future."

"The ISA/IEC 62443 series of standards is out there and information about what needs to be done by asset owners, system integrators, and product suppliers is all in there," said Mustard. "I think people need to follow it. I think product suppliers and system integrators need to do it regardless of whether asset owners ask them to do it because it's the right thing to do. I think asset owners need to understand the totality of what they need to do, and it's in there. Certification programs will help provide the verification that it's being done."

"Things have improved a lot," continued Mustard. "A few years ago, we would be talking about 62443 and half the audience wouldn't have known what it was. It's encouraging to see so many people who already understand it, and where people are actually applying it and doing real practical things with it. I'm encouraged by that, but we still have a long way to go."

ABOUT THE AUTHOR

Jack Smith is senior contributing editor for Automation.com and *InTech* digital magazine, publications of the International Society of Automation. Jack is a senior member of ISA, as well as a member of IEEE. He has an AAS in Electrical/Electronic Engineering and experience in instrumentation, closed-loop control, PLCs, complex automated test systems, and test system design. Jack also has more than 20 years of experience as a journalist covering process, discrete, and hybrid technologies.

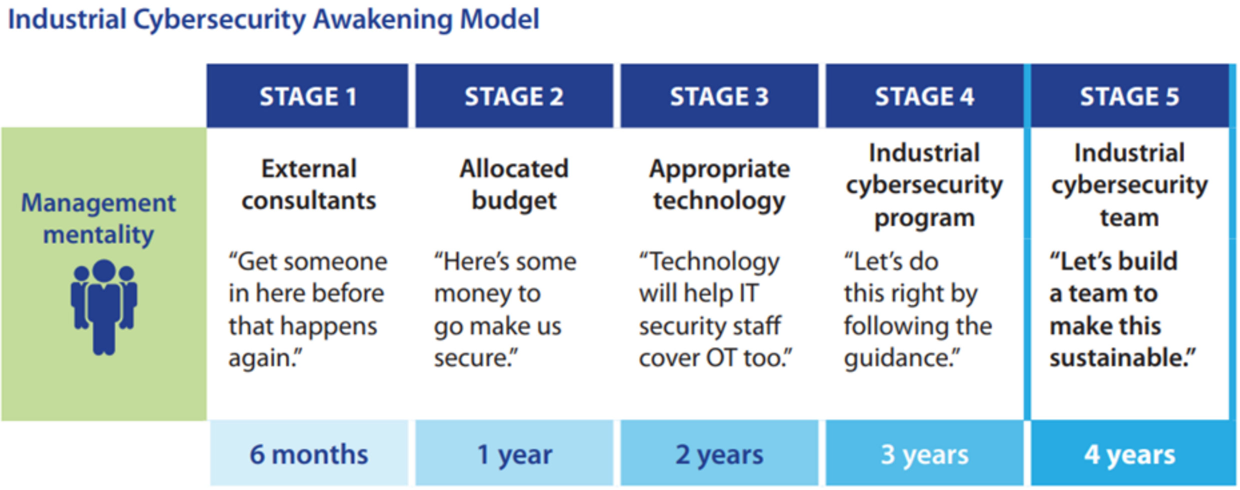
Adding ‘Industrial’ to Cybersecurity Education

By Dr. Sean McBride, Idaho State University College of Technology

> Industry, government, and academia embarked on a three-year research project to create a consensus-based OT security body of knowledge.

As organizations mature their operational technology (OT) security approach, they tend to move from a focus on technology to a focus on building a program to, finally, building a workforce that can run the program and operate the technology. This natural progression has been described as the “Industrial Cybersecurity Awakening Model” (Figure 1).

It can take four years—and sometimes much longer—to reach Stage 5 of the model where organizations intentionally develop an OT security team. The International Society of



Industrial Cybersecurity Awakening Model

	STAGE 1	STAGE 2	STAGE 3	STAGE 4	STAGE 5
Management mentality	**External consultants** "Get someone in here before that happens again."	**Allocated budget** "Here's some money to go make us secure."	**Appropriate technology** "Technology will help IT security staff cover OT too."	**Industrial cybersecurity program** "Let's do this right by following the guidance."	**Industrial cybersecurity team** **"Let's build a team to make this sustainable."**
	6 months	1 year	2 years	3 years	4 years

Figure 1. Developing an OT security team can take four years or longer for organizations.

Automation Global Cybersecurity Alliance (ISA GCA) supported a three-year research project to create a consensus-based OT security body of knowledge and has released a 125-page document and other resources. "Curricular Guidance: Industrial Cybersecurity Knowledge" describes the stages of the model and helps ensure OT security leaders can work with education and training providers that follow a consensus-based OT security body of knowledge.

In the recent past, ransomware has been a significant driver in the awakening. Those who have been in touch with their local industries know that automotive manufacturers, salad processors, and paper makers have suffered ransom demands that shut down process lines and resulted in a relatively rapid leap from Stage 1 to Stage 3. The aftermath of a breach generally leaves one or two individuals (often the electrical engineering professionals who have now been asked to pick up cybersecurity) asking for the resources required to move the "OT side of the house" to Stage 4.

Management of some organizations has contented themselves with the belief that a technology investment alone will get the job done. Stage 3 is as far as they are willing to go. But other organizations, especially those with far-flung operations, are advancing to Stages 4 and 5.

At Stage four, the IEC 62443 series of standards provides powerful concepts such as the industrial automation and control system (IACS) lifecycle, the IACS principle roles, system types, and maturity levels that are key to building a good OT security program. IEC 62443-2-1 recognizes the need for cybersecurity training by including the following requirements:

- Development of a cybersecurity training program
- Providing cybersecurity procedure and facility training
- Providing cybersecurity training for support personnel
- Validating the cybersecurity training program
- Revising the cybersecurity training over time
- Maintaining employee cybersecurity training records (64443-2-1 Req. 4.3.2.4.1-4.3.2.6.4).

Those who have been in touch with their local industries know that automotive manufacturers, salad processors, and paper makers have suffered ransom demands that shut down process lines.

When organizations begin to grapple with these training requirements, they begin to recognize serious impediments, such as:

- Lack of a widely recognized OT security body of knowledge
- Lack of consensus-based OT security work roles
- Lack of validated OT security competencies per work role
- Lack of role-specific OT security training
- No discussion of OT security competencies required of non-security personnel.

The role of workforce development

OT security leaders attempting to tackle this issue find a complex and often foreign world of workforce development literature and guidance.

Plethoric government agencies and professional training providers offer workforce development models. Within these models,

Training a Cyber-infused Generation of Automation Professionals

What would you say if someone asked how to best move towards a secure digital future for critical infrastructure and industrial automation?

In late July 2016, I was contacted by my master's thesis supervisor (Dr. Corey Schou) from Idaho State University (ISU) where I had graduated 10 years earlier. He asked whether I would be interested in teaching a course in ISU's new Industrial Cybersecurity Program.

As I had spent the first decade of my professional life in industrial cybersecurity, I thought this sounded intriguing. I cleared what I thought would be a one-night-a-week teaching commitment with my employer (FireEye/Mandiant) where I had just been appointed as director of the industrial control systems security virtual business unit and started preparing course content for "Risk Management in Cyber-Physical Systems."

I was unfamiliar with ISU's Energy Systems Education and Training Center (ESTEC) where the program was housed. So, when I walked into the ESTEC building and saw the fantastic hands-on educational equipment including programmable logic controllers, variable frequency drives, transmitters, pumps, valves, motors, conveyors and pipes, and talked with the experienced instructors, I realized how special this opportunity could be.

ESTEC is a department-level center featuring five distinct engineering technology programs: electrical, instrumentation, mechanical, nuclear operations and industrial cybersecurity. It features 40,000 sq. ft. of educational laboratory and classroom space spread across four buildings on ISU's main campus in Pocatello, Idaho.

The Industrial Cybersecurity Program at ISU is "stackable," meaning students can come into the program from high school or a variety of engineering or operational technology (OT) degrees.

Continued on next page

Continued from previous page

ESTEC was founded in 2007 with the primary objective of expanding ISU's existing industrial automation program to meet the growing demand for qualified technical professionals at the Idaho National Laboratory. Hundreds of ESTEC graduates work across the country in places like Simplot, Phillips 66, Chevron, Alyeska Pipeline, Columbia Electric Distributors, and many other industrial firms.

When I started teaching, I thought to myself, "Wow, the Idaho State Board of Education has approved the country's first industrial cybersecurity degree program. ESTEC is already a leader in preparing professionals to go into critical infrastructure environments. We need to teach cybersecurity to these students. This is exactly what the country needs. It's exactly what the world needs."

I believed it so firmly that I quit my high-paying job at FireEye to become ESTEC's Industrial Cybersecurity Program Coordinator. My responsibility was to build the program from the ground up.

Over the next seven years, I authored courses, made curriculum proposals, visited high schools to recruit students, submitted and won grants, graded assignments and exams, and hired faculty. I helped place graduates at national-level employers such as the INL, Accenture, Savannah River, National Renewable Energy Laboratory, and HDR Engineering, among others.

One of the accomplishments I am most pleased with is that the Industrial Cybersecurity Program at ISU is stackable. "Stackable" means that students can come into the program directly from high school and earn an Associate of Applied Science degree within two years, or they can come into the program from a variety of engineering or operational technology (OT) degrees—including electrical, instrumentation, mechanical and nuclear operations, as well as on-site diesel power and information technology (IT) systems. Students have completed the program from each of these entry points.

One key to this stackability is that the industrial cybersecurity courses are offered as upper division credit (300 and 400 level), meaning they can provide a pathway to a bachelor's degree. After completing industrial cybersecurity courses, students are pointed to a handful of management-oriented upper-division courses including technical writing, project management, supply chain management and organizational behavior. Once students satisfy their general education requirements, they earn a Bachelor of Applied Science in Cyber-Physical Systems.

ISU has taken program development very seriously. In 2022, the Industrial Cybersecurity Program was recognized as a National Security Agency-designated cybersecurity program of study; and, in 2024, the program achieved ABET accreditation.

So, how we are going to move towards a more secure digital future in critical infrastructure and industrial automation? I'd say we have to start with the people—the future workforce.

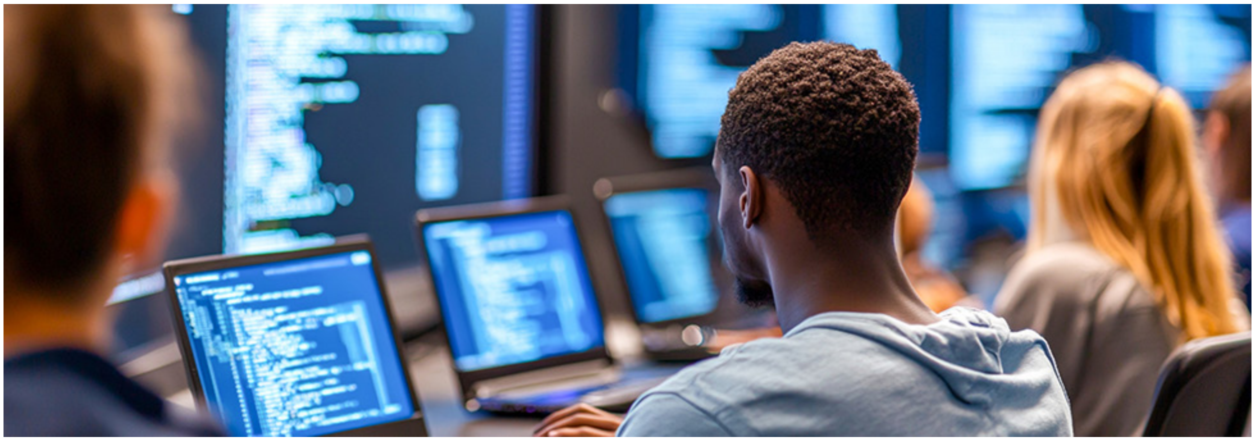
The Industrial Cybersecurity Program at ISU is an outstanding model for how to do this. Through interdisciplinary stackable pathways, we are developing a new generation of automation professionals capable of seamlessly moving between IT, OT, and cybersecurity domains.

definitions of key terms often conflict, and some terms have changed official definitions within the models over just a few years. It can be overwhelming to sort through.

With these challenges in mind, a working group composed of qualified representatives from industry, government, and academia embarked on a three-year research project to review existing OT security workforce development guidance, and where lacking, establish a consensus-based foundation.

In 2019, the Idaho National Laboratory (INL) and Idaho State University (ISU) convened 15 qualified industrial cybersecurity professionals in ISU's Simplot Decision Support Center, where they engaged in the bias-eliminating nominal group technique to identify five archetype industrial cybersecurity job roles, and initial knowledge categories not normally covered in traditional cybersecurity education.

The results of this effort were published in November 2021 as "Building an Industrial Cybersecurity Workforce: A Manager's Guide" which included job descriptions, key tasks, and hiring advice. Recognizing that despite its strengths, this document did not constitute a consensus-based body of knowledge for an emerging cybersecurity specialization, the INL, ISA Global Cybersecurity Alliance (ISAGCA), and ISU decided to validate, critique, and expand the document by involving a broader group of qualified experts.



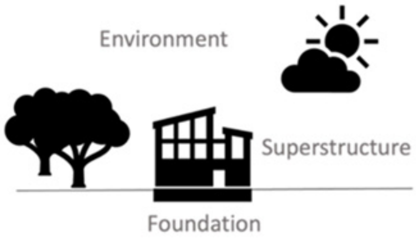


Figure 2. The 125-page ISAGCA document is organized around the analogy of a building that describes the industrial operations environment, foundation and superstructure.

In Spring 2022, the ISACGA administered a survey to professionals with interest or experience in industrial cybersecurity. The survey included up to 363 input items and received inputs from 170 qualified respondents. The survey questions, responses, analysis, and decisions are available for public review, examination, and additional analysis on the ISAGCA website. While this is an impressive level of transparency for a curricular guidance effort, the most exciting part is the guidance itself.

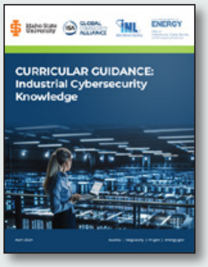
The 125-page document is an essential reference for students, instructors, administrators, and industrial cybersecurity practitioners. It is organized around the analogy of a building with three components represented in Figure 2: an environment, a foundation and a superstructure.

The Industrial Operations Environment describes the contexts (business, geopolitical, professional, and industry) within which industrial control systems and industrial cybersecurity exist. The Industrial Control Systems Foundation describes the elements (instrumentation and control, process equipment, industrial networking and communication, and process safety and reliability) that compose an industrial control system. The Industrial Cybersecurity Superstructure describes the elements (guidance and regulation, common weaknesses, events and

Resources

The International Society of Automation Global Cybersecurity Alliance (ISA GCA) supports the author's research and provides these related resources:

Whitepaper: "Curricular Guidance: Industrial Cybersecurity Knowledge,"


CURRICULAR GUIDANCE: Industrial Cybersecurity Knowledge

Webinar: "Curricular guidance to develop a new generation of industrial cybersecurity professionals"

PowerPoint Presentation

The **ISAGCA website** contains survey questions, responses, analysis, and more.

incidents, and defensive techniques) that most immediately and intuitively pertain to assuring an industrial control system.

Each component is organized into categories, topics, and subtopics to reach a level of reasonable granularity—up to six levels deep. While some topic names are identical to those found in traditional cybersecurity contexts, the study describes the unique or special considerations of those topics for industrial and OT environments.

OT security leaders attempting to achieve Stage 5 can now work with education and training providers that rely on a consensus-based OT security body of knowledge.

ABOUT THE AUTHOR

Dr. Sean McBride is director of the Informatics Research Institute at Idaho State University's College of Technology where he works to infuse engineering professionals with critical cybersecurity skills. Before joining ISU, McBride pioneered the multidisciplinary field of threat and vulnerability intelligence for industrial environments. At Idaho National Laboratory (INL) he instituted and led the vulnerability analysis and situational awareness reporting elements foundational to the DHS ICS-CERT. In 2009 he cofounded Critical Intelligence (acquired by iSIGHT Partners in 2015) to help organizations that own and operate electric generating stations, oil refineries, and water treatment plants understand threats to the industrial processes they operate.

OT Cybersecurity Is a Team Effort

Globally relevant standards and conformance programs are important, as is support for automation professionals.

By Kara Phelps

Cybersecurity was once considered an information technology (IT) challenge—cybercriminals primarily targeted software, networks and computer systems. Operational technology (OT) and IT were "air-gapped" to minimize disruptions in the event of a breach.

In recent years, however, the long-hyped convergence of OT and IT has become a commonplace reality. Industry 4.0 introduced smart technology to the world of OT, complete with better data insights, better connectivity and increased efficiencies. A connected industrial environment has undeniable benefits, but it also comes with a downside—an increased vulnerability to cyberattacks. Mitigating risk and thwarting attacks also requires a coordinated effort.

Cyber threat actors can easily put safety and continuity at risk when they attack OT. Incidents like the Colonial Pipeline ransomware attack in 2021 and the Dole ransomware attack in 2023 demonstrated the potential for cyber threats to have a severe, real-world impact. In 2024, a rising wave of cyberattacks such as those orchestrated by Volt Typhoon have targeted critical infrastructure in North America and Europe. Organizations are facing high stakes when it comes to protecting their industrial automation and control systems (IACS). According to a report by ABI Research, global enterprise spending on OT cybersecurity is expected to increase to about 21.6 billion USD by 2028.

> **“Specific standards that take account of the unique characteristics** of industrial automation and control systems should be used in preference to more general information technology standards.”

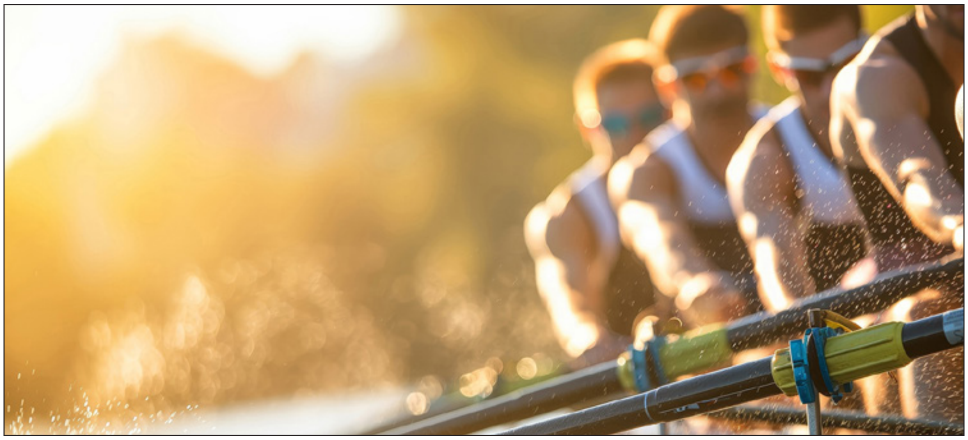
In a position paper called “Advancing Industrial Cybersecurity,” the International Society of Automation (ISA) outlines how policymakers and private-sector leaders can be best equipped to address the urgent need for improved critical infrastructure cybersecurity. Globally relevant standards and conformance programs are important, as is strong support for the automation professionals who work to ensure the safety of facilities, processes and communities.

The position paper explores the critical need for OT cybersecurity training and various directives issued by governments around the world to address the challenges of protecting critical infrastructure from cyberattacks. It discusses ISA’s commitment to developing and maintaining standards such as the ISA/IEC 62443 series, the world’s leading consensus-based standards for control systems cybersecurity. ISA provides training resources surrounding those standards, promotes the adoption of standards and works with governments around the world to adopt standards and guidance for protecting critical infrastructure.

The paper states ISA's position on advancing industrial cybersecurity, namely that: "Mandating cybersecurity measures with prescriptive regulations is undesirable. Instead, regulations should support the use of risk-based approaches based on published consensus-based technical standards and conformance measures."

It also highlights another ISA position, emphasizing the need for an OT-specific approach: "Specific standards that take account of the unique characteristics of industrial automation and control systems should be used in preference to more general information technology standards."

ISA created the ISA Global Cybersecurity Alliance (ISAGCA) to advance cybersecurity readiness and awareness in manufacturing and critical infrastructure facilities and processes. End-user companies, automation and control systems providers, IT infrastructure providers, services providers, system integrators and other cybersecurity stakeholder organizations work together through ISAGCA to proactively address growing threats. ISA also offers the leading conformity assessment program for industrial cybersecurity products and systems—ISASecure® — which certifies compliance with the ISA/IEC 62443 series of standards.



IIoT system protection

ISAGCA and ISASecure partnered to produce a white paper, "IIoT System Implementation and Certification Based on ISA/IEC 62443 Standards." This report explores the use of ISA/IEC 62443 in IACS with cloud-based functionality, also referred to as the Industrial Internet of Things (IIoT). It determines that the concepts in ISA/IEC 62443 such as risk assessment, zone and conduit partitioning and the system/component model can be applied to an IIoT IACS.

The paper's findings validate the endurance of ISA/IEC 62443 as OT continues to evolve. So does another ISASecure paper, "The Case for ISA/IEC 62443 Security Level 2 as a Minimum for COTS Components." The SL2 criteria outlined in ISA/IEC 62443 help strengthen the cybersecurity capabilities of commercial off-the-shelf (COTS) components to protect against the increasing number of intentional attacks targeting IACS.

Recent news and trends have proven that, with so much on the line, organizations must openly share information concerning new threat scenarios and adopt globally relevant standards. Awareness and media mentions of the ISA/IEC 62443 standards are growing at a rate faster than ever before. More organizations are adopting ISA/IEC 62443 requirements as they seek well-vetted, consensus-based strategies for protecting their systems, and governments are including these standards in public policies. Subject-matter experts in OT cybersecurity are also familiarizing themselves with a wide variety of use cases for ISA/IEC 62443. In 2024, OT cybersecurity is truly a team effort.

ABOUT THE AUTHOR

Kara Phelps is the communications and public relations manager for the International Society of Automation as well as ISA consortia including the ISA Global Cybersecurity Alliance (ISAGCA) and ISASecure.