WHITEPAPER

An Industry Imperative: Build a Standards-Based Cybersecurity Culture for Employees, Customers, and Partners

Key Findings Inside:

- The World Economic Forum rates a large-scale breach of cybersecurity as one of the five most serious risks facing the world today—and only 23% of companies are following minimum security guidance
- The industrial control systems cybersecurity challenge spans across processes, people, and technology
- ISA/IEC 62443 standards provide guidance for how to protect and secure processes, but people will ultimately implement and monitor these practices; automation suppliers and end users must find creative ways to train and certify their employees and contractors
- ISA's suite of cybersecurity training and certificate programs is one solution, leveraged successfully by dozens of companies and hundreds of individual experts

International Society of Automation
Setting the Standard for Automation™

Introduction

The Three-Pronged Cybersecurity Challenge: Processes, People, and Technology

The World Economic Forum now rates a large-scale breach of cybersecurity as one of the five most serious risks facing the world today. The scale of the threat is expanding drastically: by 2021, the global cost of cybersecurity breaches will reach US$6 trillion by some estimates, double the total for 2015[1]. In today's connected world, made possible through the Internet of Things (IoT), every asset owned or used by an organization is a potential vulnerability point. Devices belonging to employees, customers, and vendors often access an organization's systems, adding even more complexity to the security environment.

Recent studies have also concluded that threats and vulnerabilities continue to increase[2]:

- 47% of industrial computers were attacked in 2018—and 38,500 malware modifications were found
- 342 of 415 known vulnerabilities in ICS computers were accessible and easily penetrated remotely and without any expertise
- Only 23% of companies follow minimum security guidance

Consequences of cybersecurity incidents include physical and environmental damage for employees and communities; production loss; damage to assets and facilities; hazardous material leaks, loss, or theft; product contamination; and regulatory, legal, and civil liabilities.

The industrial control systems cybersecurity challenge spans across processes, people, and technology:

- A company's processes and communications must be secure
- Operations staff must have expertise in industrial control systems cybersecurity
- The plant's technology must be inherently secure, addressing known vulnerabilities using a standards-based approach

Processes: Leveraging Industry Standards to Secure Processes and Communication Protocols

Industries have long relied on global standards to solve technical problems and bring consistency to process and product design. Leveraging standards increases productivity, lowers costs, and keeps people and facilities safe.

The ISA/IEC 62443 series of standards is the world's only consensus-based industrial cybersecurity standard. This series defines requirements and procedures for 1) implementing electronically secure automation and control systems and security practices and 2) assessing electronic security performance. It approaches the cybersecurity challenge in a holistic way, bridging the gap between operations and information technology as well as the one between safety and cybersecurity. Given the interconnected nature of complex computer and control networks, where vulnerabilities in one sector can be exploited in other sectors, it's critical that standards apply across key industries and infrastructures.

Applying the ISA/IEC 62443 series of standards to manufacturing processes is the first step toward building a more secure future. Many major technology suppliers recognize ISA/IEC 62443 as a foundational standard to drive device hardening and have added security features to their products to be compliant with ISA/IEC 62443 standards.

Information Technology and Operations Technology: Moving from Isolation to Convergence to Integration

Information Technology (IT) is defined as hardware, software, and communications technologies that focus on the storage, recovery, transmission, manipulation, and protection of data. Operations Technology (OT) is defined as hardware and software that detects or causes a change through the direct monitoring and control of physical devices, processes, and events.

IT systems are historically used to manage complex data and information flow, but today's OT environments are leveraging them to manage complex physical processes. As a result, industries are safer, more efficient, and more reliable than ever before—but these technologies bring more security risks to facilities and operations.

Attempts to disrupt operations, steal intellectual property, and affect the quality or safety of production are steadily increasing as more cyberattacks target critical infrastructure and industrial assets. Threat actors are using IT techniques to access OT systems, and they're using OT systems that are poorly defended to get access to corporate IT networks. In many ways, cyber criminals are taking advantage of the disconnects and, in some cases, the distrust between OT and IT teams.

Today's interconnected world means that IT and OT can no longer consider security separately. This new dynamic has resulted in unfamiliar challenges for both areas, but a systematic and purposeful commitment to integration will ultimately reduce risks.

People: Developing Operational Expertise in Industrial Control Systems Cybersecurity

Industry standards assume that engineering, operations, and maintenance professionals have the knowledge and skills to define, implement, and monitor technology, business processes, and associated controls outlined in the documentation. The standards provide the guidance for how to protect processes, but the people will ultimately implement and monitor them.

According to a recent EY (formerly Ernst & Young) report, "the C-suite can no longer assume that cybersecurity is solely the responsibility of the information security or information technology departments… organizations need an integrated cybersecurity vision—one that brings together the various functions and dependencies with other parts of the organization, external key stakeholders, and third-party suppliers."

This unified vision is the foundation for a comprehensive approach to the industrial cybersecurity challenge. The report referenced above found that many attacks were successful due to two factors: 1) known vulnerabilities that hadn't been mitigated, or 2) careless, unaware employees making mistakes that increased the likelihood or severity of an attack. These two potential threat sources are entirely within companies' control.

Like quality and safety management, cybersecurity management demands continuous improvement to manage risks. Companies must continuously and purposefully identify, categorize, and mitigate cybersecurity risks. While different roles will have different requirements for expertise, all roles must contribute to a proactive and effective cybersecurity culture:

- Automation providers everywhere in the world will be expected to possess an awareness of cybersecurity topics at many levels
- Detailed knowledge of the implementation of secure systems will be required by key personnel within asset owner companies
- Everyone in a facility, regardless of job function, must have baseline understanding of cybersecurity threats and best practices

To address the personnel-focused challenges of cybersecurity, ISA has developed a series of courses and certificate programs based on the ISA/IEC 62443 standards, culminating in the Industrial Control Systems Cybersecurity Expert designation for professionals who can successfully complete the courses and exams.

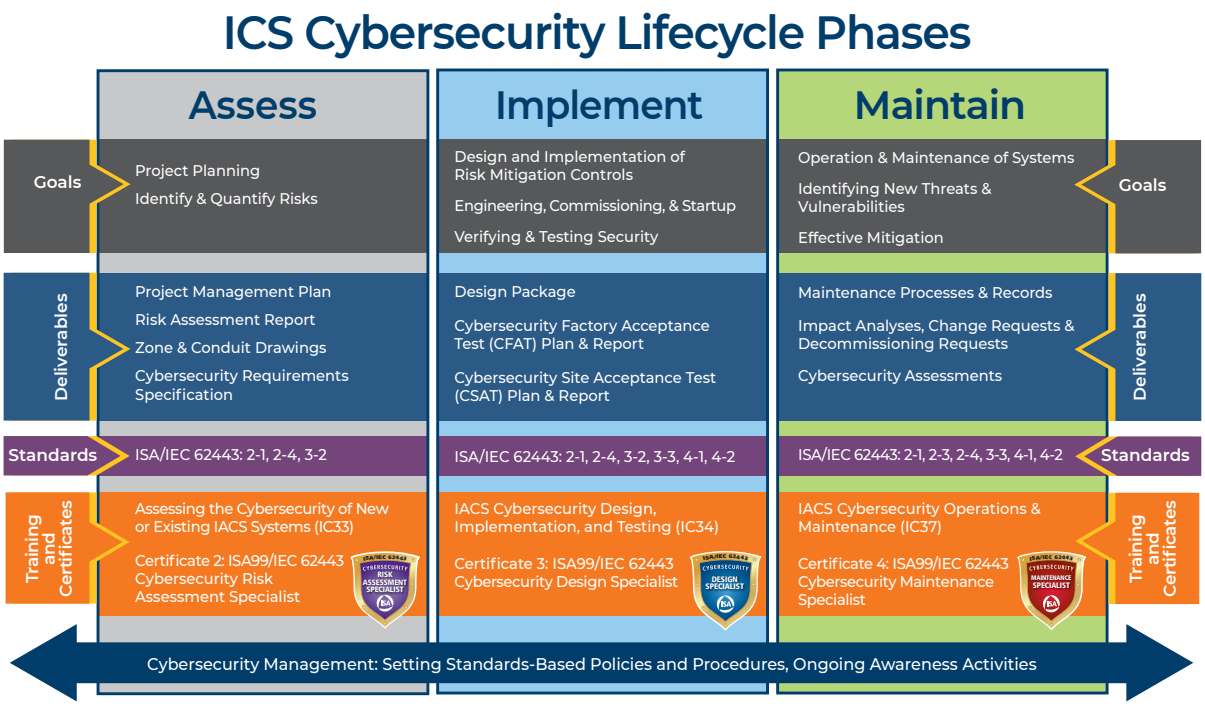
Companies face a unique set of challenges regarding the training and vetting of people:

- Employee expertise varies for automation providers who work in multiple industries and for asset owners who leverage several different production processes, making standardization of training difficult
- Companies often partner with contractors and systems integrators to service and maintain equipment and facilities, requiring universally applicable ways to validate knowledge and skills
- Employees and supply chain partners are located around the globe, so training and validation programs must be flexible and widely accessible

*Sources: [1]Cyber security regained: preparing to face cyber attacks; 20th Global Information Security Survey 2017–18; [2]Kaspersky Labs' The State of Industrial Cybersecurity 2018 and SANS' 2019 State of OT/ICS Cybersecurity Report

Overview of ISA's Industrial Cybersecurity Courses

ISA's proven expertise in IACS cybersecurity standards and compliance is the basis for a comprehensive series of ISA cybersecurity training courses (classroom and online) that address the complete lifecycle of cybersecurity knowledge requirements.



To earn each certificate, individuals must take the required course and pass an exam.

ISA Certificate 1: ISA99/IEC 62443 Cybersecurity Fundamentals Specialist

Required Course: *Using the ISA/IEC 62443 Standard to Secure Your Control Systems* (IC32E)

The move to using open standards such as Ethernet, TCP/ IP, and web technologies in supervisory control and data acquisition (SCADA) and process control networks has begun to expose these systems to the same cyberattacks that have wreaked so much havoc on corporate information systems. This course provides a detailed look at how the ANSI/ISA 99 standards can be used to protect your critical control systems. It also explores the procedural and technical differences between the security for traditional IT environments and those solutions appropriate for SCADA or plant floor environments.

ISA Certificate 2: ISA99/IEC 62443 Cybersecurity Risk Assessment Specialist

Required Course: *Assessing the Cybersecurity of New or Existing IACS Systems* (IC33)

The first phase in the IACS Cybersecurity Lifecycle (defined in ISA 62443-1-1) is to identify and document IACS assets and perform a cybersecurity vulnerability and risk assessment to identify and understand the high-risk vulnerabilities that require mitigation. Per ISA 62443-2-1, these assessments need to be performed on both new (i.e., greenfield) and existing (i.e., brownfield) applications. Part of the assessment process involves developing a zone and conduit model of the system, identifying security level targets, and documenting the cybersecurity requirements into a cybersecurity requirements specification (CRS). This course provides students with the information and skills to assess the cybersecurity of a new or existing IACS and to develop a cybersecurity requirements specification that can be used to document the cybersecurity requirements the project.

ISA Certificate 3: ISA99/IEC 62443 Cybersecurity Design Specialist

Required Course: *IACS Cybersecurity Design & Implementation* (IC34)

The second phase in the IACS Cybersecurity Lifecycle (defined in ISA 62443-1-1) focuses on the activities associated with the design and implementation of IACS cybersecurity countermeasures. This involves the selection of appropriate countermeasures based upon their security level capability and the nature of the threats and vulnerabilities identified in the Assess phase. This phase also includes cybersecurity acceptance testing of the integrated solution, to validate countermeasures are properly implemented and that the IACS has achieved the target security level. This course will provide students with the information and skills to select and implement cybersecurity countermeasures for a new or existing IACS to achieve the target security level assigned to each IACS zone or conduit. Additionally, students will learn how to develop and execute test plans to verify that the cybersecurity of an IACS solution has properly satisfied the objectives in the cybersecurity requirements specification.

ISA Certificate 4: ISA99/IEC 62443 Cybersecurity Maintenance Specialist

Required Course: *IACS Cybersecurity Operations & Maintenance* (IC37)

The third phase in the IACS Cybersecurity Lifecycle (defined in ISA 62443-1-1) focuses on the activities associated with the ongoing operations and maintenance of IACS cybersecurity. This involves network diagnostics and troubleshooting, security monitoring and incident response, and maintenance of cybersecurity countermeasures implemented in the Design & Implementation phase. This phase also includes security management of change, backup and recovery procedures and periodic cybersecurity audits. This course will provide students with the information and skills to detect and troubleshoot potential cybersecurity events as well as the skills to maintain the security level of an operating system throughout its lifecycle despite the challenges of an ever-changing threat environment.

Individuals who successfully earn all 4 certificates will be honored with ISA Certificate 5: ISA99/IEC 62443 Cybersecurity Expert.

A standard version of each course is available to the public through open enrollment. Companies can work with ISA to make custom modifications, bring these courses to their plants, or offer them through online learning management systems.

Technology: Securing the Industrial Control Systems Supply Chain Through Conformity Assessment Programs

A secure control system requires that each system, protocol, and media be secure—but many devices and legacy control systems are still insecure by design. In response to this challenge, ISA created the ISASecure® ISA/IEC 62443 Conformity Assessment Program for commercial-off-the-shelf industrial control system products. The certification program evaluates the product development practices of the supplier, along with detailed product security characteristics, with the objective of securing the ICS supply chain. The ISASecure® certification program is an ISO/IEC 17065 conformity assessment scheme that ensures control system conformance to relevant ISA/IEC 62443 cybersecurity standards. It is applied using the security lifecycle concept that forms the basis of the standards.

Asset owners and integrators who include the ISASecure® designation as a procurement requirement for control systems projects have confidence that the selected products are robust against network attacks and free from known vulnerabilities.

CONCLUSION

Applying Best Practices: End Users and Automation Suppliers Can Customize ISA's Offerings to Meet Their Unique Needs

It is critical that every organization engaged in industrial automation evaluates its current and future cybersecurity strategy—not just to scan for vulnerabilities and technology advances, but to evaluate its cybersecurity culture through the lens of its processes, its people, and its technology.

For end users and automation suppliers working to secure processes, ISA offers:

- The ISA/IEC 62443 series of standards—the world's only consensus-based industrial cybersecurity standards

For end users and automation suppliers who want to develop and validate the knowledge and skills of the people working in their plants and with their customers, ISA offers:

- A series of training courses and certificate programs based on the ISA/IEC 62443 standards, culminating in the Industrial Control Systems Cybersecurity Expert designation for professionals who can successfully complete the courses and exams; courses and exams can be delivered in classrooms, online, or in plants around the world

For automation suppliers who want to create products that are secure by design and that prove their compliance to industry standards, ISA offers:

- The ISASecure® ISA/IEC 62443 conformity assessment program for commercial-off-the-shelf (COTS) IACS products and systems

For end users who need to validate that the products they're purchasing are inherently secure, and the vendors they're entrusting to build their systems are using secure practices, ISA offers:

- The opportunity to participate in the requirements-setting process and the ability to specify ISASecure® conformity within procurement processes—the ISASecure® certifications evaluate supplier product development practices and product security characteristics with the objective of securing the IACS supply chain

Learn more about ISA's suite of cybersecurity offerings. Call us today at +1 919 849 5411.