Setting the Standard for Automation™

Safe and Secure: Multiple Challenges, One Solution

ISA has the resources your workforce needs to protect industrial automation and control systems

Standards-based
Industry-proven
Expert-developed

Industrial Cybersecurity Technical Resources

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Cybersecurity and safety are interrelated; a system cannot be safe if it is not secure.

As a global, unbiased developer of technical resources focused on process safety and control systems cybersecurity, ISA brings a unique perspective and deep understanding of today's industrial challenges.

- "A cybersecurity-related compromise in the operation of industrial control systems can undermine the basic assumptions used in the design of safety systems and procedures for operations and maintenance. This distinguishes industrial cybersecurity deliberations from those used for IT cybersecurity programs, which focus on confidentiality and privacy."—ARC Advisory Group, July 2015
- ISA's workforce development resources are widely used in dozens of industries—ISA has 36,000 members and more than 350,000 customers in over 190 countries and 25 industries
- ISA's standards are developed by international experts from across industry, government, and academia
- The ISA/IEC 62443 standards define requirements and procedures for implementing electronically secure automation and control systems and security practices, and assessing electronic security performance; ISA also offers the ISA84 series of standards, focused on the application of Electrical/Electronic/Programmable Electronic Systems (E/E/PES) in process safety
- The cybersecurity standards, and the resulting training, certification, and certificate programs, cover the complete lifecycle of cybersecurity protection
- ISA takes a holistic approach, bridging the gap between process safety and cybersecurity and approaching challenges from an operations technology perspective rather than an IT perspective

ISA is the developer and applications-focused thought leader behind the world's only consensus-based industrial cybersecurity standard. ISA's approach to the cybersecurity challenge is holistic, bridging the gap between operations and information technology; and between process safety and cybersecurity.

ISA global collaborations lead cybersecurity initiatives

ISA is recognized and depended on worldwide to lead industry's response to control systems cybersecurity vulnerabilities.

- Upon request from the US federal government, ISA and its umbrella association, the Automation Federation, helped to prepare the US Cybersecurity Framework and helped to implement the provisions of the US Cybersecurity Enhancement Act of 2014
- Representatives from the White House, NIST, FBI, Automation Federation, and ISA conducted a series of workshops throughout the United States with executives across industry sectors
- ISA has forged strong partnerships with government and academic entities through these efforts, including the US Department of Homeland Security, US Department of Commerce/NIST, US Department of Energy, US Department of Labor, the National Association of Manufacturers, and the National Rural Water Association
- Also upon request, ISA's umbrella organization, the Automation Federation, is the host organization for the LOGIIC (Linking Oil and Gas Industry to Improve Cybersecurity) Program
  - — The LOGIIC program is an ongoing collaboration of supermajor oil and natural gas companies and the US Department of Homeland Security, Science and Technology Directorate
  - — LOGIIC undertakes collaborative research and development projects to improve the level of cybersecurity in critical systems of interest to the oil and natural gas sector
- In late 2013, the US Department of Labor granted a North Carolina consortium of colleges a $23 million grant under the Trade Adjustment Assistance Community College and Career Training (TAACCCT) grants program to develop curriculum, educational degrees, certifications, and career pathways for students in Mission Critical Operations
  - — ISA was contracted to develop a Certified Mission Critical Professional (CMCP) certification program, providing an objective, third-party assessment and confirmation of the knowledge, skills and abilities needed for workers in the Mission Critical Operations field
  - — The CMCP certification is currently under development and will be launched in October 2016

> People ask me all the time...
> 'What keeps you up at night?'
> And I say...
>
> 'Spicy food,
> weapons of mass destruction,
> and cyber attacks.'
>
> **—Dutch Ruppersberger**
> US Representative
> Maryland's 2nd Congressional District

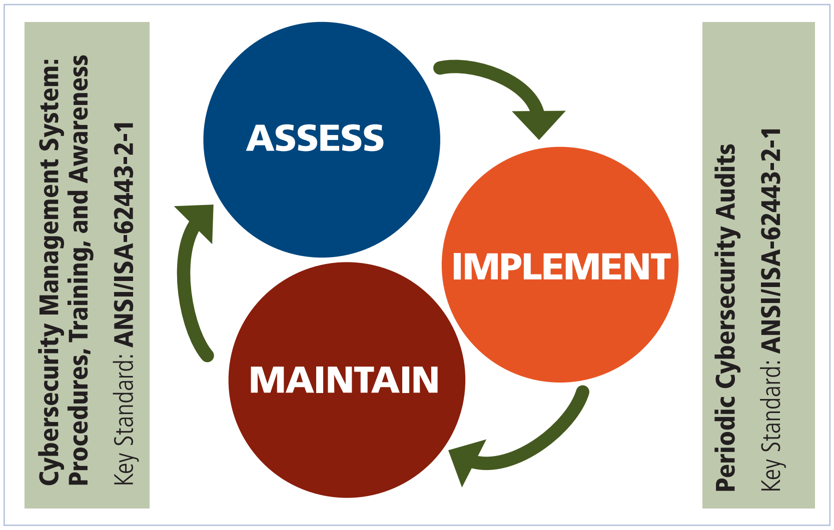
The IACS Security Lifecycle: An Overview

ISA understands the Industrial Automation and Control Systems Security Lifecycle, and builds its resources around real-world requirements for protecting your systems.

ASSESS

Key Standard: ANSI/ISA-62443-3-2

- High-Level Cyber Risk Assessment
- Allocation of IACS Assets to Security Zones or Conduits
- Detailed Cyber Risk Assessment


Cybersecurity Management System: Procedures, Training, and Awareness
Key Standard: ANSI/ISA-62443-2-1
ASSESS
IMPLEMENT
MAINTAIN
Periodic Cybersecurity Audits
Key Standard: ANSI/ISA-62443-2-1

IMPLEMENT

Key Standards: ANSI/ISA-62443-3-2 and ANSI/ISA-62443-3-3

- Cybersecurity Requirements Specification
- Design and Engineering of Cybersecurity Countermeasures
- Design and Development of Other Means of Risk Reduction
- Installation, Commissioning, and Validation of Cybersecurity Countermeasures

MAINTAIN

Key Standard: ANSI/ISA-62443-2-1 (last published as ISA-99.02.01-2009)

- Cybersecurity Maintenance, Monitoring, and Management of Change
- Cyber Incident Response and Recovery

ISA offers best-in-class training and certificate programs, backed by a rigorous, scientific, precise process led by renowned subject matter experts. Plus, ISA publishes books, technical papers, journal and magazine articles, and hosts events that focus on cybersecurity.

- ISA's training courses are vendor-neutral, developed and taught by industry experts, and offered online, in-plant, or in regional classroom locations. Choose from dozens of courses on the topics that matter most to executives, managers, engineers, and technicians—browse our full catalog by visiting **www.isa.org/trainingcatalog**
- Choose from five ISA/IEC 62443 Cybersecurity Certificate Programs—Cybersecurity Fundamentals Specialist, Cybersecurity Risk Assessment Specialist, Cybersecurity Design Specialist, Cybersecurity Maintenance Specialist, and Cybersecurity Expert; ISA also offers several safety-related certificate programs
- The ISA/IEC 62443 Cybersecurity Certificate Programs validate understanding of industrial control system cybersecurity standards, which give requirements for security assessment, design, implementation, operations, and management of devices and processes
- ISA's process for creating certificate programs is focused on industry-recognized standards and best practices; subject matter experts work with a psychometrician to shape the material included in the examinations and establish a cut score
- Hundreds of companies utilize ISA's workforce development, training, certification, and certificate programs, including Air Products & Chemicals Inc., Alyeska Pipeline Service Co., Ashland Chemical, BASF Corp., BP, Bechtel Construction Company, Cargill, Chevron, Cytec Industries, Dow Chemicals, DuPont, Eli Lilly, Emerson Process Management, General Electric, Honeywell, Jacobs Engineering, MAVERICK Technologies, Merck, MillerCoors Brewing, Pfizer, Raytheon, Siemens-Westinghouse, Southern Company, Tesoro, Total Petrochemical, Tropicana Products Inc., Valero, Xcel Energy, and dozens of water/wastewater and power plant locations around the US

Industrial Cybersecurity Standards

Given the interconnectivity of today's advanced computer and control networks—where vulnerabilities exploited in one sector can impact and damage multiple sectors—it's essential that cybersecurity standards be broadly applicable across industries or sectors. The ISA/IEC 62443 – Industrial Automation and Control Systems Security series of standards is a multi-industry initiative applicable to all key industry sectors and critical infrastructure. Developed by a cross-section of international cybersecurity subject-matter experts from industry, government, and academia, the evolving standards represent a comprehensive approach to cybersecurity.

ANSI/ISA-62443-3-3-2013, *Security for Industrial Automation and Control Systems Part 3-3: System Security Requirements and Security Levels*

This standard provides detailed technical control system requirements associated with the foundational requirements described in ISA-62443-1-1, including defining the requirements for control system capability security levels. These requirements are used along with the defined zones and conduits for the system under consideration while developing the appropriate control system target.

www.isa.org/62443-3-3

ANSI/ISA-62443-2-1-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*

This standard, the second in a multipart series that addresses the issue of security for industrial automation and control systems, describes the elements contained in a cybersecurity management system for use in the industrial automation and control systems environment and provides guidance on how to meet the requirements described for each element.

www.isa.org/62443-2-1

ANSI/ISA-62443-1-1-2007, *Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models*

The first in a series of ISA standards that addresses the subject of security for industrial automation and control systems, this standard focuses on the electronic security of these systems. The standard includes basic concepts and models related to cybersecurity for industrial control systems.

www.isa.org/62443-1-1

About the ISA99 Standards Committee

The ISA99 standards development committee brings together industrial cybersecurity experts from across the globe to develop the ISA/IEC 62443 series of standards on industrial automation and control systems security, guided by the accredited processes of the American National Standards Institute. The committee addresses industrial automation and control systems whose compromise could result in endangerment of the public or a company's employees, violation of regulatory requirements, loss of proprietary or confidential information, economic loss, or adverse impacts on national security.

"The ISA/IEC 62443 series of standards and technical reports is rooted in a set of principles and concepts for industrial systems security that have been vetted over a period of several years. It is important to remain consistent with these principles while responding to a rapidly changing threat environment. This is how we achieve standards that can stand the test of time."

Eric Cosman, ISA99 Co-Chairman

Individual Access to ISA Standards

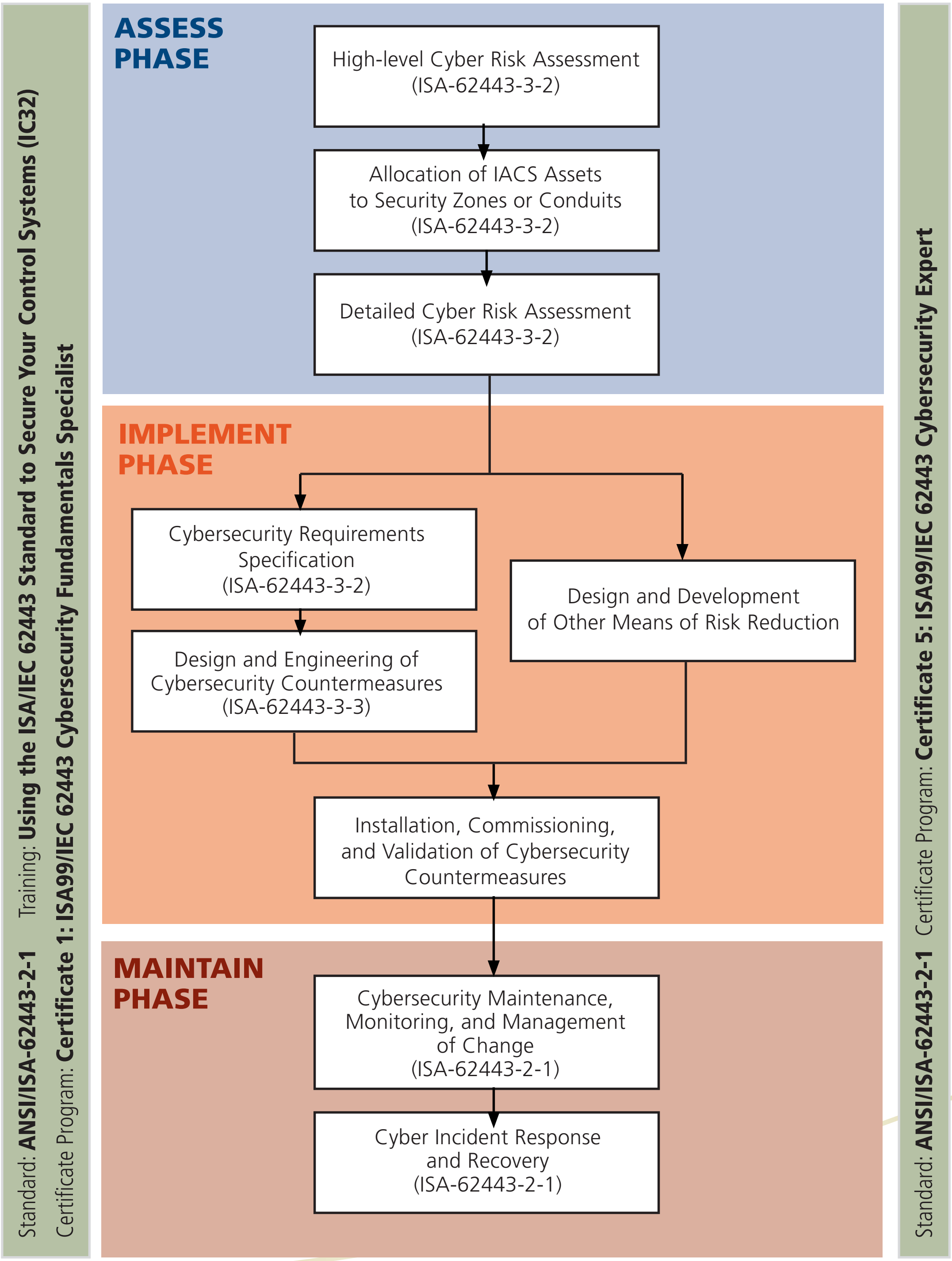
- Browse more than 400 different standards and technical reports online—**www.isa.org/findstandards**
- Join ISA and view all of ISA's standards at no cost—www.isa.org/join

Company-wide Access to ISA Standards

- Get multi-user licenses, purchase multiple copies of standards, and more—**https://www.ihs.com/products/isa-standards.html**
- Talk to an expert to assess your company's needs and options to subscribe to standards on multiple topics—call +1 844 301-7334

Industrial Cybersecurity Workforce Development and Training Resources

Securing your industrial control systems is only possible if your employees are knowledgeable and skilled in the latest cybersecurity technologies and trends. Day in and day out, you depend on your team to keep your systems and processes safe and secure. Have you given them the tools they need?



Standard: **ANSI/ISA-62443-2-1** Training: **Using the ISA/IEC 62443 Standard to Secure Your Control Systems (IC32)**

Certificate Program: **Certificate 1: ISA99/IEC 62443 Cybersecurity Fundamentals Specialist**

ASSESS PHASE

High-level Cyber Risk Assessment (ISA-62443-3-2)

Allocation of IACS Assets to Security Zones or Conduits (ISA-62443-3-2)

Detailed Cyber Risk Assessment (ISA-62443-3-2)

IMPLEMENT PHASE

Cybersecurity Requirements Specification (ISA-62443-3-2)

Design and Engineering of Cybersecurity Countermeasures (ISA-62443-3-3)

Design and Development of Other Means of Risk Reduction

Installation, Commissioning, and Validation of Cybersecurity Countermeasures

MAINTAIN PHASE

Cybersecurity Maintenance, Monitoring, and Management of Change (ISA-62443-2-1)

Cyber Incident Response and Recovery (ISA-62443-2-1)

Standard: **ANSI/ISA-62443-2-1** Certificate Program: **Certificate 5: ISA99/IEC 62443 Cybersecurity Expert**

ASSESS PHASE

Standard:
ANSI/ISA-62443-3-2

Training:
Assessing the Cybersecurity of New or Existing IACS Systems (IC33)

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

IMPLEMENT PHASE

Standards:
ANSI/ISA-62443-3-2 and ANSI/ISA-62443-3-3

Training:
IACS Cybersecurity Design, Implementation, & Testing (IC34)

Certificate Program:
Certificate 3: ISA99/IEC 62443 Cybersecurity Design Specialist

MAINTAIN PHASE

Standard:
ANSI/ISA-62443-2-1

Training:
IACS Cybersecurity Operations & Maintenance (IC37)

Certificate Program:
Certificate 4: ISA99/IEC 62443 Cybersecurity Maintenance Specialist

Classroom Training

Classroom and In-Plant Training

ISA's classroom training courses are offered in regional locations around the US and via ISA's onsite training program, which brings courses and instructors directly to your facility. Hands-on labs and learning opportunities make ISA's instructor-led training one of the best ways to simulate the real-world environment in the classroom.

Introduction to Industrial Automation Security and the ISA/IEC 62443 Standards (IC32C)

Understanding how to secure factory automation, process control, and supervisory control, and data acquisition (SCADA) networks is critical if you want to protect them from viruses, hackers, spies, and saboteurs. This one-day course teaches the basics of the ISA/IEC 62443 standards and how these can be applied in the typical factory or plant.

For upcoming course dates/locations, registration, and CEU information: **www.isa.org/CYBE/IC32C**

Using the ISA/IEC 62443 Standards to Secure Your Control System (IC32)

certificate program

The move to using open standards such as Ethernet, TCP/IP, and web technologies in SCADA and process control networks has begun to expose these systems to the same cyber-attacks that have wreaked so much havoc on corporate information systems. This two-day course provides a detailed look at how the ISA/IEC 62443 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.

For upcoming course dates/locations, registration, and CEU information: **www.isa.org/CYBE/IC32**

Industrial Networking and Security (TS12)

This five-day course studies the latest developments in networking, including practical tips on designing, implementing, and testing TCP/IP-based networks and how to apply them securely and reliably in an industrial environment. Students will discuss the functions and purposes of the elements used to create and protect an industrial network, including switches, routers, firewalls, and intrusion detection/prevention systems. This course expands practical knowledge of LAN, WAN, and Web technologies, and illustrates what is safe and practical for today's plant floor, including Internet technologies such as web servers, TCP/IP, and fiber optics. Special focus will be placed on the questions of security in the industrial setting drawing on the work of the ISA99 standards committee and the National Institute of Standards and Technology (NIST).

For upcoming course dates/locations, registration, and CEU information: **www.isa.org/CYBE/TS12**

"Companies around the world are concerned about workforce development, and that starts with upgrading the skill levels of your current employees. Employers are realizing that the continued improvement of each member of their staff is a crucial part of their overall success."

Nick Sands, CAP, P.E.
Manufacturing Technology Fellow,
DuPont Protection Technologies,
Past ISA VP of Professional Development

certificate program These courses are part of the ISA/IEC 62443 cybersecurity certificate program

Advanced Industrial Networking and Cybersecurity (TS20)

In this course you will learn about the latest developments in Industrial Control System (ICS) networking and cybersecurity. The course provides a review of basic networking and cybersecurity technology and expands your understanding of industrial network concepts by reviewing basic networking principals including TCP/UDP, IPv4/IPv6, ICS protocols, addressing, and troubleshooting. You will explore network security architectures and learn how to use layering and segmentation to improve security, as well as how web technology works and how web server capability is used in industry and the security problems engendered by such use. Practical application use of cybersecurity technologies such as firewalls, vpn, virtualization, virus scanning, and intrusion detection tools will be covered, including how to industrially harden and secure your networks and perform "red team" testing of your systems using penetration testing software. Special focus is placed on the assessment of security risks and hazards in the industrial setting using ISA/IEC 62443, NIST, and ICS cybersecurity frameworks and standards. Laboratory exercises performed in class are designed to re-enforce learning objectives and allow for active participation using a classroom network setup leveraging virtual environments.

For upcoming course dates/locations, registration, and CEU information: **www.isa.org/CYBE/TS20**

Assessing the Cybersecurity of New or Existing IACS Systems (IC33)

The first phase in the IACS Cybersecurity Lifecycle (defined in ANSI/ISA-62443-1-1) is to identify and document IACS assets and perform a cybersecurity vulnerability and risk assessment in order to identify and understand the high-risk vulnerabilities that require mitigation. Per ANSI/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 will provide 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.

For upcoming course dates/locations, registration, and CEU information: **www.isa.org/CYBE/IC33**

IACS Cybersecurity Design & Implementation (IC34)

The second phase in the IACS Cybersecurity Lifecycle (defined in ANSI/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, in order 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 in order 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.

For upcoming course dates/locations, registration, and CEU information: **www.isa.org/CYBE/IC34**

IACS Cybersecurity Operations & Maintenance (IC37)

The third phase in the IACS Cybersecurity Lifecycle (defined in ANSI/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.

For upcoming course dates/locations, registration, and CEU information: **www.isa.org/CYBE/IC37**

certificate *program* These courses are part of the ISA/IEC 62443 cybersecurity certificate program

Online Learning

ISA's online courses utilize web training modules, text materials, online evaluations, and email discussions. Students will have email access to one of ISA's world-class instructors, and have an opportunity to participate in live Q&A sessions with the instructor and other class participants.

Online Training

certificate program

Cybersecurity for Automation, Control, and SCADA Systems (IC32E)

The move to using open standards such as Ethernet, TCP/IP, and web technologies in SCADA and process control networks has begun to expose these systems to the same cyber-attacks that have wreaked so much havoc on corporate information systems. This course provides a detailed look at how the ISA/IEC 62443 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.

For upcoming course dates, registration, and CEU information: **www.isa.org/CYBE/IC32E**

Live Webinars

ISA's live webinars are interactive presentations led by industry leaders, focused on emerging issues and trends. Live webinars can be viewed by an unlimited number of participants at your location for one low fee. Plus, save up to 25% when you register for all three webinars in this series at one time! To take advantage of the series pricing, call ISA Customer Service at +1 919-549-8411 to register, as this offer is not available online.

Cybersecurity Risk Assessment for Automation Systems (IC32CW1)

Risk analysis is an important step in creating a cybersecurity plan for your automation system. Risk analysis not only identifies security vulnerabilities, but also provides the business case for the countermeasures that reduce risk. This webinar introduces control engineers to the concepts of risk analysis and how they are applied to industrial manufacturing and control systems based on the ISA/IEC 62443 standards. This webinar is also valuable for IT professionals who wish to learn the special considerations for performing risk analysis on automation systems.

www.isa.org/CYBE/IC32CW1

Firewalls and Security Zones on the Plant Floor (IC32CW2)

The network firewall is one of the most important tools in any cybersecurity designer's tool box. This webinar introduces you to the world of firewall system design, focusing on how these devices can be effectively deployed on the typical plant floor.

www.isa.org/CYBE/IC32CW2

A Tour of the ISA/IEC 62443 Security Standards (IC32CW3)

This webinar introduces the ANSI/ISA 62443 Security for Industrial Automation and Control Systems standards and explains how the standards are organized. Students will learn the terminology, concepts, and models of ISA/IEC 62443 cybersecurity and the elements of creating a cybersecurity management system.

www.isa.org/CYBE/IC32CW3

certificate program These courses are part of the ISA/IEC 62443 cybersecurity certificate program.

Certificate Programs for Individuals

certificate
program

As part of ISA's continued efforts to meet the growing need of industrial control systems professionals and to expand its global leader outreach into the security realm, ISA has developed a comprehensive, knowledge-based certificate recognition program designed to increase awareness of the ISA/IEC 62443 standards and the critical areas as they relate to the IACS lifecycle. The certificate programs are designed for professionals involved in IT and control system security roles who need to develop a command of industrial cybersecurity terminology, awareness, and understanding of the material embedded in the ISA99 standards, in order to assess, design, implement, and maintain a solid cybersecurity program for their organizations and processes.

ISA/IEC 62443 cybersecurity certificates are awarded to those who successfully complete a designated training program and pass a comprehensive multiple choice proctored exam offered through the Prometric testing centers. Individuals may register to take the training course(s) only and receive continuing education units (CEUs) for completion of the training course(s), or they can register for the affiliated certificate program which includes a separate knowledge-based examination.

Recommended experience

There are no required prerequisites for these programs; however, it is highly recommended that applicants have:

- 3-5 years of experience in the IT cybersecurity field preferably in an industrial environment—and at least 2 years specifically in a process control engineering setting
- Some level of knowledge or exposure to the ISA/IEC 62443 standards

Program Requirements

ISA/IEC 62443 designations and certificates will be awarded to individuals who meet the following program requirements:

- **Certificate 1: ISA/IEC 62443 Cybersecurity Fundamentals Specialist**
  - Successful completion of two-day, classroom training course: Using the ISA/IEC 62443 Standards to Secure Your Control Systems (IC32) or its online equivalent (IC32E).
  - Earn a passing score on the separate, multiple-choice electronic certificate exam.
- **Certificate 2: ISA/IEC 62443 Cybersecurity Risk Assessment Specialist**
  - Successful completion of three-day, classroom training course: Assessing the Cybersecurity of New or Existing IACS Systems (IC33).
  - Successful completion of Certificate 1 requirements.
  - Earn a passing score on the separate, mutiple-choice electronic certificate exam.
- **Certificate 3: ISA/IEC 62443 Cybersecurity Design Specialist**
  - Successful completion of three-day, classroom training course: IACS Cybersecurity Design & Implementation (IC34).
  - Successful completion of Certificate 1 requirements.
  - Earn a passing score on the separate, multiple-choice electronic certificate exam.
- **Certificate 4: ISA/IEC 62443 Cybersecurity Maintenance Specialist**
  - Successful completion of three-day, classroom training course: IACS Cybersecurity Operations & Maintenance (IC37).
  - Successful completion of Certificate 1 requirements.
  - Earn a passing score on the separate, multiple-choice electronic certificate exam.
- **ISA/IEC 62443 Cybersecurity Expert**
  - Individuals who achieve all Certificates (1 through 4) are designated as ISA99/IEC 62443 Cybersecurity Experts and receive confirmation and documentation relating to same.

Learn more about these certificate programs, eligibility criteria, renewal, and upcoming courses: **www.isa.org/ISA99Certificate.**

Industrial Cybersecurity Reference Publications

Industrial Automation and Control System Security Principles

Ronald L. Krutz, Ph.D., P.E.

The use of cyber warfare as a prelude or substitute for conventional attacks has gone from conjecture to reality. The obvious targets of such assaults are a nation's defense establishment, critical infrastructure, and production capabilities. Contrary to popular opinion, there are effective, structured defenses against such aggression, if they are conscientiously and properly implemented and maintained. This text merges the fundamentals of information system security and the unique requirements of industrial automation and control systems, and presents a clear and implementable formula to defend crucial elements, such as refineries, chemical plants, manufacturing operations, power plants, and pipelines. This work develops a novel protection approach based on merging the best relevant and proven government and industry standards, resulting in a practical instrument that can be straightforwardly applied to secure our valuable resources.

www.isa.org/CYBE/IndAutoCtrSec

Industrial Ethernet, Second Edition

Perry S. Marshall and John S. Rinaldi

This best-seller is a convenient installation, troubleshooting, and reference tool on one of the hottest topics in automation and process control. It will help you understand Ethernet and TCP/IP terminology, and it provides important information about industrial protocols and standards. You will quickly gain a solid grasp of Ethernet basics, the constraints of the industrial environment, and the specialized requirements of machine control. Practical reference charts and technical tips make this book an ideal quick reference source at your project meetings and on the job. Topics included in this book are installation, maintenance, troubleshooting, security tips, signaling types, Web services, Ethernet power and protocols, and wireless Ethernet.

www.isa.org/CYBE/IndEth

Industrial Network Security, Second Edition

David J. Teumim

Whether we talk about process control systems that run chemical plants and refineries, supervisory control and data acquisition (SCADA) systems for utilities, or factory automation systems for discrete manufacturing, the backbone of our nation's critical infrastructure consists of industrial networks and is dependent on their continued operation. This easy-to-read book introduces managers, engineers, technicians, and operators to principles for keeping our industrial networks secure amid rising threats from hackers, disgruntled employees, and even cyberterrorists.

www.isa.org/CYBE/IndNtwSec

Protecting Industrial Control Systems From Electronic Threats

Joseph Weiss

Aimed at both the novice and expert in IT security and industrial control systems (ICS), this book will help readers gain a better understanding of protecting ICSs from electronic threats. Cybersecurity is getting much more attention and "SCADA security" (Supervisory Control and Data Acquisition) is a particularly important part of this field, as are Distributed Control Systems (DCS), Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Intelligent Electronic Devices (IEDs), and all the other, field controllers, sensors, drives, and emission controls that make up the "intelligence" of modern industrial buildings and facilities.

www.isa.org/CYBE/ProIndCS

Inside *Industrial Automation and Control System Security Principles*

by Dr. Ronald Krutz

In Chapter 5 of his new book, *Industrial Automation and Control System Security Principles*, Ronald L. Krutz, Ph.D., P.E., examines risk management systems for industrial automation and control systems.

The chapter focuses on the methodologies for identifying and mitigating risks in automation and control systems, and providing the foundation for implementing essential security controls. Below is a sample question derived from the content covered in the chapter. Test your knowledge on this specific topic.

Which of the following is NOT characteristic of an insider threat?

a. Many insider attacks are conducted by disgruntled insiders
b. Most insider attacks do not result in serious losses or harm
c. Many insider attacks are conducted remotely
d. Many inside attackers have privileged access to computer systems

Find the answer to the question above and download (at no cost) Chapter 5 of Dr. Krutz's book at **www.isa.org/CYBE/IndAutoCtrlSec/Ch5**.

ISA Cybersecurity Tech Pack

To help you navigate your way through the potential cybersecurity threats facing you and your plant, the ISA Cybersecurity Tech Pack combines critical industry technical papers and PowerPoint presentations written and presented by world-renowned cybersecurity and automation systems experts, as well as notable ISA technical publications, including the popular *Industrial Network Security* by David Teumim and ISA's latest new title, *Industrial Automation and Control Systems Security Principles* by Ronald Krutz. As an added bonus, we have packaged our informative cybersecurity articles from *InTech* magazine to bring you this comprehensive cybersecurity technical resource package.

Capitalize on ISA's leadership in cybersecurity by ordering this compilation of valuable cybersecurity technical papers, publications, and *InTech* articles—containing the practical insights you can immediately apply in your position and within your workplace.

Technical Papers

- *Cybersecurity Implications of SIS Integration with Control Networks*
- *Establishing an Effective Plant Cybersecurity Program*
- *Stronger than Firewalls: Strong Cybersecurity Protects the Safety of Industrial Sites*
- *Applying ISA/IEC 62443 to Control Systems*
- *Improving Water and Wastewater SCADA Cybersecurity*
- *Practical Nuclear Cybersecurity*
- *LOGIIC Benchmarking Process Control Security Standards*
- *Integrated Perimeter and Critical Infrastructure Protection with Persistent Awareness*
- *Getting Data from a Control System to the Masses While Maintaining Cybersecurity—The Case for "Data Diodes"*
- *Reconciling Compliance and Operation with Real Cybersecurity in Nuclear Power Plants*
- *Wastewater Plant Process Protection—Process Hazard Analysis*
- *Water/Wastewater Plant Process Protection: A Different Approach to SCADA Cybersecurity*
- *Using Cybersecurity Evaluation Tool (CSET) for a Wastewater Treatment Plant*
- *An Overview of ISA-99 & Cybersecurity for the Water or Wastewater Specialist*
- *Cybersecurity Procurement Methodology for Digital Instrumentation and Control Systems*
- *Practical Nuclear Cybersecurity*
- *Cybersecurity Interoperability—The Lemnos Project*
- *Cybersecurity—Are We Progressing Rapidly Enough*
- *Cybersecurity in the Nuclear Power Industry*

Technical Publications

- *Industrial Automation and Control Systems Security Principles* by Ronald L. Krutz
- *Industrial Network Security, Second Edition* by David J. Teumim

InTech Magazine Articles

- *ISA fully engaged in cybersecurity*
- *Leveraging DoD wireless security standards for automation and control*
- *13 ways through a firewall: What you don't know can hurt you*
- *Defense in depth*
- *Executive Corner: What's on your mind?*
- *The Final Say: Securing industrial control systems*
- *Uninterruptible power supplies and cybersecurity*
- *Physical Security 101: Evolving 'defense in depth'*
- *Web Exclusive: Control network secure connectivity simplified*
- *The Final Say: Network security in the automation world*
- *Cybersecurity Enhancement Act*
- *Managing industrial control system cybersecurity*
- *Ramsey: The industrial sector: An environment uniquely vulnerable to cyberattacks*
- *Top ten differences between ICS and IT cybersecurity*
- *Standards Update: IACS cybersecurity*
- *Cybersecurity—Time for action*
- *The NIST cybersecurity framework*
- *ISA introduces cybersecurity certificate program*
- *Urgent need for automation systems cyberprotection*
- *Water and wastewater industry cyberattacks increasing*
- *Technology convergence presents evolving workforce development challenges in combating cyberthreats*

○ **Purchase ISA Cybersecurity Tech Pack at** www.isa.org/cybertechpack

○ **Join ISA at** www.isa.org/join **and download all of ISA's technical papers for FREE! Plus, earn a 20% discount on ISA's products!**

ISA/IEC 62443 Standards Conformance Certification

ISA/IEC 62443 Cybersecurity Conformance Certification for Products

The ISASecure® ISA/IEC 62443 conformity assessment program for commercial-off-the-shelf (COTS) IACS products and systems is the first step in securing your control systems. This certification evaluates supplier's product development practices and product security characteristics with the objective of securing the IACS supply chain.

The ISASecure certification program is an ISO/IEC 17065 conformity assessment scheme that ensures that COTS control systems conform to relevant ISA/IEC 62443 cybersecurity standards. ISASecure is applied using the security lifecycle concept that forms the basis of the ISA/IEC 62443 series of standards.

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

Visit the links below for a free PDF copy of the certification requirements.

A description of the certifications and the detailed conformance requirements are available on the **www.isasecure.org** website.

ISA/IEC 62443-3-3
System Security Assurance Certification (SSA)
This assessment certifies the COTS control system to the ISA/IEC 62443-3-3 standard.

- **Download now at www.isa.org/SSA**

ISA/IEC 62443-4-2
Embedded Device Security Assurance Certification (EDSA)
This assessment certifies that an embedded device (finite control element) meets the requirements of the ISA/IEC 62443-4-2 standard.

- **Download now at www.isa.org/EDSA**

ISA/IEC 62443-4-1
Security Development Lifecycle Assurance Certification (SDLA)
ISASecure SDLA certifies to ISA/IEC 62443-4-1 and assures that a product development organization properly considers cybersecurity in all phases of the supplier's product development lifecycle for industrial automation control systems.

- **Download now at www.isa.org/SDLA**

IEC 62443-3-3

Requirements for System Security Assurance (SSA) Certification

ISASecure Conformity Assessment Scheme for Industrial Automation and Control Systems to IEC 62443 International Cybersecurity Standards

Certified System ISASecure®

IEC 62443-3-3 • IEC 62443-4-2

t Policy Specification for nerability Identification Test (VIT)

Conformity Assessment Scheme for Industrial n and Control Systems to IEC 62443 International y Standards

ISASecure®

IEC 62443-4-1

Requirements for Security Development Lifecycle Assurance SDLA) Certification

Secure Conformity Assessment Scheme for Industrial omation and Control Systems to IEC 62443 International ersecurity Standards

ISASecure®

Learn more about ISASecure®
the ISA/IEC 62443 Standards Conformance Certification Program

ISASecure®
Phone: +1 919–990–9222

Additional Resources for Individuals and Companies

Join the ISA Safety and Security Division

As an ISA member, you'll have a chance to join two technical divisions for free—make one of them the ISA Safety and Security Division, your headquarters for the latest trends and information available regarding industrial cybersecurity and process safety. Division members get involved in programming ISA's conferences and symposia, publishing papers and articles, and discussing important topics on ISA's list serves and social media networks.

Visit **www.isa.org/Community/divatsafety**

Review the Work of the LOGIIC Program

The LOGIIC (Linking the Oil and Gas Industry to Improve Cybersecurity) program is an ongoing collaboration of oil and natural gas companies and the US Department of Homeland Security, Science and Technology Directorate. LOGIIC was formed to facilitate cooperative research, development, testing, and evaluation procedures to improve cybersecurity in petroleum industry digital control systems. The program undertakes collaborative research and development projects to improve the level of cybersecurity in critical systems of interest to the oil and natural gas sector. The program objective is to promote the interests of the sector while maintaining impartiality, the independence of the participants, and vendor neutrality. Review the work of this important working group of the Automation Federation by checking out the links below:

- Correlation Project
  Project 1 – Correlation Project
  ● **www.automationfederation.org/logiic1**
- Cybersecurity Implications of SIS Integrations with Control Networks, Paper
  Project 2 – Cybersecurity Implications of SIS Integrations with Control Networks, Paper
  ● **www.automationfederation.org/logiic2paper**
- Cybersecurity Implications of SIS Integration with Control Networks, Presentation
  Project 2 – Cybersecurity Implications of SIS Integration with Control Networks, Presentation
  ● **www.automationfederation.org/logiic2pres**
- Application Whitelisting, Presentation
  Project 3 – Application Whitelisting, Presentation
  ● **www.automationfederation.org/logiic3pres**
- Application Whitelisting, Public Report
  Project 3 – Application Whitelisting, Public Report
  ● **www.automationfederation.org/logiic3report**
- Wireless Project, Public Report
  Project 5 – Wireless
  ● **www.automationfederation.org/logiic5report**
- Virtualization Project, Public Report
  Project 8 – Virtualization
  ● **www.automationfederation.org/logiic8report**

Learn about Cybersecurity at ISA's World-Class Annual Events

ISA's technical conferences and division symposia give you a chance to network with peers and learn from the brightest minds in the industry. Many of ISA's conferences feature presentations and panel discussions focused on industrial cybersecurity.

ISA Analysis Division Symposium
Exploring the latest in process stream and laboratory method analysis

ISA International Instrumentation Symposium
Showcasing leading-edge instrumentation techniques, applications, and technologies

ISA LDAR-Fugitive Emissions Symposium
Sharing progress and best practices in Leak Detection and Repair (LDAR) programs

ISA POWID Division Symposium
Engineering the future of power generation and energy technologies

ISA Water/Wastewater and Automatic Controls Symposium
Inspiring automation innovation in the water and wastewater sector

ISA Food and Pharmaceutical Industry Symposium
Advancing automation and serialization in the secure pharmaceutical and food supply chain

ISA Process Control and Safety Symposium
Fostering safe and effective process measurement and control

- **Visit** www.isa.org/events **for more information or for a schedule of events.**

The International Society of Automation (www.isa.org) is a nonprofit professional association that sets the standard for those who apply engineering and technology to improve the management, safety, and cybersecurity of modern automation and control systems used across industry and critical infrastructure. Founded in 1945, ISA develops widely used global standards; certifies industry professionals; provides education and training; publishes books and technical articles; hosts conferences and exhibits; and provides networking and career development programs for its 36,000 members and 350,000 customers around the world.

ISA owns Automation.com, a leading online publisher of automation-related content, and is the founding sponsor of The Automation Federation (www.automationfederation.org), an association of non-profit organizations serving as “The Voice of Automation.” Through a wholly owned subsidiary, ISA bridges the gap between standards and their implementation with the ISA Security Compliance Institute (www.isasecure.org) and the ISA Wireless Compliance Institute (www.isa100wci.org).

International Society of Automation
67 T.W. Alexander Drive
P.O. Box 12277
Research Triangle Park, NC 27709
PHONE +1 919-549-8411
FAX +1 919-549-8288
EMAIL info@isa.org
www.isa.org