Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Cybersecurity Training

Safeguarding industrial automation and control systems

www.isa.org/CYBETRN

Setting the Standard for Automation™

Expert-led training with real-world application from a global leader in industrial cybersecurity

Given the increasing reliance on open standards and interconnectivity in industrial networks and control systems, the risks of cyberattack are growing and present serious threats to economic and national security.

Large-scale cyberwarfare—through acts of espionage, sabotage, and terrorism—could dismantle a nations' power grids, transportation and telecommunications systems, financial networks, manufacturing, and government functions.

As a widely recognized, world leader in cybersecurity standards development and training, the International Society of Automation (ISA) provides the proven expertise and know-how to help safeguard industrial automation and control systems. As an example, the US government is looking to integrate ISA's industrial automation and control systems standards (ISA/IEC 62443) as part of its national cybersecurity initiative.

ISA's world-renowned cybersecurity experts provide the comprehensive, practical instruction needed to immediately apply your knowledge in the workplace, and through a wide variety of learning formats:

- **One-day classroom courses**
- **Multi-day classroom courses**
- **Multi-week, online, instructor-assisted courses**
- **Live webinars**
- **Pre-recorded webinars**

In addition, to ensure flexibility and to meet varying customer needs, ISA offers cybersecurity training at a variety of locations: at ISA headquarters in North Carolina, at ISA's many regional training centers, and onsite directly at customer facilities.

Who is ISA?

Founded in 1945, ISA is a global organization that serves automation and control professionals through standards development, certification, education, training, publishing, and technical conferences and events. To learn more about ISA, visit www.isa.org/CYBETRN.

ISA Training: World-class subject-matter expertise

ISA's courses are known and respected worldwide for their unbiased, practical approach to technology application. For more than 65 years, ISA has built on its proven track record of identifying the real-world training needs of organizations and automation and control professionals, and working with leading content experts to deliver rapid, customized solutions.

Taking an ISA training course will:

- Enhance on-the-job training
- Fill in missing knowledge gaps
- Teach you the Hows and Whys
- Provide continuing education credits
- Expand your professional network

Table of Contents

ISA/IEC 62443 Cybersecurity Certificate Programs

certificate program

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 ISA/IEC 62443 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 electronically 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.

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 ISA/IEC 62443 Cybersecurity Experts and receive confirmation and documentation relating to same.

Learn more about this certificate program, eligibility criteria, renewal, and upcoming courses at: **www.isa.org/ISACyberCertificate.**

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

certificate program

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 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.

YOU WILL BE ABLE TO:

- Discuss the principles behind creating an effective long-term security program
- Interpret the ISA/IEC 62443 industrial security guidelines and apply them to your operation
- Explain the concepts of defense-in-depth, zone, and conduit models of security
- Analyze the trends in industrial system security incidents and methods hackers use to attack
- Define the principles behind the key risk mitigation techniques, including anti-virus and patch management, firewalls, and virtual private networks
- And more…

YOU WILL COVER:

- How Cyberattacks Happen
- Creating A Security Program
- Risk Analysis
- Addressing Risk
- Monitoring and Improving the CSMS
- And more…

Required for ISA/IEC 62443 Cybersecurity Fundamentals Specialist Certificate Program
(See page 3)

CLASSROOM/LABORATORY EXERCISES:

- Develop a business case for industrial security
- Conduct security threat analysis
- Investigate scanning and protocol analysis tools
- Apply basic security analysis tools software

COURSE DETAILS:

Course No.: IC32
Length: 2 Days
CEUs: 1.4

Price: $1,440 ISA Member/Group Rate
$1,620 Affiliate Member
$1,800 Community Member/List
$1,440 Multi-Registration Rate

Includes ISA Standards and Technical Reports:

- ISA/IEC 62443-1-1 (99.00.01)-2007: *Security for Industrial Automation and Control Systems Part 1-1: Terminology, Concepts, and Models* ***(A $155 Value!)***
- ISA/IEC 62443-2-1 (99.02.01)-2009: *Security for Industrial Automation and Control Systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program* ***(A $215 Value!)***
- ISA/IEC 62443-3-3 (99.03.03)-2013: *Security for Industrial Automation and Control Systems Part 3-3: System Security Requirements and Security Levels* ***(A $260 Value!)***

Recommended Resource: ISA Text: *Industrial Network Security* by David J. Teumin

2017 SCHEDULE

Research Triangle Park, NC	20–21 February
	25–26 April
Houston, TX	3–4 May
Newark, DE	31 July – 1 August
Research Triangle Park, NC	7–8 August
Newhall, CA	6–7 September
Houston, TX	2–3 October
Research Triangle Park, NC	4–5 December

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

certificate program

The move to using open standards such as Ethernet, TCP/IP, and web technologies in supervisory control and data acquisition (SCADA) systems 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 ISA/IEC 62443 standards can be used to protect your critical control systems. You will also explore the procedural and technical differences between the security for traditional IT environments and those solutions appropriate for SCADA or plant floor environments.

YOU WILL BE ABLE TO:

- Identify the principles behind creating an effective long-term security program
- Interpret the ISA/IEC 62443 industrial security guidelines and apply them to your operation
- Learn the basics of risk and vulnerability analysis methodologies
- Explain the principles of security policy development
- Define the concepts of defense-in-depth, zone, and conduit models of security
- Analyze the trends in industrial system security incidents and methods hackers use to attack
- Identify the principles behind the key risk mitigation techniques, including anti-virus and patch management, firewalls, and virtual private networks

YOU WILL COVER:

- **Week 1/Module 1:** Defining Industrial Cybersecurity
- **Week 2/Module 2:** Risk Assessment
- **Week 3/Module 3:** Threats and Vulnerabilities
- **Week 4/Module 4:** Security Policies, Programs, and Procedures
- **Week 5/Module 5:** Understanding TCP/IP, Hackers, and Malware
- **Week 6/Module 6:** Technical Countermeasures
- **Week 7/Module 7:** Architectural and Operational Strategies
- **Week 8:** Final Course Examination

COURSE MATERIALS:

- Course Noteset and Syllabus
- ISA Standards and Technical Reports:
  - ISA/IEC 62443-1-1 (99.00.01)-2007: *Security for Industrial Automation and Control Systems Part 1-1: Terminology, Concepts, and Models* ***(A $155 Value!)***
  - ISA/IEC 62443-2-1 (99.02.01)-2009: *Security for Industrial Automation and Control Systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program* ***(A $215 Value!)***
  - ISA/IEC 62443-3-3 (99.03.03)-2013: *Security for Industrial Automation and Control Systems Part 3-3: System Security Requirements and Security Levels* ***(A $260 Value!)***

Recommended Resource: ISA Text: *Industrial Network Security* by David J. Teumin

COURSE DETAILS:

Course No.: IC32E
Length: 8 Weeks
CEUs: 1.4
Price: $1,440 ISA Member/Group Rate
$1,620 Affiliate Member
$1,800 Community Member/List
$1,440 Multi-Registration Rate

Required for ISA/IEC 62443 Cybersecurity Fundamentals Specialist Certificate Program
(See page 3)

2017 SCHEDULE

Online ..... 28 January – 17 March
10 April – 2 June;
17 July – 8 September;
25 September – 17 November;
20 November – 12 January 2018

Assessing the Cybersecurity of New or Existing IACS Systems

certificate program

Part of the ISA's Cybersecurity Certificate Program

The first phase in the IACS Cybersecurity Lifecycle (defined in ISA/IEC 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 ISA/IEC 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.

YOU WILL BE ABLE TO:

- Identify and document the scope of the IACS under assessment
- Specify, gather or generate the cybersecurity information required to perform the assessment
- Identify or discover cybersecurity vulnerabilities inherent in the IACS products or system design
- Interpret the results of a process hazard analysis (PHA)
- Organize and facilitate a cybersecurity risk assessment for an IACS
- Identify and evaluate realistic threat scenarios
- Identify and assess the effectiveness of existing countermeasures
- Identify gaps in existing policies, procedures and standards
- Evaluate the cost, complexity and effectiveness of new countermeasures in order to make meaningful recommendations
- Establish and document security zones and conduits
- Develop a cybersecurity requirements specification (CRS)

CLASSROOM/LABORATORY EXERCISES:

- Performing an IACS asset criticality assessment
- Critiquing system architecture diagrams
- Developing a data flow diagrams
- Researching IACS vulnerabilities
- Using vulnerability scanning tools
- Cybersecurity Risk Assessment Exercise
- Creating a zone & conduit diagram
- Critiquing a cybersecurity requirements specification
- Developing a cybersecurity test specification

WHO SHOULD ATTEND:

- Control systems engineers and managers
- System Integrators
- IT engineers and managers industrial facilities
- IT corporate/security professionals
- Plant Safety and Risk Management

RECOMMENDED PRE-REQUISITE:

ISA Course IC32 or equivalent knowledge/ experience.

COURSE DETAILS:

Course No.: IC33
Length: 3 days
CEUs: 2.1
Price: $2,000 ISA Member/Group Rate
$2,250 Affiliate Member
$2,500 Community Member/List
$2,000 Multi-Registration Rate

2017 SCHEDULE

Research Triangle Park, NC..... 22–24 February
Houston, TX..... 9–11 May
Newark, DE.....2–4 August
Newhall, CA ..... 12–14 September
Houston, TX..... 4–6 October

IACS Cybersecurity Design & Implementation

certificate program

Part of the ISA's Cybersecurity Certificate Program

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.

YOU WILL BE ABLE TO:

- Interpret the results of an ICS cybersecurity risk assessment
- Interpret a cybersecurity requirements specification (CRS)
- Develop a conceptual design based upon information in a well-crafted CRS
- Explain the security development lifecycle process and deliverables
- Perform a basic firewall configuration and commissioning
- Design a secure remote access solution
- Develop system hardening design specification
- Implement a basic network intrusion detection system
- Develop a Cybersecurity Acceptance test plan (CFAT/CSAT)
- Perform a basic CFAT or CSAT

YOU WILL COVER:

- Introduction to the ICS Cybersecurity Lifecycle
  - Assessment phase
  - Implementation phase
  - Maintenance phase
- Conceptual Design Process
  - Interpreting risk assessment results
  - Cybersecurity requirements specifications
  - Developing a conceptual design
  - Conceptual design specification
- Detailed Design Process
  - Security Development Lifecycle (SDL)
  - Types of technology
  - Selecting appropriate technology
  - Developing a detailed design
  - Documenting the design/specification
- Design & Implementation Examples
  - Firewall design example
  - Remote access design example
  - System hardening design example
  - Intrusion detection design example
- Testing
  - Developing test plans
  - Cybersecurity Factory Acceptance Testing
  - Cybersecurity Site Acceptance Testing

CLASSROOM/LABORATORY EXERCISES:

- Firewall configuration & commissioning
- Remote access
- Intrusion detection
- System Hardening

RECOMMENDED PRE-REQUISITE:

ISA Courses IC32 and IC33 or equivalent knowledge/experience.

COURSE DETAILS:

Course No.: IC34
Length: 3 days
CEUs: 2.1
Price: $2,000 ISA Member/Group Rate
$2,250 Affiliate Member
$2,500 Community Member/List
$2,000 Multi-Registration Rate

2017 SCHEDULE

Research Triangle Park, NC..... 15–17 March
Houston, TX..... 16–18 May
Pensacola, FL .....7–9 June
Newhall, CA ..... 19–21 September
Research Triangle Park, NC..... 1–3 November

IACS Cybersecurity Operations & Maintenance

certificate program

Part of the ISA's Cybersecurity Certificate Program

The third phase in the IACS Cybersecurity Lifecycle (defined in ISA/IEC 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 every changing threat environment.

YOU WILL BE ABLE TO:

- Perform basic network diagnostics and troubleshooting
- Interpret the results of IACS device diagnostic alarms and event logs
- Develop and follow IACS backup and restoration procedure
- Understand the IACS patch management lifecycle
- Develop and follow an IACS patch management procedure
- Develop and follow an antivirus management procedure
- Define the basics of application control and whitelisting tools
- Define the basics of network and host intrusion detection
- Define the basics of security incident and event monitoring tools
- Develop and follow an incident response plan
- Develop and follow an IACS management of change procedure
- Conduct a basic IACS cybersecurity audit

YOU WILL COVER:

- Introduction to the ICS Cybersecurity Lifecycle
- Network Diagnostics and Troubleshooting
- Application Diagnostics and Troubleshooting
- IACS Cybersecurity Operating Procedures & Tools
- IACS incident response

CLASSROOM/LABORATORY EXERCISES:

- Network diagnostics and troubleshooting
- Intrusion detection alarm
- Event monitoring
- Configuration management
- Patch management
- Anti-virus management
- Whitelisting
- Vulnerability scanning tools
- Incident response
- Backup and recovery

WHO SHOULD ATTEND:

- Operations and maintenance personnel
- Control systems engineers and managers
- System Integrators
- IT engineers and managers industrial facilities
- Plant Safety and Risk Management

RECOMMENDED PRE-REQUISITE:

ISA Courses TS06, TS12, IC32, IC33 and IC34 or equivalent knowledge/experience.

COURSE DETAILS:

Course No.: IC37
Length: 3 days
CEUs: 2.1
Price: $2,000 ISA Member/Group Rate
$2,250 Affiliate Member
$2,500 Community Member/List
$2,000 Multi-Registration Rate

2017 SCHEDULE

Research Triangle Park, NC	21–23 March
Houston, TX	23–25 May
Columbia, IL	12–14 July
Research Triangle Park, NC	9–11 August
Newhall, CA	26–28 September

Industrial Networking and Security

You will learn about 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. You 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 will expand your practical knowledge of LAN, WAN, and Web technologies. This course 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).

YOU WILL BE ABLE TO:

- Identify standards for analog dial-up connections and modems
- Apply TCP/IP protocols, addressing, and troubleshooting
- Estimate where web technologies can safely be used for process control
- Identify security technologies such as firewalls, proxy servers, virus scanning, and intrusion protection
- Perform basic security scanning on your networks and perform "hardening" of your computers
- And more...

YOU WILL COVER:

- TCP/IP Networking
- Secure Architectures
- Packets and Protocols
- Building a Plant Floor Web Server
- Network Security Issues
- And more...

CLASSROOM/LABORATORY EXERCISES:

- Use TCP/IP diagnostic tools in Windows-2000/XP
- Use network analyzers to troubleshoot
- Configure a security firewall for the plant floor
- Perform a basic security scan on a target system
- And more...

COURSE DETAILS:

Course No.: TS12
Length: 5 days
CEUs: 3.5
Price: $3,080 ISA Member/Group Rate
$3,465 Affiliate Member
$3,855 Community Member/List
$3,080 Multi-Registration Rate

Part of ISA's System Wide Awareness Training (S.W.A.T.) Learn more at: **www.isa.org/swatcourses**

2017 SCHEDULE

Research Triangle Park, NC..... 13–17 February; 22–26 May
Part of ISA's System-wide Awareness Training (S.W.A.T.)
Newark, DE..... 24–28 July
Houston, TX..... 25–29 September

Control Systems Security and ISA/IEC 62443 Webinar Series

Improve your ISA/IEC 62443 knowledge with these 90-minute, live webinars!

Save up to 25%

when you register for all three webinars in this series at one time! To take advantage of the series pricing, you must call ISA Customer Service at +1 919-549-8411 to register as this offer is not available online.

Cybersecurity Risk Assessment for Automation Systems

Course No.: IC32CW1
Dates: 5 April; 6 September
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.

Using Firewalls and Security Zones on the Plant Floor

Course No.: IC32CW2
Dates: 19 April; 13 September
The network firewall is one of the most important tools in any cybersecurity designer's toolbox. This webinar introduces the industrial controls engineer to the world of firewall system design, focusing on how these devices can be effectively deployed on the typical plant floor to help meet the ISA/IEC 62443 security standards.

A Tour of the ISA/IEC 62443 Security Standards

Course No.: IC32CW3
Dates: 3 May; 20 September
This webinar introduces you to the ISA/IEC 62443 Security for Industrial Automation and Control Systems standards and how these are organized. You will be given a brief introduction to the terminology, concepts, and models of ISA/IEC 62443 cybersecurity and elements of creating a cybersecurity management system.

WEBINAR DETAILS (PER SEMINAR):

You can provide these live quality seminars at your location for an unlimited number of participants for one low site fee:

Pricing (per site): $280 ISA Member
$315 Affiliate Member
$350 Community Member/List
$280 Multi-Registration Rate

Can't attend? Missed the live events?
Recorded versions of these sessions are also available, and are free for ISA members.

Bring ISA cybersecurity training right to you!
All of ISA's cybersecurity training courses can be taught at your company location through ISA's Onsite Training. Contact ISA at **+1 919-549-8411** or at **info@isa.org** for more information.

Dates and locations are subject to change. Please check website for current availability.

ISA is accredited by the International Association for Continuing Education and Training (IACET). ISA complies with the ANSI/IACET Standard, which is recognized internationally as a standard of excellence in instructional practices. As a result of this accreditation, ISA is authorized to issue the IACET CEU.

ACCREDITED IACET PROVIDER
Provider #1001262

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).

EP30-6862-1116

International Society of Automation
67 T.W. Alexander Drive
P.O. Box 12277
Research Triangle Park, NC 27709

Get the security and data communications training you need from the ISA/IEC 62443 experts!
Register or learn more at www.isa.org/CYBETRN