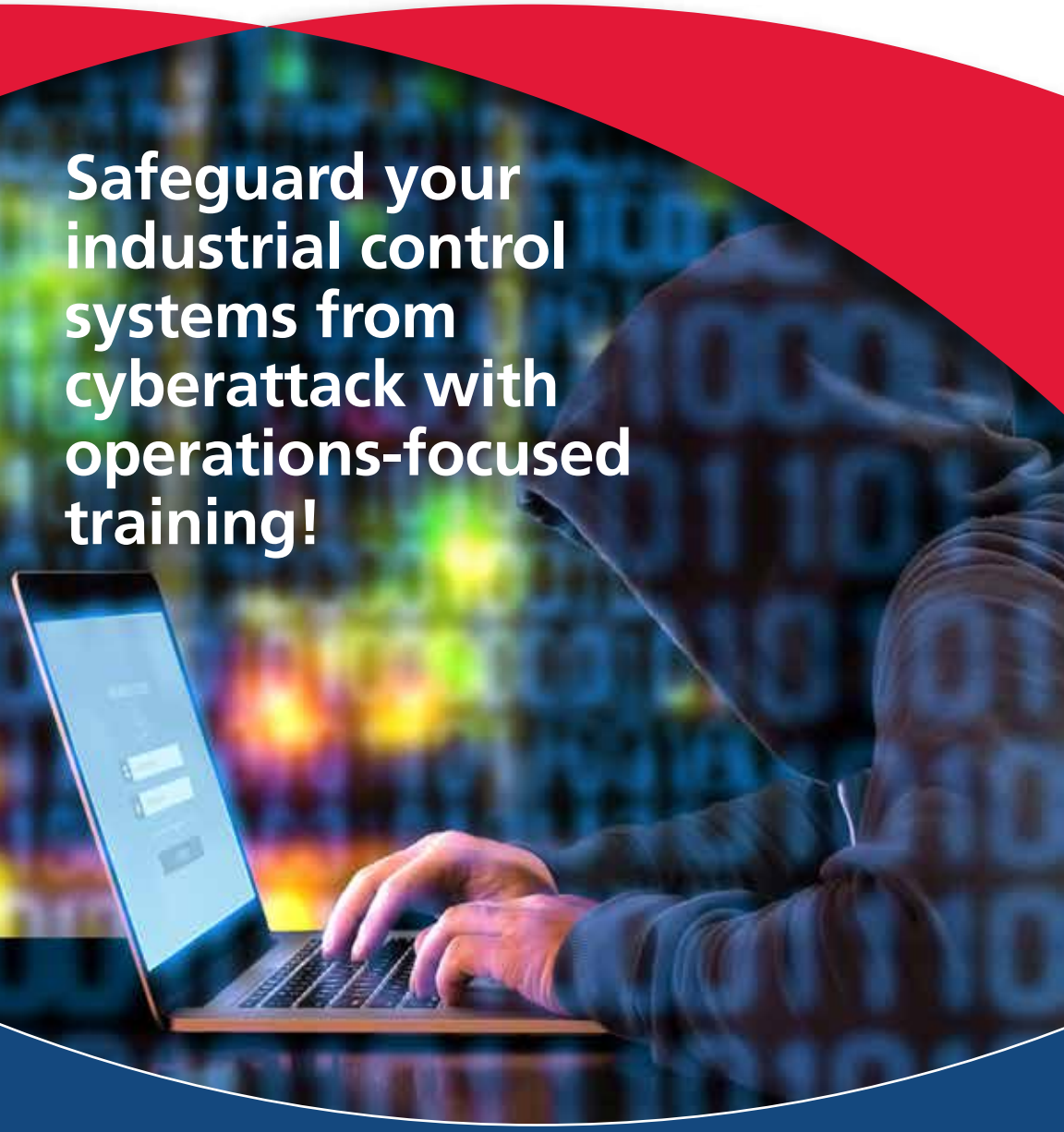
Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Safeguard your industrial control systems from cyberattack with operations-focused training!



IACS Cybersecurity Training Course Series
Complete 2019 Schedule Inside!
www.isa.org/Cyber2019

Setting the Standard for Automation™

Make Your Cybersecurity Training World-Class in 2019!

Attend One of Our IACS Cybersecurity Training Course Series Events!

The course series format offers four highly integrated industrial cybersecurity courses over four weeks in one location! 2019 course series events are scheduled in Houston, TX and Newhall, CA. Choose to enroll in only the course or courses that meet your needs.

2019 IACS Cybersecurity Training Course Series Event Schedule

Course #	Title	Houston, TX	Newhall, CA
IC32	Using the ISA/IEC 62443 Standards to Secure Your Control Systems	6–7 May	9–10 September
IC33	Assessing the Cybersecurity of New or Existing IACS Systems	8–10 May	11–13 September
IC34	IACS Cybersecurity Design & Implementation	14–16 May	17–19 September
IC37	IACS Cybersecurity Operations & Maintenance	21–23 May	24–26 September

Education & Training

ISA is recognized worldwide as a leader in non-biased, vendor-neutral education and training programs for automation professionals. Industry professionals—whether an experienced engineer, practicing technician, or newcomer to the industry—can hone their skills at ISA's regional training centers, through onsite training programs at their company, or via distance education.

Who will benefit most by attending this special training event?

- Control system engineers and managers
- System integrators
- IT engineers and managers of industrial facilities
- Plant managers
- Plant safety and risk management personnel

These industrial cybersecurity courses comprise the most comprehensive set of skills-based operational technology (OT) cybersecurity training in the marketplace—covering how to best leverage the ISA/IEC 62443 series of industrial automation and control system (IACS) standards through a full-circle exploration of the IACS cybersecurity lifecycle.

- Instruction covers the complete lifecycle of industrial automation and control system (IACS) cybersecurity: assessment, design, implementation, operations, and maintenance
- Based on ISA/IEC 62443, the world's only consensus-based series of IACS standards
- Rigorous, hands-on instruction—from industry experts using industry-supported IACS equipment—developed by ISA, the global leader in industrial cybersecurity standards and training

Register today!
www.isa.org/Cyber2019
info@isa.org • +1-919-549-8411

IC32

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

Certificate 1

Successful completion of this course is required in order to sit for the ISA/IEC 62443 Cybersecurity Fundamentals Specialist exam. Certificate exam fee is included with course registration.

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 program security
- Interpret the ANSI/ISA99 industrial security guidelines and apply them to your operation
- Define the basics of risk and vulnerability analysis methodologies
- And more…

The course covers many topics, including:

- Understanding the current industrial security environment
- How cyberattacks happen
- Creating a security program
- Risk analysis
- Addressing risk with security policy, organization, and awareness
- And more...

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

Earn Digital Badges to display on your profile. Choose from four different cybersecurity certificate program levels and earn a digital badge when you complete each cybersecurity course and pass the corresponding certificate exam. Earn all four and you will automatically receive the ISA/IEC62443 Cybersecurity Expert badge.

Course Details:
Course No.: IC32
Length: 2 Days
CEUs: 1.4
Price: $1,640 ISA Member
$1,820 Affiliate Member
$2,000 Community Subscriber/List
$1,640 Multi-Registration Rate

Certificate 1 Exam Fee: Included in the price of the course

RETURN
to Course Series Schedule

IC33

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

Certificate 2

Successful completion of this course is required in order to sit for the ISA/IEC 62443 Cybersecurity Risk Assessment Specialist exam. Certificate exam fee is included with course registration.

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 in order 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. brown-field) 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 of 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
- Organize and facilitate a cybersecurity risk assessment for an IACS
- Identify and evaluate realistic threat scenarios
- Identify gaps in existing policies, procedures, and standards
- And more…

Classroom and hands-on, equipment-based laboratory exercises include:

- Critiquing system architecture diagrams
- Asset inventory
- Gap assessment
- Windows vulnerability assessment
- Capturing ethernet traffic
- Port scanning
- And more…

Course Details:

Length: 3 days
CEUs: 2.1
Price: $2,200 ISA Member
$2,450 Affiliate Member
$2,700 Community Subscriber/List
$2,200 Multi-Registration Rate

Certificate 2 Exam Fee: Included in the price of the course

RETURN
to Course Series Schedule

IC34

IACS Cybersecurity Design and Implementation (IC34)

Certificate 3

Successful completion of this course is required in order to sit for the ISA/IEC 62443 Cybersecurity Design Specialist exam. Certificate exam fee is included with course registration.

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, 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.

You will be able to:
- Interpret the results of an ICS cybersecurity risk assessment
- Develop 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
- And more…

The course covers many topics, including:
- Introduction to the ICS cybersecurity lifecycle
- Conceptual Design Process
- Detailed Design Process
- Design and Implementation Examples
- Testing

Classroom and hands-on, equipment-based laboratory exercises include:
- Develop a physical and cybersecurity plan
- Configure a perimeter firewall
- Configure an ICS firewall
- Install and use SNORT!
- Configure Windows local group policy objects
- Install MS Security Compliance Manager (SCM)
- And more…

Course Details:
Length: 3 days
CEUs: 2.1
Price: $2,200 ISA Member
$2,450 Affiliate Member
$2,700 Community Subscriber/List
$2,200 Multi-Registration Rate

Certificate 3 Exam Fee: Included in the price of the course

RETURN
to Course Series Schedule

IACS Cybersecurity Operations and Maintenance (IC37)

Successful completion of this course is required in order to sit for the ISA/IEC 62443 Cybersecurity Maintenance Specialist exam. Certificate exam fee is included with course registration.

Certificate 4

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.

You will be able to:
- Perform basic network diagnostics and troubleshooting
- Interpret the results of IACS device diagnostic alarms and event logs
- Implement IACS backup and restoration procedures
- Describe the IACS patch management lifecycle and procedure
- Apply an antivirus management procedure
- Define the basics of application control and white listing tools
- And more…

The course covers many topics, including:
- Introduction to the ICS cybersecurity lifecycle
- Network diagnostics and troubleshooting
- Application diagnostics and troubleshooting
- IACS cybersecurity operating procedures and tools
- IACS incident response

Classroom/Laboratory Exercises:
- Asset inventory
- ICS device hardening
- Application control/whitelisting
- PLC backup and configuration management
- Change management (MOC form)
- Event detection tracking and log monitoring
- Vulnerability scanning
- Troubleshooting and forensics
- And more…

Course Details:
Length: 3 days
CEUs: 2.1
Price: $2,200 ISA Member
$2,450 Affiliate Member
$2,700 Community Subscriber/List
$2,200 Multi-Registration Rate

Certificate 4 Exam Fee: Included in the price of the course

RETURN
to Course Series Schedule

2019 IACS Cybersecurity Training Course Series Event Schedule

Course #	Title	Houston, TX	Newhall, CA
IC32	Using the ISA/IEC 62443 Standards to Secure Your Control Systems	6–7 May	9–10 September
IC33	Assessing the Cybersecurity of New or Existing IACS Systems	8–10 May	11–13 September
IC34	IACS Cybersecurity Design & Implementation	14–16 May	17–19 September
IC37	IACS Cybersecurity Operations & Maintenance	21–23 May	24–26 September

www.isa.org/Cyber2019

info@isa.org • +1 919-549-8411

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

EP30-9385-0119

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

All ISA Industrial Cybersecurity Training Course Series classes will be filled on a first-come-first-served basis. Don't miss your chance to attend this unique ISA training event! Register today at:
www.isa.org/Cyber2019