International Society of Automation
United Kingdom Section

IEC62443 CYBER SECURITY TRAINING BROCHURE

13-14th October 2025
15-17th October 2025
From 09:00AM to 05:00PM

REGISTER NOW

IN PERSON TRAINING

SCHEDULED COURSES

IC32 :Using the ISA/IEC 62443 Standards to Secure Your Control Systems

Course: IC32
Length: 2 days
ISA-member price: € 1,650
Non ISA-member price: € 2,050
Program registration: Click Here

IC33 :Assessing the Cybersecurity of New or Existing IACS Systems

Course: IC33
Length: 3 days
ISA-member price: € 2,395
Non ISA-member price: € 2,995
Program registration: Click Here

YOUR PATHWAY TO BECOMING AN IEC 62443 CYBERSECURITY EXPERT !

Location :
The GAMBICA Association Ltd,
Rotherwick House,
3 Thomas More Street,
London, E1W 1YZ, United Kingdom

For More Information
info@isa-uk.org

IC32- Using the ISA/IEC 62443 Standards to Secure Your Control Systems:

Description:

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/ISA99 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 ISA/IEC 62443 industrial security framework and apply them to your operation
- Define the basics of risk and vulnerability analysis methodologies
- Describe the principles of security policy development
- Explain the concepts of defense in depth and zone/conduit models of security
- Analyze the current trends in industrial security incidents and methods hackers use to attack a system
- Define the principles behind the key risk mitigation techniques, including anti-virus and patch management, firewalls, and virtual private networks

You will cover:

- **Understanding the Current Industrial Security Environment:** What is Electronic Security for Industrial Automation and Control Systems? | How IT and the Plant Floor are Different and How They are the Same
- **How Cyberattacks Happen:** Understanding the Threat Sources | The Steps to Successful Cyberattacks
- **Creating A Security Program:** Critical Factors for Success/Understanding the ANSI/ISA-62443-2-1 (ANSI/ISA-99.02.01-2009)- *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*
- **Risk Analysis:** Business Rationale | Risk Identification, Classification, and Assessment
- **Addressing Risk with Security Policy, Organization, and Awareness:** Cyber Security Management System Scope | Organizational Security | Staff Training and Security Awareness
- **Addressing Risk with Selected Security Counter Measures:** Personnel Security | Physical and Environmental Security | Network Segmentation | Access Control
- **Addressing Risk with Implementation Measures:** Risk Management and Implementation | System Development and Maintenance | Information and Document Management
- **Monitoring and Improving the CSMS:** Compliance and Review | Improve and Maintain the CSMS
- **Validating or Verifying the Security of Systems:** What is being done? | Developing Secure Products and Systems

Includes ISA Standards:

- ANSI/ISA-62443-1-1 (ANSI/ISA-99.00.01-2007), *Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts & Models*
- ANSI/ISA-62443-2-1 (ANSI/ISA-99.02.01-2009), *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*
- ANSI/ISA-62443-3-3, *Security for industrial automation and control systems: System security requirements and security levels*

ISA
International Society of Automation
United Kingdom Section

ISA/IEC 62443 CYBERSECURITY FUNDAMENTALS SPECIALIST ISA

The GAMBICA Association Ltd, Rotherwick House,
3 Thomas More Street,
London, E1W 1YZ, United Kingdom

info@isa-uk.org

Kindly use the registration link in the post to secure your seat.

IC33 - Assessing the Cybersecurity of New or Existing IACS Systems:

Description:

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. 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
- Organize and facilitate a cybersecurity risk assessment for an IACS
- Identify and evaluate realistic threat scenarios
- Identify gaps in existing policies, procedures and standards
- Establish and document security zones and conduits
- Prepare documentation of assessment results

Classroom/Laboratory Exercises:

- Asset Inventory
- Initial Risk Assessment
- Windows Vulnerability Assessment
- Port Scanning
- Using Vulnerability Scanning Tools
- Perform a pentest
- Creating a zone & conduit diagram
- Perform a detailed cyber risk assessment

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

Required:

- To take exam for IC33, IC34 and IC 37, it is mandatory that you have attended the IC32 training and passed the IC32 exam.
- To participate in the training, it is minimum recommended Prerequisite to have ISA Course IC32 or equivalent knowledge/experience.

ISA™

International Society of Automation
United Kingdom Section

ISA/IEC 62443
CYBERSECURITY
RISK
ASSESSMENT
SPECIALIST
ISA

TThe GAMBICA Association Ltd, Rotherwick House,
3 Thomas More Street,
London, E1W 1YZ, United Kingdom

info@isa-uk.org

Kindly use the registration link in the post to secure your seat.

Benefits of IEC 62443 Cybersecurity Certification

1. **Industry-Recognized Expertise**: Gain a globally recognized credential in industrial cybersecurity, enhancing your professional credibility and opening new career opportunities.
2. **Comprehensive Skill Development**: Learn essential concepts, including risk assessment, network segmentation, access control, and security policies tailored to industrial environments.
3. **Stay Ahead of Threats:** Stay up to date with the latest cybersecurity practices for Industrial Automation and Control Systems (IACS), protecting critical infrastructure against evolving threats.
4. **Hands-on Experience:** Our program includes practical labs, real-world case studies, and exercises to bridge theory and practice, ensuring you're prepared for real-world challenges.
5. **Improved Organizational Security**: Certified professionals can better design, implement, and maintain a robust cybersecurity management system, improving the security posture of their organization.

Why Choose Us?

- **Best-in-Class** Trainers: Our courses are delivered in partnership with ISA Europe, featuring top trainers with extensive industrial experience and practical expertise.
- **Hands-on Labs**: Experience real-world scenarios through our carefully designed labs that provide hands-on exposure to industrial systems, vulnerabilities, and security solutions.
- **Networking Opportunities:** Join an exclusive community of top cybersecurity professionals across the UK, fostering valuable industry connections.
- **Real-World Focus**: Our training programs are designed to address real-world industrial cybersecurity challenges, ensuring practical, actionable learning.
- **Personalized Attention:** With limited seats per session, we ensure personalized attention, enabling an interactive and engaging learning environment.
- **Pathway to Advanced Certification:** Our foundational courses prepare you for advanced certification exams like IC33, IC34, and IC37, helping you progress along your professional certification journey.

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

Prerequisite

- **IC32**: There are no required prerequisites for taking this course; however, it is highly recommended that applicants have at least one to three years of experience in the cybersecurity field with some experience in an industrial setting.
- **IC33**: To participate in the training, it is minimum recommended prerequisite to have completed the ISA Course IC32 or possess equivalent knowledge/experience.

ISA™

International Society of Automation

United Kingdom Section

Training Agenda

IC32: Using the ISA/IEC 62443 Standards to Secure Your Control Systems

- **Date**: 13th - 14th October 2025
- **Time**: 9:00 AM - 5:00 PM
- **Duration**: 2 Days
- **Key Takeaways:**
  - Secure SCADA and industrial control systems using ISA/IEC 62443 standards
  - Learn risk analysis, defense-in-depth, and security policy development
  - Hands-on exercises: PCAP live capture analysis and industrial network security

IC33: Assessing the Cybersecurity of New or Existing IACS Systems

- **Date**: 15th - 17th October 2025
- **Time**: 9:00 AM - 5:00 PM
- **Duration:** 3 Days
- **Key Takeaways:**
  - Conduct cybersecurity risk assessments for IACS systems
  - Develop security zones, conduits, and cybersecurity requirements
  - Hands-on exercises: Vulnerability scanning, asset inventory, and risk assessments

Training Fees

As per EU2025 rates:

Non-Members:

- IC32: € 2,050
- IC33: € 2,995

Members:

- IC32: € 1,650
- IC33: € 2,395

Location

The GAMBICA Association Ltd, Rotherwick House, 3 Thomas More Street, London, E1W 1YZ, United Kingdom

How to register

- **IC32 Course Registration**: Click Here
- **IC33 Course Registration**: Click Here

For inquiries, email: info@isa-uk.org

Note: This is an in-person classroom training. For live or on-demand training options, please visit the ISA website:

ISA/IEC 62443 Cybersecurity Certificate Program.

ISA

International Society of Automation
United Kingdom Section