International Society of Automation
United Kingdom Section

IEC62443 CYBER SECURITY TRAINING BROCHURE

11-13th August 2025
13-15th August 2025

From 09:00AM to 05:00PM

REGISTER NOW

IN PERSON TRAINING

SCHEDULED COURSES

IC34 :IACS Cybersecurity Design & Implementation

Course: IC34
Length: 3 days
ISA-member price: € 2,395
Non ISA-member price: € 2,995
Program registration: **Click Here**

IC37 :IACS Cybersecurity Operations & Maintenance

Course: IC37
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
Tower Room, School Green Center, Shinfield,
Reading, RG2 9EH, United Kingdom

For More Information
info@isa-uk.org

IC34 - IACS Cybersecurity Design & Implementation:

Description:

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
- Perform a basic firewall configuration and commissioning
- Design a secure remote access solution
- Develop system hardening specification
- Implement a basic network intrusion detection system
- Develop and perform a Cybersecurity Acceptance test plan (CFAT/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:

- Build the Board
- Configure Firewalls and DMZ
- Network Device Hardening
- Define Policies and Procedures
- Setup Remote Access
- Use Part 62443-3-3 to validate SL-A

ISA

International Society of Automation
United Kingdom Section

ISA/IEC 62443
CYBERSECURITY
DESIGN SPECIALIST
ISA

IC37- IACS Cybersecurity Operations & Maintenance

Description:

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 every changing threat environment.

You will be able to:

- Understanding 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 life cycle and procedure
- Apply an antivirus management procedure
- Define the basics of application control and white listing tools
- Define the basics of network and host intrusion detection
- Define the basics of security incident and event monitoring tools
- Implement an incident response plan
- Implement an IACS management of change procedure
- Conduct a basic IACS cyber security audit

You will cover:

- **Introduction to the ICS Cybersecurity Lifecycle**: Identification & Assessment phase, Design & Implementation phase, Operations & Maintenance phase
- **Network Diagnostics and Troubleshooting**: Interpreting device alarms and event logs, early indicators, network intrusion detection systems, network management tools
- **Application Diagnostics and Troubleshooting**: Interpreting OS and application alarms and event logs, early indicators, application management and whitelisting tools, antivirus and endpoint protection tools, SIEM tools
- **IACS Cybersecurity Operating Procedures & Tools**: Management of change, backup, configuration management, patch management, antivirus management, cybersecurity auditing – including relevant tools for each
- **IACS Incident Response**: Incident response planning, investigation, and system recovery.

ISA

International Society of Automation
United Kingdom Section

ISA/IEC 62443 CYBERSECURITY MAINTENANCE SPECIALIST ISA

Tower Room, School Green
Center, Shinfield, Reading,
RG2 9EH, UK

info@isa-uk.org

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

IC37- IACS Cybersecurity Operations & Maintenance

Classroom/Laboratory Exercises:

- Build The Board
- Patch Management
- Whitelisting
- Snort Intrusion Detection System
- Monitoring
- Versioning and Backups
- Incident 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 Resources :

- ISA-62443-1-1-2007, Security for Industrial Automation and Control Systems – Part 1: Terminology, Concepts & Models
- ISA-62443-2-1-2009, Security for Industrial Automation and Control Systems – Part 2-1: Establishing an Industrial Automation and Control Systems Security Program
- ANSI/ISA-62443-3-3 (99.03.03)-2013 Security for industrial automation and control systems – Part 3-3: System security requirements and security levels

Contact us :

For any questions or enquiries, please feel free to contact us at:
✉ **info@isa-uk.org**

To stay updated on upcoming events and training opportunities:
🔗 Follow us on LinkedIn: ISA UK LinkedIn
🌐 Visit our website: https://isa-uk.org/

ISA™
International Society of Automation
United Kingdom Section

ISA/IEC 62443 CYBERSECURITY MAINTENANCE SPECIALIST ISA

Tower Room, School Green
Center, Shinfield, Reading,
RG2 9EH, UK

✉ 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

- **IC34** & **IC37**: To participate in the training, it is minimum recommended prerequisite to have completed the ISA Course IC32 or possess equivalent knowledge/experience. To take the exam, it is mandatory to have attended and passed IC32.

ISA™

International Society of Automation
United Kingdom Section

Training Agenda

IC34: IACS Cybersecurity Design & Implementation

- **Date**: 11th - 13th August 2025
- **Time**: 9:00 AM - 5:00 PM
- **Duration**: 3 Days
- **Key Takeaways:**
  - Design and implement cybersecurity controls using ISA/IEC 62443 standards
  - Develop cybersecurity requirements, conceptual and detailed system designs
  - Hands-on exercises: Firewall configuration, remote access setup, SDL, and acceptance testing

IC37: IACS Cybersecurity Operations & Maintenance

- **Date**: 13th - 15th August 2025
- **Time**: 9:00 AM - 5:00 PM
- **Duration:** 3 Days
- **Key Takeaways:**
  - Operate, monitor, and maintain cybersecurity throughout the IACS lifecycle
  - Perform diagnostics, patch management, backups, and incident response
  - Hands-on exercises: Patch management, whitelisting, IDS setup, and incident recovery

Training Fees

As per EU 2025 rates:

Members:

- IC34: € 2,395
- IC37: € 2,395

Non-Members:

- IC34: € 2,995
- IC37: € 2,995

Location

Tower Room, School Green Center, Shinfield, Reading, RG2 9EH, United Kingdom

How to register

- **IC34 Course Registration**: Click Here
- **IC37 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