ISA/IEC 62443-Focused OT Cybersecurity Training for Asset Owners and Operators

Asset owners and operators can learn about how to employ the ISA/IEC 62443 series of standards to help create and maintain resilient systems.

Training overview

Cyber threats continue to bombard manufacturers– no matter the industrial sector. With threats becoming more sophisticated and the attack surface becoming larger, now is the time for engineers active in the creation, operation and maintenance of industrial automation and control systems (IACS) to strengthen their cybersecurity knowledge.

To that end, UL Solutions offers a 4-day course of operational technology (OT)-cybersecurity training heavily focused on the ISA/IEC 62443 series of standards developed to secure industrial automation and control systems. ISA/IEC 62443 series of standards helps inform asset owners/operators on securing IACS throughout their entire lifecycle.

This training includes several standards, technical reports (TR) and technical specifications (TS). During this interactive training, you will learn to make educated choices about the implementation of security based on the ISA/IEC 62443 series of standards.

This training has a core focus on the following ISA/IEC 62443 sub-standard most relevant to IACS asset owners:

- **2-1:** Security program requirements for IACS Asset Owners

The course will cover an overview of all the following sub-standards and explore how they apply to asset owners in defining their roadmap for processes and system integration, system design, assessment and certification needs and required investment:

- **2-3:** Patch management in the IACS environment
- **2-4:** Security program requirements for IACS service providers

- **3-1:** Security technologies for industrial automation and control systems
- **3-2:** Security risk assessment for system design
- **3-3:** System security requirements and security levels
- **4-1:** Secure product development lifecycle requirements
- **4-2:** Technical security requirements for IACS components
- **ISO-27xxx:** Information Technology – Security Techniques – Information Security Management Systems (only relevant parts for OT cybersecurity)

Additionally, the course provides an overview of the IACS lifecycle. It reviews cybersecurity risk assessment, developing zones and conduits, cybersecurity requirements definition, evaluation and profiles, designing secure systems, security and maturity level definition and application, design concepts, operations requirements, security monitoring and incident response and maintenance of cybersecurity countermeasures executed in the implementation phase.

Training topics

- Introduction to ISA/IEC 62443 series of standards
- ISA/IEC 62443 terminology, concepts and models
- Industry 4.0/5.0 trends and challenges
- Cyberattacks in IACS — vulnerabilities and consequences
- IACS concepts, principal roles and architecture
- Purdue Model
- Regulations in OT cybersecurity
- Asset owner security program policy and procedure requirements for an IACS in operation
- Security levels and maturity levels
- Security development lifecycle view
- Defense in depth
- Zero trust in OT
- Security supply chain
- Risk assessment and management from an asset owner's perspective
- Threat modeling
- Vulnerabilities and countermeasures
- Challenges of IACS patch and update management
- Recommended requirements for IACS product suppliers
- Security design that embraces ISA/IEC 62443 architecture
- Security management
- Specification of security requirements
- Secure implementation
- Security verification and validation testing
- Organizational security measures
- Configuration management
- Network and communications security
- Component security
- Protection of data
- User access control
- Event and incident management
- System integrity and availability
- Management of security-related issues
- Security guidelines
- Security program development and management
- Security policies and procedures
- Compliance and auditing
- Best practices for implementation

UL Solutions

This course

- Provides a detailed view of how asset owners/operators can use the ISA/IEC 62443 series of standards to better protect control systems in general and those used in critical infrastructures.
- Enhances staff's ability to protect critical assets and can help support a smoother, more effective gap analysis process as part of certification. It facilitates the journey toward achieving ISA/IEC 62443 certification, helps staff fortify assets and facilities against potential cyber risks and supports compliance with international security standards.
- Supports your organization in building your IACS security program related to ISA/IEC 62443-2-1.
- Provides details to address cybersecurity for an IACS in operation by providing requirements for establishing, implementing, maintaining and continually improving an IACS security program.
- Provides details to define, implement and maintain the process, personnel and technology-based capabilities intended to reduce the cybersecurity risk of an IACS.
- Explores the procedural and technical differences between the security for traditional IT environments and those solutions appropriate for distributed control systems (DCS), programmable logic controllers (PLC), safety instrumented systems (SIS), supervisory control and data acquisition (SCADA) or OT plant floor environments.
- Addresses how solution providers acting as integrators and ongoing support of industrial automated control systems interact with asset owner/operators as part of the overall supply chain throughout the lifecycle.
- Provides details on the importance of organizational commitment from top to bottom for IACS security program success.

Training objectives

Upon successful completion of this training, the attendees should be able to:

- Understand security capabilities and reduce IACS security risks to a tolerable level.
- Determine the right level of security for products and systems.
- Update and maintain the system to the level of security required.
- Recognize security problems.
- Increase security awareness by communicating existing threats and current attack vectors.
- Demonstrate what services, systems and products to integrate and operate in accordance with security needs.
- Raise the level of knowledge about relevant security methods, security systems and standards, which helps to define security requirements for systems integrators and control products suppliers.
- Manage supply chain complexity.
- Build trust across your supply network.
- Understand and help minimize the risk of integrating IT and OT infrastructure.
- Control operations in terms of cybersecurity resilience
- Take care of the product and system security due diligence.
- Demonstrate security compliance.
- Instill cybersecurity rigor into your processes.
- Create a tailored, risk-based way of assessing security.
- Demonstrate validation of security to third parties, such as regulators.
- Provide clarity and guidance to suppliers.
- Build resilient operations and business continuity.
- Establish continuous control over the operations in terms of cybersecurity resilience.
- Meet regulatory requirements.

UL Solutions

Training target audience

- Operations and maintenance personnel
- Control systems engineers and managers
- Plant maintenance staff
- System integrators
- IT engineers and managers of industrial facilities
- Information security management system (ISMS) architects and responsible managers and operators
- Quality managers
- Plant safety and risk management
- Project and product leaders
- Developers of control systems, software application and network components for industrial automation and energy distribution and generation
- Testers, test and validation engineers
- Programmers
- Certification and compliance experts
- Managed service providers
- Maintenance service providers
- Chief information security officer (CISO) and chief security officer (CSO)

Safety. Science. Transformation.™

Training duration

This training is available for private delivery to your organization and is customized exclusively for up to 15 staff members. All training sessions will be in a virtual (live on-line instructor led) format.

- Four days
- A one-hour workshop on the last training day: On the last day of the training program, we will conduct a mini one-hour workshop. During this workshop, participants will use the knowledge gained from the training to identify and address gaps in their current cybersecurity measures based on the ISA/IEC 62443series of standards. This will occur at a real-world asset owner facility and the participant will provide relevant sample documentation for the preparation of this workshop. The main objective of this workshop is to offer practical insights and actionable strategies to enhance the cybersecurity posture of the asset owner, helping to confirm compliance with the ISA/IEC 62443 sub-standards.
- Dates are flexible. UL Solutions can conduct training on any mutually agreed dates.

To learn more and contact us, visit **UL.com/iec62443**

LEARN MORE

2190531