Design and integrate secure solutions, services and systems with ISA/IEC 62443

Cybersecurity training for engineers designing and integrating solutions, services and systems for industrial applications based on ISA/IEC 62443-2-4, 3-2 and 3-3

Course overview

Industrial automation and control systems (IACS) face the same risks as information systems due to the use of commercial off-the-shelf (COTS) technologies, increased networking, the move to using ethernet and transmission control protocol/internet protocol (TCP/IP), as well as the increased use of web technologies.

This course provides a detailed look at how solution and service providers and system integrators can use the ISA/IEC 62443 standards and framework for IACS security to protect critical control systems. It also explores the procedural and technical differences between the security for traditional IT environments and those services appropriate for distributed control systems (DCS), programmable logic controllers (PLCs), safety instrumented systems (SIS) or supervisory control and data acquisition (SCADA) for plant floor environments.

The system integrator has a vital role in the supply chain and the security of an IACS solution. This course addresses solution providers acting as integrators and ongoing support of industrial automated control systems and how they interact with asset owners/operators as part of the overall supply chain throughout the owner/operator's lifecycle.

This three-day training course focuses on the ISA/IEC 62443 standard. The ISA/IEC 62443 standards are for securing industrial automation and control systems (IACS) throughout their lifecycle. The series includes several standards, technical reports and technical specifications. During the interactive training for system integrators, we will prepare you to make informed choices about the implementation of security based on the ISA/IEC 62443 family of standards, considering security issues related to control and automation systems. This training focuses on the three IEC 62443 sub-standards most relevant to IACS system integrators:

- 2-4 – Security program requirements for IACS service providers.
- 3-2 – Security risk assessment for system design.
- 3-3 – System security requirements and security levels.

The course will also provide an overview of all the other sub-standards and how they apply to system integrators for defining their road map for processes and system integration — design, assessment and certification needs and required investment.

UL Solutions

Training topics

- Introduction to ISA/IEC 62443
- Understanding the framework of ISA/IEC 62443
- Overview of the automation cybersecurity lifecycle
- Industry 4.0 trends and challenges
- Cyberattacks in IACS – vulnerabilities and consequences
- IACS concept, principal roles and architecture
- Recommended requirements for IACS solution, service and system integrators
- Security levels and maturity levels
- Defense in depth
- Zero Trust
- Security for Industrial Internet of Things (IIoT) devices
- Security supply chain
- Cybersecurity risk assessment
- Developing zones and conduits
- Cybersecurity requirement specification (CSRS)
- Designing secure systems
- Security level determination and verification
- Detailed design considerations and operations requirements
- Vulnerabilities and countermeasures
- Challenges during IACS patch and update management
- Security design embracing ISA/IEC 62443 architecture
- Specification of security requirements
- Secure by design
- Secure implementation
- Security verification and validation testing
- Management of security-related issues
- Security guidelines

Objectives

Upon successful completion of this training, you will be able to:

- Facilitate your communication with other stakeholders, such as suppliers, operators and regulators, as you all speak the "same language."
- Determine the right level of security for products and systems.
- Update and maintain the system to the necessary level of protection.
- Gain IT and industrial cybersecurity knowledge in recognizing security problems as required by modern IACS.
- Increase your security awareness by communicating existing threats and current attack vectors.
- Demonstrate that services, systems and products are developed and integrated by following security needs.
- Establish security by design for your systems and products by understanding relevant security methods, security systems and standards.
- Manage supply chain complexity.
- Build trust across your supply network.
- Understand and help to minimize the risk of integrating IT and operational technology (OT) infrastructure.
- Meet customer demands regarding requirements from specific industries.
- Enhance brand protection.
- Control operations in terms of cybersecurity resilience.
- Take care of the product and system security due diligence.
- Demonstrate your security compliance to a wide range of target markets and customers.
- Differentiate products/systems based on security against competitive products/systems.
- Gain a competitive advantage and enhance your market position.
- Make your components' security transparent and accessible to system integrators and end users.
- Embed security into development processes.
- Instill cybersecurity rigor into your processes.
- Use a tailored, risk-based way of assessing security.
- Demonstrate validation of security to customers.

UL Solutions

Optional UL Certified CCSP Professional Exam

Participants who complete all three training days are eligible to take a two-hour certification exam. Those who pass the exam are individually certified as a UL Certified Cyber Security Professional (UL-CCSP), System Integrator, ISA/IEC 62443-3-3, -2-4. The training can be completed both in-person or remotely. Regarding remote training, we can schedule time slots convenient for you.

Upon successfully completing the UL-CCSP exam, participants will receive a certificate and badge that they can use to demonstrate their competence in ISA/IEC 62443-3-3 and -2-4. The certification is good for three years, after which individuals may recertify.

Target audience

- Project and product leaders
- Control systems engineers and managers
- System integrators
- Developers of control systems and software applications, network components for industrial automation and energy distribution and generation
- Test and validation engineers
- Programmers
- Compliance engineers

Why choose UL Solutions?

The knowledge you can trust – Our experienced staff will support you from the initial design stage of product development through testing and production with advisory, testing and certification services. Our experts can assist you in understanding the certification requirements for your specific markets.

Speed and efficiency – Our cost-effective systems and state-of-the-art facilities help accelerate your time to market.

Single-source provider – UL Solutions meets all your compliance needs and, by bundling safety, performance, security and interoperability services, also help save you valuable time and money.

Global reach and access – Our global network of expert engineers helps you understand your specific market application's various national and international requirements.

For more informatioin visit UL.com/IEC62443.

UL Solutions

Safety. Science. Transformation.™

IMS22CS618472
045.01.1122.EN.CYB