Design secure products and components in accordance with ISA/IEC 62443 with confidence

Cybersecurity training for engineers developing components and products for industrial applications based on ISA/IEC 62443-4-1 and 4-2

Course overview

The use of commercial off-the-shelf (COTS) technologies and the increase in the networking of industrial automation and control systems (IACSs) have exposed IACSs to similar vulnerabilities as information systems. The product supplier has a key role to play in the supply chain and the security of an IACS.

This three-day training course focuses on the ISA/IEC-62443 standard. The ISA/IEC 62443 series of standards was developed to secure IACSs throughout their life cycle. It currently includes several standards, technical reports (TRs) and technical specifications (TSs). Completing this interactive training for component and product manufacturers will help empower you to make educated 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 certification training has a core focus on Part 4 of ISA/IEC 62443, which provides detailed requirements for IACS products:

- 4-1 – Secure product development life cycle requirements
- 4-2 – Technical security requirements for IACS components

The course will also provide an overview of all the substandards and how they apply to your process and product cybersecurity assessment and certification needs as well as your required investment.

Training topics

- Introduction to ISA/IEC 62443
- Understanding the framework of ISA/IEC 62443
- Industry 4.0 trends and challenges
- Cyberattacks in IACS — vulnerabilities and consequences
- IACS concept, principal roles and architecture
- Security levels and maturity levels
- Secure life cycle view
- Defense in depth
- Zero trust
- Security for IIoT devices
- Security supply chain
- Risk assessment and management from a product perspective
- Threat modeling
- Vulnerabilities and countermeasures
- Challenges during IACS patch and update management
- Recommended requirements for IACS product suppliers
- Security design embracing ISA/IEC 62443 architecture

UL Solutions

- Security management
- 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:

- Help establish security by design for your systems and products
- Determine the right level of security for products and systems
- Execute product 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
- Make your components' security transparent and accessible to system integrators and end users
- Embed security into development processes
- Instill cybersecurity rigor into your processes
- Demonstrate validation of security to customers

Optional UL Certified CCSP Professional Exam

Participants who complete all three days of training are eligible to take an online certification exam. Those who pass the exam are individually certified as a UL Certified cybersecurity professional (UL-CCSP), product manufacturer, ISA/IEC 62443-4-1, -4-2.

Training can be completed in person or remotely. If completed remotely, the three days of training can be arranged in time slots convenient to you.

Upon successfully completing the UL-CCSP exam, participants will receive a certificate and badge that they can use to demonstrate their competence in the ISA/IEC 62443 4-1 and 4-2 IACS products. The certification is good for three years, after which point individuals may recertify.

Target audience

- R&D teams
- Developers of control systems, software applications and network components for industrial automation and energy distribution and generation
- Testers — test and validation engineers
- Programmers
- Project and product leaders
- Compliance engineers
- Procurement managers
- CISOs
- CIOs
- Functional safety experts with foundational knowledge in OT- or cybersecurity

Why choose UL Solutions?

Knowledge you can trust

Our experienced staff can support you from the initial design stage of product development through testing and production. 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 can help accelerate your time to market.

Single-source provider

UL Solutions can help you meet all your compliance needs and, by bundling safety, performance, security and interoperability services.

Global reach and access

Our global network of expert engineers can help you understand the various national and global requirements for your specific market application.

For more information, visit UL.com/IEC62443

UL Solutions

Safety. Science. Transformation.™

IMS22CS588927
044.01.1122.EN.CYB