Accelerate your cyber readiness with IEC 62443

Security certification for industrial automation and control systems (IACS)

Prepare for digitization with cybersecurity solutions

Greater pressure to demonstrate strong security practices

The growth of digitization in manufacturing and critical infrastructure demands that products become smarter and more interconnected. As a result, they also become more vulnerable to cyber threats. Network segmentation and firewalls for these components are no longer a sufficient means to address cyber threats due to the increased use of standardized hardware and software components in networked automation and control systems. Greater connectivity has added significant benefits to production such as data analytics, predictive and preventive maintenance, remote management and interoperability of systems. With these benefits also comes the added challenge of security of the control infrastructure from cyber threats.

Today, asset owners of plants or critical infrastructure are demanding suppliers of industrial automation systems to provide evidence of their security diligence in their practices and supply chain management. The IEC 62443 family of standards provides guidance for manufacturers and system integrators to build strong security measures into their processes to help mitigate these security risks for asset owners.

UL IEC 62443 solutions to fit your needs

UL has a suite of cybersecurity testing and certification services for IEC 62443 to fit your needs. The IEC 62443 family of standards has cybersecurity requirements for industrial automation control systems that a manufacturer or system integrator needs to instill cybersecurity rigor into their processes. Certification to these standards is an easy way to demonstrate to customers that your organization has done the due diligence of building cybersecurity into your processes and practices with a trusted third party.

The UL portfolio of cybersecurity services for IEC 62443 incorporates cybersecurity testing, including relevant tests required for a strong Secure Development Lifecycle (SDLC) process, certification to the published requirements of IEC 62443 and training.

UL Cybersecurity Assurance Program (UL CAP) for IEC 62443		
Testing	• Penetration testing • Source code analysis	• Vulnerability analysis • Fuzz testing
Certification	• IEC 62443-2-4 • IEC 62443-4-1	• IEC 62443-3-3 • IEC 62443-4-2 (pending publication)
Training	• IEC 62443 • Threat analysis	• Security best practices
Advisory	• Gap assessment	

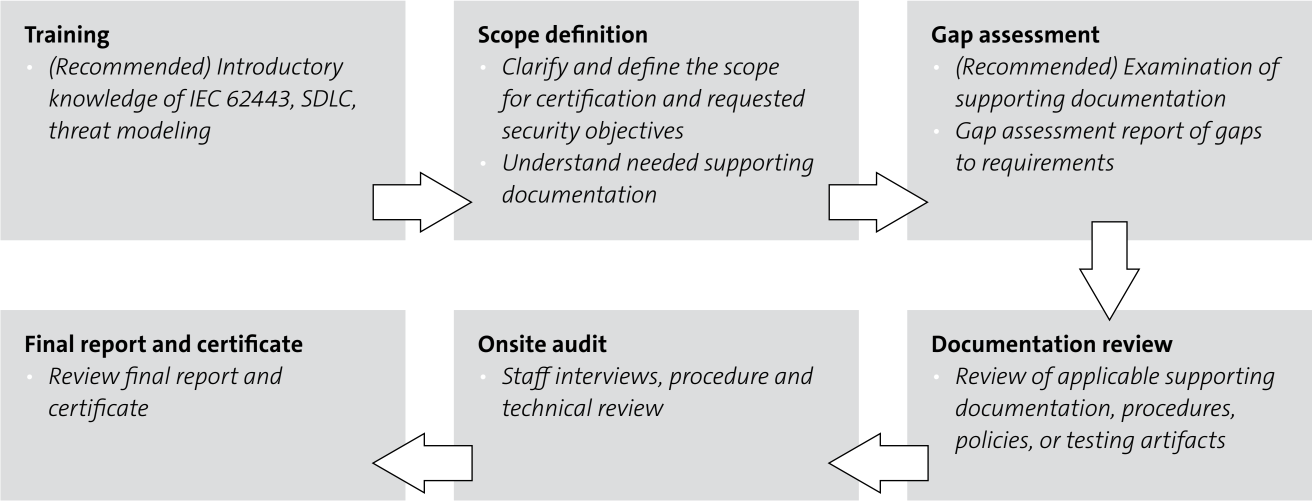
System integrators can take advantage of aligning organizational security practices with IEC 62443-2-4 or security functions with IEC 62443-3-3. Manufacturers can provide security assurance to customers of their secure software development lifecycle process utilizing IEC 62443-4-1 and security functions in IEC 62443-3-3. UL is with you every step of the way to guide you through the process - starting from defining the scope of security requirements to testing and certification.

Gain global market access

The IECEE, the IEC system for Conformity Assessment Schemes for Electrotechnical Equipment and Components, has created a conformity assessment scheme called the Industrial Cybersecurity Program for the IEC 62443-2-4, IEC 62443-4-1 and IEC 62443-3-3 standards. As a global certification provider, UL is an approved National Certification Body (NCB) able to issue CB test reports and certificates. This enables UL to provide testing and certification services for our ICS customers and stakeholders. With long term experience in cybersecurity, our security experts can guide you every step of the journey to achieving your desired security objectives.

Engage with UL early in the security journey

Whether you are ready to begin a certification project or if you would rather start with understanding IEC 62443 better, UL will guide you through the process.



Training
- *(Recommended) Introductory knowledge of IEC 62443, SDLC, threat modeling*

Scope definition
- *Clarify and define the scope for certification and requested security objectives*
- *Understand needed supporting documentation*

Gap assessment
- *(Recommended) Examination of supporting documentation*
- *Gap assessment report of gaps to requirements*

Documentation review
- *Review of applicable supporting documentation, procedures, policies, or testing artifacts*

Onsite audit
- *Staff interviews, procedure and technical review*

Final report and certificate
- *Review final report and certificate*

Why choose UL?

UL combines over a century of expertise in industrial automation control system safety and deep technical prowess in security testing and secure software development practices. We provide a standards-based Cybersecurity Assurance Program (CAP) for the full cybersecurity lifecycle with the greatest depth of cybersecurity expertise to our customers. UL has been an independent trusted provider of advisory, testing and certification services in safety and security for many stakeholders including government, asset owners, system integrators and manufacturers.

Knowledge You Can Trust – our experienced staff will advise you through the full cybersecurity lifecycle. Our experts can assist you in understanding the certification requirements for your specific markets.

Speed & Efficiency – utilizing over 160 cybersecurity tools,our cost-effective systems and state-of-the-art facilities cut through the red tape and help accelerate your time to market.

Single Source Provider – UL meets all of your compliance needs and, by bundling security, safety, performance and interoperability services, also helps save you valuable time and money.

Global Reach & Access – our global network of expert cybersecurity engineers helps you understand the various national and global requirements for your specific market application.

For more information visit UL.com/IEC62443 or email: ULCyber@ul.com

Empowering Trust™