Enhance your cyber readiness with IEC 62443 services

Cybersecurity for system integrators and maintenance service providers

Build trust with your customers through quality assurance

With the increased connectivity and use of standard communications protocols with Industry 4.0, the need to protect critical industrial systems, automation and controls from cybersecurity threats continues to increase dramatically. As a result, system integrators and maintenance service providers must be able to mitigate liability risk and sustain their manufacturers to the required security levels for brand protection. Integrating and maintaining your system to the necessary level of security is crucial in managing supply chain complexity and meeting customer requirements.

The IEC created the international IEC 62443 family of standards to protect industrial and control systems from security breaches. It aims to mitigate risks for industrial and facility communication networks and to build automation and controls by defining procedures for implementing electronically secure plants, facilities and systems across industries.

For industrial control system (ICS) integrators and users of control systems, compliance to the IEC 62443 family of standards is a powerful way to achieve increased brand protection and expanded competitive advantage.

UL Solutions provides cybersecurity compliance and advisory services for the entire supply chain from component manufacturers, system integrators and asset owners to end users.

Industries served

- Discrete manufacturing
- Process industry
- Oil and gas
- Renewables
- Automotive
- Power generation (electrical) and distribution (grid)
- Electrical and electronic equipment
- Pharmaceutical

Industry cybersecurity challenges

- Demonstrating validation of security to customers.
- Understanding and minimizing the risk of integrating Internet of Things (IoT) and operational technology (OT) infrastructure.
- Differentiating products and systems based on security.
- Confirming the purchase of secure systems and products.
- Integrating with insecure systems already in place.

UL Solutions

Applicability of IEC 62443

IEC 62443 family of standards				
Process industry and discrete manufacturing				
Manufacturers		**Integrators/service providers**		**Operators/owners**
IEC 62443 4-1	IEC 62443 4-2	IEC 62443 3-3	IEC 62443 2-4	IEC 62443 2-1

Our IEC 62443 services help to inspire confidence in the cybersecurity rigor of your processes and products. We offer a suite of cybersecurity advisory, testing and certification services for IEC 62443 standards to fit your security needs.

Benefits of IEC 62443 for system integrators and maintenance service providers

Updating and maintaining the system to the level of security required

Mitigating liability risks

Managing supply chain complexity and risk

Meeting customer demands with regards to requirements from specific industries

UL Solutions

Critical solutions for system integrators and maintenance service providers

Market enablement
As regulations continue to increase and become more restrictive, you must know the applicable regulations or requirements and how you can achieve and sustain compliance. UL Solutions offers expertise in cybersecurity and conformity assessment for industrial applications. We support market enablement and cybersecurity scoping for your organization globally as the first step in your cybersecurity journey.

Training
During an interactive training or tailored workshop, we will empower you to make educated choices based on the IEC 62443 standards, considering security issues related to your industrial control and automation system. We can customize your training to meet specific requirements, such as system architecture design, risk assessment and cybersecurity policy development. The workshops will dive into industry best practices, defining your road map for process and system cybersecurity assessment, certification needs and required investment.

Technical requirements workshop and compliance road-mapping
We provide interactive workshops and sit-down discussions to support mapping your business needs with technical requirements resulting in a robust cybersecurity road map for your systems. These sessions also include the compliance road map regarding standard applicability and efficient implementation across various systems and components mapped to multiple geographies.

Operational technology (OT) risk assessment
We can support industrial automation and control system (IACS) security requirements by assessing the likelihood of threats. We will evaluate the worst-case scenario if a cyber asset is compromised, supporting your goal to match your customer's needs related to the maturity level of OT systems. We can identify the risks related to the designed industrial automation and control systems and provide a holistic perspective from our OT cybersecurity experts, including the detailed report regarding risk assessment based on IEC 62443-3-2. The OT risk assessment service includes:

- Methodology overview.
- Vulnerability overview for the OT environment.
- Gap analysis between the plant's existing state and security requirements.
- Mitigation plan for the exposed risk level.
- Evaluating existing countermeasures and recommending additional countermeasures.
- Road map on how to develop or improve the security program.

Building the control system cybersecurity management system (CSMS) for IACS
We can support your organization in building your IACS cybersecurity management system to align with your CSMS related to IEC 62443-2-1.

This service includes various elements from four main categories:

- Risk analysis.
- Addressing risk with the CSMS.
- Monitoring and improving the CSMS.
- Mapping between ISO/IEC 27001 and IEC 62443-2-1.

Gap analysis
We offer a constructive review that will provide you with the differences between your current and desired state for meeting IEC 62443-2-4 and IEC 62443-3-3 requirements, considering the maturity level goals of the organization or security level goals of your systems. Results are provided in a gap analysis report that can be customized to include testing.

Documentation review and support
We can provide IEC 62443-oriented documentation reviews to support you in achieving the desired maturity/security level. We use a four-level metric to indicate the level of readiness of the defined processes and technical documentation. We can propose security-relevant changes to make the document support the essential requirements and enhancements. Our team will advise you on the following activities before and after the submission of your project documentation to the auditors:

- Advise on writing conformity statements.
- Conformity evidence.
- Final document review.
- Support the team's gap closures.
- Prepare the team for auditor interviews.

Certification
We can assess and certify system integrators and maintenance service providers to give confidence to plant owners and operators. We offer assessment and certification options to respond efficiently and sustainably to your needs.

Surveillance and inspection
Our surveillance and inspection services help verify if you took sufficient security measures to maintain your certification status. At the end of the inspection, you will receive a report with the results you can use to determine the right actions to help demonstrate the maturity and security level meets the set goals.

For service providers and system integrators, certification to IEC 62443 standards helps you demonstrate your security compliance to a wide range of target markets and customers.

UL Solutions is ANAB accredited according to IEC 17065 and IEC 17025, which implements ISASecure® certification processes and provides conformity assessments as per IEC 62443 for industrial cybersecurity certification with the ISASecure scheme. Therefore, we can conduct cybersecurity assessments as an accredited ISASecure certification body (CB).

Additionally, we are a CB Testing Laboratory (CBTL) in the CB Scheme for IEC 62443. Our experts can deliver cybersecurity assessment and certification services to IEC 62443 standards under the IECEE CB scheme. The CB Scheme includes some of the sub-standards in the IEC 62443 framework, for assessment and certification.

Complimentary to the IECEE CB and ISASecure schemes, UL Solutions operates its Cybersecurity Assurance Program (CAP), which leads to UL Solutions-issued IEC 62443 certificates.

Finally, we can assess other requirements at your request, such as product specifics, cyber aspects of intended use, contractual requirements between operator and system integrator, for instance, or regulatory requirements (federal, state, or regional), resulting in a more robust cybersecurity strategy. We can also offer other training and advisory services that address secure product development, cybersecurity in smart ecosystems and supply chain risk management

For more information on UL Solutions IEC 62443 cybersecurity services, visit UL.com/IEC62443.

UL Solutions

Safety. Science. Transformation.™

IMS23CS1206271
039.02.0823.EN.CYB