Enhance your cyber readiness with IEC 62443 solutions

Cybersecurity for system integrators and maintenance service providers

Build trust with quality assurance across your supply network

With the increased connectivity and use of standard communications protocols that come with Industry 4.0, the need to protect critical industrial systems, building automation and controls from cybersecurity threats continues to increase dramatically. As a result, system integrators and maintenance service providers need to be able to mitigate liability risk and uphold their manufacturers to required security levels to ultimately protect your own brand. The ability to integrate and maintain your system to the level of security required is crucial in managing supply chain complexity and meeting customer requirements.

The international IEC 62443 family of standards was created to lay the foundation of cybersecurity robustness. It aims to mitigate risks for industrial and building communication networks, building 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.

Industries served

- Oil and gas
- Renewables
- Energy and power
- Utilities
- Electrical and electronic equipment

Industry cybersecurity challenges

- Demonstrating validation of security to customers
- Understanding and minimizing risk of integrating Internet of Things (IoT) and Operational Technology (OT) infrastructure
- Differentiating products/ systems based on security
- Ensuring purchase of secure systems and products
- Integrating with insecure systems already in place

We help support those efforts with assessments of your procedures and policies, following IEC 62443-2-4. Moreover, we offer an assessment for organizations integrating ICS systems and components in which we verify the secure way in which these products are deployed within the network, following IEC 62443-3-3.

Applicability of IEC 62443

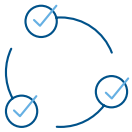
IEC 62443 family of standards				
Process industry and discrete manufacturing				
Manufacturers		**Integrators/Service providers**		**Operators/Owners**
IEC 62443 4-1	IEC 62443 4-2	IEC 62443 3-3	IEC 62443 2-4	IEC 62443 2-1

Our IEC 62443 cybersecurity solutions help to instill cybersecurity rigor into your processes and systems. We offer a suite of cybersecurity 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

Enhancing brand protection

Key IEC 62443-2-4 and IEC 62443-3-3 solutions

Training
During an interactive training or tailored workshop, we will empower you to make educated choices based on the IEC 62443 family of standards, taking into account security issues related to control and automation systems. The course will dive into industry best practices, defining your roadmap for process and system cybersecurity assessment and certification needs and required investment.

Gap analysis
We can provide a constructive review that will provide you with the differences between your current and desired state for meeting IEC 62443 sub-standards. Results will be provided in a gap analysis report that can be customized to include testing if necessary or requested.

System security architecture review
We can identify the potential risks or gaps relative to IEC 62443 sub-standards, which we will then take into account to conduct your customized security design and architecture review.

Certification
We can assess and certify system integrators and maintenance service providers to give assurance to plant owners and operators. We offer a choice of assessment and certification options to respond to your needs in the most efficient and sustainable way.

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 that will help ensure the security level meets the set goals.

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

We are a recognized leader in cybersecurity assessment and certification services to UL 2900 and IEC 62443 standards, including through the UL Cybersecurity Assurance Program or CAP, and other training and advisory services that address secure product development, cybersecurity in smart ecosystems and supply chain risk management.

For more information on UL's IEC 62443 cybersecurity solutions, email us at IMSecurity@UL.com or visit IMS.UL.com/IEC62443.

Empowering Trust®