

Accelerate your cyber readiness with IEC 62443 services

Cybersecurity for component manufacturers

Demonstrate the cybersecurity posture of your organization and products to system integrators, operators and facility owners

Digital technologies have successfully penetrated the manufacturing sector and continue to do so at an ever-increasing rate. This merging of the cyber and physical worlds means improved efficiency and flexibility, but also increases the exposure of your critical manufacturing infrastructure to cyber risks. As a component or product manufacturer, it's crucial to understand how to assess the security of product quality and manage security risks to navigate the cybersecurity of your factory automation and process controls. Proving the security of your product to your customer is essential.

The IEC created the international IEC 62443 family of standards to lay the foundation of cybersecurity robustness. It aims to mitigate risks for industrial communication networks by defining procedures for implementing electronically secure plants, facilities and systems across industries.

For component and product manufacturers, compliance with IEC 62443 standards can help demonstrate the security of your systems and components and enhance your market position. UL Solutions offers assessments focused on your product and manufacturing development procedures (following IEC 62443-4-1) and the individual product's security functionalities and robustness.

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



Industries served



Manufacturing



Oil and gas



Renewables



Automotive



Power generation (electrical) and distribution (grid)



Electrical and electronic equipment



Pharmaceutical

Industry cybersecurity challenges

- Embedding security into development processes
- Determining the right level of security for products/systems
- Demonstrating validation of security to customers
- Differentiating products/systems based on security
- Meeting the evolving demands of asset owners and system integrators

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 services can help you instill cybersecurity rigor into 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 certification for component manufacturers



Assess the security and quality of the product.



Prove to customers that you implemented a required security level in an efficient way.



Provide a competitive advantage.



Gain recognition for high standards of cybersecurity.

Key services for component manufacturers

Market enablement

As regulations continue to increase in number and become more restrictive, it is essential to be aware of the regulations or requirements driving customer demands, learn which apply and understand how you can achieve and sustain compliance. UL Solutions offers expert knowledge in cybersecurity standards, conformity assessments and regulations in industrial applications. We can 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 family of standards, taking into account security issues related to components used in control and automation systems. We can customize our training to meet your specific requirements, such as secure product development life cycle, maturity level in your process and security level in your products. The workshop will also cover an overview of all the substandards and how they apply to your efforts to define your road map for process and product cybersecurity assessment and certification needs, as well as the investment it will require from you.

Gap analysis

We offer a constructive review that will detail the differences between your current and desired state for meeting IEC 62443-4-1 and IEC 62443-4-2 requirements, considering your organization's security-level goals. We can also customize your gap analysis report to include testing.

Technical requirements workshop and compliance road mapping

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

Documentation review and support

We can provide IEC 62443-oriented documentation reviews to support you in achieving your desired 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 can advise you on the following activities before and after you submit your project documentation to the auditors:

- Writing conformity statements
- Conformity evidence
- Reviewing the final documentation
- Supporting the team in closing any gaps
- Preparing the team for interviews with auditors

Penetration testing

Our penetration tests provide clear insights into the security level of your product, system and infrastructure. After the penetration test, you will receive a report with the test results, including demonstrated vulnerabilities within your product, system and infrastructure.

Certification

We can assess the conformity of your product to various IEC 62443 substandards that best fit your individual needs in terms of efficiency and cost. We can work with you to develop a sustainable conformity assessment and certification strategy that considers your supply chain needs, existing and upcoming regulatory requirements and local recommendations.

Surveillance and inspection

Our surveillance and inspection services can help determine whether you took sufficient security measures to maintain your certification status. At the end of the inspection, you

will receive a report you can use to determine the actions that will help ensure that your security level meets your set goals.

For product and component manufacturers, compliance with IEC 62443 standards helps you demonstrate your security compliance to a wide range of target markets and customers.

Our experts can help define your road map for process and product cybersecurity assessment and certification services to UL 2900, the Standard for Software Cybersecurity for Network-Connectable Products, and IEC 62443 standards. Additionally, we are a CB Testing Laboratory (CBTL) in the CB Scheme for IEC 62443. Talk to us about the UL Cybersecurity Assurance Program (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 Solutions' IEC 62443 cybersecurity services, visit [UL.com/IEC62443](https://www.ul.com/IEC62443).



Safety. Science. Transformation.™

© 2022 UL LLC. All rights reserved.
IMS22CS517113
038.01.0922.EN.CYB