Accelerate your cyber readiness with IEC 62443 solutions

Cybersecurity for component manufacturers

Demonstrate your cybersecurity posture to system integrators and end users

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, but also results in an increased exposure of your critical manufacturing infrastructure to cyber risk. As a component or product manufacturer, it's important 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 international IEC 62443 family of standards was created 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 to IEC 62443 standards can help demonstrate the security of your systems and components and enhance your market position. We offer assessments focused on your product and manufacturing development procedures (following IEC 62443-4-1) as well as on the security functionalities and robustness of the individual product components (following IEC 62443-4-2).

Industries served

- Manufacturing
- Oil and gas
- Renewables
- Automotive
- Energy and power
- Electrical and electronic equipment

Industry cybersecurity challenges

- Embedding security into development processes
- Determining right level of security for products/systems
- Demonstrating validation of security to customers
- Differentiating products/systems based on security

Applicability of IEC 62443

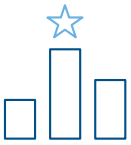
IEC 62443 family of standards				
Process industry and discrete manufacturing				
Manufacturers		**Integrators/Service providers**		**Operators/Owners**
IEC 62443 4-1	IEC 62443 4-2	IEC 62443 3-3	IEC 62443 2-4	IEC 62443 2-1

Our IEC 62443 cybersecurity solutions help to instill cybersecurity rigor into your processes and products. We offer a suite of cybersecurity 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 IEC 62443-4-1 and IEC 62443-4-2 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 also cover an overview on all the sub-standards and how they apply to you for defining your roadmap for process and product cybersecurity assessment and certification needs, and required investment.

Gap analysis
We can provide a constructive review that show you 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.

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 results of the test including demonstrated vulnerabilities within your product, system and infrastructure.

Certification
We can assess the conformity of your product to various IEC 62443 sub-standards 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, taking into consideration supply chain needs, existing and upcoming regulatory requirements and local recommendations.

Surveillance and inspection
Our surveillance and inspection services verify if 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 the security level meets the set goals.

For product and component manufacturers, 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 defining your roadmap for process and product cybersecurity assessment and certification services to UL 2900 and IEC 62443 standards. 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's IEC 62443 cybersecurity solutions, email us at IMSecurity@UL.com or visit IMS.UL.com/IEC62443.

Empowering Trust®

UL and the UL logo are trademarks of UL LLC © 2020.
0820