Contact us

IEC 62443-4-1 and IEC 62443-4-2 standards for Industrial Cybersecurity

Thanks to our IECEE CB testing laboratory, jtsec Applus+, authorized for industrial cybersecurity, we can provide security evaluations for components and products under IEC 62443-4-1 and IEC 62443-4-2 standards.

The IEC 62443 Series for Industrial Cybersecurity

The IEC 62443 series of standards, introduced by the International Electrotechnical Commission (IEC), aims to safeguard industrial automation and control systems (IACS) through comprehensive guidelines and best practices. There are two specific standards in the series that address IAC components cybersecurity: **the IEC 62443-4-1 and IEC 62443-4-2.**

To demonstrate compliance with these 2 standards, manufacturers can subject their products to testing and certification under the IEECE CB Scheme, a global program applicable in over 50 countries.

IEC 62443-4-1 and IEC 62443-4-2 standards

Evaluation and certification under the IEC 62443-4-1 standard cover the secure development and lifecycle of the product. On the other hand, the IEC 62443-4-2 standard focuses on the security requirements for components like embedded devices, network components, host components and software applications.

Main requirements of IEC 62443-4-1 and IEC 62443-4-2 standards

Applus+ Laboratories provides evaluation and certification for the following standards:

IEC 62443-4-1

Requirements for product lifecycle development. These 47 process requirements work to secure development of IACS device products throughout their life cycle. There are four maturity levels, showing the requirements that have been evaluated and their level of maturity.

Maturity Level	IEC 62443-4-1 Description
Initial	• Product development is not (or not fully) documented. • There is no consistency between projects • There is no repeatability processes
Managed	• Manage development according to written policies. • Evidence of experience/training of staff who will carry out the process. • You have updated your procedures to conform to this document, but have not yet implemented all of them. • Development will always be done according to documented plans, even in times of stress.
Defined	• Performance can be replicated throughout the supplier's organization. • The processes have been practiced. • Evidence exists to demonstrate this practice.
Improving	• Using appropriate process metrics, product suppliers monitor product efficiency and performance and demonstrate continuous improvement in these areas.

IEC 62443-4-2

Technical Security Requirements for IACS components. A catalog of 141 requirements that should be met by industrial components. It has four security levels depending on established requirements to be met. More information at the jtsec Applus+ official site.

Security level	Attack type			
	Violation Type	Means Type	Resource Level	Motivation

SL-1	Coincidental	N/A	N/A	N/A
SL-2	Intentional	Simple	Low	Low
SL-3	Intentional	Sophisticated	Moderate	Moderate
SL-4	Intentional	Sophisticated	Extended	High

IEC 62443-4-1 and IEC 62443-4-2 Evaluation and Certification Process

IEC 62443-4-1 and IEC 62443-4-2 evaluation involves the vendor, the testing laboratory and the certification body.

The first step is preparing our organization to ensure a successful certification. We can help you with a Gap Analysis and support the development of the relevant documentation.

Then, the vendor must make a formal request for certification and evaluation to a National Certification Body (NCB). This NCB will then proceed to process the application and assign a CB Testing Laboratory (CBTL) to oversee conducting the evaluation.

As a CBTL, jtsec Applus+ forms an essential part of this process. Our job is to evaluate the product and issue a test report. Before issuing a certificate, an NCB ensures everything is in order by reviewing and validating this test report. Right now, we work with an external NCB, but Applus+ Laboratories is in process to become NCB for IEC 62443-4-1 and IEC 62443-4-2.

If the applicant wants to receive an additional certificate from a national certification body, they can do so by sending their certificate, alongside the test report to any other NCB.

Benefits of IEC 62443-4-1 and IEC 62443-4-2 standards for Industrial Cybersecurity

The IEC 62443-4-1 and IEC 62443-4-2 certificate ensures the product's resilience against cybersecurity threats. This in turn helps strengthen security through its whole lifecycle and builds market acceptance and trust amongst the integrator and end-users (the asset owner).

Additionally, it facilitates product acceptance across markets. More than 50 countries form part of and participate in the IEC CB Scheme certificate. The acquired mutual recognition from this certification helps reduce the number of tests and avoids differentiations in criteria certification among countries.

Why choose Applus+ Laboratories for IEC 62443-4-1 and IEC 62443-4-2 standards for Industrial Cybersecurity

We are experts in a wide range of cybersecurity industries. Here's why we're your best choice:

- We know your time to market is important. Our engineers will be dedicated to meeting deadlines and expectations.
- We are one of the leading labs in product cybersecurity worldwide, and we participate as editors in the ERNCIP thematic group for 'Industrial Automation and Control Systems (IACS) and we are members of the ECSO Working Group 'Standardization, Certification and Supply Chain Management' as well as many other standardization committees.
- We are also CBTL and NCB for electrical safety, covering a wide range of equipment.