Quick guide for Machine Builders

Real vs. Fake: How to recognize a valid cybersecurity certificate

Why it's important to understand the difference

In today's industrial landscape, cybersecurity is no longer a value-add but a market and regulatory requirement. However, not all documents that look like certifications actually are. Understanding the difference helps you choose reliable suppliers and avoid technical, legal, and reputational risks.

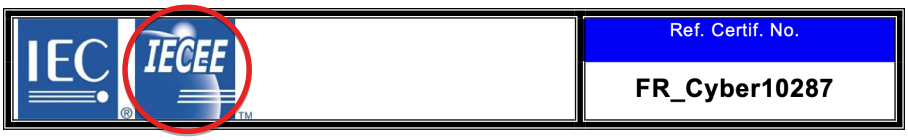
General certifications like ISO 27001 certify the company's organization, but they do not certify that a specific product is secure against cyberattacks. For that, you need a **specific Product Certification (IEC 62443-4-2).** Don't assume the hardware is secure just because the supplier has an ISO 27001 badge. Always check for the **specific IEC 62443 certificate** of the component itself.

What a real certification is

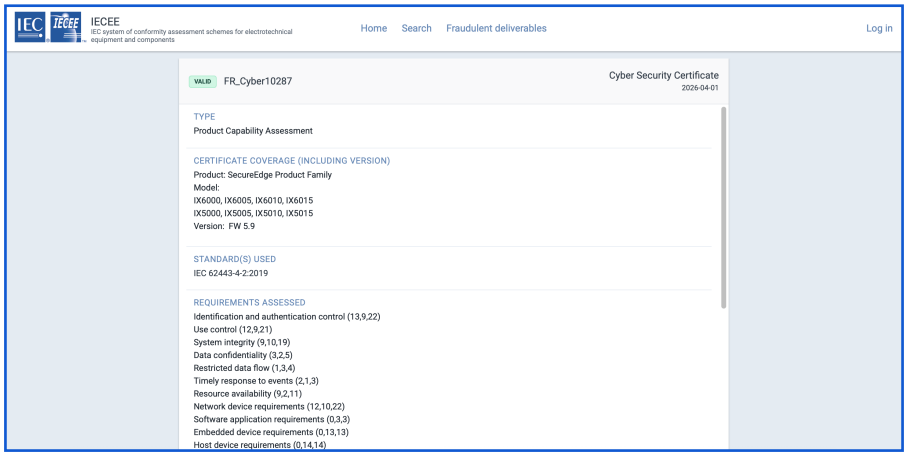
If you take a look at our **IEC 62443-4-2 certificate,** you can see the features of an authentic industrial cybersecurity certification:

- It's issued by an independent accredited certification body (e.g., Bureau Veritas, TÜV, or UL):

- It follows an official international scheme, such as the one managed by the **IECEE** (IEC system of conformity assessment schemes for electrotechnical equipment and components):



- It can be publicly verified through global databases:



- **It clearly specifies:**
  The exact standard certified (e.g., a specific part of the standard) and the Security Level or Maturity Level achieved, according to the type of certification:

Standard	IEC 62443-4-2:2019
Requirements Assessed *The 3-tuple represents (Passed requirements, requirements assessed as Not Applicable, Total number of requirements)*	Identification and authentication control (13,9,22) Use control (12,9,21) System integrity (9,10,19) Data confidentiality (3,2,5) Restricted data flow (1,3,4) Timely response to events (2,1,3) Resource availability (9,2,11) Network device requirements (12,10,22) Software application requirements (0,3,3) Embedded device requirements (0,13,13) Host device requirements (0,14,14) Security Level: SL2

- The product or component covered:

Certificate Coverage (including Version)	Product: SecureEdge Product Family Model: IX6000, IX6005, IX6010, IX6015 IX5000, IX5005, IX5010, IX5015 Version: FW 5.9

Think of it like a driver's license. A 'Declaration' is just your friend saying you drive well. A 'Certification' is the official document issued by the government after you passed the exam.

The red flags of 'self-declaration'

A declaration of conformity or non-accredited statement:

- May be issued by a consultancy firm or unauthorized third parties.
- Does not involve recognized independent audits.
- Often lists multiple standards (e.g., NIST, BSI, OWASP) without actually certifying any of them
- Cannot be verified in official registries.

In short: it's a declaration, not proof.

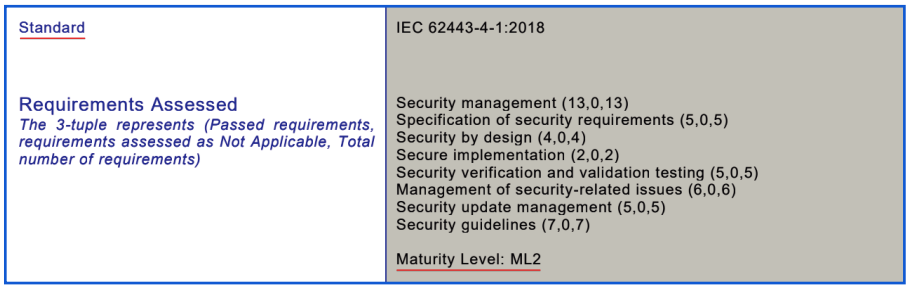
How to quickly verify a supplier

When a supplier claims to be certified, always request the following elements, which can be found for example in our **IEC 62443-4-1** certificate on secure software development:

- Official certificate number:

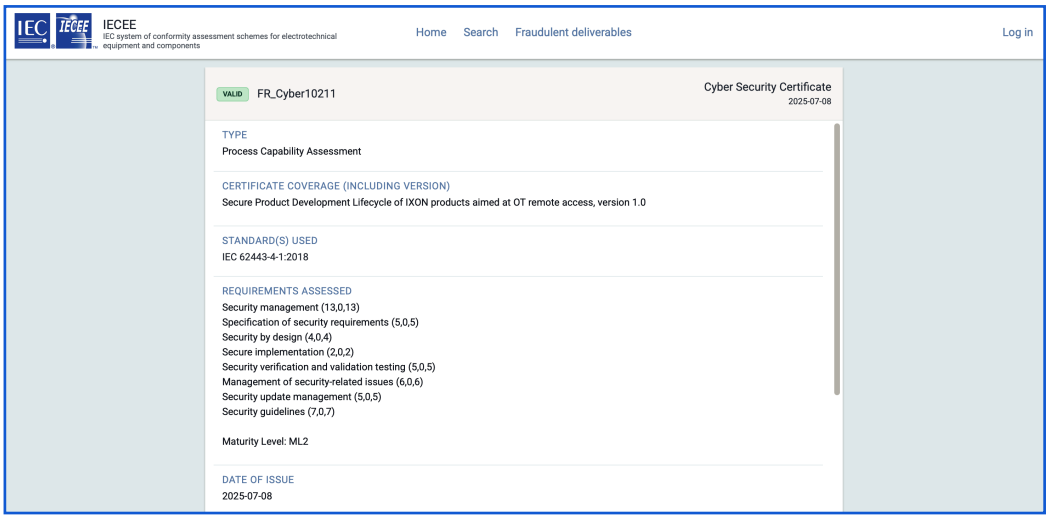
- Issuing body:

- Standard and Security Level or Maturity Level, depending on the certification:



- link to the public registry: **certificates.iecee.org**

Example:



If they cannot provide these, or a direct link to the certificate in the registry, it is likely not a real certification.

How IXON supports machine builders

A real certification demonstrates compliance verified by independent third parties. Using certified industrial components facilitates the **IEC 62443-3-3** certification process for the machine, which is increasingly requested by end customers in the industrial sector.

In fact, new European regulations increasingly refer to IEC requirements. By using components that are already IEC-certified, it is possible to demonstrate compliance more quickly with the obligations set out by **NIS2**, the **Cyber Resilience Act** (CRA), and the new **Machinery Regulation (EU) 2023/1230.**

Want to know more about IXON certifications and products?

Check our Trust Center or contact your account manager.

trust.ixon.cloud ›

IXON