IEC 62443 certification: Cyber Security for Industrial Automation & Control Systems (IACS)

Digitalisation and technological developments offer great opportunities for manufacturing industries. However, if not properly secured, threats and risks can arise which may lead to cyberattacks or disruption of processes. Daily operations and business continuity could potentially be halted resulting in different types of unfavorable outcomes. The IEC 62443 certification of your Industrial Automation and Control Systems (IACS) is a substantial way to address key cyber security aspects of industrial systems.

Kiwa's experts combine IEC 62443 knowledge with extensive cyber security experience to improve the digital security and safety of your IACS environment, ensuring secure operations now and in the future. Implementing the standard improves the cyber security level of your organisation's OT/ICS/SCADA environment.

What is the IEC 62443 standard?

The IEC 62443 standard is intended to secure Industrial Automation and Control Systems (IACS). It provides a systematic and practical approach that covers every aspect of cyber security for industrial systems. There are four parts to the IEC 62443 standard, which aim at four different IACS levels: General, Policies & procedures, System and Components. The following image illustrates how the different parts fit in relation to each other:

On a general level the IEC 62443 certification audits address three main topics for arranging cyber security in the OT (Operational Technology) domain: human interactions, technologies and policies & procedures involved in the operation of the industrial process that can affect or influence its safe, secure, and reliable operation. The CIA triad (Confidentiality, Integrity and Availability) of cyber security can also be traced back across the different parts of this standard.
The IEC 62443 focuses on Operational Technology (OT) and this link is similar to that of the ISO 27001 in relation to Information

Cyber security Certification
Kiwa Nederland
NL.CyberSecurity.Certification@kiwa.com
+31 (0)88 998 33 70

Technology (IT). However, there are also important differences. Within IT, confidentiality of data is essential. While within OT aspects such as integrity and availability are paramount, as these play a major role in aspects such as health, safety and environment. This makes it necessary to view integral cyber security from the perspective of both domains.

IEC 62443 certification by Kiwa

An IACS includes more than the technology that comprises a control system. It also includes the people and work processes needed to ensure the output, safety, integrity, reliability and security of the control system. Without sufficiently trained people, risk-appropriate technologies and countermeasures and work processes throughout the security lifecycle, an OT environment could be more vulnerable to several types of cyberattacks. Therefore it is becoming increasingly important for organisations to arrange the cybersecurity of their OT environment. Although several measures can be taken, getting certified according to the framework of the IEC 62443 standards offers a good head start for cybersecurity in OT environments. Kiwa helps by certifying your component, system or organisation depending on your role as a stakeholder within an OT-environment.

Four IEC 62443 roles and layers of responsibilities

The IEC 62443 defines four distinct layers of responsibilities which are eligible for certification. Your business or organisation can fit any of these four categories:

1. Asset Owners: Operate and maintain site-specific OT systems. For certification of asset owners subparts: IEC 62443-2-1, IEC 62443-2-4 and IEC 62443-3-2 are applicable.
2. System Integrators: Engineer and integrate different industrial solutions, parts and components into site-specific systems. The IEC 62443-2-4 and IEC 62443-3-3 are subparts which are applicable for certification of system integrators.
3. Automation Suppliers: Design and manufacture industrial solutions, parts and components which are supplied to asset owners. The subparts which are applicable for automation suppliers certification are: IEC 62443-2-4, IEC 62443-3-3 and the IEC 62443-4-1.
4. Automation Products: These are products or components which are used in site-specific systems. Commonly they are also delivered to asset owners by a supplier. For certification the IEC 62443-4-2 is used as a basis.

The following steps are taken into account for IEC 62443 certification by Kiwa:

1. Depending on the subject that needs to be certified, Kiwa requests the necessary documentation according to either one of the four previously specified roles/categories.
2. Based on these documents Kiwa starts the first assessment in order to measure the compliance of your organisation to a subpart(s) of the IEC 62443.
3. After the first assessments, Kiwa performs an on-site audit together with your employees who are responsible for the cyber security aspects of your organisation.
4. If there are discrepancies or doubts, the customer is requested to clarify or resolve these.
5. If there are no doubts left and compliance can be proven, Kiwa proceeds to issue a certificate of conformity for the subpart(s) of the IEC 62443 of the assessments.

Take the extra leap in protecting your business or organisation

Cyber security Certification
Kiwa Nederland
NL.CyberSecurity.Certification@kiwa.com
+31 (0)88 998 33 70

With digitalisation, internet technology and everything surrounding it, cyber security has become something organisations should not take lightly. For the OT/industrial domain the IEC 62443 offers handles to optimise the cyber resilience of your components and systems.
Ultimately, any organisation involved in industrial automation, irrelevant of the scale, can benefit from the IEC 62443 audit. An IEC 62443 certificate enables you to proof that your industrial system or component is safe and secure against cyber security threats. IEC 62443 certification by a trusted independent third-party demonstrates to your stakeholders that the cyber resilience of your OT system is addressed according to a leading standard. By doing so you are taking the extra leap in protecting your customers, systems, organisation and business.

Why Kiwa?

Kiwa has been involved in various ways in industrial systems and installations for a long time. For example testing and certifying HVAC parts and systems, performing FPC audits in factories and assessing involved personnel. Addressing systems according to the IEC 62443 certificate requires in-depth knowledge and experience in both the digital domain and industrial automated systems. Moreover, an approach that addresses the complete digital landscape of IACS or SCADA systems ensuring cyber security is essential.
By partnering with Kiwa you are ensured of a third party which has the right proficiency to assist you with your IEC 62443 certification. Our experts are also properly trained and experienced in industrial automation systems as well as cyber security. We are your partners for progress!

Cyber security Certification
Kiwa Nederland
NL.CyberSecurity.Certification@kiwa.com
+31 (0)88 998 33 70