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

Digitalization and the Internet of Things (IoT) offer great opportunities for manufacturing industries. However, if not properly secured they can cause vulnerability, leading to cybercrime and attacks by hackers. This can seriously damage daily operations and business continuity. IEC 62443 certification addresses all cybersecurity aspects of industrial systems, ensuring secure operations now and in the future. Kiwa's experts combine IEC 62443 knowledge with extensive cyber security experience, enabling you to be as secure as you need to be.

What is IEC 62443 certification?

The IEC 62443 (or ANSI/ISA 62443) standard is intended to secure Industrial Automation and Control Systems (IACS). It provides a systematic and practical approach that covers every aspect of cybersecurity for industrial systems. There are four series of IEC 62443 standards, aimed at four different IACS levels: General, Policies & procedures, System and Components. Which standards apply to each level is made clear in the image below.

The IEC 62443 audit addresses all human resources, ICT and policies 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 cybersecurity can also be traced back in these standards. In comparison, the ISO 27001 focuses on Information Technology (IT) and the IEC 62443 focusses on Operational Technology (OT).

Four IEC 62443 security levels

An IACS includes more than the technology that comprises a control system. It also includes the people and work processes needed to ensure the 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 IACS could be more vulnerable to a cyberattack.
One of the ways the IEC 62443 standards approach the cybersecurity of OT systems is by making use of security levels. It defines four security levels (SL): from SL 1 (Casual or Coincidental violations) to SL 4 (Nation State). The security levels ensure systems are classified based on their inherent risks. The compromise of one industrial system will have less or more of a disastrous impact than another. However, all of these modern industrial systems need to have their processes, technology and human interaction in proper order to be resilient against cyber threats.

Take the extra leap in protecting your business

With digitalization, internet technology and everything surrounding it, cyber security has become something organizations should not take lightly. The IEC 62443 series of standards are targeted towards ‘end users’ and ‘solution providers’. However, the term ‘solution provider’ is coined broadly and essentially refers to manufacturers, system integrators and vendors.
Many industrial organisations have ‘legacy’ equipment (i.e. mechanical systems). Legacy equipment is often outdated and custom-made. Many times it forms the basis upon which developments are made and is therefore difficult to replace due to the investment required. But also legacy equipment should be secured well, even if no direct web connection exists. After all, viruses, etc. can also be spread via an usb stick. In modern industrial systems, equipment tends to be more up-to-date.
Ultimately, any organization 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 cybersecurity threats. By doing so you are taking the extra leap in protecting your customers, system 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 cybersecurity is essential. At Kiwa we are adept in all the aspects required for properly assessing systems according to the IEC 62443. Our experts are also properly trained and experienced in industrial automation systems as well as cybersecurity. We are your partners for progress!

Kiwa N.V.
Sir Winston Churchill-laan 273
2288 EA Rijswijk
P.O. Box 70
2280 AB Rijswijk
info@kiwa.nl