

International cyber security certification



The rapid development of the digitalization of everything brings with it many challenges. In the forefront is the ever-increasing concern

of cyber security to protect against threats to the electronic systems that have become so vital to users. Both industry and governments are continuously seeking ways to reduce the risks.

The security of digital systems is an increasing concern not only for businesses, government and defense, but to individuals and society in general.

IEC Standards and Conformity Assessment Systems

Testing and third-party assessment of products and systems to relevant standards may play a vital role in addressing those concerns, and international initiatives are taken in this regard.

Industry is a major contributor in the development of IEC Standards and is also one of the primary stakeholders in the IEC Conformity Assessment (CA) Systems, along with regulators and the operating testing/certification bodies.

IEC Standards for cyber security deal with specific sectors. The IEC 62443 series focusses on operational technology (OT) to ensure critical systems (e.g. electrical supply) operate as intended, and the ISO/IEC 27000 series addresses how to manage the security of information technology (IT) to ensure secure flow and accuracy of data.

Both are needed and complement other sector-specific standards such as the IEC 62351 series for the electrical energy sector.

The IECEE cyber security certification programme

Among the IEC CA Systems, the IECEE CB scheme has a programme to test and certify cyber security of electrotechnical products and systems in the electrotechnical sphere, based on applicable IEC Standards.

Although this programme was originally developed for the industrial automation sector, it can be applied to any sector with critical infrastructure, including medical, utility and automotive.

More information about the IECEE cyber security certification programme can be found in the IECEE operational document OD 2061 at www.iecee.org.

International solution for regional needs

An example of a governmental step taken in this context is the EU cyber security certification framework.

This calls for certification solutions that can attest that products and services with information and communication technology (ICT) comply with specified cyber security requirements. They should be recognized in all member states, thus making it easier for businesses to trade across borders and for purchasers to understand the security features of the product or service.

Within this European framework, it is stated that international standards and certification schemes shall be used as much as possible, to avoid creating trade barriers and to ensure coherence with international initiatives.

Other IEC cyber security activities

—
Additionally, IEC is also working with the United Nations to create a common international regulatory framework for cyber security. The UN recommends employing global cyber security certification services, such as those offered by IECEE, when available and appropriate.

IECEE also cooperates with IECQ, the IEC Quality Assessment System for Electronic Components, regarding certification of cyber security management systems in the electrotechnical sector, particularly also related to supply chain management systems. Find out more at www.iecq.org/about/ap-scheme.

For more information on cyber security visit basecamp.iec.ch.



IEC System of Conformity
Assessment Schemes
for Electrotechnical Equipment
and Components

3 rue de Varembe
PO Box 131
CH-1211 Geneva 20
Switzerland

T +41 22 919 0211
secretariat@iecee.org
www.iecee.org