Secura

A BUREAU VERITAS COMPANY

INDUSTRIAL PRODUCTS STANDARDS AND CERTIFICATION

What are the best options for your products?

SECURA

Vestdijk 59
5611 CA Eindhoven
Netherlands

Karspeldreef 8
1101 CJ Amsterdam
Netherlands

T +31 (0)88 888 3100
E info@secura.com
W secura.com

Follow us on

1. Industrial Products & Threats Landscape

Industrial Control Systems (ICS) can be found in many nations' critical infrastructures. These include nuclear plants, oil & gas industry, transportation, chemicals processing, and other process industries. Examples of such systems can be Distributed Control Systems (DCS), Programmable Logic Controllers (PLC), smart meters or Supervisory Control and Data Acquisition systems (SCADA). Due to their wide spread, as well as the criticality of domains in which they are used, the security of Industrial Control Systems and components should be equally taken into account, together with other aspects such as performance or safety.

The importance of cybersecurity in modern industrial environments has come even further into discussion in light of recent practical attacks that have been put in place. While these attacks are highly targeted and sometimes also involve state actors, they do raise concerns about the security capabilities of the off-the-shelf products, as well as the larger systems in which these are further embedded.

Finally, it needs to be kept in mind that the security of an industrial site is in the end as strong and the weakest link included in that site. Even if some industrial components do not have a key role in the architecture of the site (or are not used in a key role), exploiting a vulnerability embedded into such components can be sufficient for attackers to get access to much more high-risk elements of the system.

Finally, industrial components have also another characteristic that other market domains do not always share: they should be made to last. In the industrial domain, it is not common to change the PLCs or the DCS systems in the organization every couple of years. On the contrary, it is expected that these components will be integrated and used with high performance for an extensive period of time. That being said, it is critically important not only that these components and systems come without vulnerabilities the moment when they are bought, but they are also able to keep their security in time, for example by means of patches or software updates. All of these put together result in a very particular and important threat landscape that industrial components need to address.

Table of Contents

1. Industrial Products & Threats Landscape 3

2. Reference Standards & Certification Schemes for Industrial Products 4

3. Focus on IECEE 5

4. Focus on Common Criteria 6

5. What is the Best Option for your Product? 8

6. Conclusion 10

2. Reference Standards & Certification Schemes for Industrial Products

Acknowledging that industrial components and systems need to have a strong focus on their security capabilities and functionalities, the last years we have seen a wide range of standards, frameworks and best practice documents published on this matter. Therefore, we are currently at a moment when some manufacturers are concerned about which are the best sources to follow, as this will obviously have a strong timeline and budget impact.

To briefly summarize, at this moment we have in place an extensive list of publications which manufacturers can consider in order to approach security into their products. Without the purpose of making this an exhaustive list, relevant examples include the **IEC 62443, UL 2900 family, ENISA Best Practices for connected products, NIST SP 800-53** or the **NIST SP 800-82**. The list can of course become much more extensive if we consider additional publications that are issued by smaller security organizations, and furthermore if we consider other local requirements which are published for specific countries and regions.

The **IEC 62443** family of standards is currently seen as the main publication to govern the security needs of the industrial domain. The family is structured in several parts, addressing all dimensions of industrial security. Parts of the IEC 62443 family include:

- Organizational and processes security
- Industrial risk management
- Solution and asset integration requirements
- System and components security capabilities requirements
- Product development lifecycle requirements

Besides the topic of issuing relevant standards, there is of course the discussion on certification options for industrial products.

Here the concerns can be even stronger, as a good certification program for needs to have in place several aspects, such as:

- Clear requirements and testing methodology
- Smooth assessment and certification process, resulting in a limited effort approach
- High international visibility and recognition of the resulting certificate

Furthermore, there is the topic of creating a certification program that addresses the long lasting time of industrial products – the products need to remain compliant not only in their off-the-shelf state, but also after multiple years of operation. Having these constraints in mind, there are currently several certification options that are possible options for manufacturers.

Common Criteria certification is arguably the most recognized certification program for IT products, with its results recognized in many countries across multiple continents. To provide some alternatives to Common Criteria, the recent years have seen the development of other, industrial focused certification schemes, such as **IECEE** (scheme operated by the IEC organization), or ISASecure. Both IECEE and **ISASecure** operate based on the IEC 62443 family of standards.

In this multitude of available standards and certification options, it is critical for manufacturers to get the best decision regarding the specific standard or certification in which they will invest their efforts. With the aim of providing more clarity on the topic, the rest of this document will focus on two specific programs, the **Common Criteria international security certification** and the **IECEE certification**.

3. Focus on IECEE

3.1. What is the IECEE scheme?

The IECEE scheme is operated by IEC and includes in its scope multiple international IEC standards. Recently, under the scope of the scheme were added several parts of the cybersecurity related IEC 62443 standard. Based on these standards, systems and components from various domains can be evaluated and certified, increasing their market value and recognition.

The following security standards are in the scope of the IECEE scheme:

- **IEC 62443-2-4:** Certification for product integrators and service providers
- **IEC 62443-3-3:** Certification for systems security capabilities
- **IEC 62443-4-1:** Certification for product manufacturers' development processes
- **IEC 62443-4-2:** Certification for components security capabilities

3.2. How to Test and Certify Based on IECEE scheme?

The following stakeholders are involved in the certification process:

- Customers are initiating the certification request, providing the product to be evaluated, as well as the required evidence related to the product or the associated processes.
- Licensed Test Labs are performing the technical assessment on the product or organization in scope, finally drafting the compliance report. This report will be shared with the Certification Body.
- The Certification Body supervises the whole process and finally receives the compliance report drafted by the Test Lab. The Certification Body will review the report and decide if a certificate of compliance can be issued. The Certification Body will issue the certificate if all the applicable requirements are met.

An IECEE evaluation can be conducted on an industrial product, system, solution or development set of processes. The aim of the IECEE scheme is to allow evaluations to be performed as much as possible based on documentation provided by the sponsor. This is also from a practical point of view – industrial systems can often be highly complex, which makes practical testing in a lab infeasible. Audits on location and witnessing of testing can be used to raise confidence in the evaluation results.

4. Focus on Common Criteria

4.1. What is Common Criteria?

The **Common Criteria for Information Technology Security Evaluation**, shortly referred to as Common Criteria or CC, is an **international standard for independent security evaluation and certification of IT products** implemented as hardware, firmware or software.

Common Criteria consists of three main parts plus the recommended methodology to perform evaluations:

- **Part 1:** Introduction and general model, April 2017, version 3.1, revision 5;
- **Part 2:** Security functional components, April 2017, version 3.1, revision 5;
- **Part 3:** Security assurance components, April 2017, version 3.1, revision 5;
- **Common Methodology for Information Technology Security Evaluation** (further referred to as CEM), April 2017, version 3.1, revision 5.

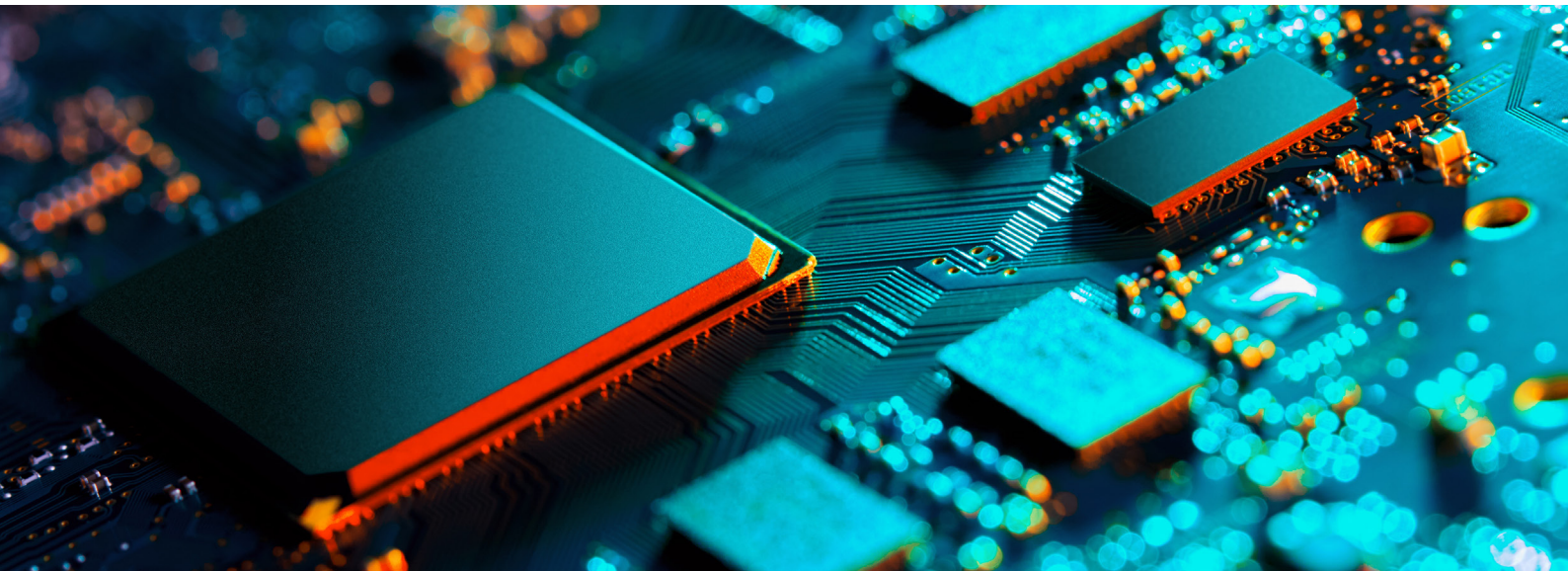
Several stakeholders are involved in a CC evaluation, as follows:

- **Sponsor of the evaluation.** The party that plans to certify a product (could be either a developer of the product or a third party).
- **National certification scheme.** National CC scheme, providing own set of tailored rules for evaluation and certification of IT products, based on the CC standard.
- **IT Security Evaluation Facility (ITSEF).** Accredited and licensed lab specialized in performing CC evaluations for a particular class of IT products.

Under Common Criteria, it is possible to evaluate and certify a broad range of products, including:

- Smart cards and ICs
- Software and application products
- Operating systems
- Antivirus and network protection software
- Network equipment
- Embedded devices such as IoT, printers, automotive components, medical devices, industrial products, etc.

A Common Criteria evaluation can be conducted based on seven increasing assurance levels, each of the levels coming with more stringent requirements that need to be fulfilled by the product, as well as the evaluation methodology. A resulting Common Criteria certificate is mutually recognized in a wide range of countries, spread across the EU, Asia, North America, Australia or UK. Given its history, tradition and large number of issued certificates, Common Criteria is one of the most recognized certification methodologies across the world.



4.2. How to test & certify based on Common Criteria?

Common Criteria introduces seven different levels of evaluation (EAL1 to EAL7) depending on the level of assurance in the security of the evaluated product. According to CC, higher assurance results from the application of greater evaluation effort. The increasing level of effort is based upon:

- **Depth of evaluation** - the effort is greater because it is deployed to a finer level of design and implementation detail;
- **Coverage of evaluation** – the effort is greater because more evaluation requirements are in scope
- **Rigor of evaluation** - the effort is greater because it is applied in a more structured, formal manner.

The assurance increases with every level and the "default" levels in a CC evaluation are identified in the following way:

- **EAL1** – functionally tested;
- **EAL2** – structurally tested;
- **EAL3** – methodically tested and checked;
- **EAL4** – methodically designed, tested and reviewed;
- **EAL5** – semi-formally designed and tested;
- **EAL6** – semi-formally verified design and tested;
- **EAL7** – formally verified design and tested.

Selecting the desired evaluation level is based on the preference of the manufacturer. Typically, embedded products including industrial components and systems are suited for a lower level evaluation (e.g. EAL 1 to EAL 3). This is due to the typical security capabilities embedded into such products, as well as the relatively medium associated evaluation effort.

The evaluation activities include a combination of several elements, such as:

- Evaluation of the product's Security Target (the overview of the product's security scope and capabilities)
- Design review of the products and overview of its interfaces and architecture
- Review of the product's guidance requirements
- Review of the product's development life cycle processes
- Validation and penetration testing of the product's security capabilities.

The conducted assessment activities are documented in several deliverables that are shared with the certification scheme. Once these deliverables are agreed by the scheme, a final certificate is issued and published on the Common Criteria portal.

5. What is the Best Option for your Product?

As it was highlighted above in this document, currently manufacturers of industrial products have several options in place in order to allow for certification of their products. Some specific case studies have been presented for the Common Criteria and IECEE certification schemes.

In the end, which one of these options is the best for manufacturers to take, and based on which can this decision be taken? While the final answer will depend strongly on certain aspects that are manufacturer related, the table below aims to summarize the characteristics of these schemes against several selected aspects.

Characteristic	IECEE Certification	Common Criteria Certification
International recognition	**IECEE certificates are internationally recognized**, with countries spread across multiple continents including EU and USA.	**Common Criteria is widely known,** being mutually recognized in multiple countries spread across the world.
Value of certificate	The IECEE certificate is issued based on evaluations in line with the IEC 62443 applicable requirements. As IEC 62443 is the most recognized family of standards in the industrial domain, **the resulting value of an IECEE certificate is very good**. Moreover, more and more asset owners are starting to ask for IECEE certification in order to consider such products in their systems.	**A Common Criteria certificate is mutually recognized in multiple countries,** all over the world. Many times, large institutions or asset owner organizations will ask for a CC certificate in order to sign a partnership with a device manufacturer. Finally, having a CC certificate can represent a strong differentiator against competitors.
Flexibility of the process	The IECEE methodology of evaluation has been developed in the last years within special task forces at IEC. The resulting methodology combines documentation review with testing. The goal is however to **allow flexibility concerning testing, such that partial use can be made of customer supplied test results**. This will make the whole process more efficient and quick.	Common Criteria is **a very carefully defined evaluation process**. All the evaluation activities are documented, and a project cannot deviate from them. The relation between the stakeholders is clear and strict.

Required effort 	An IECEE certification will vary in effort based on the complexity of the evaluation target, however the **essence of the scheme is to keep the effort minimized.** As an estimation, 20-25 days can be considered for a medium complexity component.	The effort depends per the level of evaluation, and **will progressively increase among the seven possible levels in Common Criteria.** As a rought indication, 40 – 60 person days can be expected for a Level 2 evaluation, which is a well suited level for consumer IoT devices.
Required involvement from the manufacturer 	The main aim of IECEE certification is to make the whole process smooth for the all the involved parties. Clear checklists of documents are in place to guide the manufacturers. **During the evaluation, manufacturers can support for example in witnessing testing or audits of processes**, in order to make the whole evaluation effort more efficient.	In a CC evaluation, **the manufacturer holds an important role.** The manufacturer is responsible for drafting the evaluation evidence, in a particular format required by the CC scheme. A site-audit can be part of the evaluation process as well.
Project Duration 	**The duration of the project, including the drafting of the final report and issuing of the certificate is minimized,** the whole process being possible to be finalized within 1-2 months.	Typically, **Common Criteria projects do not result in quick verdicts.** Of course, the duration strongly depends on the evaluation level. As an indication, a duration of 3-4 months can be considered relevant for an evaluation based on Level 2[1].
Specific Value for Consumer IoT Products 	A certification based on IECEE could be an important milestone for a manufacturer of industrial products. Such a certificate will represent an **appreciated label particularly among users and integrators of such equipment**, while on the other hand being mutually recognized across multiple countries.	Common Criteria is a highly recognized evaluation and certification scheme. Therefore, the value of such certificate will be of importance, including in the domain of consumer IoT products. Besides offering possibilities for governmental or large asset owners access, **a CC certificate can be an important differentiator against the competitors.**

[1] *This indication is given considering an evaluation performed under the Dutch Common Criteria scheme, NSCIB.*

6. Conclusion

This document aimed to describe the existing standards and certification options applicable for the domain of industrial products. Luckily, we do not lack in terms of available standards. In fact, this can even be considered to be an element that sometimes provides confusion among the manufacturers: which standard or certification scheme would be the best one to follow.

Common Criteria has traditionally been the main international certification program for IT products, applicable therefore also for industrial components and systems. On the other hand, the IECEE certification scheme came with an approach that aims to make the evaluation of these devices smoother and with less involvement from the manufacturer. Moreover, based on IECEE, also development processes, as well as integrated solutions can be certified, which makes this scheme particularly interesting for the industrial domain. Both Common Criteria and IECEE can result in valuable certificates. While Common Criteria will provide direct international recognition, an IECEE certificate will attract the attention especially among users and integrators of industrial products.

Would you like more guidance on which option might be the best for your product, or more information about industrial products standards and certification?

If yes, feel free to contact Secura's experts for more help.

About Secura

Secura is your independent cybersecurity expert. Secura provides insights to protect valuable assets and data. We make cybersecurity tangible and measurable in the field of IT, OT and IoT. With security advice, testing, training and certification services, Secura approaches cybersecurity holistically and covers all aspects from people, policies, organizational processes to networks, systems, applications and data.

For more information, please visit: **secura.com.**

Keep updated with the latest insights on digital security and subscribe to our periodical newsletter: secura.com/subscribe.

Follow us on

Contact us today at info@secura.com or visit secura.com for more information.

SUBSCRIBE

TO OUR NEWSLETTER

Secura

A BUREAU VERITAS COMPANY

BUREAU VERITAS

Shaping a World of Trust