Technical Report

Common Criteria and ISA/IEC 62443 comparison: Which is right for your company?

UL Solutions

Safety. Science. Transformation.™

Table of contents

Introduction

Companies that seek the guidance of security standards have several reference documents to choose from. Chief among them is the NIST Cybersecurity Framework, PCI DSS, ISO 21434 and ISO 27001. Also in play are ISA/IEC 62443, Industrial Communication Networks, Network and System Security, and ISO/IEC 15408, Common Criteria for Information Technology Security. As ISA/IEC 62443 rapidly gains momentum, many security professionals may be wondering whether they should migrate from Common Criteria to ISA/IEC 62443 or perhaps use both frameworks.

Any framework creates costs and requires resources, from training staff, to conducting testing and conformity assessments, to certification through third parties. In choosing and using a framework, informed decisions and a well-thought-out certification strategy lay the foundation for efficiency and sustainability. This paper provides a comparison of ISA/IEC 62443 and Common Criteria, to support informed decision-making and strategy planning and help companies decide if one or both frameworks are best suited to their business needs.

Common Criteria goes back to the 1990s; however, good reasons exist to select the newcomer ISA/IEC 62443 for operational technology (OT). As the undisputed leading framework in this segment, it continues to expand its scope further in applicability, content and capabilities.

Both frameworks use slightly different terminology. Common Criteria (CC) is a blend of three standards, ITSEC (Europe), CTCPEC (Canada) and TCSEC (U.S.) and goes back to the 1990s. In a second step in 1999, Common Criteria became an ISO/IEC standard, the ISO/IEC 15408. At this moment of time standards about conformity assessment did not yet exist. Their publication started in 2004 with the publication of ISO/IEC 17000 on “Conformity assessment - Vocabulary and general principles.” In consequence the standards and conformity assessment related vocabulary in CC differs in some cases from the one used in ISA/IEC 62443, which came after 2004. The terminology differences need to be considered to understand ISA/IEC 62443. This paper uses the terminology in ISA/IEC 62443.

The Common Criteria framework

The Common Criteria security evaluation includes a catalog of security functional requirements (SFRs) — what the product must do—and security assurance requirements (SARs) — what an evaluator must test, audit or inspect to gain assurance that the product meets the SFRs. The SFR and SAR nomenclature is based on a strict taxonomy of classes, families and components. Evaluations against the standard are performed according to ISO/IEC 18045, The Common Methodology for Information Technology Security Evaluation (CEM). It describes the techniques for evaluating products against each SFR and SAR.

Common Criteria evaluations comprise a threat analysis, specific SFRs to mitigate those threats and the SARs to provide assurance. One of seven prepackaged set of SARs determines the evaluation assurance level (EAL).

All this information may be documented in a protection profile (PP) for reuse between different products of the same type. The product security target (ST) references a PP or includes this information directly, along with a high-level description of how the product meets the SFRs.

Conformity assessment schemes

Common Criteria operates under national certification bodies or schemes with a mutual recognition agreement (CCRA). The testing part of each scheme is typically done through private test labs within their country. Protection Profiles have been developed most often by and for government agencies' needs. This meant quite often highly application specific requirements and no baseline security requirements. In consequence, their usability cross-border was limited. To overcome this restriction, CC has introduced cPP, which stands for Collaborative Protection Profile. As a result, CCRA countries support the development of cPPs by technical communities for commercial-off-the-shelf product types. In this way, different products evaluated against the same PP create more consistent, comparable security evaluations even at lower assurance levels.

CCRA countries mutually recognize evaluations up to EAL2, which include all the internationally developed cPPs. In addition, each country may also evaluate products to higher assurance levels.

Adoption and suitability

Common Criteria originated from three security standards that date back to the 1980s, which have been developed to create requirements for products purchased by government agencies for civil and military applications. While still primarily the focus of defense and government security deployments, Common Criteria has been adopted for many other uses such as integrated circuits, smart cards, security modules and a broad array of network devices and security software. Furthermore, as an extensible framework, efforts are under way to adapt Common Criteria for cloud deployments as well as systems evaluation.

The ISA/IEC 62443 framework

The ISA/IEC 62443 framework comprises 14 standards (also called sub-standards) and technical reports (Figure 1). It was formed as the national standard ANSI/ISA 62443 and became an international standard as ISA/IEC 62443.

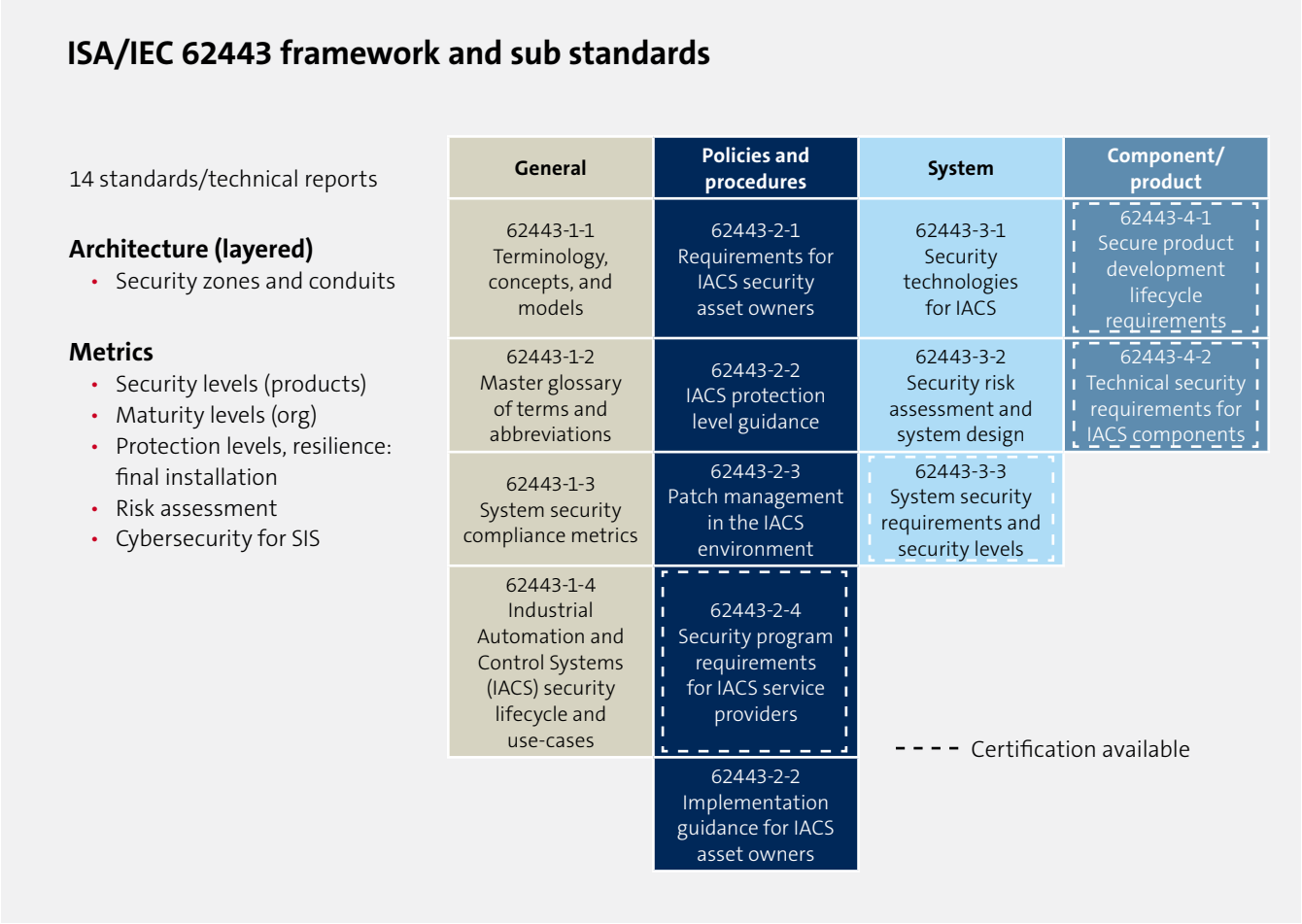
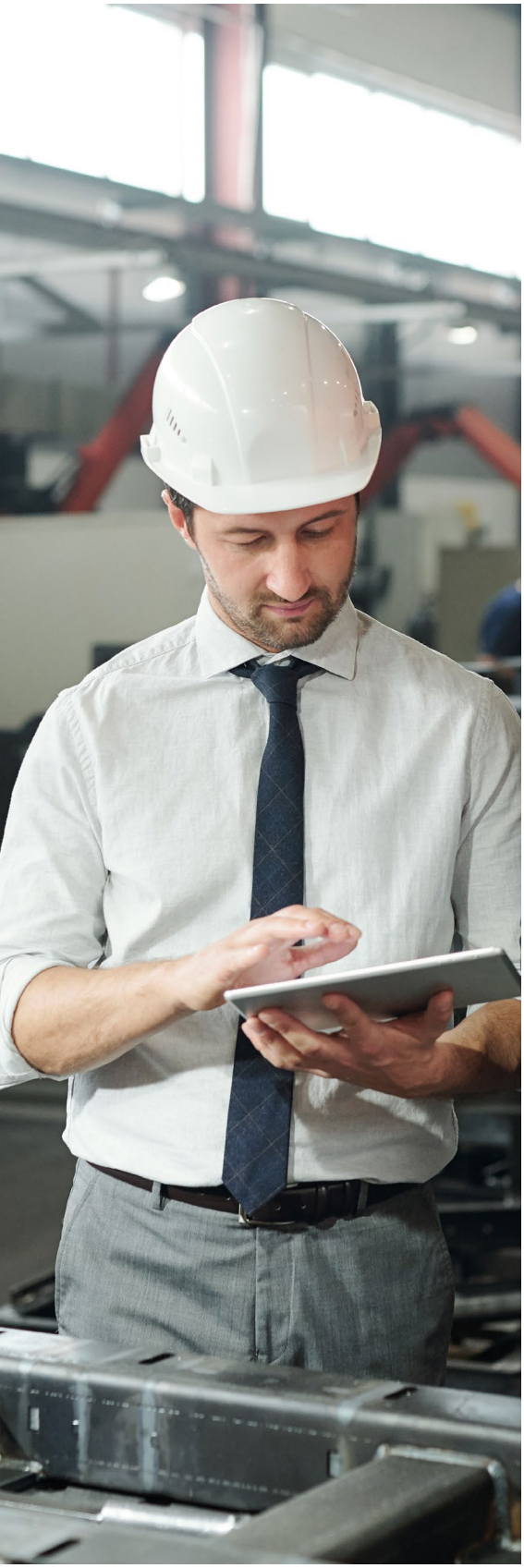


Figure 1. ISA/IEC 62443 Overview

ISA/IEC 62443 goes beyond product certification and covers systems, operations and services like system integration and maintenance services provisioning. Products are viewed as components to systems and labeled as such. ISA/IEC 62443 also pertains to information security management systems (ISMS) in OT, processes for secure components development, service provider capabilities and risk management for OT environments.

The sub-standard IEC 62443-2-1 describes a cybersecurity management system (CSMS) for OT that applies to operations and asset owners. ISO/IEC 27001, Information Security Management Systems (ISMS), is the foundation for the sub-standard. The concept of building a CSMS on the foundation of an ISO/IEC 27001 ISMS will gain increased visibility in the sub-standard Edition 2 scheduled to be published in 2024.



Conformity assessment schemes

Conformity assessment for ISA/IEC 62443 sub-standards can be done with a larger choice of schemes than with Common Criteria. The schemes can be allocated to three categories:

1. IECEE CB certification system (most widespread globally). IECEE is the conformity assessment branch of the global IEC standards organization, IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components. The IECEE offers schemes for all sub-standards in the IEC 62443 framework, for assessment and certification.

   The IECEE conformity assessment schemes represent a ubiquitous platform to build proprietary systems or schemes upon. The conformity assessment schemes do not have to be developed from scratch, which is advantageous in terms of efforts and costs for applicants.

2. ISASecure©. This is a certification system for industrial control systems cybersecurity, owned by the ISA Security Compliance Institute (ISCI). ISASecure enables a subset of the ISA/IEC 62443 sub-standards to be assessed and certified.

3. Certification body proprietary schemes or systems. Conformance assessments embrace additional requirements such as product specifics, cyber aspects of intended use, contractual requirements between operator and system integrator, for instance, or regulatory requirements (federal, state, or regional).

   UL operates - complementarily to the IECEE scheme - its UL CAP scheme which leads to UL IEC 62443 certificates, providing benefits to customers as just mentioned.

IECEE and ISASecure assure – within each framework - mutual recognition, which means that results of tests and assessments, along with certificates, can be used and are recognized by any other national certification body for further testing, assessment and certification purposes. For IECEE, mutual recognition is global. For ISASecure, it is multi-country.

Adoption and suitability

Designed for industrial automation and control systems (IACS), ISA/IEC 62443 also has been adopted by energy generation and distribution, energy efficiency, facility management and other industry segments. The standard addresses the complex interaction of numerous systems in terms of cybersecurity.

The systems usually comprise many products and components, which are described with security and protection levels. Organizations that develop components or products, along with system integrators and maintenance services providers and operators, are gauged by maturity levels. ISA/IEC 62443 addresses the product view and the process and organization view. This interlink is a prerequisite to achieving resilient operations in discrete and process manufacturing as well as in energy generation and distribution (grid operations).

Comparison of Common Criteria and ISA/IEC 62443

Commonalities

Because Common Criteria pertains to the certification of products, it has the most commonalities with IEC 62443-4-2, Security IACS — Technical Security Requirements for IACS Components. The requirements of IEC 62443-3-2, 62443-3-3 and 62443-4-1 cover broad system design, system-level requirements, and process and governance requirements, so there is overlap with some Common Criteria functional and assurance requirements. These requirements include aspects of change management, design modularity, binary artifact integrity and secure update, verification testing, vulnerability assessment, design validation, guidance documentation and flaw remediation.

The Common Criteria SFRs are determined either by the threat analysis or the referenced PP. ISA/IEC 62443 is more prescriptive. Requirements are based on one of four security levels deemed appropriate for the security zone determined by the system security analysis.

As for nomenclature, the Common Criteria security requirements are grouped in classes, whereby in IEC 62443-4-2 they are called foundational requirements (FR). For instance, the Common Criteria class FIA: Identification and Authentication has its counterpart in FR 1, Identification and Authentication Control. Specific requirements differ in quantity and content but generally cover identification and authentication, audit logging, confidentiality and integrity of communications, system integrity, availability and secure update.

Like most certification approaches, Common Criteria and ISA/IEC 62443 component and system certifications evaluate security posture for a specific component version or system configuration. Common Criteria schemes provide a validity lifetime of the certificate of five years. IEC 62443 certifications are valid either with or without expiration date. IECEE CB schemes have no expiration date. Alternatively, the validity can be limited by other certification schemes. Security Compliance Institute (ISCI) ISASecure® schemes define the validity period as three years.

Security requirements often come in different flavors; however, protection against vulnerabilities and threat-related safeguards often involves similar methods and technologies. As such, for manufacturers with products involving IT, OT or cybersecurity, the migration from Common Criteria to ISA/IEC 62443 represents an effort, but not a major one.

Differences

IEC 62443-4-2 and -3-3 differ from Common Criteria product certification in seven major ways.

1. Common Criteria is built as a framework wherein specific requirements must be selected or specified. Common Criteria uses seven levels to describe and assess product security assurance, called EAL. IEC uses prescribed requirements pertaining to security levels for components and systems, labeled SL1 to SL4.

2. ISA/IEC 62443 implements OT-specific security requirements. Whereas IT (think office IT) is primarily about confidentiality, integrity and availability (CIA), in this order of priority, OT security focuses on availability, integrity and confidentiality (AIC), in this order.

    - All cyber functionality is considered always as priority 2, whereby safety is priority 1. This core requirement is labeled Support of Essential Functions.

3. Common Criteria focuses on a standalone Target of Evaluation, whereas ISA/IEC 62443 embraces components as a part of systems. Systems are operated by an asset owner. Security requirements differ to a large extent among three stakeholder groups: component manufacturers, service providers and asset owners (Figure 2).

    An example of sharing responsibilities between these stakeholders is the “Compensating Countermeasures” requirement. It states that system integrators should add specific protective measures, which are needed but have not or cannot be delivered within a component.

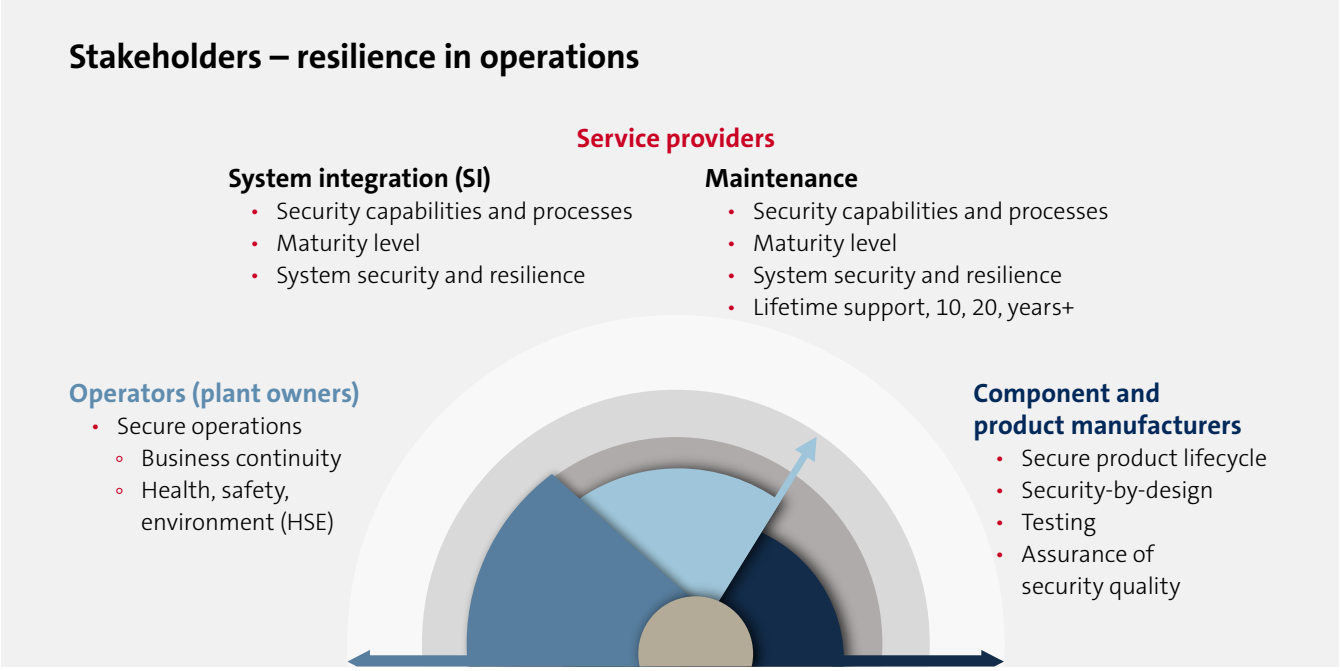


Figure 2. ISA/IEC Shared Responsibilities

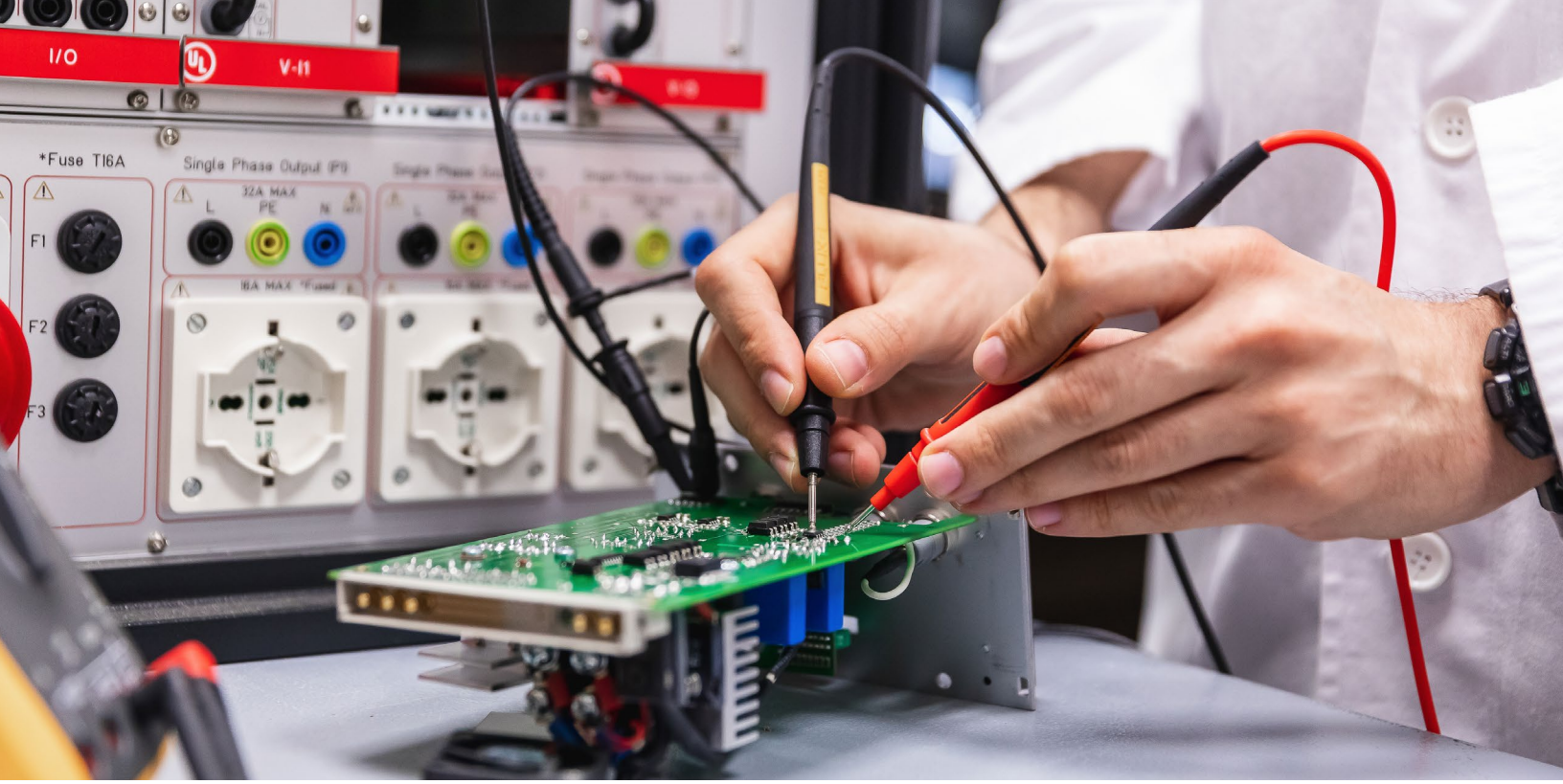
4. ISA/IEC 62443 stringently adheres to the mantra, "Security is a process, not a product. (Bruce Schneier, CryptoGram, May 15, 2000). Products provide some protection, but the only way to effectively do business in an insecure world is to put processes in place that recognize the inherent insecurity in the products. The trick is to reduce your risk of exposure regardless of the products or patches." Therefore, an IEC 62443-4-2 product certification requires a mandatory IEC 62443-4-1 assessment (or certification) of the product development site and secure product development lifecycle. The latter is a one-time exercise. For all additional products that run through the same processes, no further assessment is required.

    - It should be noted that Common Criteria can provide more stringent process requirements. Common Criteria offers seven EALs. The higher the level, methods range from informal to semi-formal to formal.

5. PP is a concept in Common Criteria, and there is no direct counterpart in ISA/IEC 62443. However, IEC 62443 profiles are being developed to address products, services and process requirements.

6. ISA/IEC 62443 does not require a certification body, operating under the IECEE certification system, to conduct testing as a prerequisite to issuing a product certificate. The assessment focuses on the capabilities, expertise and processes to conduct testing. However, the standard requires that manufacturers conduct the testing.

7. Whereas ISA/IEC 62443 has OT security-specific requirements, the functional requirements and assurance activities in Common Criteria can be much more specific and detailed. For example, ISA/IEC 62443 requires the capability to provision and protect transmitted information confidentiality, whereas Common Criteria specifies the exact cryptographic algorithms, protocols and protocol-specific implementation requirements as well as specific test assurance activities for each protocol.



Conclusion

While overlap exists between Common Criteria and ISA/IEC 62443, both frameworks are meaningfully different in terms of policies, procedures, metrics and range of security levels and related assessment methodologies. Understanding where they differ can help organizations decide whether to migrate from Common Criteria to ISA/IEC 62443 or to use both frameworks. Common Criteria has been designed primarily for high-security needs, as in public sector deployments and military systems. ISA/IEC 62443 has been designed from the beginning for industrial applications, making it the best fit for these cases.

For companies that already use Common Criteria, a migration strategy is recommended. Whether the strategy uses ISA/IEC 62443 only or both frameworks depend on the company's products and services portfolio and history of conformity assessment and certification.

How UL Solutions can help

UL Solutions offers the certification and support services to help companies migrate from Common Criteria to ISA/IEC 62443 or add ISA/IEC 62443 testing, assessment or certification to their security products, processes and services. We have leading expertise in both Common Criteria and ISA/IEC 62443 testing, assessment, certification, training and advisory services.

On this foundation, UL Solutions is ideally equipped to support the journey toward OT security, helping companies achieve resilient systems in operation around the world.

For more information, visit UL.com/IEC62443 or UL.com/CommonCriteria.

UL.com/Solutions

IMS22CS517143
046.01.1122.EN.CYB