IEC 62443 and the Trellix / WaveLinx System

Introduction

Building owners and operators are tapping into the power of smart building systems at an accelerating pace. This trend of increasing connectivity is driven by the wealth of new data it unlocks, the benefits of improved insight into building operations, and the opportunity to differentiate tenant spaces. These advantages, however, are accompanied by a heightened concern around cybersecurity quality and potential vulnerabilities.

At Cooper Lighting, we are not only a provider of smart lighting systems—we also own and operate buildings, and act as tenants. With skin in the game, we build cybersecurity into our connected products for our customers and for ourselves. Thanks to our *secure by design* philosophy, cybersecurity is embedded in every connected product and platform we bring to market. Our secure development approach helps us manage cybersecurity risk throughout the product life cycle, from threat modeling and requirements analysis to verification and ongoing maintenance.

But we don't stop there. We employ third-party cybersecurity certification to deliver the accredited, independent proof our customers need to trust the products installed in their facility. To this end, all Cooper Lighting connected products are certified against the IEC 62443-4-2 standard by an authorized third-party cybersecurity lab.

What is IEC 62443?

The ISA/IEC 62443 series of standards were developed by the ISA (International Society of Automation), a non-profit global organization founded in 1945. These standards were subsequently adopted by the IEC (International Electro-technical Commission), a non-profit organization founded in 1906. The scope of ISA/IEC 62443 is "to define the elements necessary to establish a cyber-security management system (CSMS) for industrial automation and control systems (IACS), and to provide guidance on how to develop those elements." [IEC] 62443-2-1

The original purpose of the 62443 standards, to protect industrial control systems against cyber-threats at critical facilities like refineries, conventional power plants, and nuclear power plants, is a testament to their diligence and thoroughness.

The ISA committee developing the technical requirements initially considered IT standards and practices for use in IACS. These turned out to be insufficient, however, and the committee soon realized "this was not sufficient to ensure the safety, integrity, reliability, and security of an IACS. This is because the consequences of a successful cyberattack on an IACS are fundamentally different. While the primary consequences of a successful cyberattack on IT systems is financial and privacy loss due to information disclosure, the consequences for an IACS may additionally include loss of life or health, damage to the environment, or loss of product integrity." [2] As a result, the IEC 62443 standards address issues unique to OT (Operational Technology) systems.

Why is IEC 62443 important?

According to Gartner, there were expected to be 5.8 billion enterprise and automotive IoT (Internet of Things) endpoints in 2020, a 21% increase from 2019. According to a 2018 report from Trustwave, "Sixty-one percent of [organizations] surveyed who have deployed some level of IoT [Internet of Things] technology have had to deal with a security incident related to IoT."

With the rapid increase in IoT products deployment in Operational Technology systems comes increased concern around vulnerabilities from inadequate cybersecurity. The techniques used by attackers to exploit software vulnerabilities and weak links in ecosystems are growing exponentially. Furthermore, these attacks are becoming increasingly sophisticated, harder to protect against, and more costly than ever. According to US federal agencies, 31,000 cybersecurity incidents were reported in 2018. A study undertaken by IBM Security and Ponemon estimated the average cost of a data breach in 2019 was $3.9M.

To achieve widespread adoption of IoT technologies and unlock their tremendous potential in the commercial space, manufacturers must build cybersecurity into their connected products. This protects not only consumers and businesses, but also the manufacturers themselves. In addition, end users will need to implement comprehensive security strategies to protect their corporate networks, systems, and data from attacks, damage, and unauthorized access.

In defining the security requirements for OT (Operational Technology) products and systems, the IEC 62443 series of standards are valuable not only to end users but equipment vendors as well.

COOPER Lighting Solutions

Risk Mitigation

End users typically evaluate vendor products using criteria such as features, price, and delivery terms. When it comes to cybersecurity, however, specifying features can be a complex process. IEC 62443 simplifies this by allowing end users to specify a target security level instead of trying to manage a cumbersome list of features.

IEC 62443 defines four levels of system security requirements. These security levels, along with the skills, motivations, means, and resources of the attacker being addressed, are summarized in the table below.

Level	Definition	Skills	Motivations	Means	Resources
1	Protection against casual or coincidental violation	No attack skills	Mistakes	Non-intentional	Individual
2	Protection against intentional violation using simple means with low resources, generic skills, and low motivation (Cybercrime, Hacker)	Generic	Low	Simple	Low (isolated individual)
3	Protection against intentional violation using sophisticated means with moderate resources, IACS-specific skills, and moderate motivation (Hacktivist, Terrorist)	IACS Specific	Moderate	Sophisticated	Moderate (Hacker Group)
4	Protection against intentional violation using sophisticated means with extended resources, IACS-specific skills, and high motivation (Nation State)	IACS Specific	High	Sophisticated (Campaign)	Extended (Multi-disciplinary teams)

Thanks to IEC 62443, end users can evaluate vendor products more easily based on their compliance with a targeted security level. For example, an end user who needs to address attacks from generic hackers or cybercriminals should implement a system that meets the Level 2 requirements.

Secure products and systems

It has been difficult, historically, for a vendor to clearly show that their product is more secure than what a competitor is offering. Equipment vendors, like Cooper Lighting, can now certify their products and systems using the IEC 62443 standards. By designing and certifying solutions to the IEC 62443 security levels, a vendor can clearly differentiate their cybersecurity capabilities by comparing a product certified to Level 2 standards against competitive offering certified at Level 1.

A vendor can elect to certify by end device (IEC 62443-4-2) or by system (IEC 62443-3-3), and they can opt for self-certification or third-party certification. As discussed later in this paper, Cooper Lighting strongly believes that compliance should be validated by an independent third party. End users, for their part, should adopt cybersecurity certifications in their purchase requirements.

What does the IEC 62443 series of standards cover?

The IEC 62443 standards address every aspect of security at the product, system, and development process level. The relevant standard documents, described below, are arranged into four groups by their focus and intended audience.

The **General** group of documents address topics common to the entire series. They are:

- **62443-1-1, Terminology, concepts, and models definition** – Introduces the concepts and models used in the series.
- **62443-1-2, Master glossary of terms and abbreviations** – Lists the terms and abbreviations used in the series.
- **62443-1-3, System security conformance metrics** – Describes the methodology to develop quantitative metrics, as derived from the process and technical requirements in the standards.
- **TR62433-1-3, IACS security lifecycle and use-cases** – Provides a more detailed description of the lifecycle for IACS security, along with some use cases.

The **Policies and Procedures** group of documents focus on the policy and procedural aspects of IACS security. They are:

- **62443-2-1, Establishing an IACS security program** – Describes what is required to define and implement an effective IACS cybersecurity management system.
- **62443-2-2, IACS security program ratings** – Provides a methodology for evaluating the level of protection provided by an operational IACS against the requirements in the ISA/IEC 62443 series of standards.
- **62443-2-3, Patch management in the IACS environment** – Provides guidance on managing patches for IACS.
- **62443-2-4, Security program requirements for IACS service providers** – Specifies requirements for IACS service providers such as system integrators and maintenance providers. This standard was developed by IEC TC65/WG10.
- **TR62443-2-5, Implementation guidance for IACS asset owners** – Provides guidance on what is required to operate an effective IACS cybersecurity program.

The **System Requirements** group of documents address requirements for the automation system. They are:

- **62443-3-1, Security technologies for IACS** – Describes the application of various security technologies to an IACS environment.
- **62443-3-2, Security risk assessment for system design** – Addresses cybersecurity risk assessment and system design for IACS. The output of this standard is a Zone and Conduit model, along with the associated Risk Assessments and Target Security Levels. These are documented in the Cybersecurity Requirements Specification.
- **62443-3-3, System security requirements and security levels** – Describes the IACS requirements by security level.

The **Component Requirements** group of documents include information about the more specific and detailed requirements associated with the development of IACS products. They are:

- **62443-4-1, Product security development life-cycle requirements** – Specifies process requirements for the secure development of products used in industrial automation and control systems. It defines an SDL (Secure Development Lifecycle) for developing and maintaining secure products.
- **62443-4-2, Technical security requirements for IACS components** – Describes the IACS component requirements by security level. Components include embedded devices, network components, host devices, and software applications.

Self-certification at Signify

Signify, Cooper Lighting's parent company, has a CCoE (Cybersecurity Center of Excellence) team that maintains guidelines and requirements for all Signify products and development processes, including its Cooper Lighting division products. The Signify guidelines and requirements are a collection of the security requirements defined in various industry standards, including: NIST SP 800-53; NIST SP 800-82; FIPS 140-2; NIST SP 800-124; IEC 62443; UL 2900; and local regulations such as California Bill SB-327. These requirements provide a unified way to develop a product that complies with multiple security standards.

The cybersecurity team works with all product development teams to ensure our cybersecurity requirements are met. They conduct product design reviews while the product is in its infancy to make sure the design includes security best practices and recommendations. A product review is used to walk through the concept of the product. Based on this, a data flow diagram is created to depict the overall flow of data in the product, and an architectural analysis is performed to identify the criticality of components. The team also identifies sensitive and personal data, and verifies compliance with applicable data protection regulations, including the GDPR (General Data Protection Regulation) and California Consumer Privacy Act (CCPA)

After these reviews, the team performs a threat modeling and security requirements analysis. Threat modeling allows the team to assess the risks related to components identified in the architectural analysis. These risks are used to prioritize security requirements and additional mitigations for the product. Identifying issues at the design stage lowers the odds of finding flaws in later stages.

Why did we choose IEC 62443 certification?

There are many cybersecurity certifications in the market, but a survey conducted by Cooper showed that UL 2900 and IEC 62443 are the most recognized cybersecurity standards in the automation industry. Although they overlap to some extent, the two standards have different sets of technical requirements.

The Signify CCoE recently carried out an analysis revealing that a product conforming to IEC 62443-4-1 and IEC 62443-3-3 would be 90% compliant with UL 2900-1 technical requirements. Conversely, a product conforming to UL 2900-1 would be just 50% compliant with IEC 62443-4-1 technical requirements, and only 60% compliant with IEC 62433-3-3 technical requirements.

IEC 62443 also enables an organization to have their development process certified by a third-party certification lab. In fact, Signify is the first lighting company in the world to be awarded a security certification for its connected lighting development process (IEC62443-4-1). The Signify process was certified by DEKRA, an authorized cybersecurity certification lab. This confirms that Signify's development of connected lighting systems adheres to a certified secure development process, and illustrates the company's leadership in embedding security in every aspect of its products, systems, and services.

Trust is paramount

At Cooper Lighting we believe that **trust is paramount** in a connected world. We strongly believe that **self-certification is not enough to build trust between manufacturers and end users**. Therefore, Cooper Lighting Solutions has decided to complement its internal assessment by having **all connected products certified by an authorized cybersecurity certification lab**. Examples of connected products include the WaveLinx Wireless Area Controller and Trellix Core.

This will include the major phases described below.

1. **Document for Product, Processes, and Use** – The lab assesses product documentation to ensure it provides the information required for users to secure their system. In addition, they assess the documentation of the overall process used to manufacture and distribute the product.
2. **Risk Controls and Management** – The lab reviews how the product manages access control, user authentication, and authorization. The lab will also assess how users can access all available interfaces on the product (e.g., Ethernet, HDMI, USB), to ensure only interfaces that are needed are enabled. The lab will also verify software integrity, including any cryptography capabilities—the mechanisms used to encrypt and decrypt data, allowing a product to store sensitive information or transmit it across insecure networks while readable only by the intended recipient or application.
3. **Product Assessment** – The lab evaluates the product to identify any of the following: known malware; vulnerabilities reported under the NVD (NIST National Vulnerability Database); common software weaknesses in source code; malformed data on various protocols; and interfaces accessible to an outside party. It also evaluates the vendor's risk assessment plan and performs structured penetration testing, including the following: attempting to engage a product in a denial of service; attempting to access by unauthorized means; attempting to exploit vulnerabilities; and attempting to circumvent risk and security controls. Finally, they would also conduct a series of test such as SAST (Static Application Security Test), DAST (Dynamic Application Security Testing), IAST (Interactive Application Security Testing) and SCA (Software Composition Analysis).

Conclusion

Third-party certification to IEC 62443, the most recognized international cybersecurity standard, by an authorized cybersecurity lab will provide the accredited and independent proof our customers need for peace of mind. They can rest more easily knowing that when Cooper Lighting products are installed in their facility, those products meet globally recognized security standards.

References

1. IEC 62443-2-1
   https://webstore.iec.ch/publication/7030
2. Quick Start Guide: An Overview of ISA/IEC 62443 Standards Security of Industrial Automation and Control Systems
   https://gca.isa.org/isagca-quick-start-guide-62443-standards

Cooper Lighting Solutions
1121 Highway 74 South
Peachtree City, GA, 30269
P: 770-486-4800
www.cooperlighting.com
For service or technical assistance:
1-800-553-3879

Canada Sales
5925 McLaughlin Road
Mississauga, Ontario, L5R 1B8
P: 905-501-3000
F: 905-501-3172