ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

The IEC 62443 Series of Standards: How to Defend Against Infrastructure Cyberattacks

Christophe Tremlet, Director, Business Management

Abstract

This article explores the foundational reasoning and benefits of the IEC 62443 series of standards—a set of protocols designed to ensure cybersecurity resilience and protect critical infrastructures and digital factories. This leading standard offers an extensive layer of security; however, it raises several challenges for those seeking certification. We will explain how security ICs provide essential assistance to organizations striving to reach certification goals for industrial automated control systems (IACS) components.

Introduction

Despite the potential for increasingly sophisticated cyberattacks, IACS have previously been slow to adopt security measures. This has been partly due to the lack of common references for designers and operators of such systems. The IEC 62443 series of standards offers a way forward towards more secure industrial infrastructures, but firms must learn how to navigate its complexities and understand these new challenges in order to make use of it successfully.

Industrial Systems Are at Risk

The digitalization of critical infrastructures such as water distribution, sewage, and power grids has made uninterrupted access essential for everyday life. However, cyberattacks are still one of the causes of disruption to these systems and they are expected to grow.[1]

Industry 4.0 calls for highly connected sensors, actuators, gateways, and aggregators. This increased connectivity increases the risk of potential cyberattacks, making security measures more critical than ever. The creation of organizations such as the U.S. Cybersecurity and Infrastructure Security Agency (CISA) illustrates the importance and demonstrates a commitment to safeguarding critical infrastructures and ensuring their resilience against cyberattacks.[2]

Why IEC 62443?

In 2010, the emergence of Stuxnet thrust industrial infrastructures into a state of vulnerability.[3] Stuxnet was the world's first publicized cyberattack indicating that attacks could successfully target IACSs from afar. Subsequent attacks have solidified the realization that industrial infrastructures can be harmed through remote attacks that can target a specific type of equipment.

Government agencies, utilities, IACS users, and equipment makers quickly understood that IACS needed to be protected. While governments and users naturally leaned towards organizational measures and security policies, equipment makers investigated possible hardware and software countermeasures. However, adoption of security measures was slow due to:

- the complexity of the infrastructures
- the different interests and concerns of stakeholders
- the variety of implementations and available options
- the lack of measurable objectives

Overall, stakeholders faced uncertainty about the right level of security to target, one which carefully balanced protection with costs.

The International Society for Automation (ISA) launched working groups to establish common references under the ISA99 initiative, which finally led to the release of the IEC 62443 series of standards. This set of standards is currently organized into four levels and categories, shown in Figure 1. Thanks to its comprehensive scope, the IEC 62443 standard encompasses organizational policies, procedures, risk assessment, and security of hardware and software components. The complete scope of this standard makes it uniquely adaptable and reflective of current realities. Additionally, the ISA has taken a comprehensive approach when addressing the various interests of all stakeholders involved in an IACS. In general, security concerns are different from

one stakeholder to another. For example, if we think about IP theft, the IACS operator will be interested in protecting manufacturing processes while an equipment maker may be concerned with protecting an artificial intelligence (AI) algorithm from being reverse engineered.

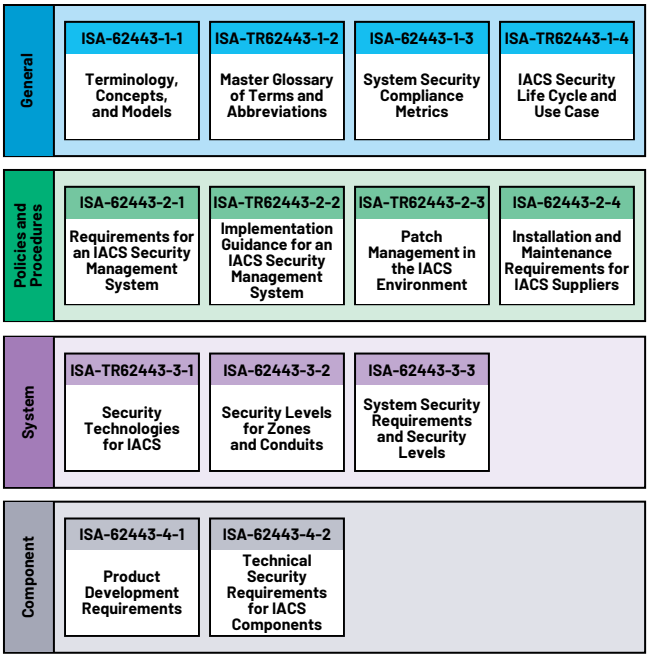

Figure 1. The IEC 62443 is a comprehensive security standard.

Also, because IACS are complex by nature, it's essential to consider the entire security spectrum. Procedures and policies alone are insufficient if not supported by secure equipment, while robust components are useless if their secure usage is not properly defined by procedures.

The chart in Figure 2 shows the adoption rate of the IEC 62443 standards through ISA certifications. As expected, a standard defined by industry key stakeholders has accelerated the implementation of security measures.

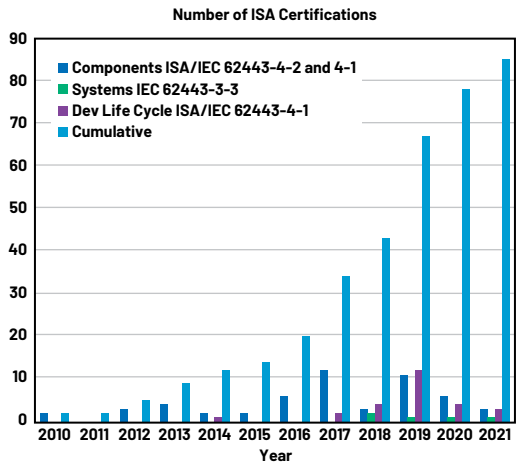

Figure 2. The number of ISA certifications over time.[4]

Getting IEC 62443 Compliance: A Complex Challenge

The IEC 62443 is an incredibly comprehensive and effective standard for cybersecurity, yet its complexity can be overwhelming. The document itself is nearly 1000 pages in length. Acquiring a clear understanding of cybersecurity protocols involves a learning curve and reaches beyond absorbing the technical language. Each section within IEC 62443 must be understood as a part of a larger whole, as the concepts are interdependent (as shown in Figure 3).

For example, as per IEC 62443-4-2, a risk assessment targeting the entire IACS must be conducted and the outcomes will condition the decisions that determine the target security levels for equipment.[5]

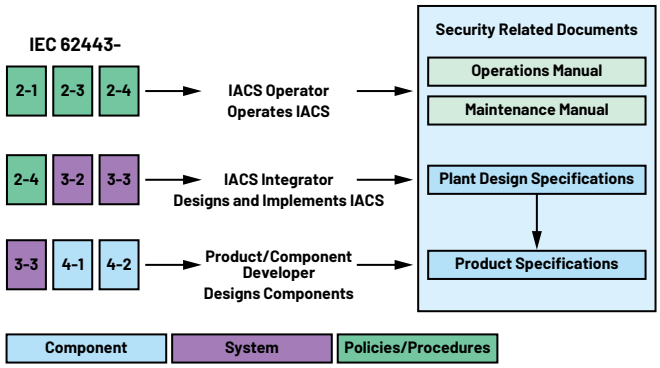

Figure 3. A high level view of the certification process.

Designing IEC 62443 Compliant Equipment

Highest Security Levels Call for Hardware Implementation

The IEC 62443 defines security levels in straightforward language as shown in Figure 4.

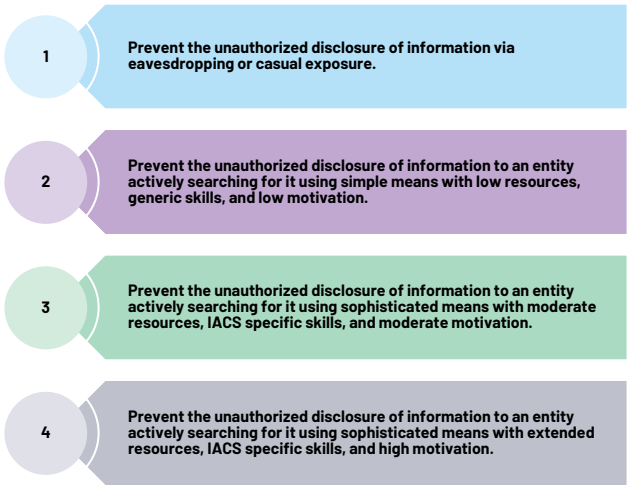

Figure 4. The IEC 62443 levels of security.

The IEC 62443-2-1 mandates a security risk assessment. As an outcome of this process, each component is assigned a target security level (SL-T).

As per Figure 1 and Figure 3, some parts of the standard deal with processes and procedures while IEC 62443-4-1 and IEC 62443-4-2 address the components' security. Component types as per IEC 62443-4-2 are software applications, host devices, embedded devices, and network devices. For each component type, IEC 62443-4-2 defines the capability security level (SL-C) based on the component requirement (CR) and requirement enhancement (RE) they meet. Table 1 summarizes SL-A, SL-C, SL-T, and their relationship.

Table 1. Security Levels Summary

	Target Security Level	Capability Security Level	Achieved Security Level
Acronym	(SL-T)	(SL-C)	(SL-A)
Definition	The security level equipment should reach according to the system-level risk assessment	The security level equipment is capable of according to the CRs it supports as per IEC 62443-4-2	The security level that equipment achieves
Objective	SL-T ≥ level defined by risk assessment	SL-C ≥ SL-T	SL-A ≥ SL-T

Let's take the example of a network-connected programmable logic controller (PLC). Network security requires that the PLC is authenticated so that it does not become an entry door for attacks. A well-known technique is public key-based authentication. With regards to the IEC 62443-4-2:

- Level 1 does not consider public key cryptography
- Level 2 requires the commonly adopted processes such as certificates signature verification
- Levels 3 and 4 call for hardware protection of the private keys used in the authentication process

Starting at Security Level 2, many security functions are required, including mechanisms based on cryptography involving secret or private keys. For security levels 3 and 4, hardware-based protection of security or cryptography functions is required in many cases. This is where industrial component designers will benefit from turnkey security ICs, embedding essential mechanisms such as:

- Secure key storage
- Side-channel attacks protection
- Commands taking care of functions such as
  - Message encryption
  - Digital signature computation
  - Digital signature verification

These turnkey security ICs relieve IACS component developers from investing resources into complex security primitive design. Another benefit of using security ICs is to inherently take advantage of the natural isolation between general-purpose functions and dedicated security functions. The strength of security functions is more easily evaluated when security is concentrated in an element rather than spread throughout the system. Also gained from this isolation is the preservation of the verification of the security function across software and/or hardware modifications of the component. Upgrades can be performed without the need to reassess the complete security function.

Furthermore, secure ICs vendors can implement extremely strong protection techniques that are not accessible at the PCB or system level. This is the case of hardened EEPROM or Flash memory or physical unclonable function (PUF) that can achieve the highest level of resistance against the most sophisticated attacks. Overall, security ICs are a great foundation to build system security.

Securing at the Edge

Industry 4.0 means sensing everywhere, any time, and thus calls for the deployment of more edge devices. IACS edge devices include sensors, actuators, robot arms, PLCs with their I/O modules, etc. Each edge device is connected to a highly networked infrastructure and becomes a potential entry point for hackers. Not only does the attack surface expand proportionally with the number of devices, but the diverse composition of devices inherently expands the variety of attack vectors. "Given existing platforms, there's a lot of viable attack vectors and increased exposure of both the endpoint and the edge devices," said Yaniv Karta, CTO of the app security and penetration-testing vendor, SEWORKS. As an example, in a complex IACS, not all sensors come from the same vendor, nor do they share the same architecture in terms of microcontrollers, operating systems, or communication stacks. Each architecture potentially carries its own weaknesses. As a result, the IACS accumulates and is exposed to all their vulnerabilities, as illustrated by the MITRE ATT&CK database[6] or the ICS-CERT advisories.[7]

Moreover, with the Industrial Internet of Things IoT (IIoT) trend of embedding more intelligence at the edge,[8] devices are being developed to make autonomous system decisions. Therefore, it is even more critical to ensure that device hardware and software can be trusted given these decisions are critical to safety, operation of the system, and more. Additionally, protecting the R&D IP investments of device developers from theft—related to AI algorithms, for example—is a common consideration that can drive the decision to adopt the protection that a turnkey security IC can support.

Another important point is that insufficient cybersecurity may negatively impact functional safety. Functional safety and cybersecurity interactions are complex and discussing them would deserve a separate article, but we can highlight the following:

- IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems mandates cybersecurity risks analysis based on IEC 62443.
- While IEC 61508 focuses primarily on hazard and risk analysis, it mandates subsequent security threat analysis and vulnerability analysis each time a cybersecurity occurrence is serious.

The IACS edge devices we listed are embedded systems. IEC 62443-4-2 defines specific requirements for these systems such as malicious code protection mechanisms, secure firmware updates, physical tamper resistance and detection, the root of trust provisioning, and integrity of the boot process.

Meet Your IEC 62443 Objectives with ADI's Secure Authenticators

Secure authenticators, also referred to as secure elements, from Analog Devices have been designed to address these requirements with ease of implementation and cost efficiency in mind. Fixed-function ICs that come with a full software stack for the host processor are turnkey solutions.

As a result, security implementation is delegated to ADI and components designers can focus on their core business. Secure authenticators are the root of trust by essence, providing secure and immutable storage of root keys/secrets and sensitive data representative of the state of the equipment, such as firmware hashes. They feature a comprehensive set of cryptographic functions including authentication, encryption, secure data storage, life cycle management, and secure boot/update.

ChipDNA™ physically unclonable function (PUF) technology utilizes the naturally occurring random variation in wafer manufacturing processes to generate cryptographic keys rather than storing them in traditional EEPROM of Flash. The variations exploited are so small that even the expensive, most sophisticated, invasive techniques used for chip reverse engineering (scanning electron microscopes, focus ion beams, and microprobing) are inefficient to extract keys. No technology outside of integrated circuits can reach such a level of resistance.

Secure authenticators also enable certificates and chains of certificate management.[9]

In addition, ADI offers a highly secure key and certificate preprogramming service in its factories, so that original equipment manufacturers (OEMs) can receive parts already provisioned that can seamlessly join their public key infrastructure (PKI) or enable offline PKI. Their robust cryptographic capabilities enable secure firmware updates and secure boot.

Secure authenticators are the best option to add high grade security to an existing design. They save the R&D effort of rearchitecting a device for security for a low BOM cost. For example, they do not require changing the main microcontroller. As examples, the DS28S60 and MAXQ1065 secure authenticators address all levels of the IEC 62443-4-2 requirements as illustrated in Figure 5.

The DS28S60 and MAXQ1065 3 mm × 3 mm TDFN packages make them suitable for the most space-constrained design and their low power consumption perfectly addresses the most power-constrained edge devices.

Table 2. DS28S60 and MAXQ1065 Key Parameters Summary

Device Features	DS28S60/MAXQ1065
Operating Temperature	–40°C to +105°C
Host Interface	SPI (I²C in development)
Supply Voltage	1.62 V to 3.63 V
Maximum Active Current	3 mA
Typical Idle Current (25°C)	0.4 mA
Power Down Current (25°C)	100 nA

IACS component architectures already featuring a microcontroller with the security functions to address IEC 62443-4-2 requirements can also benefit from secure authenticators for keys and certificate distribution purposes. This would save the OEMs or their contract manufacturers from investing in costly manufacturing facilities needed to handle secret IC credentials. This approach would also protect keys stored in microcontrollers to be extracted through debugging tools such as JTAG.

Full portfolio and product details can be found at analog.com/en/product-category/secure-authenticators.html.

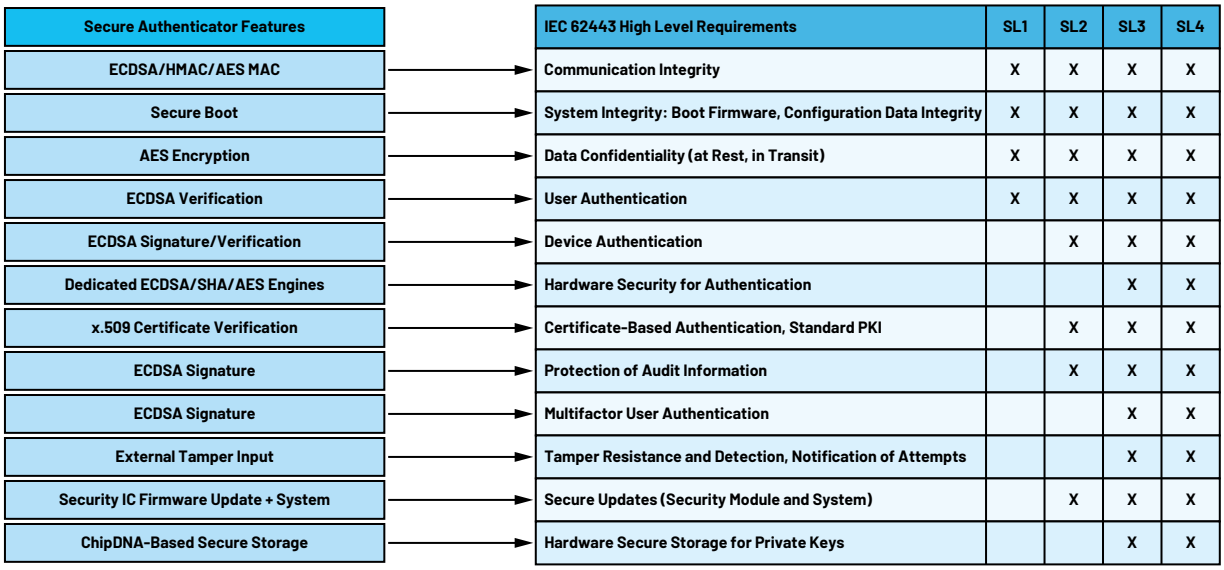

Figure 5. Secure authenticators features mapping to IEC 62443 requirements.

Conclusion

By putting together and adopting the IEC 62443 standard, IACS stakeholders have paved the road for dependable and safe infrastructures. Secure authenticators are the bedrock of the future of IEC 62443 standard-compliant components requiring robust hardware-based security. OEMs can design with assurance, knowing that secure authenticators will help them achieve the certifications they seek.

References

[1] Lorenzo Franceschi-Bicchierai. "Ransomware Gang Accessed Water Supplier's Control System." Vice, August 2022.

[2] "Protecting Critical Infrastructure." Cybersecurity and Infrastructure Security Agency.

[3] Bruce Schneier. "The Story Behind The Stuxnet Virus." Forbes, October 2010.

[4] "ISASecure CSA Certified Components." ISASecure.

[5] Patrick O'Brien. "Cybersecurity Risk Assessment According to ISA/IEC 62443-3-2." Global Cybersecurity Alliance.

[6] ATT&CK Matrix for Enterprise." MITRE ATT&CK®.

[7] "Cybersecurity Alerts & Advisories." Cybersecurity and Infrastructure Security Agency.

[8] Ian Beavers. "Intelligence at the Edge Part 1: The Edge Node." Analog Devices, Inc., August 2017.

[9] "Trust Your Digital Certificates—Even When Offline." Design Solutions, No.56, May 2017.

About the Author

Christophe Tremlet is a director of business management for the secure authenticator product line in EMEA. He has more than 25 years of experience related to security ICs and he has managed product engineering and applications. Christophe was a chief technical officer at Innova Card, a startup specializing in secure microcontrollers, and he has held engineering and business positions at Maxim Integrated. After three years at Thales as a marketing and sales director, Christophe joined Analog Devices.