ANALOG DEVICES

Industrial Cybersecurity Demystified

VISIT ANALOG.COM/CYBERSECURITY

THE TRUSTED EDGE OF THE MODERN DIGITAL FACTORY

Digital transformation has been a catalyst for change in industry, with digitization producing more and more data to enable real-time decision-making for increased automation and enhanced process efficiency. To maximize the use of this data, digital enterprises have become increasingly networked which requires the convergence of the OT (operational technology) and office IT (information technology) networks. This rapid technology advancement has unlocked the power of the intelligent edge, making seamless edge to cloud connected operations possible. With the advancing adoption of digital connectivity technology bringing increased bandwidth and access to insights from all corners of the process plant and factory floor, a heightened level of cybersecurity vulnerability needs to be considered. With IP addressability at all nodes and the removal of gateway devices brought about by newer industrial Ethernet technology infrastructures, securing devices and systems from cyberattack is paramount. Not only are the potential costs of these attacks extremely high, they can also endanger human lives in the case of safety-related control systems.

Today, companies need to consider how to operate in a world where industrial automated control systems (IACS) are resilient to cyberattacks. Control systems manage commands, regulate the behavior of other devices and pose a threat to the entire manufacturing infrastructure if attacked. Cyberattacks can be invasive or non-invasive. In an invasive attack, a cybercriminal opens the device's enclosure to manipulate its memory content, replace firmware, or probe PCB traces. Non-invasive attacks are usually performed remotely through communication ports and target security flaws in the device's firmware.

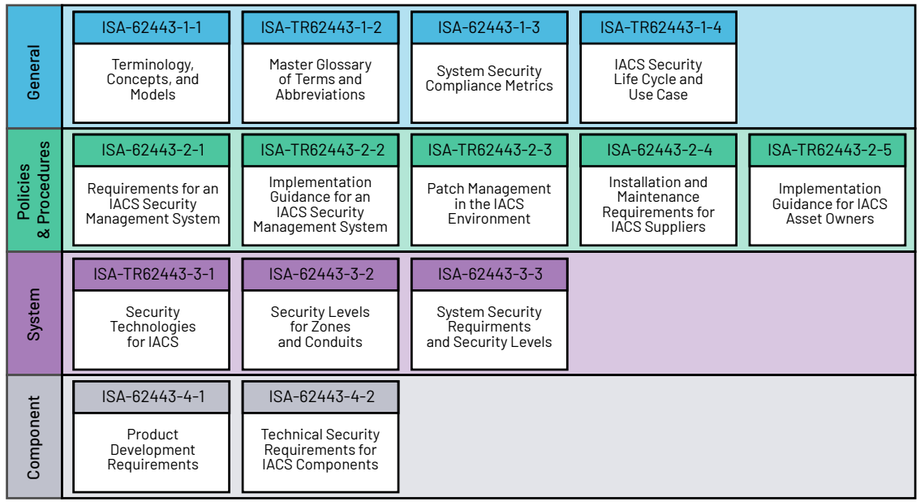


Figure 1: *IEC 62443 Series Security Standard*

The EU Cyber Resilience Act (CRA) is a new EU law governing the cybersecurity of digital products sold in the EU with a global impact on manufacturers, developers and vendors of "products with digital elements" (PDEs) destined for the EU market, including the introduction of compulsory product CE markings by 2027. This has resulted in a prioritization of upfront security considerations being built into new product development cycles, as failure to do so could mean that new products in development today will not meet the standards required to be sold into the EU market after 2027.

INTERESTED IN LEARNING MORE? Read "*The IEC 62443 Series of Standards: How to Defend Against Infrastructure Cyberattacks*" Technical Article from Analog Devices

To facilitate adoption of the CRA provisions, the European Union Agency for Cybersecurity (ENISA) has mapped the EU CRA requirements to the IEC 62443-4 standard. The IEC 62443 series of standards is designed to address cybersecurity for operational technology in automation and control processes. This leading standard offers an extensive layer of security to prevent attacks and mitigate their effects. It is organized into four levels and categories – "General" topics that are common to the entire series; "Policies & Procedures" focuses on methods and processes associated with IACS security; "System" outlines requirements at the system level and "Component" provides detailed requirements for IACS products.

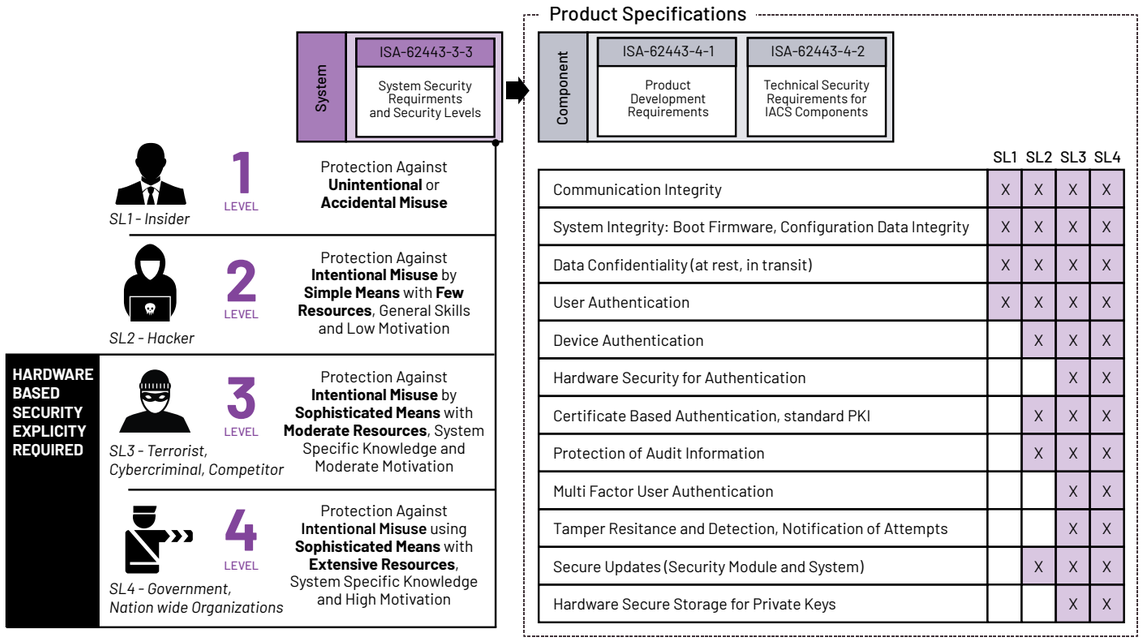


Figure 2: *IEC 62443 Component Requirements mapped to desired System Security Levels*

To design a secure component, it is important to first decide the level of security a device will require by performing a risk assessment. The outcome of the assessment will clarify if a device needs to withstand Level 1 "Insider" attacks, which are typically unintentional or accidental misuse security breaches; Level 2 "Hackers" intentionally seeking to do harm on limited resources; up to Level 3 "Cybercriminal" and Level 4 "Governments" who intend harm and have sophisticated resources to attack systems.

The combination of ISA-62443-3-3 "System Security Requirement and Security Levels" and the component level specifications (ISA-62443-4-1, ISA-62443-4-2) prescribe how to design secure components that can withstand cyberattacks. Based on the desired security levels, specific requirements need to be catered for within the design. All levels require confidentiality for data identified as sensitive. Device authentication is required for security levels SL2-SL4, while hardware secure storage for private keys is specified for any device looking to achieve SL3-SL4 operation. ADI's secure product development lifecycle is certified to IEC-62441-4-1:2018.

UNDERSTANDING INDUSTRIAL SECURITY VULNERABILITIES

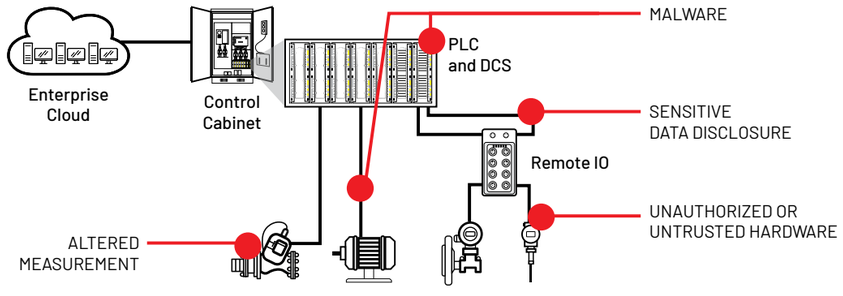


Figure 3: *Common Security Vulnerabilities in Industrial Applications*

Within an industrial setting, there are a number of areas of vulnerability that need to be secured to ensure the integrity of the operating infrastructure. Let's consider four common ones, all of which can be secured against with turnkey secure ICs, embedding essential mechanisms such as secure key storage and relieving IACS component developers from investing resources into complex security primitive design. The addition of a **secure IC** to a non-secure system increases the level of system security without forcing an architectural redesign. Such a device must be specialized, incorporating strong cryptography functions, yet be flexible enough to support a variety of system-level security functions. See Selection Tables for specific product recommendations.

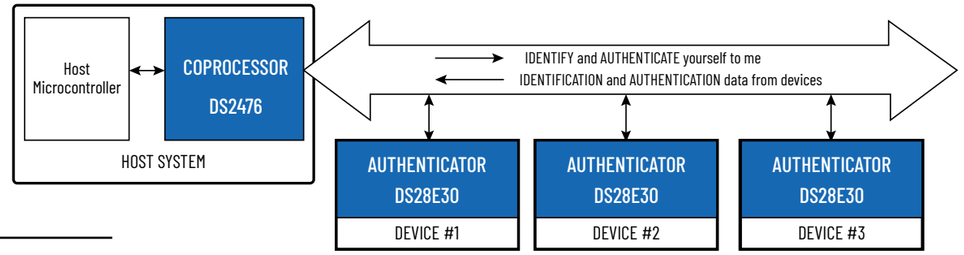


Figure 4: *How Secure Authenticators and Coprocessors can Simplify Cryptography*

UNAUTHORIZED OR UNTRUSTED HARDWARE

Establishing trust between devices can be accomplished using challenge-response **authentication**, which relies on a shared secret key in the case of symmetric authentication, or a private/public key pair for asymmetric authentication. While the public key is designed to be known publicly, both the secret key and private key are a security risk - if stolen, the security of the entire network is at risk.

Although the public key doesn't need to be kept secret, it is important to know the public key is genuine. A device can have their public key and device ID certified by a third-party certificate authority (CA), who issue a digital certificate. During the key authentication process, the CA's public key can be used to verify that the supplied device public key is authentic.

Challenge-response authentication is reliant on the ability to generate a true random bit stream referred to as a nonce. The use of a strong randomly generated nonce on each exchange protects against the possibility of a "replay attack". Secure authenticators can be used as turnkey authentication solutions capable of performing challenge-response authentication.

SENSITIVE DATA DISCLOSURE

Protection of data at rest within a device or in transit when communicating with other systems on the network relies on encryption. Using proven **encryption** methods such as the advanced encryption standard (AES), sensitive data disclosure can be avoided.

In situations where attacks are at the device level, where the data is considered at rest, secure memory storage ensures that, even if the memory is accessed, all data is encrypted with methods that utilize the random characteristics of the individual device when manufactured to create a physically unclonable function (PUF). In PUF-based ChipDNA® **secure authenticators** from Analog Devices, each key is generated as a precise analog characteristic of the IC and is never stored in memory, making it immune to all known invasive attack tools and capabilities.

Where data is in transit, encrypting the message data ensures no sensitive information will be disclosed to anyone eavesdropping on the network. The Transport Layer Security (TLS) protocol is the most used protocol for protecting data in transit, ensuring **authenticity**, **integrity** and **confidentiality** of the communication.

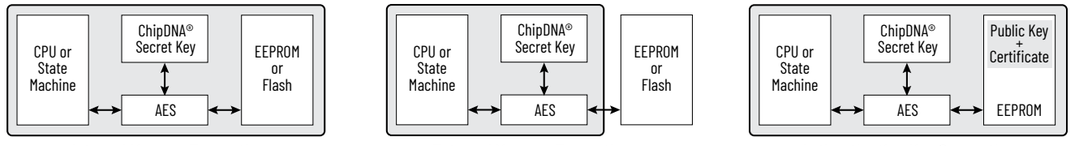


Figure 5: *ChipDNA® PUF Security Configurations*

MALWARE

Any device connected to a non-secure network, like the internet, can be vulnerable to malware attacks. Devices that require updates from manufacturers need a means to verify that the update is authorized and not modified. **Digital signatures** ensure that only verified firmware is accepted. Devices that have secure boot functionality ensure the authentication of a device's firmware on power-up. If modified firmware has been introduced to the device, the system will refuse to boot up as the firmware is no longer a cryptographic match to what the manufacturer originally implemented on the device, and the digital signature is invalid.

ALTERED MEASUREMENT

Data manipulation, or altered edge device measurements, can result in distorted perceptions of the health of a system. As more systems are automated, the ability to ensure data-driven decisions are being made from trusted measurements is vital. If a bad actor is maliciously trying to influence edge device operation or tamper with status messages, verifying commands through signatures eliminates the potential for altered measurements affecting operations.

KEY TAKEAWAYS

For a system to be secure, devices need the ability to create trusted connections using **authentication**. Devices need to ensure information **confidentiality** using encryption and decryption and be capable of verifying the **integrity** of commands to minimize the potential attack points that a bad actor could exploit to gain control over industrial processes. Turnkey secure ICs from Analog Devices provide these capabilities, increasing system security without forcing IACS architectural redesign.

DIGITAL CERTIFICATES AND PROVISIONING

A message signed by a **digital signature** from the sender can be used to prove that the message is sent by the sender and it is unaltered. However, a digital signature alone cannot prove the identity of the sender. Proof of identity is achieved using a **digital certificate**. This digital document contains public key and ID information that can be used to verify the ownership of the key. As a service, the certificates and keys can be programmed by ADI on behalf of the customer. By leveraging digital certificates and secure provisioning practices, industrial organizations can significantly enhance their cybersecurity infrastructure, ensuring the integrity, confidentiality, and authenticity of their critical systems and data.

Digital Certification

Digital document verifying key ownership

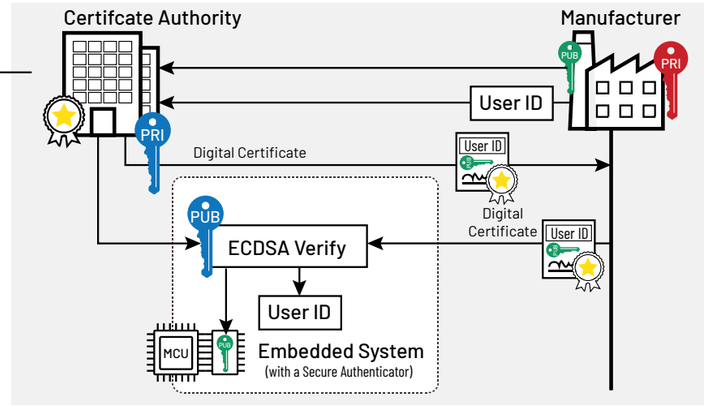


Figure 6: *Using a Certificate Authority to generate a Digital Certificate*

FIRMWARE UPDATE

Critical firmware updates can be deployed to devices in the field using signed messages, guaranteeing the firmware is both authentic and unmodified.

Signed Messages

Ensure authenticity and integrity of information

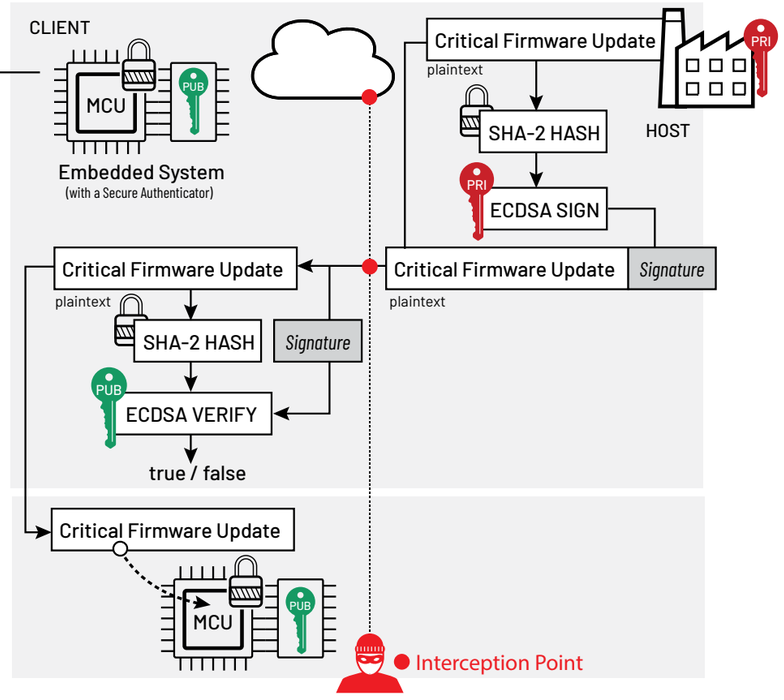


Figure 7: *Firmware Update Process*

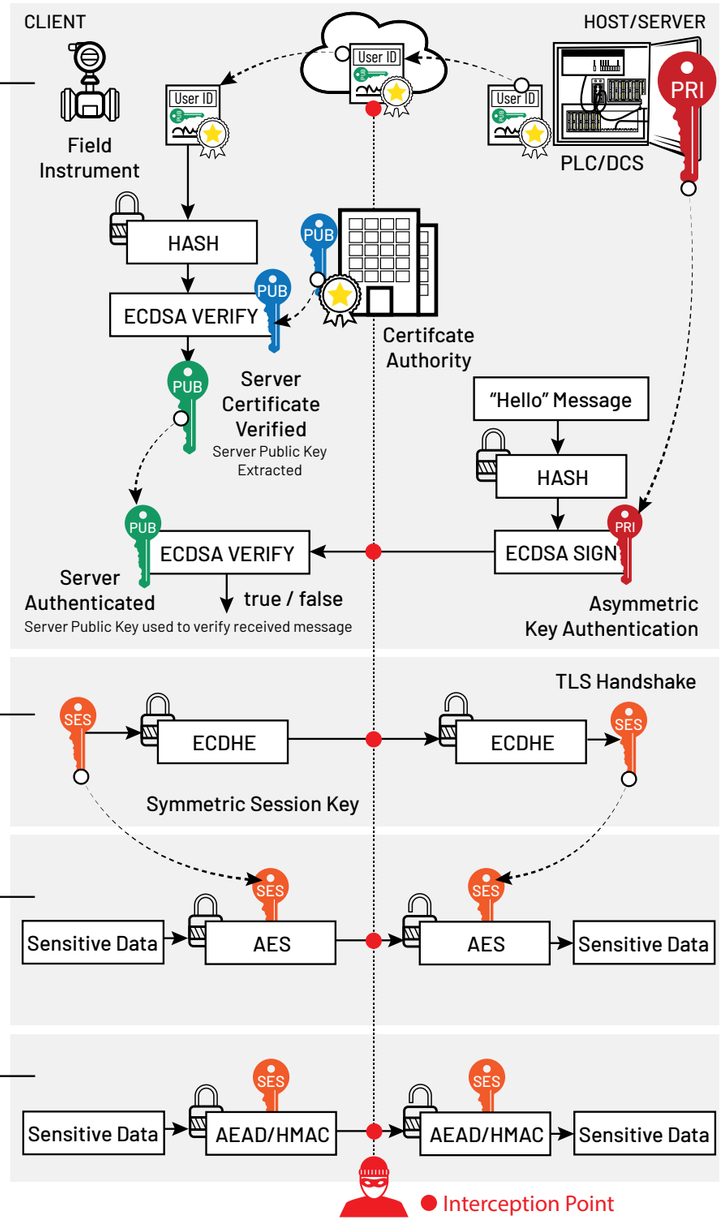
HARDWARE AUTHENTICATION AND SECURE COMMUNICATION

A hardware authentication process begins with a key pair exchange between a host (PLC) and a client (field instrument). Captured below is a certification-based authentication process that happens in two stages: first the client verifies the host/server certificate using the CA public key so that the host public key is trusted. The public key is then used to verify the signature of a nonce (in this case, the "Hello" data previously exchanged) computed by the host. In the TLS protocol, once the server has been authenticated, using the symmetric ECDH or ECDHE algorithm, a shared communication key (also known as a session key) is created. This session key is further used to encrypt payload data so that the server and client can exchange confidential information. TLS guarantees integrity either by authenticated encryption (e.g. AES GCM or AES CCM) or by appending a HMAC (Hash-based Message Authentication Code). After the communication has ended, the session keys are discarded.

Figure 8: *Hardware Authentication and Communication Process*

TLS Server Authentication

Server certificate verification and authentication



For commonly used cybersecurity terms, check out this glossary.

ADI Assure™ is a suite of products that provides robust protection against security threats to deliver a persistent state of assurance. With our trusted edge solutions, the security boundary is closer to the data's origin, resulting in higher confidence in its authenticity and trustworthiness. We are committed to helping our customers to meet industry cybersecurity standards and regulatory requirements swiftly and bolster their defenses against evolving security threats throughout the life of their products. Our leading-edge technologies such as **ChipDNA® PUF**, tamper-resistant key storage, and advanced crypto algorithms enhance security architectures and provide heightened resistance against invasive and non-invasive attacks. Our rich portfolio of scalable and flexible security solutions with hardware-based root of trust and software services offers sustained protection and ease of integration, ultimately safeguarding systems, accelerating the cybersecurity certification journey, and enabling resilience for the long term.

DEVICE SELECTION FOR HARDWARE AUTHENTICATION, ANTI-COUNTERFEITING, CALIBRATION AND USAGE CONTROL

AUTHENTICATORS	Secret Key SHA-2	Secret Key SHA-3	Public Key ECDSA	Secret Key SHA-2 & Public Key ECDSA
I2C	DS28C22	DS28C50* DS28C16	DS28C36* DS28C39*	DS28C40
1-Wire	DS28E(L)25 DS28E(L)22 DS28E(L)15	DS28E50* DS28E16	DS28E38* DS28E39* DS28E30	DS28E36 DS28E40
NFC	MAX66240 MAX66242	MAX66250		
COPROCESSORS				
I2C	DS2465	DS2477*		DS2476 DS2478
NFC	MAX66300	MAX66301		

** ChipDNA® PUF Technology*

SECURE IC FOR SECURE BOOT, SECURE FIRMWARE UPDATES, SECURE COMMUNICATION, AND TLS SUPPORT

SECURE ELEMENT		ECDSA	ECDH	AES 128/256	Certificates	TLS Software Stack
SPI	DS28S60*	X	X	X	Custom	
SPI	MAXQ1065*	X	X	X	x.509	OpenSSL, mbedTLS, WolfSSL

** ChipDNA® PUF Technology*

ANALOG DEVICES

VISIT ANALOG.COM/CYBERSECURITY