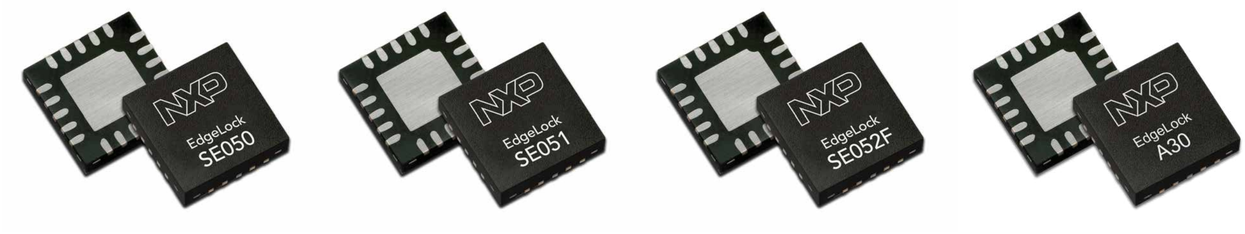
Use Case

EdgeLock® secure elements
and authenticators

Securing the Industrial IoT

Securing the Industrial IoT

Integrating a secure element into an industrial device adds security and integrity to the design, by protecting against unauthorized access and data manipulation, and is also a convenient way to meet the strict standards such as ISA/IEC 62443 and the EU Cyber Resiliance Act (CRA).



Challenge

The Industrial Internet of Things (IIoT) can represent a significant risk, since connected IIoT devices are enticing targets for cyber criminals looking for unauthorized access to the network. Taking advantage of weak security protections, hackers are known to use IIoT devices as entry points. Once inside, they have the potential to manipulate or steal data generated by sensors, disrupt production processes or, worse yet, trigger a complete shut-down of operations. To address these risks, several standards and regulations, such as IEC 62443 and the Cyber Resilience Act (CRA), have been established or are currently being developed.

ISA/IEC 62443: Addressing cybersecurity for operational technology (OT) in industrial automation and control systems (IACS), this set of standards provides cybersecurity reference architectures as well as direction of security processes, requirements, technology, controls, security acceptance and factory testing, product development, security lifecycles, and a cybersecurity management system (CSMS). The standards, which are applicable to manufacturing and processing plants and facilities, include five Security Level (SL) grades, ranging from SL 0, the minimum, to SL 4, the "most vulnerable" level, so developers can find the suitable level of protection for uptime, safety and intellectual property.

Cyber Resilience Act (CRA): This EU-wide legislation, the first of its kind, describes the cybersecurity requirements for hardware and software products with digital elements. All products with digital elements sold in the EU, regardless of their place of origin or date of introduction, must comply by December 11, 2027. The CRA requires products to be 1) secure by default, 2) equipped with mechanisms that mitigate the effect if a vulnerability is found and exploited, and 3) covered by processes that ensure a security incident is addressed professionally and resolved quickly. The CRA requirements also span the design, development and maintenance of products. Details of the conformance process and product categories continue to evolve, making it important to check specifics before starting a design.

IIoT devices that conform to ISA/IEC 62443 and CRA standards can be trusted to protect data and minimize risk, because they use industry-recognized mechanisms to address and mitigate current and future security vulnerabilities. Implementing the security requirements by ISA/IEC 62443 and CRA standards, however, can be challenging to those who don't regularly work with security processes.

Applications

PLCs

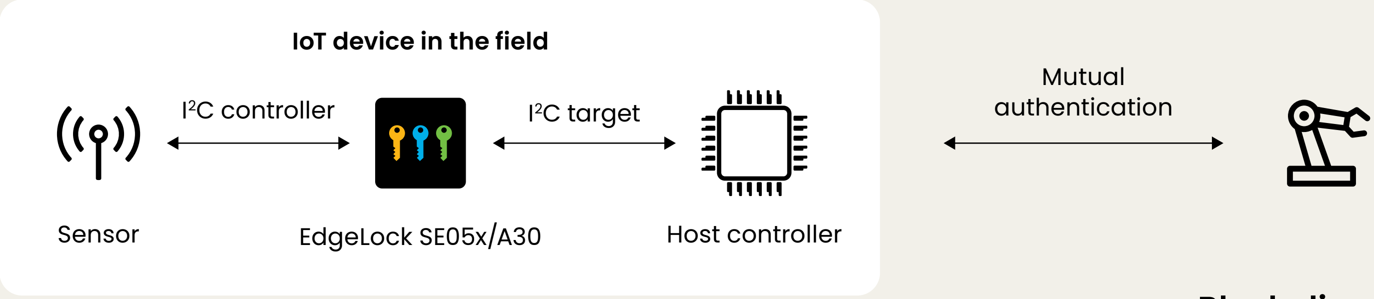
Motor drives

Motion control

Robotics

Industrial networking devices

HMI



Block diagram

Solution

The EdgeLock SE05x secure elements (SE) and the EdgeLock A30 secure authenticator (SA) are tamper-resistant, CC EAL 6+ certified platforms that help secure IIoT devices and meet the stringent requirements of ISA/IEC 62443 and CRA standards, while eliminating much of the complexity of the security implementation.

The EdgeLock SE05x/A30 comes with a pre-installed feature rich security applet, designed for use with the IIoT, as well as an extensive set of enablement in terms of middleware components that simplify integration. It includes extensive countermeasures to address the most recent attack scenarios and includes well-established security primitives, such as ECC and AES cryptography algorithms.

When used as a root of trust, the EdgeLock SE05x/A30 also supports on-chip key generation, with hardware-based secure key storage. To reduce time-to-market and cost for complex PKI infrastructures, the EdgeLock SE05x/A30 can be preconfigured with credentials, during production or before shipment from a distributor. Also, because the credentials are securely stored in silicon, and never leave the IC, the chain of trust is preserved during the entire product lifecycle. The result is true end-to-end security for IIoT devices.

The EdgeLock SE05x/A30 platform is designed to satisfy the ISA/IEC 62443 requirements relating to device identity, crypto functionality, secure provisioning, secure storage, and secure protocols. In particular, the EdgeLock SE05x/A30 provides the IIoT device with a secure identity that is then used with mutual authentication, sensor authentication, cloud onboarding, and other IIoT tasks. As shown in the block diagram, the EdgeLock SE05x/A30 connects to the host controller using an I²C target device. The secure communication channel, established by middleware and a secure channel between the SE/SA and host, uses the preinjected credentials in the EdgeLock SE05x/A30 as part of the authentication process.

Learn more

The NXP Design Community site offers helpful hints, easy-to-follow how to's and detailed application notes for use with the EdgeLock secure elements and authenticators, while our product pages link to detailed specs, designs tools & software, training & support and more.

NXP Design Community

community.nxp.com/t5/Secure-Authentication/bd-p/secure-authentication

EdgeLock SE050 Secure Element

nxp.com/SE050

EdgeLock SE051 Secure Element

nxp.com/SE051

EdgeLock SE052F Secure Element

nxp.com/SE052F

EdgeLock A30 Secure Authenticator

nxp.com/A30

EdgeLock 2GO

nxp.com/EdgeLock2GO

Application notes

Ease ISA/IEC 62443 compliance with EdgeLock SE05x

Ease ISA/IEC 62443 compliance with EdgeLock A30

Ease CRA compliance with EdgeLock Discrete Portfolio

nxp.com/iotsecurityusecase

Date of release: October 2025