NXP EdgeLock™ SE050

Use Case:
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 requirements of ISA/IEC 62443 standards.

APPLICATIONS

IACS	PLCs	Motor drivers	Sensors	Smart robotics

CHALLENGE

As part of the growing trend toward Industry 4.0, manufacturers across industries are investing in the Industrial Internet of Things (IIoT), to help use resources more efficiently and increase productivity. Driven in part by advances in sensor technology and wireless connectivity, the widespread availability of sophisticated data analytics, and the expansion of edge computing, the IIoT offers new ways for manufacturers to improve operational efficiency and enhance decision-making.

At the same time, though, the 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.

The Industrial Automation and Control Systems (IACS) used to support critical infrastructure, for example, are particularly

PLUG&TRUST

NXP

Securing tomorrow's IoT. *Today.*

vulnerable targets of attack. The ISA/IEC 62443 series of standards, developed by industrial cyber security experts, is designed to protect IACS deployments for their entire lifecycle and, as a result, has gained global support as a way to improve the safety, availability, integrity, authenticity, and confidentiality of IIoT systems.

IIoT devices that conform to ISA/IEC 62443 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 standards, however, can be challenging to those who don't regularly work with security processes.

SOLUTION

The EdgeLock SE050 is a tamper-resistant, CC EAL 6+ certified platform that helps secure IoT devices and meet the stringent requirements of ISA/IEC 62443 standards, while eliminating much of the complexity of the security implementation.

The EdgeLock SE050 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 RSA cryptography algorithms.

When used as a root of trust, the EdgeLock SE050 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 SE050 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 SE050 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 SE050 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 SE050 connects to the host controller using an I²C slave device. The secure communication channel, established by middleware and based on Secure Channel Protocol (SCP), uses the pre-injected credentials in the EdgeLock SE050 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 SE050. The EdgeLock SE050 Product Page links to detailed specs, designs tools & software, training & support, and more.
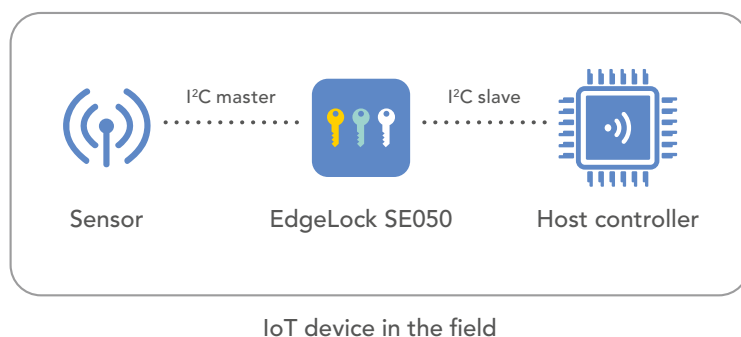
▶ **NXP Design Community**
  https://community.nxp.com/community/identification-security/secure-authentication/overview

▶ **EdgeLock SE050 Product Page**
  www.nxp.com/SE050

BLOCK DIAGRAM

Sensor   I²C master   EdgeLock SE050   I²C slave   Host controller   Mutual authentication

IoT device in the field

PLUG&TRUST