NXP EdgeLock™
SE050

Use Case:
Protect Sensor Data

Adding secure elements to a distributed sensor network protects against manipulation and unauthorized access to sensor data, so backend operation is safer and more reliable.

APPLICATIONS

Smart energy
(solar panels, gas pipelines, utility grids, etc.)

Machine monitoring
(temperature, pressure and humidity sensors)

Robotics

CHALLENGE

The distributed sensor networks used to monitor physical and environmental conditions often make use of sensors that operate on their own, without human supervision. These unattended sensors are prime targets for security attacks, with hackers either trying to manipulate sensor operation, so as to modify, copy, or steal data, or using compromised sensors to disrupt network operation.

Allowing tainted sensor data onto the network can lead to serious consequences, since inaccurate readings can trigger false conclusions in backend algorithms or unwanted reactions by personnel or machines in potentially dangerous situations.

PLUG&TRUST

NXP

Securing tomorrow's IoT. *Today.*

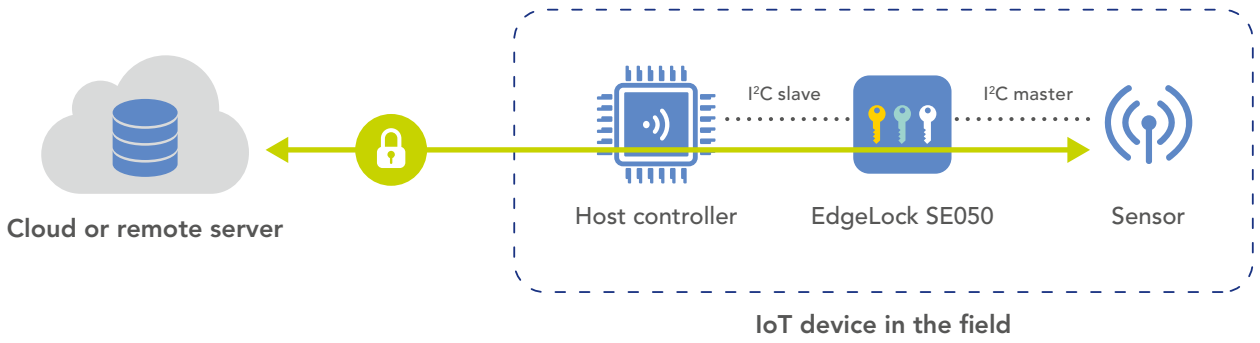
SOLUTION

The EdgeLock SE050 secure element connects directly via the I²C master interface to the sensors and protects the sensor data from manipulation. Located between the host controller and its associated sensors, the EdgeLock SE050 acts as a gatekeeper, verifying that all connected sensor data is locally generated and encrypted on EdgeLock SE050.

Before transmission to any network or cloud, EdgeLock SE050 establishes a secure SCP03 channel to the host controller and the cloud so data is sent securely. Ideally suited for use in the Internet of Things (IoT), EdgeLock SE050 is a Plug & Trust device that offers enhanced CC EAL 6+ based security for unprecedented protection against the latest attack scenarios.

- **Proof of Origin**
  The EdgeLock SE050 authenticates each sensor and verifies the integrity of transmitted sensor data to prevent data manipulation.
- **Local Encryption**
  The EdgeLock SE050 protects data from being disclosed while in transit. It encrypts and signs sensor data and then sends it to the host microcontroller using a secure communication channel based on the SCP03 protocol. At the server, when sensor data arrives for treatment and analysis, the encrypted and signed transmission verifies that the data it contains can be trusted as original and unharmed.

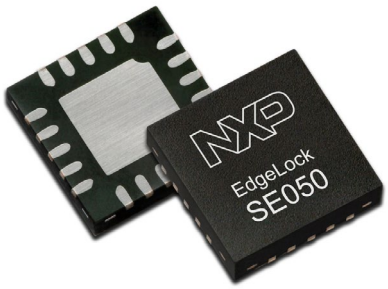
BLOCK DIAGRAM



LEARN MORE

The NXP Design Community site offers helpful hints and easy-to-follow how-to's, along with a full application note for configuring the EdgeLock SE050 as part of a distributed sensor network. The EdgeLock SE050 product page links to detailed specs, designs tools & software, training & support, and more.

- **NXP Design Community**
  community.nxp.com/community/identification-security/secure-authentication
- **EdgeLock SE050 Product Page**
  www.nxp.com/SE050



Find all information on **www.nxp.com/SE050**

Date of release: October 2019