Meeting IEC 62443
with NXP EdgeLock® Security

Technology Six Pack

June 2024

Industry faces challenges…

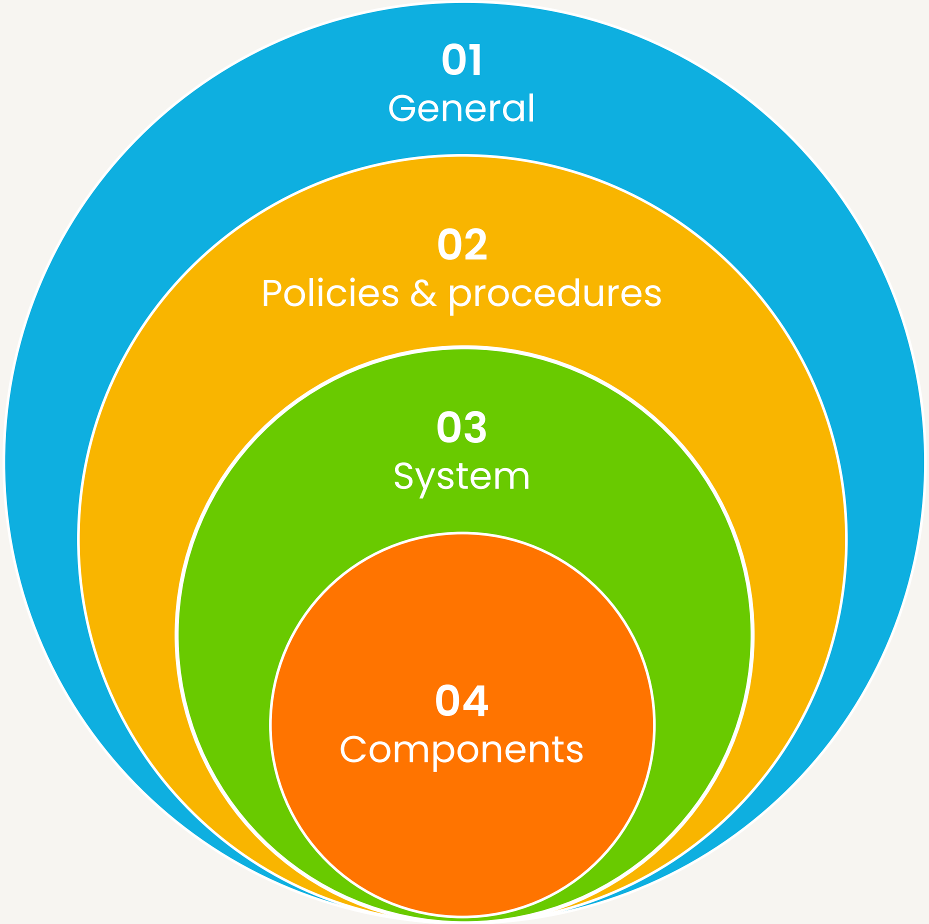
Connectivity opens routes into sensitive and critical infrastructures such as industrial & healthcare

Vulnerabilities left on devices are threats putting at risk availability of infrastructures & services, people safety and assets

Authentication in connected industrial networks is a must, as is confidentiality of sensitive data

Device security to protect from cyber threats and unauthorized access is essential

IEC 62443: a holistic protection scheme for industrial facilities



1-1	Terminology & concept
1-2	Master glossary
1-3	System Security compliance metrics
1-4	IACS security lifecycle and use case
2-1	Requirements for an IACS security management system
2-2	Implementation guidance
2-3	Patch management
2-4	Installation & maintenance
3-1	Security technologies for IACS
3-2	Security levels for zones conduits
3-3	System security requirements and levels
4-1	Product development requirements
4-2	Technical security requirements for IACS

IEC 62443 security levels

SL4 Intentional violation with sophisticated means and extended resources

SL3 Intentional violation with sophisticated means and moderate resources

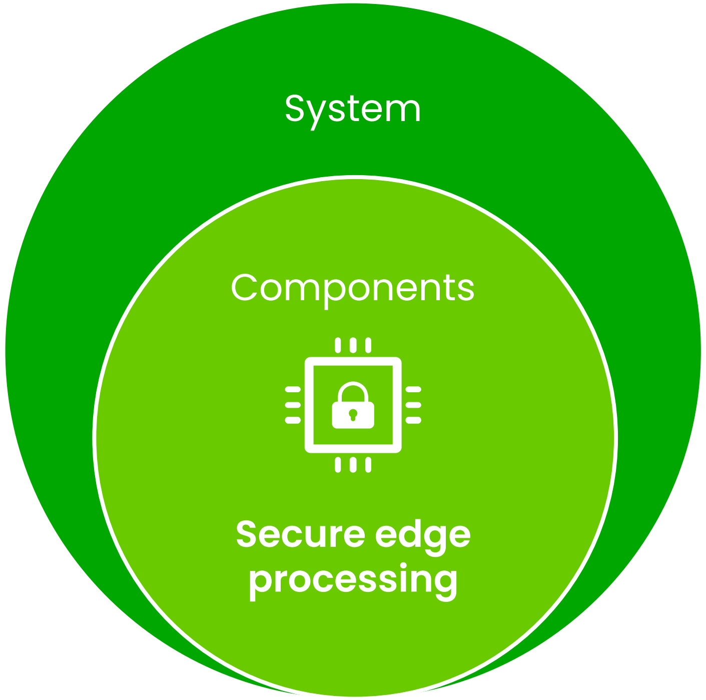
SL2 Intentional violation with simple means and low resources

SL1 Unintentional or coincidental violation

IEC 62443-4-2 sets of requirements

- Identification and authentication control
- Use control
- System integrity
- Data confidentiality
- Restricted data flow
- Resource availability
- Timely response to events

Silicon and its firmware are at the core of industrial infrastructures security

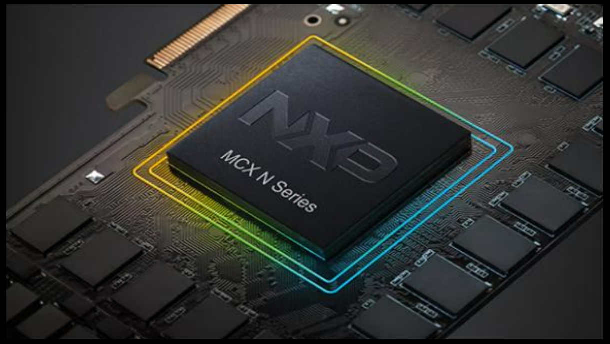


Secure edge processing

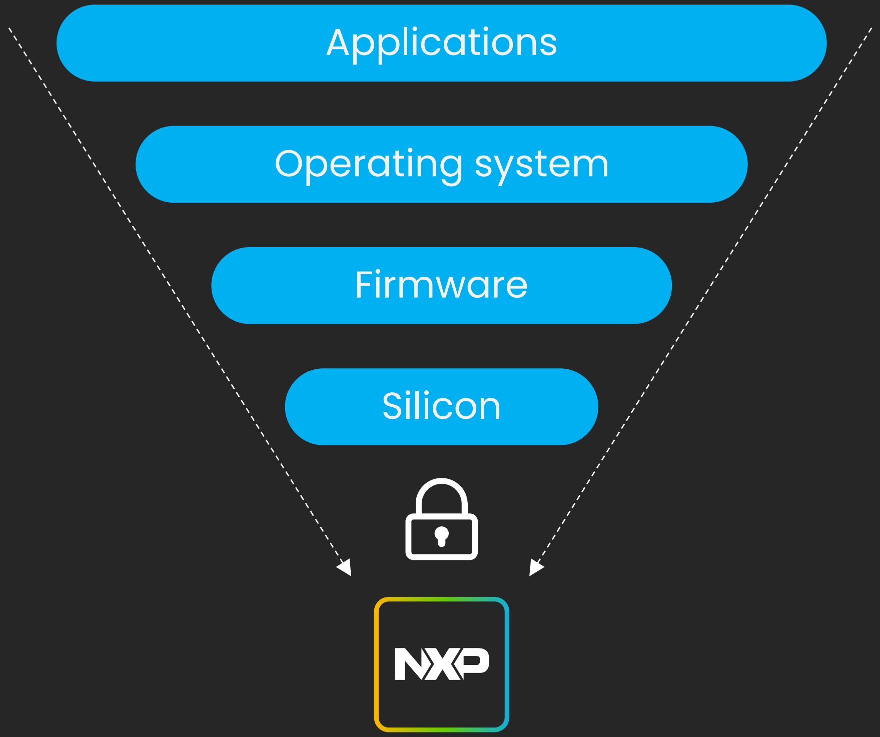
Secure application processors

Secure industrial networking controllers

Secure microcontrollers



Towards a silicon-based trust anchor to protect security functions



Silicon is the heart of the device

Connected devices are complex systems where software operating at different layers of abstraction executes over hardware

Silicon is trustworthy

The hardware is something that is inherently trustworthy. It’s something that can be relied upon, with a very high degree of confidence.

Implementation matters

Effective security solutions are the result of a strict development process, with clearly defined design rules, multiple iterations of careful review, and full control over the many sub-components involved in the design

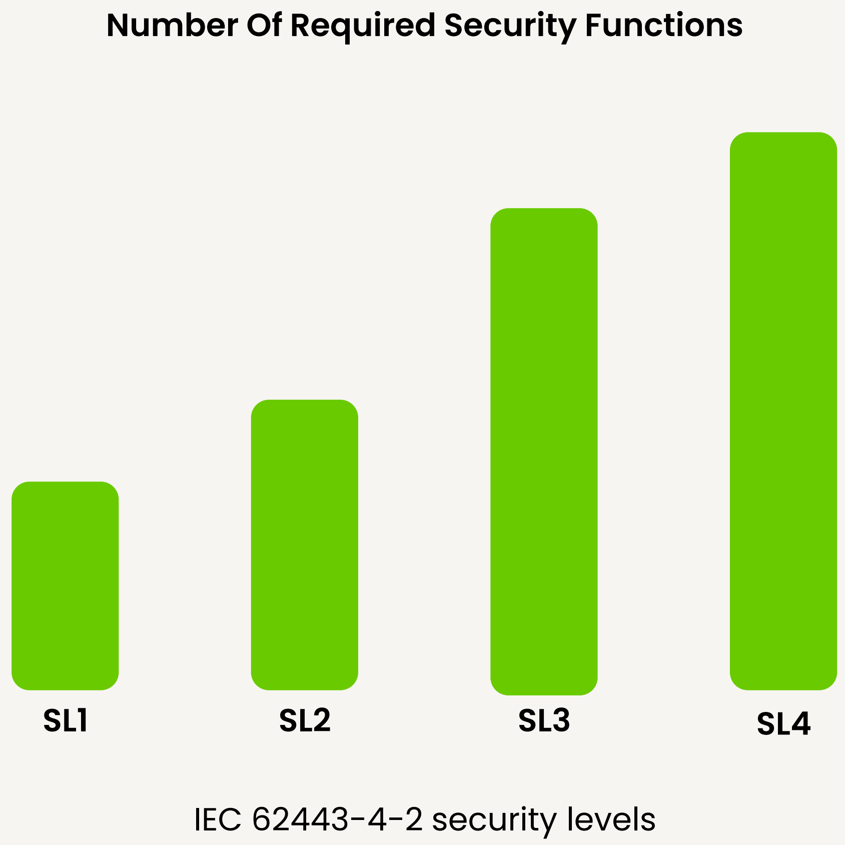
Hardware security level versus target IEC 62443 security level
A selection based on risk management

The number of required security functionalities by the standard increases with the targeted 62443-4-2 security level

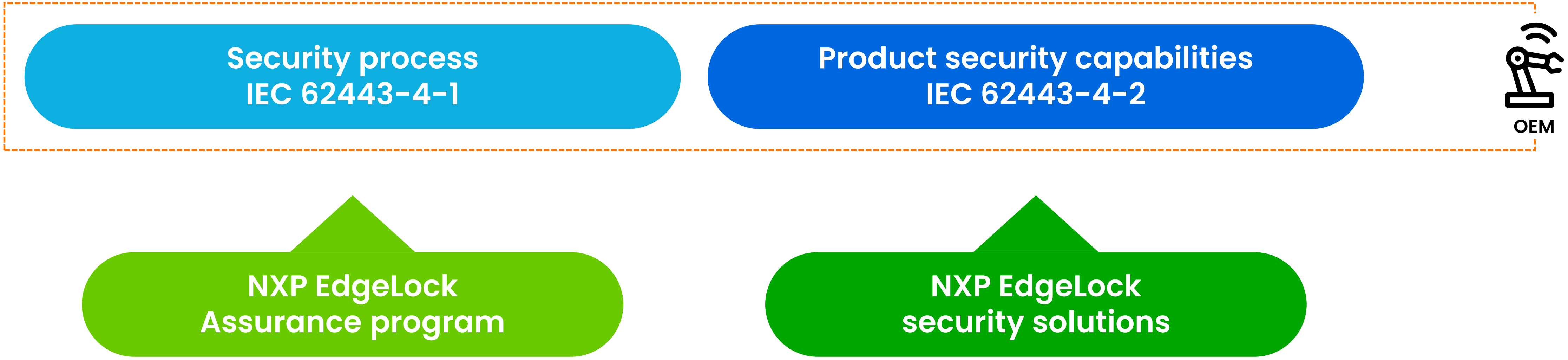
More hardware-based security is required beyond SL2

However, the standard does not specify robustness of required protection mechanisms and does not quantify attacker means & resources for each security level

The adequate level of countermeasures is subject to interpretation by certifying labs and will depend on intended usage conditions and exposure of the equipment to cyber risks (in manufacturing and in field)



NXP supports equipment manufacturers in meeting industry standards



Security process
IEC 62443-4-1

Product security capabilities
IEC 62443-4-2

OEM

EDGELOCK® ASSURANCE by NXP

NXP EdgeLock
Assurance program

NXP EdgeLock
security solutions

Certified EDGELOCK® ASSURANCE by NXP

The NXP EdgeLock Assurance provides confidence & assurance that NXP components have been developed with security in mind and according to the industry's best security practices; they have been thoroughly reviewed and comply with relevant standards

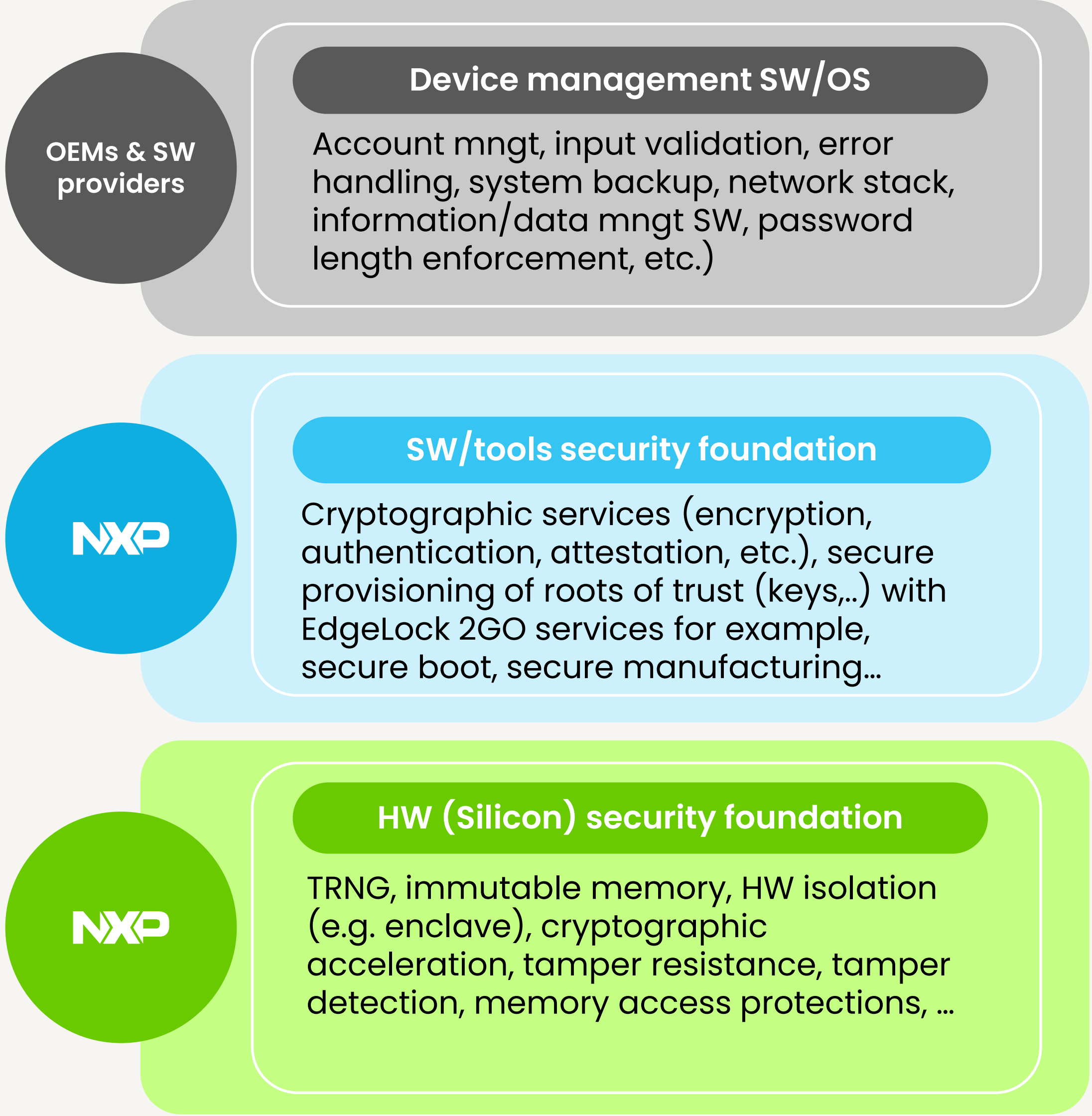
The EdgeLock technology includes dedicated secure elements, security integrated into MPUs/MCUs as well as NXP security services to implement and protect Security Functions for 62443-4-2. Secure Element SE051 has received IEC 62443-4-2 certification.

NXP security maturity process has been 62443-4-1 certified

EDGELOCK™ SECURITY

NXP

Implementation of IEC 62443-4-2 security



OEMs & SW providers

Device management SW/OS

Account mngt, input validation, error handling, system backup, network stack, information/data mngt SW, password length enforcement, etc.)

NXP

SW/tools security foundation

Cryptographic services (encryption, authentication, attestation, etc.), secure provisioning of roots of trust (keys,..) with EdgeLock 2GO services for example, secure boot, secure manufacturing…

NXP

HW (Silicon) security foundation

TRNG, immutable memory, HW isolation (e.g. enclave), cryptographic acceleration, tamper resistance, tamper detection, memory access protections, …

NXP HW security scales to meet various risks levels

- Most NXP MPUs & MCUs feature the minimum HW security foundation to support IEC 62443-4-2, even for higher security levels such as SL3!

- NXP offers a variable number of security functions at various robustness levels to meet different HW anchoring levels for desired cyber risk and performance levels (e.g., Time Sensitive Networks)

NXP offers a portfolio of scalable solutions to address various risk & security levels at the edge

NXP MCU/MPU

Essential Security

w/wo TrustZone®

- Secure initialization
- Secure access
- Secure connections
- Data protection
- Secure Processing Environment (optional)

NXP MCU/MPU

EDGELOCK SECURE ENCLAVE

Advanced Security

with integrated **EdgeLock Secure Enclave**

Cyber Resilience:

- Enhanced protection of critical security functions
- Advanced capabilities to manage security over device lifecycle

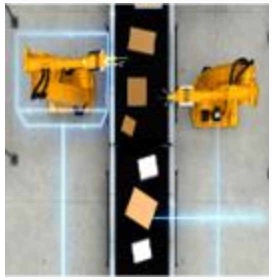
NXP MCU/MPU + NXP SE05x/A5

EDGELOCK SECURE ENCLAVE

High Security

adding companion **EdgeLock Secure Element**

- Security further enhanced with protection of credentials against advanced HW attacks



Comprehensive security solutions to cover IEC 62443-4-2 requirements

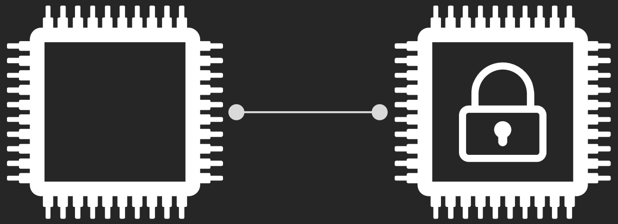
	Essential		Advanced	High
Suitability for IEC 62443-4-2	✓	✓	✓	✓
Number of **security functions** anchored in HW	🟩▨	🟩🟩	🟩🟩🟩	🟩🟩🟩🟩
NXP devices: (examples)	i.MX RT10xx i.MX RT116x/117x	i.MX6/7/8/8M/8x LPC55S6x/2x/1x/0x i.MX RT500/600	i.MX 8ULP, i.MX 9x i.MX RT1180, MCX N, MCX W7x, K32W132, RW61x, LPC55s3x	Same as advanced security MCU/MPUs with SE05x/A5x

NXP cutting-edge security technologies, made for resilience in a dynamic cybersecurity landscape

EdgeLock Secure Enclave

Dedicated security unit integrated in NXP MCU/MPU

- Enhanced isolation for protection of critical security functions required by regulations
- Advanced capabilities for device monitoring and availability protection
- Protection of sensitive data & credentials
- Available on latest NXP MCU/MPUs



EdgeLock SE05x/A5x

Secure Elements & Secure Authenticators

- Secure vault for credentials with protection against SW and advanced HW attacks
- Certified Common Criteria EAL6+, and FIPS
- Optional personalization with custom credentials at NXP manufacturing
- Can be plugged to any type of ASIC or processor

EdgeLock 2GO

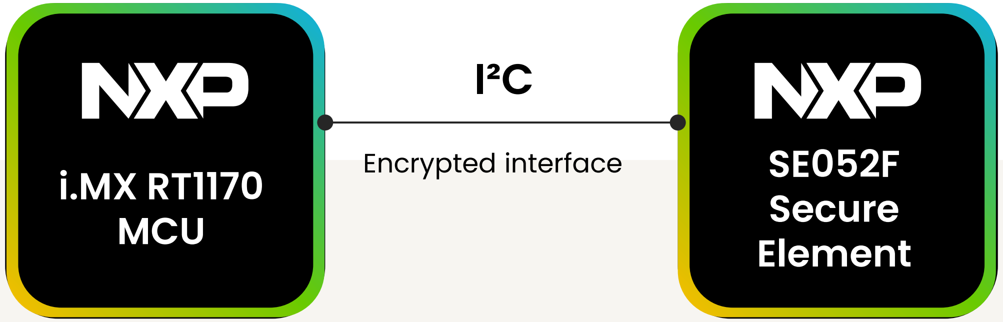
NXP cloud services for credential management

- Easy deployment of Root of Trust credentials on devices
- Management of credentials over-the-air and over device lifecycle
- Native integration on EdgeLock Secure Enclave, Secure Elements & Secure Authenticators

A modular approach with EdgeLock Discrete

- Secure boot
- Secure update
- Secure debug
- Accelerated cryptography
- Physical unclonable function (PuF)
- Tamper detection
- On-the-fly external Flash decryption

- Tamper resistant key storage
- Optional personalization with custom credentials at NXP
- Key management with NXP EdgeLock 2GO
- FIPS 140-3 L3 certified
- Common Criteria EAL6+ certified



(Example of combination)

MPU/MCUs “Essential security” combined with EdgeLock SE05x/A5x for an enhanced profile of security functions

EdgeLock hardware

EdgeLock 2GO

Security functions available on NXP products support IEC62443-4-2 requirements

Required Security Capability (IEC 62443-4-2)	Supporting security functions by NXP EdgeLock Security[1]
Identification & authentication control	HW based authentication (device, SW, sub-system) Secure credential Install (keys, passwords, certificates, etc.) Root of Trust credential pre-injection at silicon manufacturing Key management services (manufacturing, over-the-air) Cryptographic processing /credential isolation
Use Control	Cryptographic services for access control Usage policies on credentials, Secure Connect Device Lifecycle management
System integrity	Secure SW & credential Install, Secure boot, Device (runtime) attestation, Secure Update, Device lifecycle management, Secure debug, Secure connect, Secure key storage/management, SW/data/processing isolation, physical tamper resistance, tamper detection, Damage control & device recovery
Restricted data flow	Processing/Data isolation (on-chip firewalling) Privileged access to data, secure connect
Data confidentiality	(Accelerated) data encryption, Authentication (data access), Secure key storage/management
Resource availability	Secure update, Damage control & device recovery
Timely response to events	Tamper/anomaly detection, Secure update Damage control & device recovery

[1] Please check NXP product datasheets/security manual for availability of specific security functions

Key benefits of using NXP’s EdgeLock security solutions

- Reduced cost on SW development and physical protections built at equipment casing or operation site level
- Simpler path to certification with facilitated proof of compliance; in particular, NXP Secure Element is IEC 62443-4-2 certified
- Increased flexibility in the usage conditions of equipment, larger market potential
- Relaxed manufacturing conditions and easier deployment of security
- Cautious & future-proof approach in a dynamic regulation landscape, especially with new regulations (e.g. CRA) more demanding in terms of resilience
- OEM IP protection, especially in product platforming strategies

NXP support OEM's certification by mapping NXP security features to IEC 62443-4-2 requirements

Application Notes

Ease ISA/IEC 62443-4-2 compliance

with **i.MX 8XLite**

Application Notes

Ease ISA/IEC 62443-4-2 compliance

with **i.MX RT1180**

Application Notes

Ease ISA/IEC 62443-4-2 compliance

with **i.MX 8ULP**

Application Notes

Ease ISA/IEC 62443-4-2 compliance

with **i.MX 93**

Application Notes

Ease ISA/IEC 62443-4-2 compliance

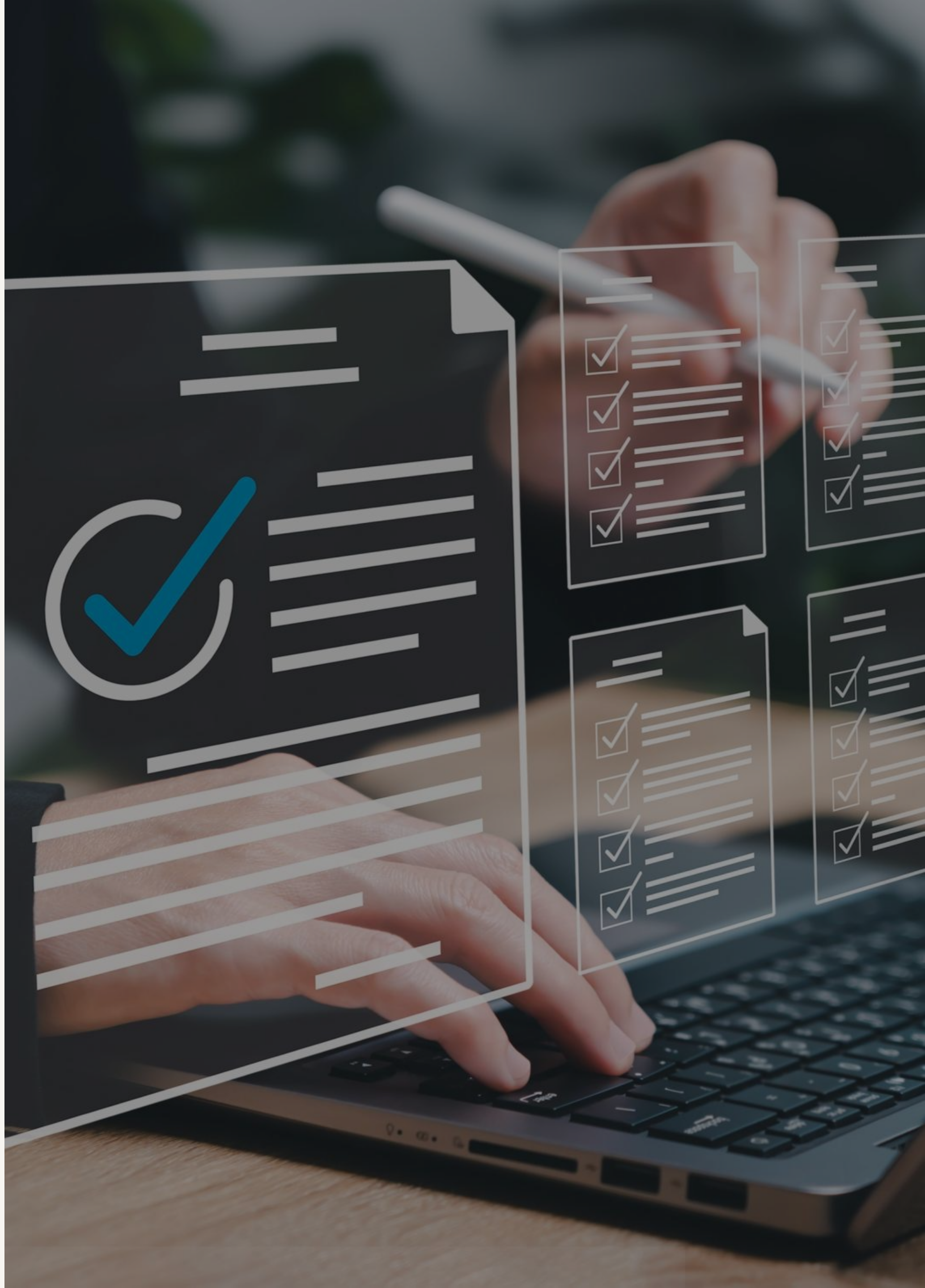
with **MCX N**

Application Notes

Ease ISA/IEC 62443-4-2 compliance

with **SE05x**

nxp.com/security



Use case examples - NXP Secure Edge Processors

(EdgeLock Secure Enclave inside)

NXP

i.MX RT1180

Secure industrial networking

- Realtime message authentication & encryption on Time Sensitive Networks (TSN)
- Network segmentation and data flow restriction
- Secure remote configuration

NXP

i.MX 93

Secure EV charger

Secure connections:

- Charger to Cloud (TLS - remote control & monitoring, billing),
- Charger to EV (ISO 15118)
- Charger to Grid (IEC 61850)

NXP

MCX N

Device integrity upgrade

- Upgrade of legacy, non-secure equipment with authenticated boot, Post-Quantum secure

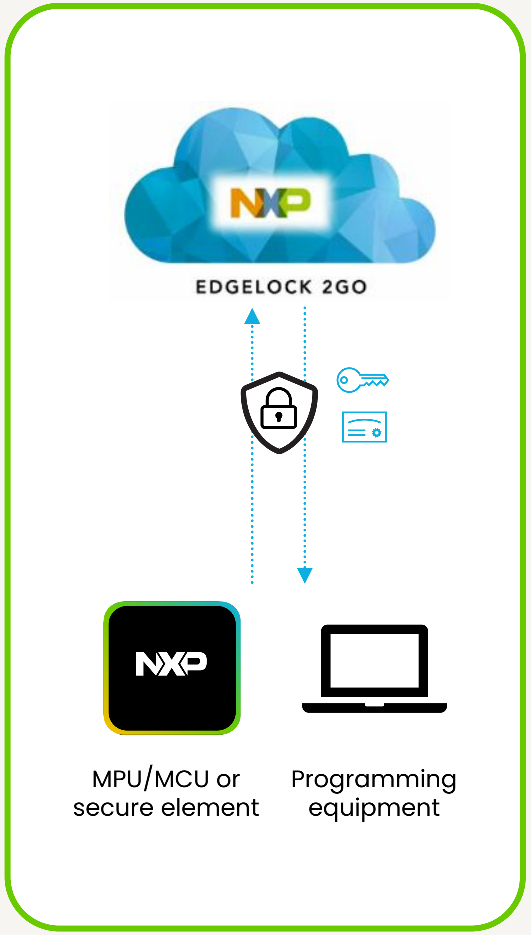
  (Device retrofit or design update – ensures device loads and executes trusted SW delivered by manufacturer)

Use cases examples: EdgeLock 2GO key management platform

Onboarding of industrial devices
Generation & injection of globally verifiable device identity (private key & certificate) to ensure only legitimate devices can connect to an infrastructure

Access to cloud service
Generation, injection and over-the-air renewal of credentials to access cloud services

Secure injection of FW decryption keys
Protection of FW IP in untrusted manufacturing



IEC 62443 and EU Cyber Resilience Act: Same principles but with more resilience, obligations and legal implications

- Cyber Resilience Act (CRA) is an upcoming European regulation introducing mandatory cybersecurity requirements for hardware and software products, throughout their whole lifecycle
- Both IEC 62443 standard and CRA converge high-level on the security capabilities to a large extent
- However, there is currently **no mechanism of (partial) CRA conformance** based on the 62443 certifications
- CRA has also **additional obligations** not covered by 62443, among others towards vulnerability/incident management over device lifecycle (detection, reporting, handling, patching), as well as open source
- The CRA **extends the need for cyber resilience** in order to manage device security over time
- The **legal implications** of CRA require careful demonstrability of security functionality, security robustness and security assurance level, based on device exposure to risk

nxp.com/security

NXP EdgeLock Security
Made for compliance & resilience

- Compliance to IEC 62443 standard increasingly becomes important to access industrial & healthcare markets

- NXP offers scalable solutions to address IEC 62443 4-2 requirements at various security levels

- NXP EdgeLock solutions facilitate and accelerate the certification and compliance with comprehensive solutions. NXP Security Maturity Process is 62443-4-1 certified

- NXP solutions address the various aspects of practical deployment and integration of security, from real time authentication requirements in TSN to secure injection of root of trust credentials in untrusted manufacturing facilities nxp.com