MAKING IT EASIER TO ACHIEVE IEC 62443 SECURITY COMPLIANCE FOR INDUSTRY 4.0

Joppe Bos, Senior Principal Cryptographer
Competence Center Crypto & Security
JUNE 2022
AGENDA

• Industry 4.0: Opportunities & Threats

• IEC 62433: the New Industrial Standard Security Requirements for Industrial Automation Control Systems

• Security Primitives

• Security Product Certification for Industrial IoT: SESIP, IEC 62443-4-1, and IEC 62443-4-2 + EdgeLock SE051

• Putting it All Together: i.MX RT Industrial Drive Development Platform
INDUSTRY 1.0
Mechanization, steam power, weaving loom

INDUSTRY 2.0
Mass production, assembly line, electrical energy

INDUSTRY 3.0
Automation, computers, electronics

INDUSTRY 4.0
Cyber physical systems, internet of things, networks
A COMPANY FALLS VICTIM TO A CYBER ATTACK EVERY 39 SECONDS

THE AVERAGE TOTAL COST OF A RANSOMWARE ATTACK

$4.62 MILLION

Source: 2021, IBM, 2021 Cost of a Data Breach Report
Industrial IoT devices are potential targets for those seeking unauthorized access to the network, malicious control of the device or theft of IoT collected data or theft of intellectual property.

INDUSTRIAL IOT REQUIRE SECURITY BY DESIGN

Machine to machine authentication of industrial devices.

Connection of devices to clouds, servers and backends. Credential storage in secure hardware. Encryption of data.

Authentication and protection of industrial sensor data.

Secure authorized access to machines and data (HMI).

Late stage configuration for a particular setup, installing specific network parameters, entering log data and customizing devices for geographic regions.

WiFi network onboarding and credential protection.
IEC 62433: THE NEW INDUSTRIAL STANDARD

Security requirements for Industrial Automation Control Systems

Collaborative Development

- ISA-62443 (and IEC 62443) is a series of standards being developed by two groups:
  - ISA99 → ANSI/ISA-62443
  - IEC TC65/WG10 → IEC 62443
- In consultation with:
  - ISO/IEC JTC1/SC27 → ISO/IEC 2700x

References:
- https://www.isa.org/isa99/
IEC 62443 – OVERVIEW

Security levels provide guidance for protection against different security violations

- **Intentional violation** with: Sophisticated means and extended resources **SL 4**
- **Intentional violation** with: Sophisticated means and moderate resources **SL 3**
- **Intentional violation** with: Simple means and low resources **SL 2**
- **Unintentional or coincidental violation** **SL 1**
- No special protection required. **SL 0**

**General Information**

- **Part 1**: Terminology concepts and models
- **Part 2**: Master glossary of terms and abbreviations
- **Part 3**: System security compliance metrics
- **Part 4**: IACS security lifecycle and use-case

**Policies & Procedures**

- **Asset Owner (Factory operations)**
  - **Part 1**: Requirements for IACS security management system
  - **Part 2**: Implementation guidance for an IACS security management system
  - **Part 3**: Patch management in the IACS environment
  - **Part 4**: Requirements for IACS solution suppliers

- **System integrator (design and deployment)**
  - **Part 1**: Security technologies for IACS
  - **Part 2**: Security levels for zones and conduits
  - **Part 3**: System security requirements and security levels

- **Automation Device Supplier (product develop.)**
  - **Part 1**: Product development requirements
  - **Part 2**: Technical security requirements for IACS components

**Depends on the design and implementation for a specific automation project**

Figure taken from IEC 62443
I will design my product to be compliant with IEC 62443.

This is too complex.

How can I realize these requirements in my product?

~200 Pages
SECURITY PRIMITIVES MAP TO REQUIREMENTS

Security Primitives includes mapping table and application process

22 Security Functional Primitives
4 Security Process Primitives

Legislation  Standards  Certification  Guidelines
A framework is needed that

- Maps certification and standards criteria as well as use case requirements to product capabilities (and vice versa)
- Provides a common nomenclature across IoT security concerns
- Identifies and defines the needs of an IoT device or system based on system security and standard prerequisites
- Supports the selection and integration of associated solutions to fulfill those requirements
EXAMPLE USE CASE: SMART SURVEILLANCE CAMERA

The smart surveillance camera records video footage and transmits it to the cloud.

For this, it needs to **securely communicate** with the cloud backend. To ensure the video stream has not been tampered with, the camera needs to **ensure and attest device integrity**, needs to **detect anomalies and react to them**, and apply **cryptographic algorithms such as signatures** to the video stream.

These requirements are all **Security Primitives** and can directly be mapped to products – and product features – as well as requirements from standards such as IEC 62443.
SECURITY PRIMITIVES IN CONTEXT

Use Cases

Security Primitives

Features of NXP Products

Requirements of IEC 62443

Requirements of FIPS 140-3

SESIP

Legislation

Security Level
• Multi-phase process for use cases, compliance, and product evaluation
• Order of the phases is interchangeable
• The phases themselves and the knowledge required in each of them are decoupled – not every domain expert is required in each step
• Detailed description in the whitepaper (Section 3)
EXEMPLARY USE CASE

• Industrial smart surveillance camera
  - Signature on recorded (live) content stream
  - Secured real-time connection to the cloud
  - Tamper protection and detection

• Simplified example to illustrate the process
  - Compliance to IEC 62443 4-2 (security functional) required
  - Selection of suitable products based on Security Primitives
SECURITY PRODUCT CERTIFICATION FOR IOT

SESIP: Security Evaluation Standard for IoT Platforms
• A security evaluation & certification framework
SUPPORT OF IEC 62443-4-1 REQUIREMENTS

NXP security maturity process has been IEC 62443-4-1 certified
Support of IEC 62443-4-2 Requirements

Assessment of technical features of EdgeLock SE051 applicable for IEC 62443-4-2
PUTTING IT ALL TOGETHER
I.MX RT INDUSTRIAL DRIVE
DEVELOPMENT PLATFORM
i.MX RT INDUSTRIAL DRIVE DEVELOPMENT PLATFORM

- 800 MHz performance
- Industrial qualified i.MX RT1170 crossover MCU
- On-board NXP secure element: EdgeLock SE05x

✓ Real time deterministic communication
Demonstrates and guides how to enable a field device as TSN end point in a TSN enabled network.

✓ Multi-axis servo control
Demonstrates and guides how to leverage our MCU peripherals and Gate Drivers for single to multiple motor control.

✓ Fault detection
Demonstrates and guides how to leverage NXP’s analog and digital technology for instantaneous fault detection

Daughter Card
Control board, which integrates MCU chip, debugging interface and Ethernet TSN port.

Digital Board
Expansion board for Daughter Card, integrates multiple peripherals for communication, security and display.

Power Stage Board
Transforms the control commands into power signals to drive servo motor (200W up to 450W)
Standardized Industrial Cybersecurity

Provides meaningful guidance and collateral to ease their IEC 62443-4-2 certification journey with NXP product.

Note: users should notice that this platform only serves as a reference, it does not grant automatic IEC 62443-4-1/2 certification to their products.
CONCLUSION

• Industry 4.0: The use of cyber physical systems and Internet of Things result in higher productivity and better efficiency at reduced costs

• Increase in sophisticated scalable industrial cyberattacks

• Industry response: IEC 62443 cybersecurity for operational technology in automation and control systems

• NXP products such as the SE051 secure element comply with IEC 62443-4-2: Technical security requirements for IACS components

• This enables easier compliance as illustrated by the i.MX RT Industrial Drive Development Platform

**NXP simplifies the path to achieve IEC 62443 security compliance for Industry 4.0**
TECHNOLOGY SHOWROOM

JOURNEYS BY DESIRED ENGAGEMENT
Self-guided tour
Live-streaming at set times
Guided tours

60+ VIRTUAL DEMOS
Focus on system solutions
Set up along NXP verticals

JOURNEYS BY DESIRED FOCUS
Low Power Innovations
Advanced Analog
Connectivity
Edge & AI/ML
Safety & Security

SHOWROOM.NXP.COM