SESIP: Journey Towards a Powerful Methodology

PUBLIC

Gavin Yao
Competence Center Crypto & Security, CTO
APRIL 2022

SECURE CONNECTIONS FOR A SMARTER WORLD

PUBLIC

NXP, THE NXP LOGO AND NXP SECURE CONNECTIONS FOR A SMARTER WORLD ARE TRADEMARKS OF NXP B.V.
ALL OTHER PRODUCT OR SERVICE NAMES ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS. © 2022 NXP B.V.

Knowing is Not Enough; We must Apply
Willing is Not Enough; We must Do

- Johann Wolfgang von Goethe

OVERVIEW

- Motivations
- Pilot for both SESIP and PSA Certified
- Towards IEC62443
  - Function mapped
  - Process compliance
  - Evaluation report summary

HORIZONTAL CERTIFICATION SCHEME IS IN DEMAND TO ADDRESS VARIOUS REQUIREMENTS

Government Legislation:

- European Cyber Security Act
- Singapore CSL
- S.734 - Internet of Things Cybersecurity Improvement Act of 2019
- Cal. SB-327

Baseline Requirements:

- MATTER (Zigbee etc)
- ETSI 303 645 (Consumer)
- NISTIR 8259 (Device Manufacturers)
- UL 2900 (SW)

Sector Specific:

- ISO/SAE 21434 (Auto)
- IEC 62443 (Industrial)
- NFC/FiRa/CCC
- Hospital & at-home Patient Monitoring
- Personal Health & Fitness Monitoring

TYPES OF CERTIFICATION

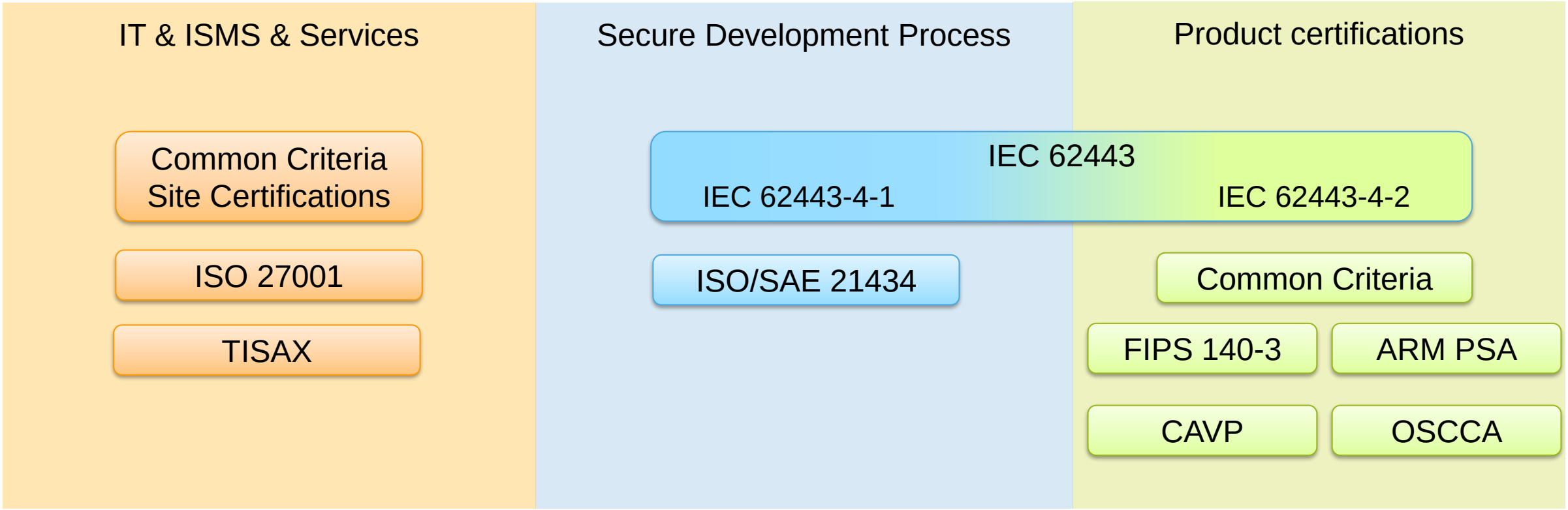
ISMS Services	Secure Development Process	Product Certifications
Certify the Security philosophy of the company how we protect data, deal with security incidents, etc.	Ensure that we develop security products through concepts like security by design, ensure development process controls and security gates are in place	Verification of the security functionality of the end product
Concept • Security mindset	Concept • Security processes and procedures	Concept • Secure solutions

Trusted Supply Chains

Security by Design

NXP drives a holistic approach and cover all 3 types of certifications providing proof points for customers

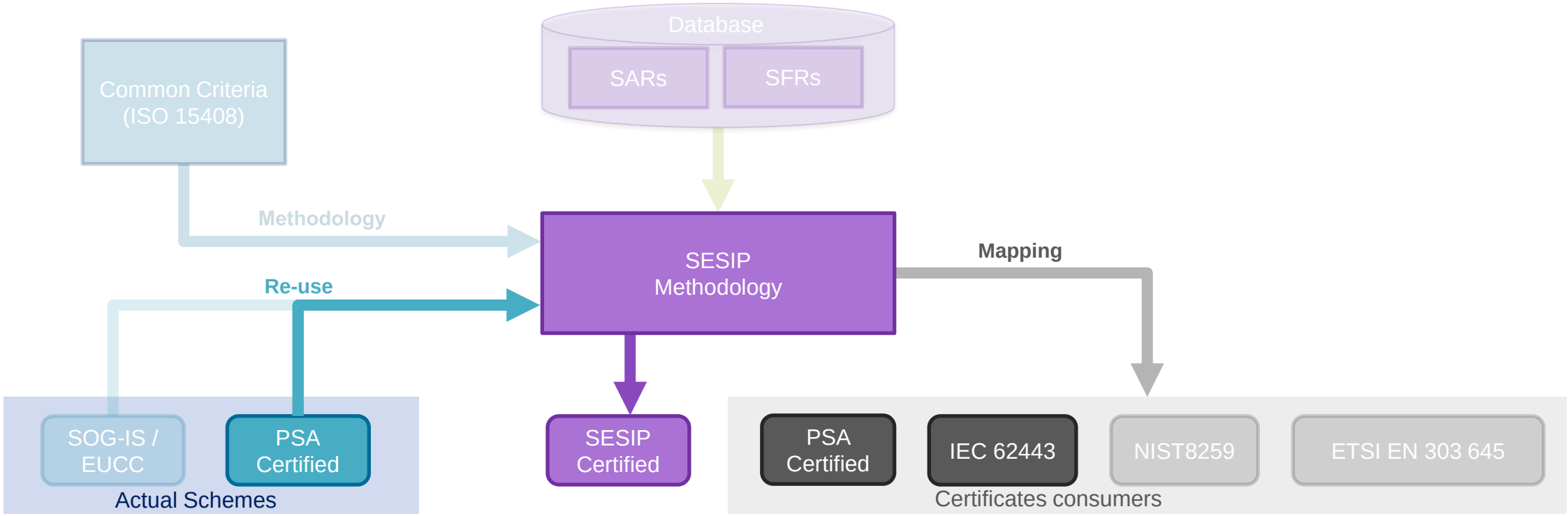
SESIP PROVIDES FLEXIBILITY TO ADAPT STANDARDS



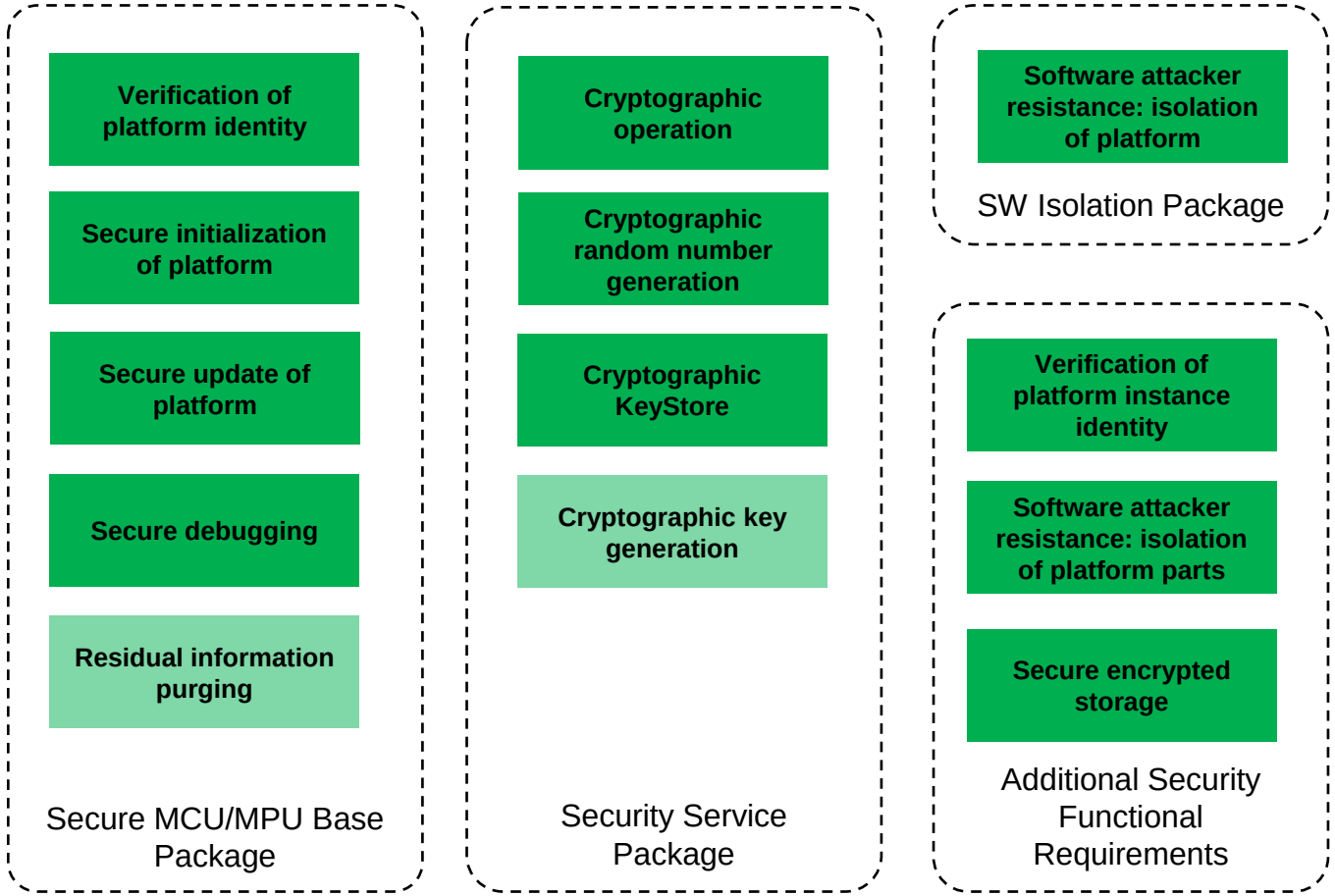
SESIP is designed to harmonize and address the requirements horizontally

SESIP SPIRIT: REUSE AND HARMONIZATION

- Allows reuse of existing certificates into SESIP and reuse of SESIP certificates by other standards based on “Mapping” documents with little additional effort
- Harmonization of requirements and testing activities



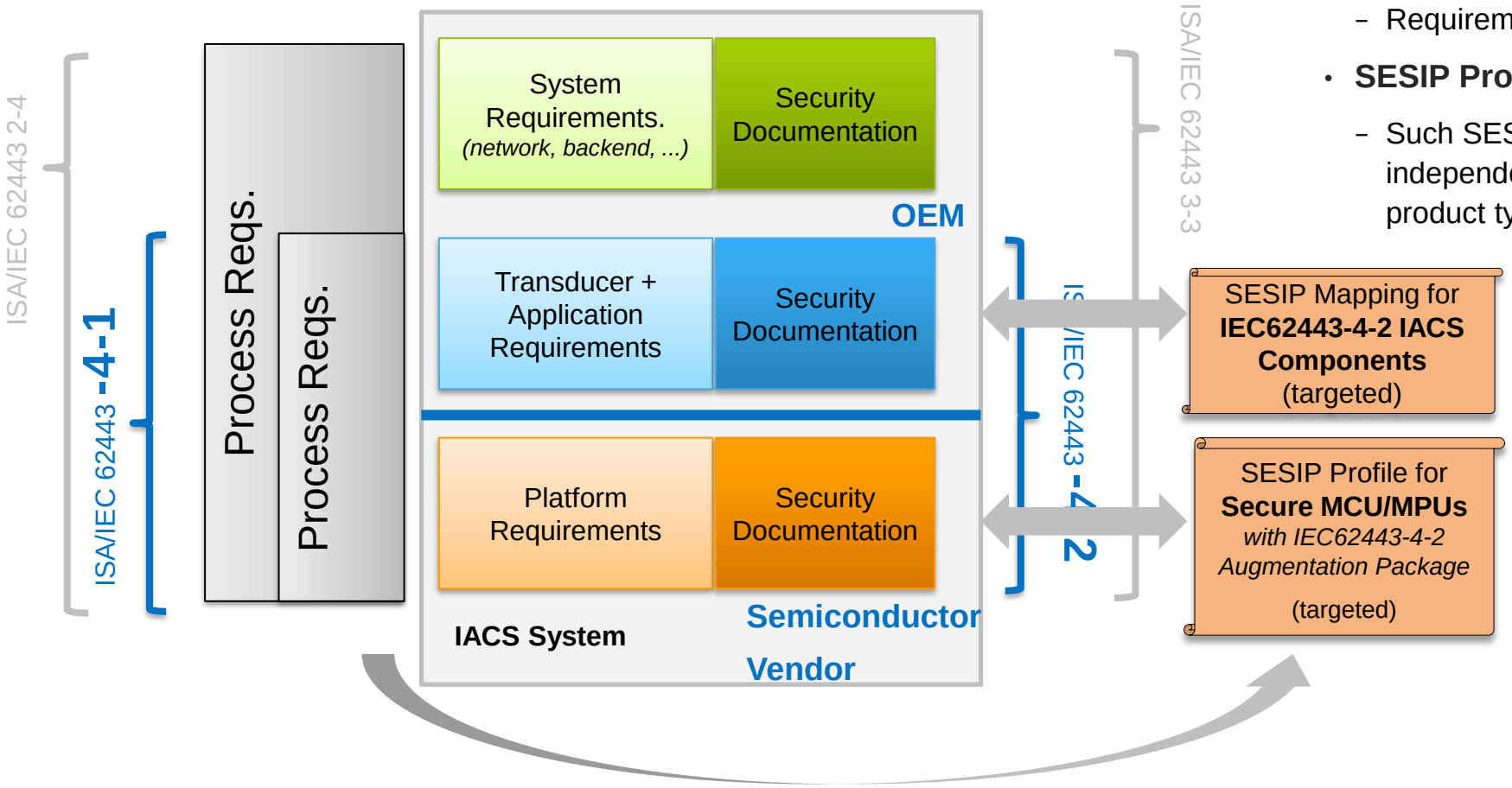
LPC55S16: ONE EVALUATION, SESIP2 AND PSA2 BOTH CERTIFIED



- One product: LPC55S16
- One integrated evaluation
  - Conformed to SESIP profile for Secure MCUs and MPUs
    - Profile later donated to GP
  - Most results reused for PSA evaluation
- Two Certificates
  - Certified in Q3'2020; before the publish of SESIP profile for PSA L2

TOWARDS IEC62443

Leveraging SESIP composition approach



- **Challenge: no common set of requirements**
  - IEC 62443 specifies technical requirements for industrial IoT, but on device level at the finest granularity
  - Requirement on development process
- **SESIP Profiles (SP) fill this void**
  - Such SESIP Profile is a product (implementation) independent security claim that applies to an entire product type or class of devices

TOWARDS IEC62443: APPLICABLE REQUIREMENTS MAPPED INTO SFRS

Verification of Pla
Verification of Pla
Attestation of Pla
Physical attack re
Attestation of Pla
Attestation of App
Cryptographic Ke
SW attacker resis
Secure Install of A
Factory Reset of I
Secure Update of
Secure Communi
Attestation of App
Secure Encrypted
Reliable Index
SW attacker resis
SW attacker resis
Secure Update of
Secure initializati
Residual informat
Secure Communi
Cryptographic op
Cryptographic ran
Cryptographic ke
Secure Uninstall

3.3.5.3 Cryptographic KeyStore

The platform provides the application with a way to store *cryptographic keys*, *PINs* such that not even the application can compromise the *authenticity, integrity, confidentiality* of this data. This data can be used for the cryptographic operations *encryption, decryption, signature generation, MAC generation, key derivation, shared secret generation*.

Conformance rationale:

Cryptographic keys are stored [redacted] (see Section 3.2 of [7]).

[redacted] s implemented as defined in:

- **IEC62443-4-2 CR 1.1 - Human user identification and authentication** [24];
- **IEC62443-4-2 CR 1.1 (1) - Unique identification and authentication** [24];
- **IEC62443-4-2 CR 1.1 (2) - Multifactor authentication for all interfaces** [24];
- **IEC62443-4-2 CR 1.3 - Account management** [24];
- **IEC62443-4-2 CR 1.4 - Identifier management** [24];
- **IEC62443-4-2 CR 1.5 - Authenticator management** [24];
- **IEC62443-4-2 EDR/NDR 3.12 - Provisioning product supplier roots of trust** [24];
- **IEC62443-4-2 EDR/NDR 3.13 - Provisioning asset owner roots of trust** [24].

Regarding CR1.1 and CR 1.1 (1), [redacted]

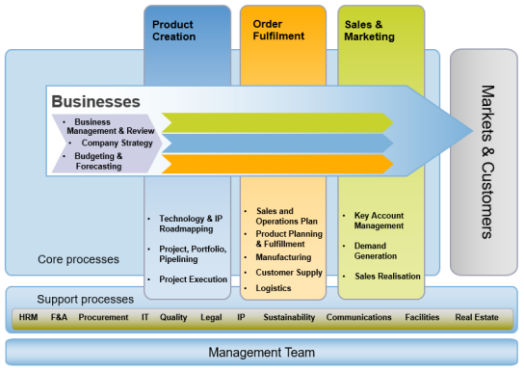
Regarding CR 1.1 (2), [redacted]

Regarding CR 1.3 and 1.4, [redacted]

Regarding CR 1.5 [redacted]

TOWARDS IEC62443: PROCESS PACKAGE

Development Processes



Process Certified

CERTIFICATE

No. IITS1 109577 0003 Rev. 00

Holder of Certificate: NXP Semiconductors N.V.
Chief Technology Office
High Tech Campus 60
5656 AG Eindhoven
THE NETHERLANDS

Site(s): NXP Semiconductors N.V. Chief Technology Office
High Tech Campus 60, 5656 AG Eindhoven, THE NETHERLANDS

Certification Mark:

Type: Industrial IT Security

Scope of Certificate: Business Creation and Management (BCaM) Process and Product Security Incident Response Process (PSIRP)

The process framework is centrally managed and enforced by the declared site. It applies to all NXP R&D projects. For more details on scoping, see the certificate report referenced below. This certificate report is an annex to the certificate, which can be requested from the holder.

Applied Standard(s): IEC 62443-4-1:2018
PPF 1500382021 (IEC 62443-4-1: Full ML3 Process Profile)

The Certification Body of TÜV SÜD Product Service GmbH certifies that the company mentioned above has established and is maintaining a management system which meets the requirements of the listed standards. The results are documented in a report.
See http://www.tuvsud.com/ps-cert for details.

Report No.: 20CR015033

Valid until: 2024-11-15

Date, 2021-12-10 (Enrico Seidel)

Page 1 of 1
TÜV SÜD Product Service GmbH · Certification Body · Ridlerstraße 65 · 80339 Munich · Germany

ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Process Application Verificaiton in SESIP Evaluation

- IEC62443-4-2 requires that product **development process** is **conformance** to **IEC62443-4-1**
- NXP processes are IEC62443-4-1 certified

3.2 Security by Design and Process Compliance

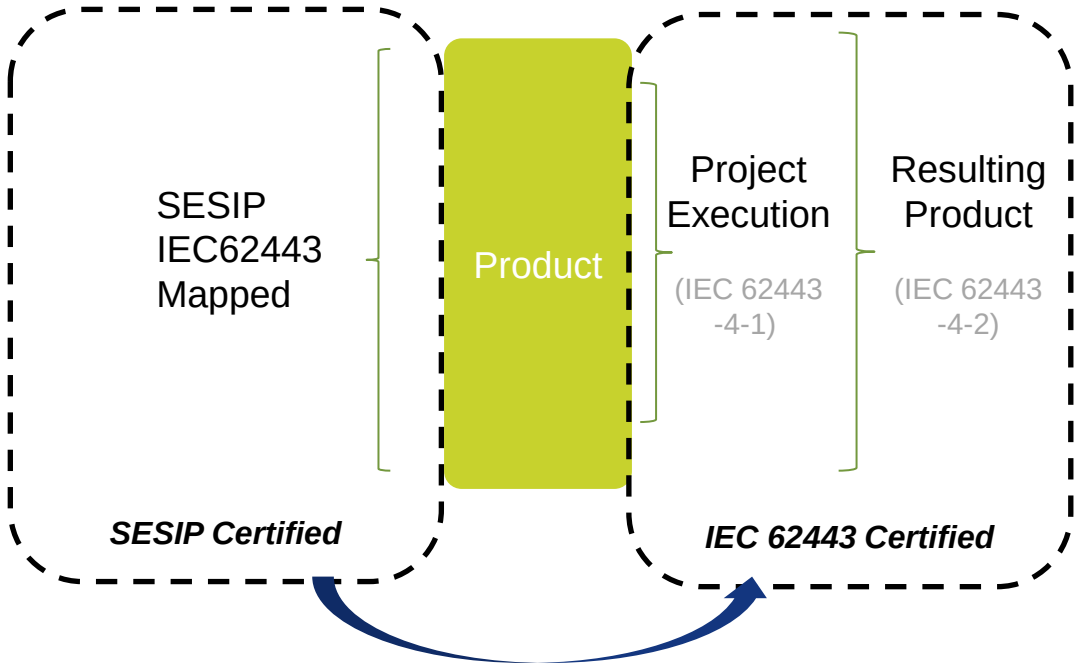
For the development of the platform, secure product development process according to *NXP BCaM framework* have been applied, and this process has been certified for compliance to *IEC62443-4-1: Security for Industrial Automation and Control Systems - Part 4-1: Secure Product Development Lifecycle Requirements*.

Process Compliance Visible in Security Target and Certified

SESIP PROOF OF CONCEPT
EASE IEC 62443-4-2 COMPLIANCE

IEC62443 assessment can intake SESIP

- Threat Model
- Vulnerability Test
- Incident Management
- Secure Guidance
- Process compliance
- …



PROVIDING COMPLIANCE PROOF TO IEC62443 CERTIFIER

Sector/Industry Community

SESIP Profile

provides

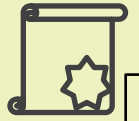
NXP

SESIP Security Target

provides

- Threat Modelling
- Threat Mitigation (Security Mechanisms)
- Mapping to the larger system requirements (what is covered by the subcomponent)
- Standard Requirement mapped in

Customer



SESIP Certificate

- Certificate
- Provides proof of a pass
- Shows the scope of the certification

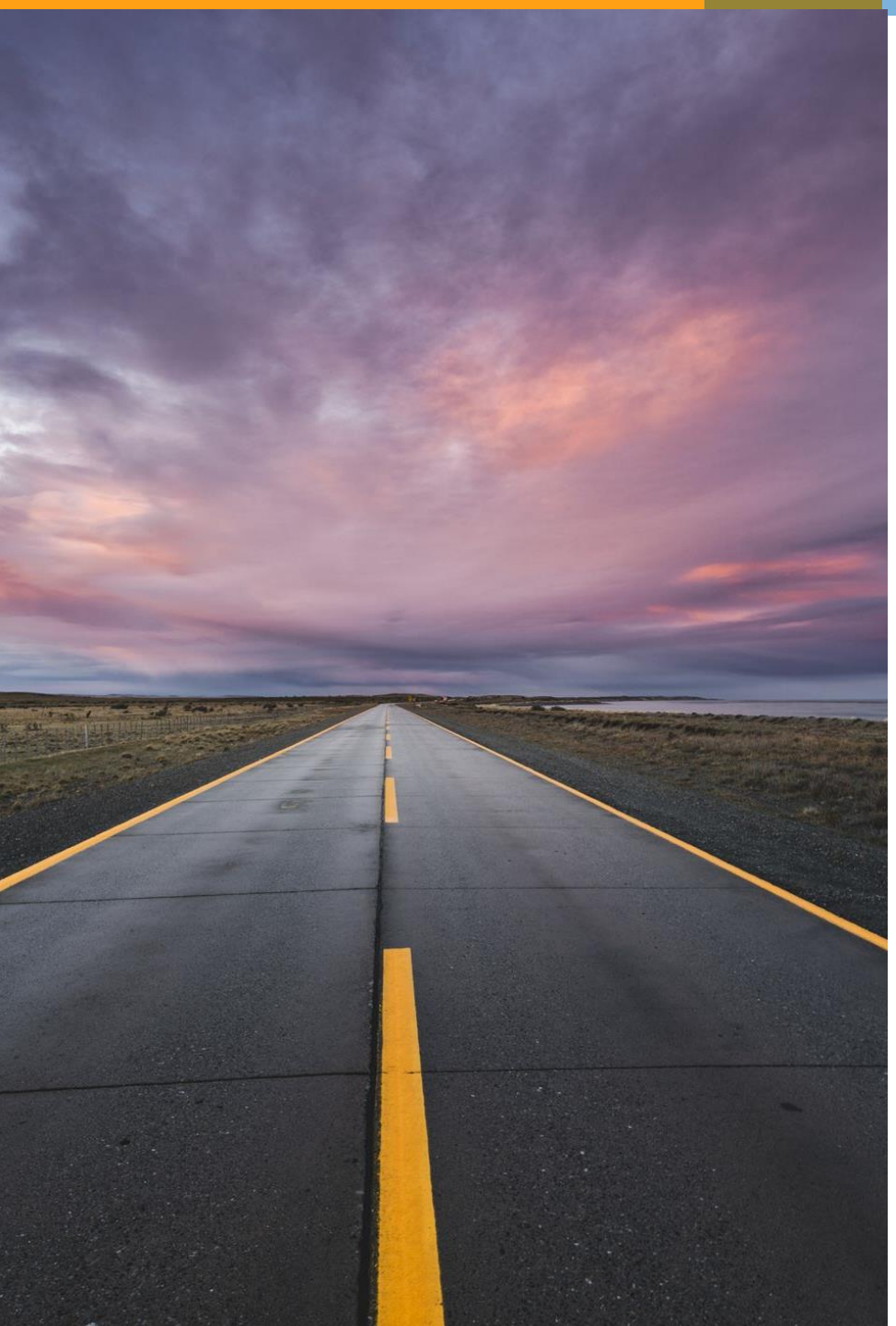
Test Report

- Test Report for Customer and Composition
- Shows how the security requirements were verified
- Details what testing was performed
- Allows the customer lab to easily negate test cases (already covered)

EVALUATION REPORT SUMMARY

- Multi-party sharable
  - Customers
  - Evaluator for composition
- Understandable
  - No CC background mandated
- To provide summary of testing covered
  - To provide assurance and compliance proof
- Target to become a standard SESIP Deliverable
  - Template under construction

Contents



A Journey of a Thousand Miles Begins with a Single Step

- Lao Tzu

THANK YOU.

TOGETHER, WE'RE NOT JUST ADVANCING
TECHNOLOGY, WE'RE ADVANCING SOCIETY.

NXP

SECURE CONNECTIONS
FOR A SMARTER WORLD

SECURE CONNECTIONS
FOR A SMARTER WORLD

NXP, THE NXP LOGO AND NXP SECURE CONNECTIONS FOR A SMARTER WORLD ARE TRADEMARKS OF NXP B.V. ALL OTHER PRODUCT OR SERVICE NAMES ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS. © 2022 NXP B.V.