Global Platform®

SESIP Automotive
Roadmap & Profile Development

May 2026

Salvador Ruiz Sedeño, SESIP Technical Automotive WG Member

Agenda

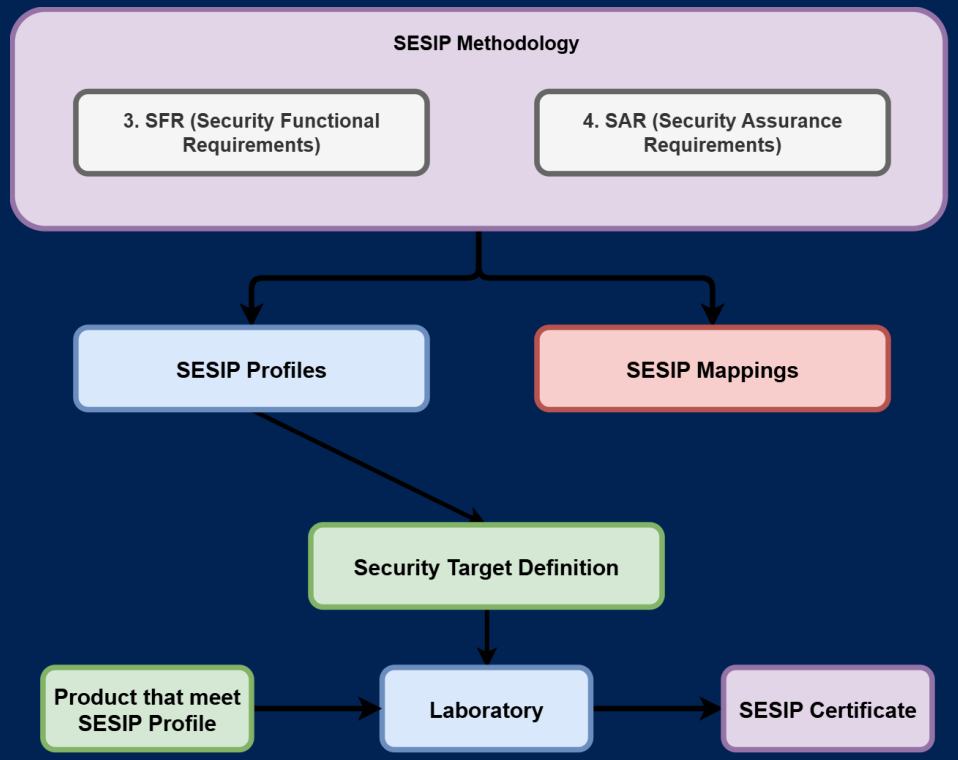
- How SESIP Profiles Standardize Security Requirements
- SESIP Automotive Profiles Roadmap
- SESIP Profiles
  - CMOS Image Sensor
  - SAE J3101 (HPSE)
  - ECU

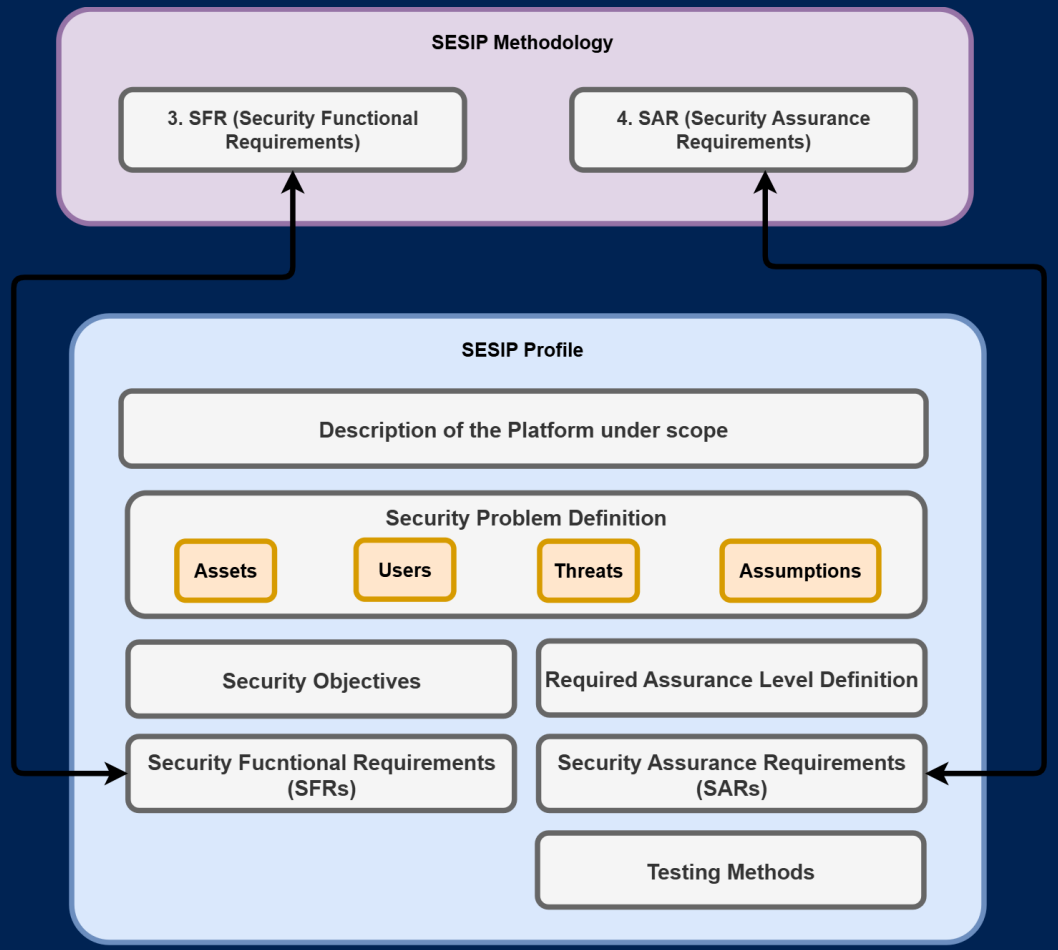
Global Platform®

SESIP

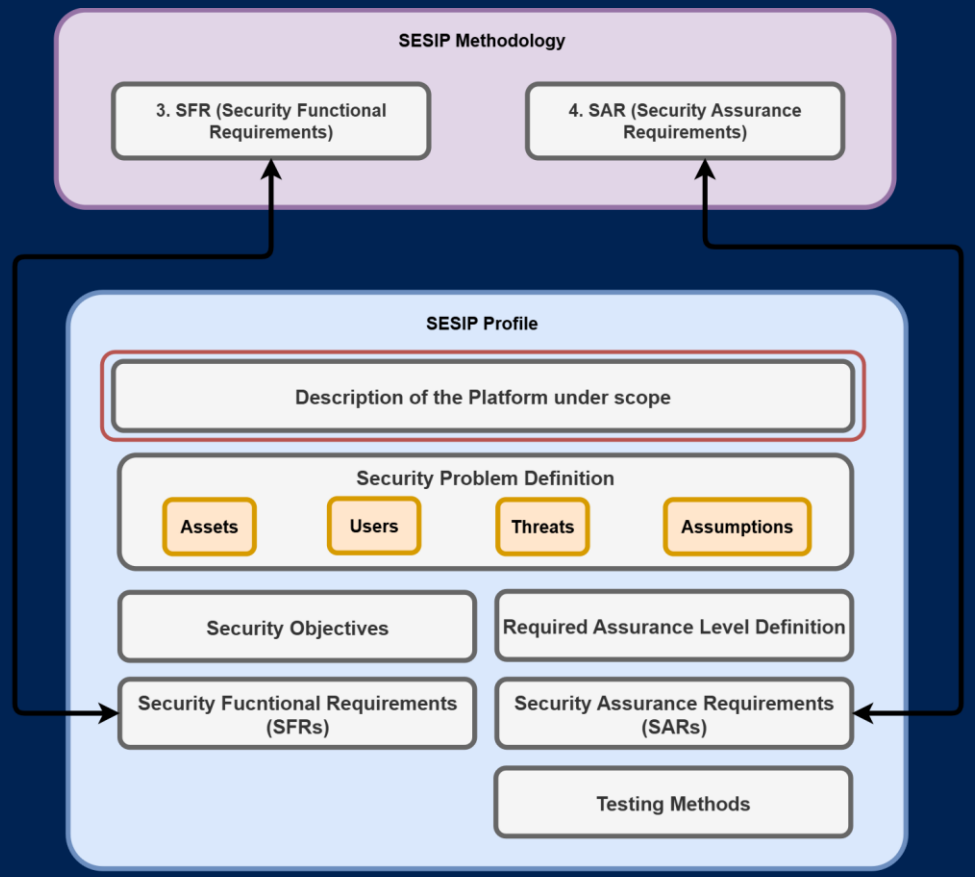
How SESIP Profiles Standardize Security Requirements Across Automotive Items and Components

SESIP Profiles: Standardizing Security Requirements





SESIP Profiles: Platform Description



2.1 Platform Component Functional Overview and Description

AN The following description provides a generic overview of the Electronic Control Unit (ECU) as the Target of Evaluation (TOE). It shall be refined in the Security Target to describe the actual hardware, software, and configuration of the ECU being certified, including any dependencies on pre-certified SESIP components (e.g., Secure MCU/MPU, Secure External Memory, J3101-conformant HPSE).

This section provides a generic functional overview of the Electronic Control Unit (ECU) platform as the Target of Evaluation (TOE) under this SESIP Profile. The description establishes a common reference model that shall be refined and instantiated in the Security Target (ST) to reflect the actual hardware, software, configuration, and selected security packages of the ECU being evaluated.

In the context of this profile, the ECU platform represents the combination of hardware and low-level software components that together provide a secure execution environment for ECU functionality. The platform is responsible for enforcing foundational security properties independently of the application logic executed on top of it.

The ECU platform typically consists of one or more of the following elements:

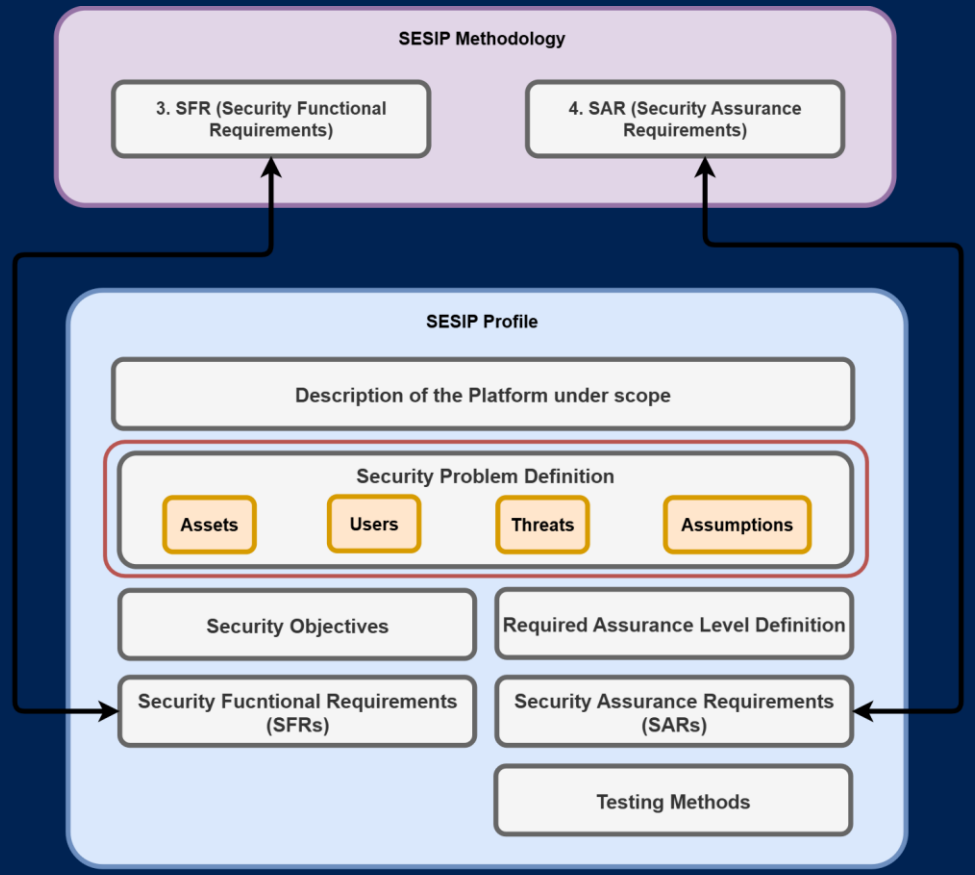
- Processing hardware, such as an MCU, MPU, or SoC, including internal memories, peripherals, and network interfaces.
- Boot and initialization components, including immutable or protected boot code, bootloaders, and early initialization firmware.
- Runtime environment, such as an RTOS, embedded operating system, hypervisor, or equivalent low-level execution environment.
- Platform security services, providing functionality such as cryptographic operations, key management, secure storage, secure update, isolation, and access control.
- Communication subsystems, implementing in-vehicle or external communication stacks (e.g. CAN, LIN, Automotive Ethernet, DoIP).

Depending on the ECU architecture, these functions may be implemented within a single integrated component or distributed across multiple Platform Parts.

The ECU platform may rely on one or more pre-certified platform parts to provide specific security services. Typical examples include:

- A GP certified SE / TEE.
- A SESIP-certified MCU/MPU providing secure boot, cryptographic acceleration, and key storage.
- A J3101-conformant Hardware-Protected Security Environment (HPSE) offering hardware isolation and physical attack resistance.
- Optionally, a Secure External Memory that provides authenticated and/or encrypted storage for firmware, data, or logs.

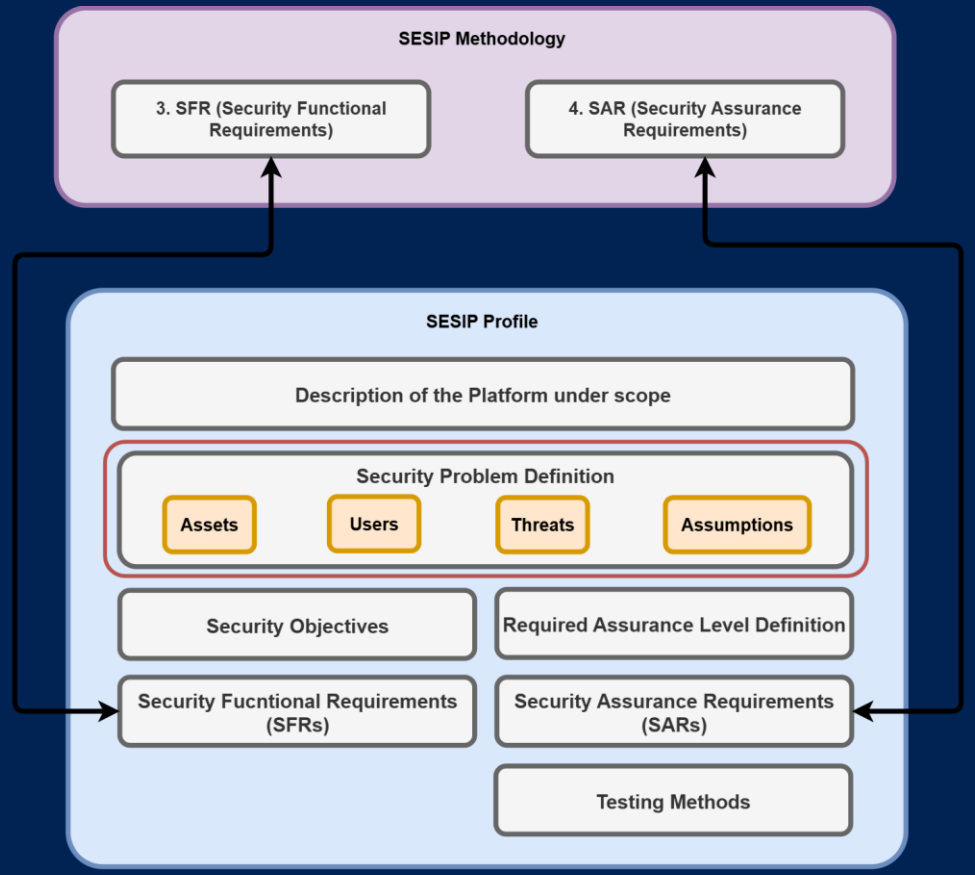
SESIP Profiles: Assets



3.1 Assets

Asset Name	Description	Protected Attributes
Boot Code / Immutable Bootloader	The immutable code (often stored in ROM or flash-protected region) that initiates the secure boot process and validates subsequent firmware.	Integrity, Authenticity, Availability
Firmware / Application Code	Executable software loaded after the boot stage, responsible for implementing ECU functionality and security services.	Integrity, Authenticity
Secure Update Mechanism	Logic and associated metadata (manifest, version counter, signature) that authenticate and install software or configuration updates.	Integrity, Authenticity, Availability, Traceability
Device Identity (ECU ID)	Unique identifier assigned at provisioning or manufacturing that binds the ECU to its vehicle or domain.	Integrity, Authenticity, Confidentiality (if identity credentials include secret material)
Cryptographic Keys	Private or symmetric keys used for encryption, authentication, or integrity verification (e.g., TLS, diagnostics, firmware signing).	Confidentiality, Integrity, Authenticity
Certificates and Public Keys	Public-key certificates or OEM public keys used to verify updates, firmware, or communication peers.	Integrity, Authenticity

SESIP Profiles: Users / Subjects

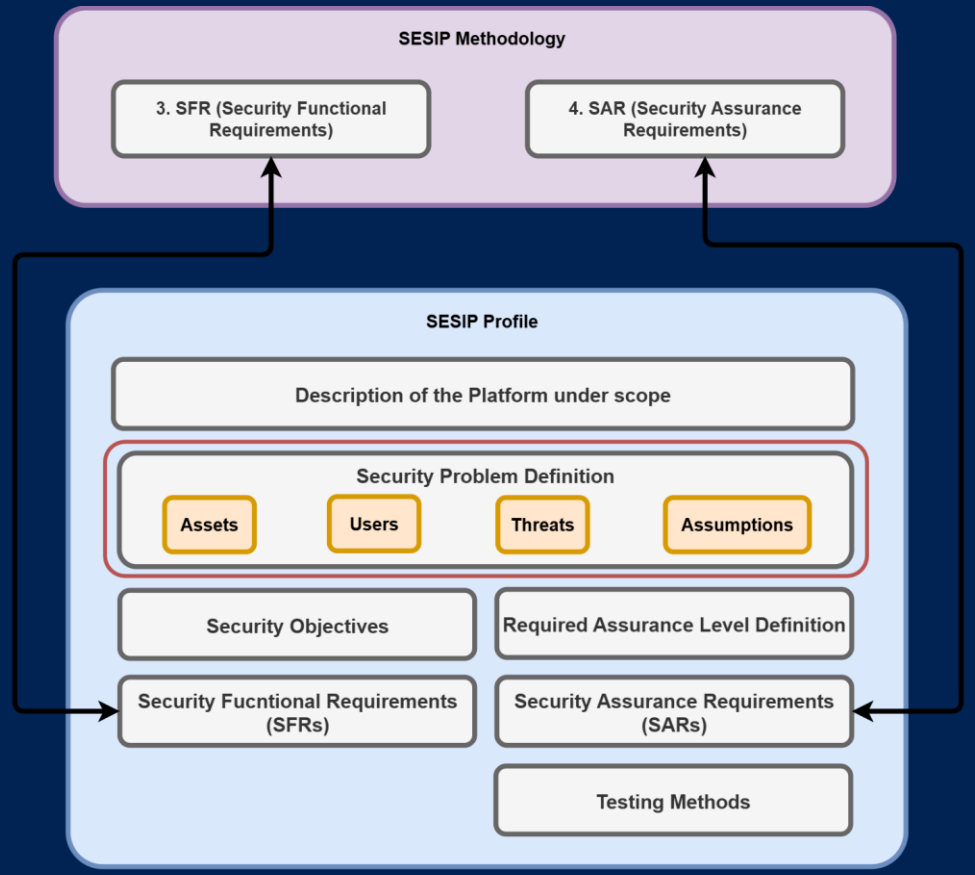


3.2 Users / Subjects

This section defines the users and subjects that interacts with the Target of Evaluation (TOE), including their roles, privileges and potential security concerns.

Entity / Subject	Role or Description	Typical Access / Privileges	Trust Level
OEM (Original Equipment Manufacturer)	The vehicle manufacturer responsible for ECU design, signing firmware, defining update and key management policies.	Full administrative authority: signing of trusted firmware, configuration of root keys, enabling diagnostic modes.	Trusted
Tier-1 / ECU Supplier	Implements or integrates the ECU hardware and firmware according to OEM requirements. May also perform provisioning and testing.	Manufacturing access: secure provisioning, factory tests, calibration, and flashing of firmware images.	Trusted (during manufacturing only)
Authorized Service / Workshop	Uses diagnostic tools to perform maintenance, firmware updates, or configuration under OEM control.	Controlled diagnostic access (UDS/DoIP) through authenticated challenge-response or certificate-based mechanisms.	Conditionally Trusted
Vehicle Owner / Fleet Operator	Owns or operates the vehicle; may initiate updates or consent to diagnostic operations via OEM backend.	Limited access to user interfaces and update consent mechanisms; no direct access to ECU internals.	Untrusted (except via OEM workflow)
End User / Driver	Uses the vehicle and indirectly causes ECU operation. No privileged or direct access	None beyond legitimate vehicle use.	Untrusted

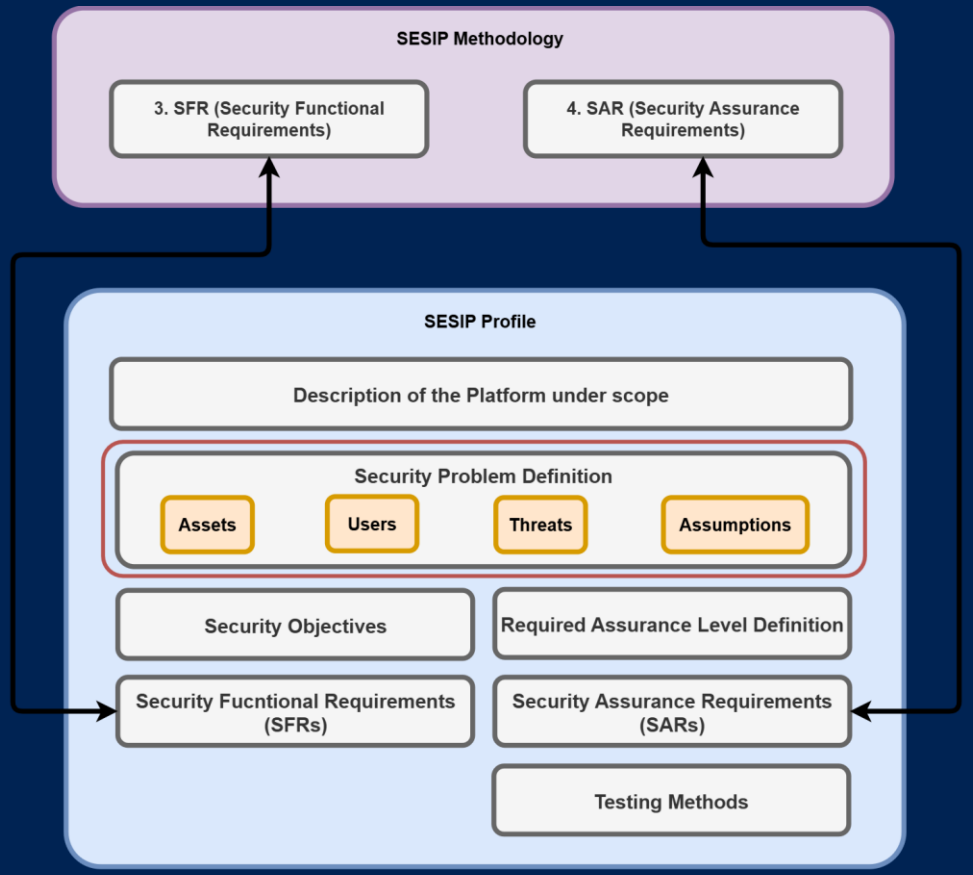
SESIP Profiles: Threats



3.3 Threats

Threat	Description	Security Impact
Unauthorized Access to Cryptographic Keys	An attacker gains access to cryptographic keys (e.g., authentication, encryption, or signing keys) stored in the ECU. This may enable unauthorized decryption, impersonation, or compromise of secure communication.	Confidentiality, Integrity, Authenticity
Unauthorized Modification of Cryptographic Keys	An attacker modifies, replaces, or deletes cryptographic keys, leading to failure of authentication, data decryption, or incorrect digital signatures.	Integrity, Availability
Unauthorized Changes to Firmware	An attacker modifies, injects, or replaces ECU firmware to introduce malicious functionality, disable security mechanisms, or alter system behavior.	Integrity, Authenticity, Availability
Unauthorized Execution of Code	An attacker executes unauthorized or malicious code within the ECU, bypassing security restrictions, escalating privileges, or gaining control over secure operations.	Integrity, Authenticity, Availability
Bypassing Access Controls	An attacker accesses protected memory, configuration data, or security-sensitive regions of the ECU without authorization, violating defined security policies.	Confidentiality, Integrity
Loading of Unauthorized or Malicious Firmware	An attacker circumvents secure boot or update verification mechanisms to load untrusted or malicious firmware.	Integrity, Authenticity

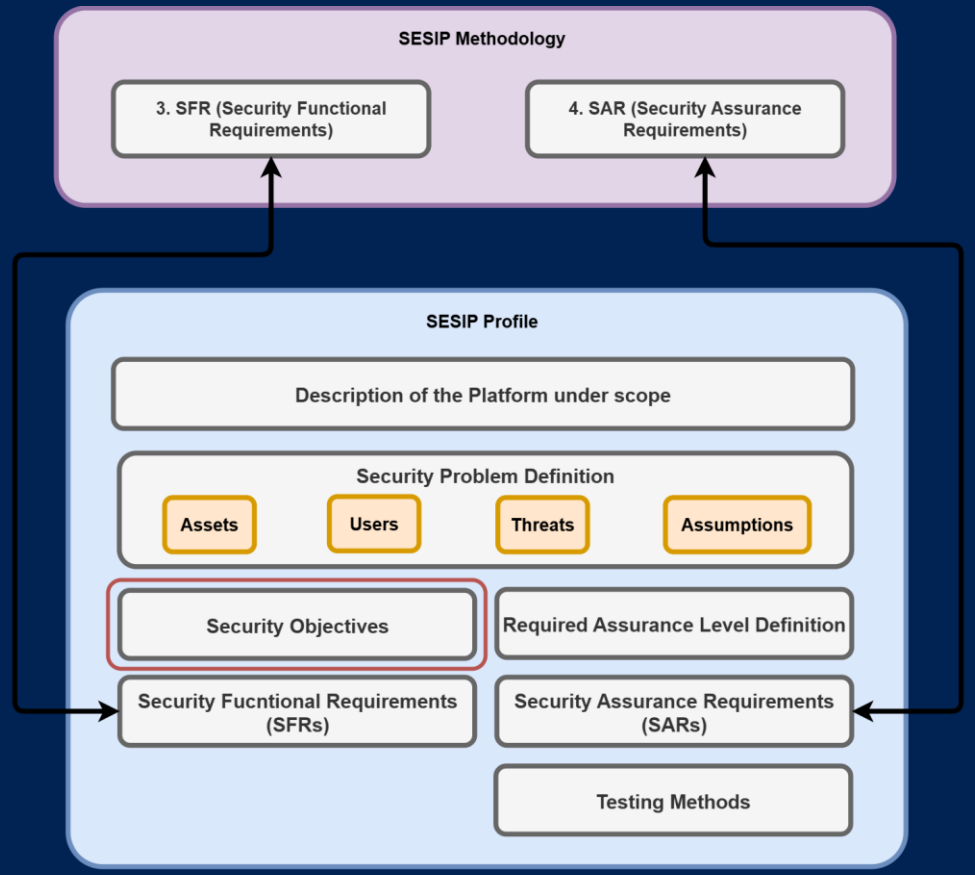
SESIP Profiles: Assumtions



3.5 Assumptions

- MPU/MCU or HPSE used within the TOE is already certified according to the appropriate GlobalPlatform Protection Profile.
- TOE is manufactured and provisioned in a secure environment, ensuring that no malicious modifications, backdoors, or unauthorized key insertions occur during production.
- Cryptographic keys and certificates used for authentication, encryption, and attestation are generated, stored, and distributed in a secure manner by the operational environment.

SESIP Profiles: Security Objectives

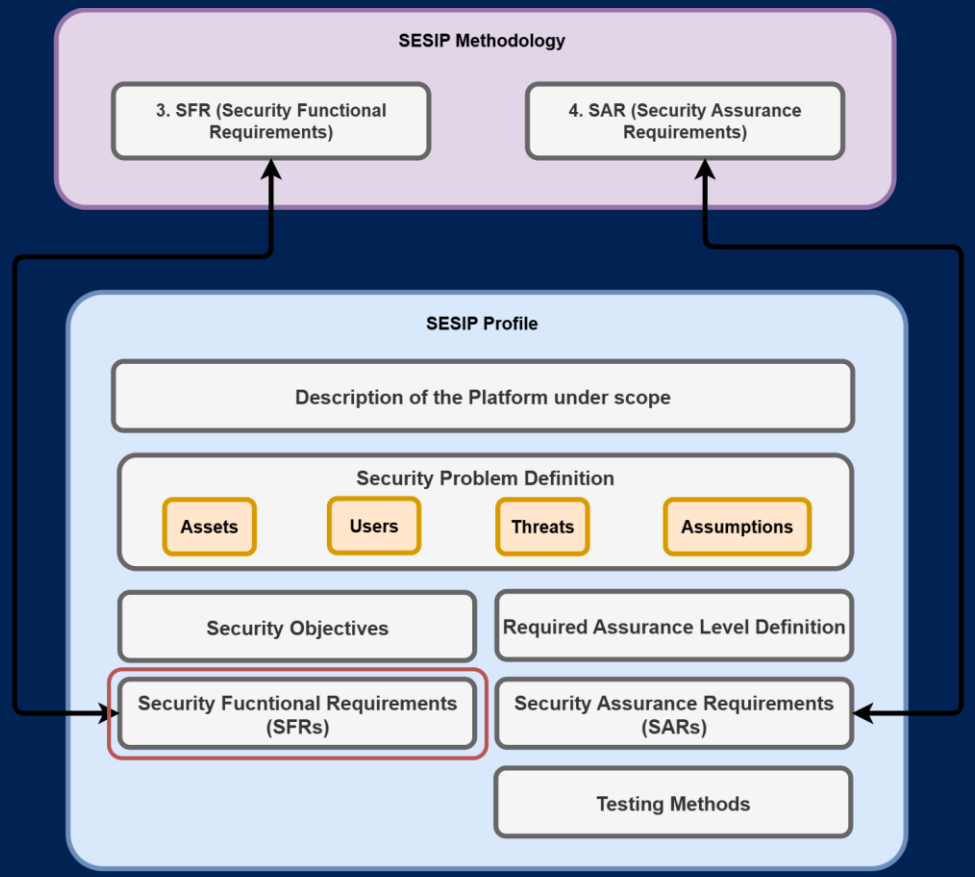


4 SECURITY OBJECTIVES FOR THE PLATFORM

For the platform to fulfil its security requirements, the environment (technical or procedural) must fulfil the following objectives.

Security Objective ID	Security Objective Name	Description
O.PLATFORM.01	**Secure Acceptance of Platform Components**	The ECU firmware and applications shall verify the authenticity, integrity, and correct version of all underlying platform components (e.g., MCU/MPU firmware, HPSE, or secure bootloader) prior to use, as described in the relevant platform documentation.
O.PLATFORM.02	**Application of Security Guidance**	The development, manufacturing, and integration environments shall protect all security-relevant material (e.g., firmware signing keys, provisioning data, credentials) at a security level equivalent to that of the ECU platform, following the official security guidance.
O.PLATFORM.03	**Secure Boot Usage**	The ECU firmware shall make use of the secure boot functionality provided by the underlying platform, ensuring that only authenticated and integrity-verified code is executed at startup, as specified in the platform documentation.
O.PLATFORM.04	**Secure Handling of Sensitive Material**	The ECU manufacturer or integrator shall handle all sensitive material (e.g., keys, credentials, calibration data) in accordance with platform security guidelines. Any deviations shall be justified and supported by equivalent protective measures.

SESIP Profiles: Security Functional Requirements (I)



5.3.2 Diagnostic Authenticated Access Control

Requirement

The Platform allows only diagnostic operations corresponding to <list of access levels> that are identified, authenticated, and authorized through <list of authentication mechanisms>.

INFO	In typical ECU implementations: - Access to protected diagnostic services (e.g., firmware update, memory write, parameter calibration) requires the establishment of a secure session after successful authentication. - Authentication may rely on mechanisms such as: - Challenge–response (seed/key) exchanges (e.g. under UDS SecurityAccess 0x27). - Certificate-based mutual authentication (e.g., TLS for DoIP). - Digital signature or token verification for OEM-proprietary protocols. - Upon successful authentication, the ECU transitions to a privileged access level, unlocking the diagnostic services associated with that level.

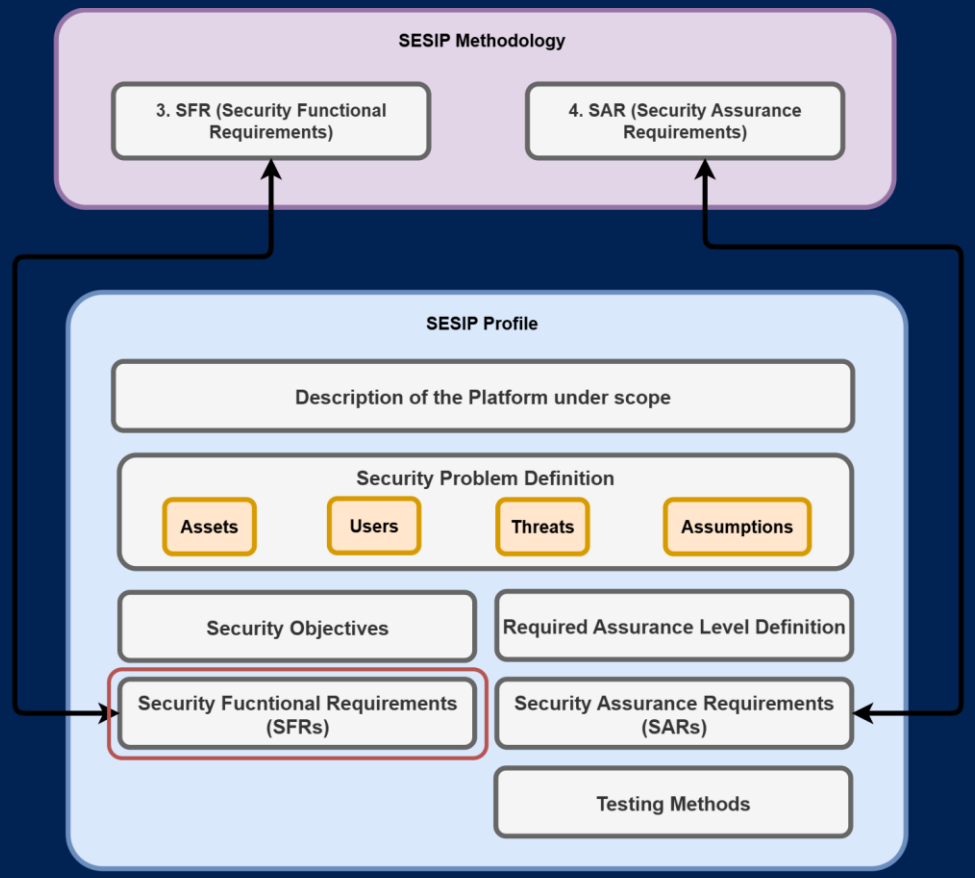
Value

This SFR requires the Platform to ensure that authentication mechanisms are enforced for accessing diagnostic operations bound to specific access levels, as defined in the diagnostic security policy or OEM-specific configuration.

Each access level corresponds to a defined set of permitted operations (e.g., read data, write memory, firmware update), and may require a distinct authentication strength or credential type (e.g., workshop, development, OEM backend).

This ensures that only authenticated entities possessing valid credentials for the corresponding access level can perform restricted diagnostic functions.

SESIP Profiles: Security Functional Requirements (II)



5.3.4 Attempt Limiting and Lockout

Requirement

The Platform enforces attempt limiting for <list of diagnostic authentication mechanisms> and applies a <temporary or permanent> lockout after <defined threshold> consecutive failed authentication attempts.

INFO	If authentication mechanisms rely on asymmetric cryptography (e.g., digital signatures or mutual TLS), where brute-force attempts are computationally infeasible, this requirement may be removed (via strikethrough) in the Security Target (ST) with justification.

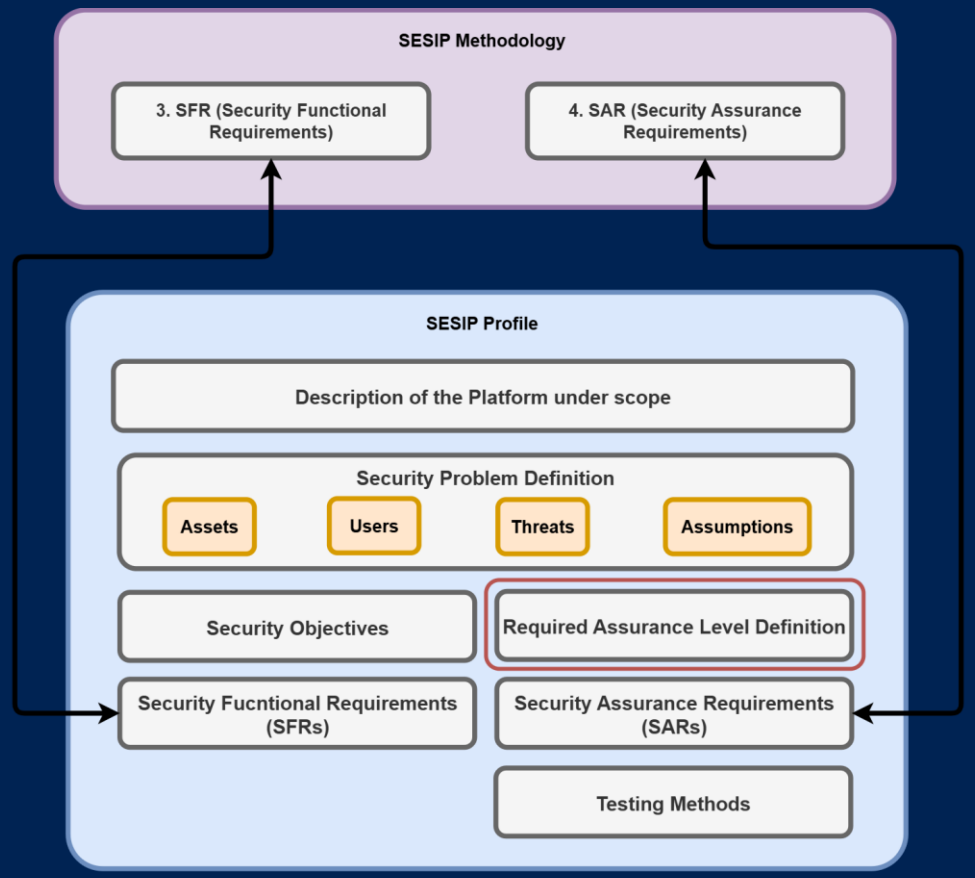
Value

This SFR ensures that repeated unauthorized attempts to authenticate or gain elevated diagnostic access are detected and mitigated.

The Platform must prevent unrestricted brute-force or replay attempts against authentication mechanisms (e.g., seed/key exchanges, password or token-based unlocks).

Lockout conditions may be temporary (e.g., session-based delay or timeout) or permanent (e.g., requiring authorized reset or power cycle).

SESIP Profiles: Assurance Level Definition



The required assurance level and applicable security features depend primarily on two independent factors:

Dimension	Assumption	Meaning	Consequence for the TOE
Physical access to the ECU	Trusted User Only	The ECU is embedded in the vehicle, not easily removable, and can only be accessed by authorised workshops using controlled tooling and procedures.	Hardware tamper-resistance (R-2) and zeroisation mechanisms are optional. Best-practice side-channel protection is sufficient. Focus on secure boot, authenticated diagnostics, and controlled update processes.
	Any User	The ECU can be physically removed, probed, resold, or reused by unauthorised parties. Physical possession by an attacker is realistic (e.g., aftermarket, replacement, or telematics units).	Hardware tamper-resistance and zeroisation hooks (R-2) are recommended. Secure storage and credential protection become mandatory. Audit logging and anti-rollback mechanisms are encouraged for forensic and lifecycle assurance.
Software executing on the ECU	Trusted Code Only	All ECU software is developed, signed, and released by the OEM or Tier-1 supplier. Secure boot is enforced and prevents execution of unverified firmware.	Software isolation can rely on the trusted platform's secure boot chain. The TOE shall focus on firmware authenticity, update verification, and secure diagnostics. Partitioning within the ECU may not be required.
	Any Code	The ECU may execute or interface with third-party or open-source components (e.g., adaptive or app-enabled ECUs, infotainment, or connected telematics).	The TOE must rely on the platform's isolation mechanisms and claim additional hardening, including secure-session management, input validation, and enhanced audit logging (R-1). Runtime monitoring and secure update verification are strongly recommended.

Typical ECU configurations covered by this SESIP Profile include:

Config ID	Description	Mandatory Packages	Optional Packages	Intended SESIP Level
CFG-BASE	Standard ECU implementing the Core Package only.	Core Package	None	SESIP Level 2
CFG-EXT-SEC	ECU with enhanced security services such as Secure Diagnostics, Secure Logging, or Secure Storage.	Core Package	Functional Packages	SESIP Level 2–3
CFG-PROT	ECU implementing additional network security measures for CAN, Ethernet, or DoIP communications.	Core + Protocol Packages	Functional (optional)	SESIP Level 2-3
CFG-HIGH-ASSURANCE	ECU including recommended requirements anti-rollback, secure manufacturing, or OTA client capabilities,	Core + Optional Capabilities	Functional / Protocol	SESIP Level 3–5

SESIP Profiles: Assurance Level Requirements

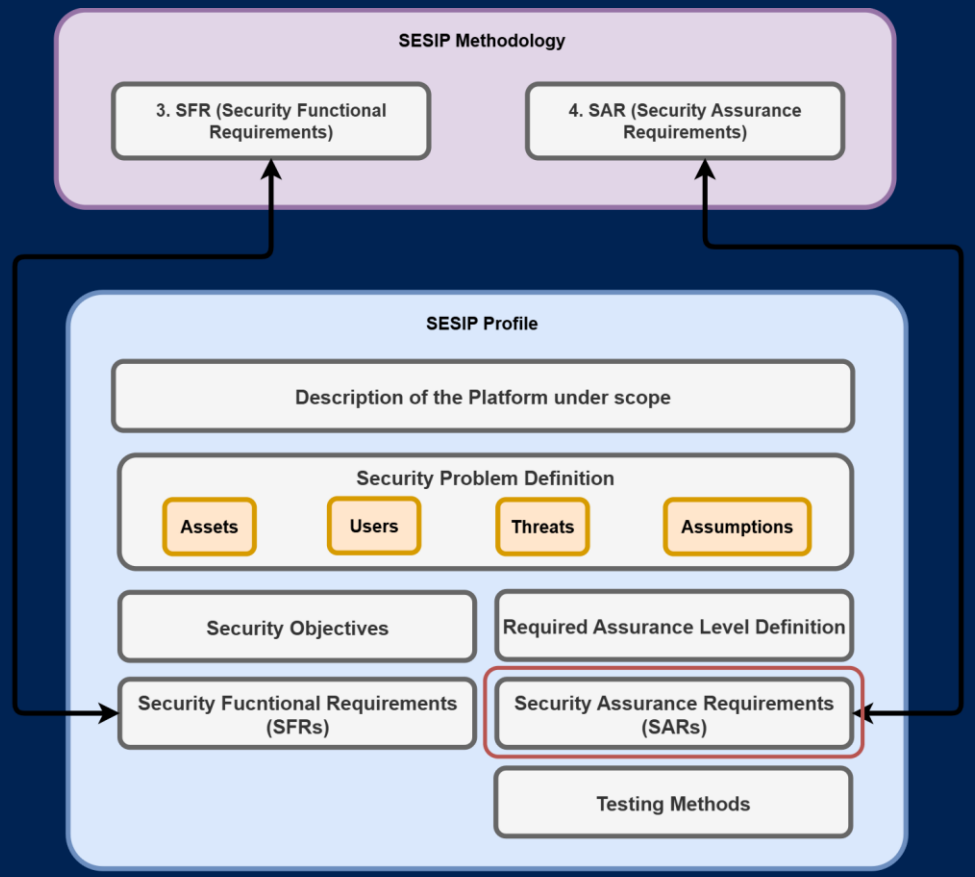


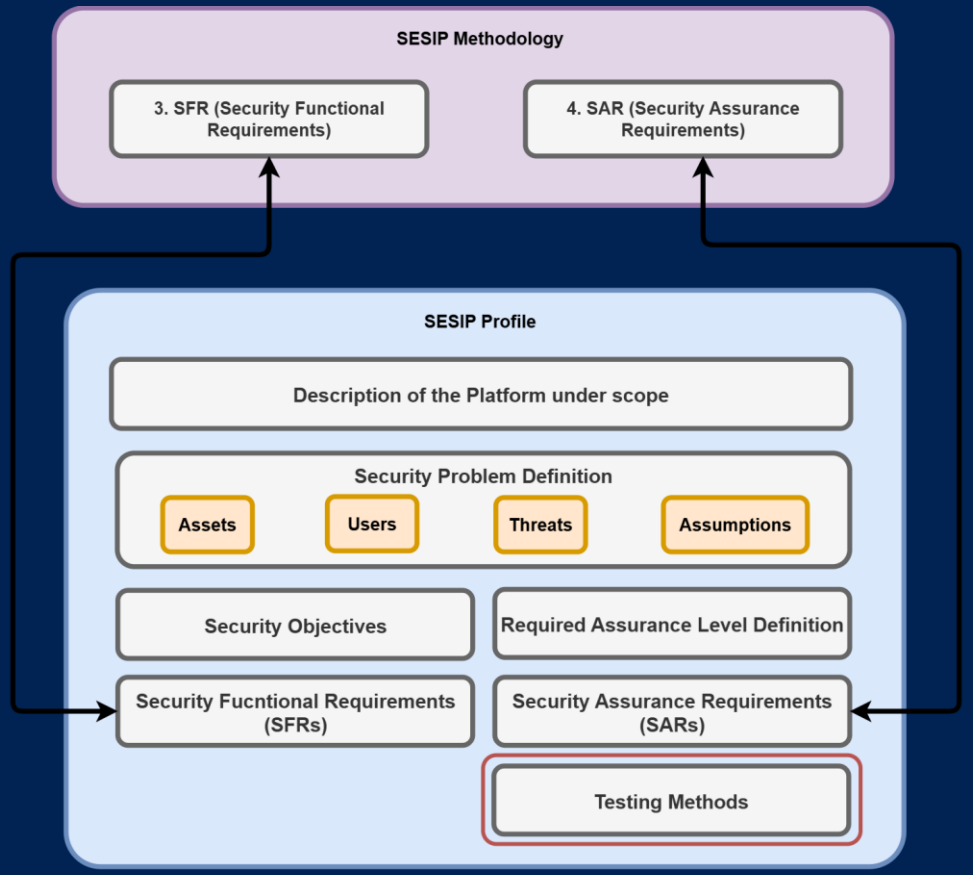
Table 4-2: SESIP2 Assurance Requirements

Assurance Class	Assurance Families
ASE: Security Target evaluation	*ASE_INT.1* *ST Introduction* *ASE_OBJ.1* *Security requirements for the operational environment* **ASE_REQ.3** **Listed security requirements** *ASE_TSS.1* *TOE summary specification*
ADV: Development	ADV_FSP.4 Complete functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	*ALC_FLR.2* *Flaw reporting procedures*
ATE: Tests	ATE_IND.1 Independent testing: conformance
AVA: Vulnerability Assessment	AVA_VAN.2 Vulnerability analysis

Table 4-3: SESIP3 Assurance Requirements

Assurance Class	Assurance Families
ASE: Security Target evaluation	*ASE_INT.1* *ST Introduction* *ASE_OBJ.1* *Security requirements for the operational environment* **ASE_REQ.3** **Listed security requirements** *ASE_TSS.1* *TOE summary specification*
ADV: Development	ADV_FSP.4 Complete functional specification **ADV_IMP.3** **Complete mapping of the implementation representation of the TSF to the SFRs**
AGD: Guidance documents	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMS.1 TOE CM coverage ALC_FLR.2 Flaw reporting procedures
ATE: Tests	ATE_IND.1 Independent testing: conformance
AVA: Vulnerability Assessment	AVA_VAN.3 Focused vulnerability analysis

SESIP Profiles: Testing Methods



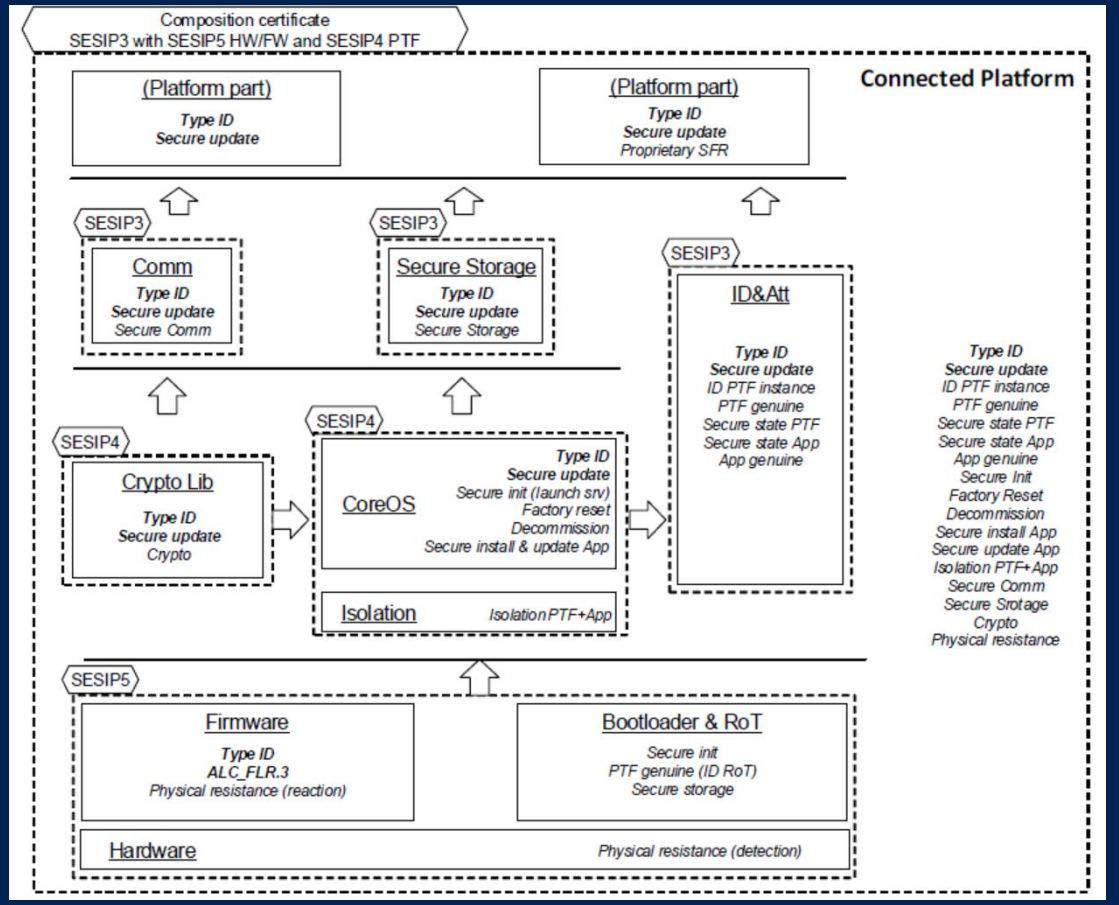
Profiles can include detail about testing methods:

- **Functional testing** → validate security behavior
- **Vulnerability analysis** → assess design & implementation
- **Fuzzing** → test interface robustness
- **Penetration testing** → validate resistance to attackers

But, why for items and components?

- **Due to the Composition and Reusability:**

Thanks to composition and reusability, SESIP Profiles can standardize security requirements across all the items and components that make up a modern automotive system



Global Platform®

SESIP

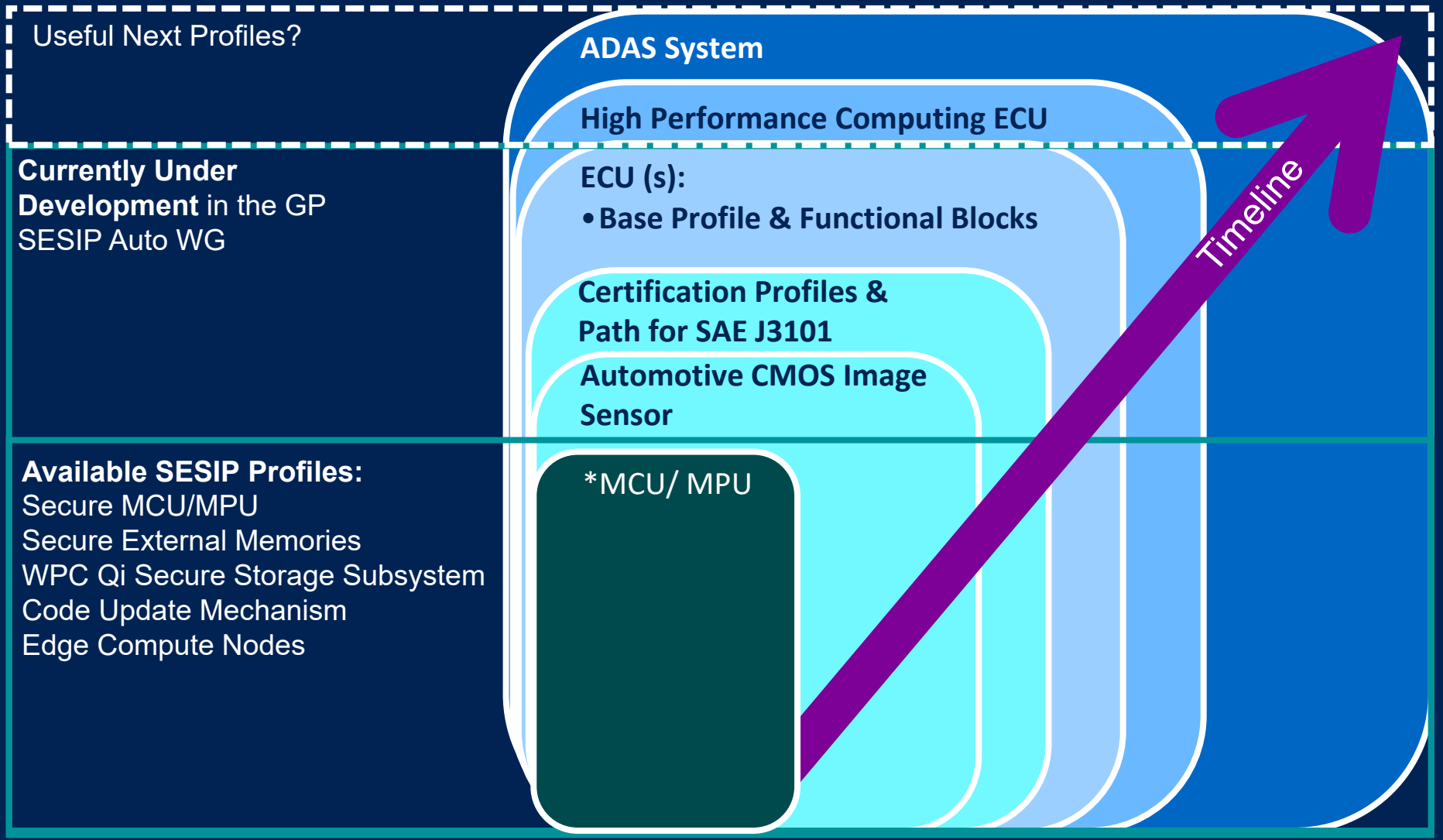
Profiles & Roadmap

SESIP Automotive Profiles Roadmap

Useful Next Profiles?

Currently Under Development in the GP SESIP Auto WG

Available SESIP Profiles:
Secure MCU/MPU
Secure External Memories
WPC Qi Secure Storage Subsystem
Code Update Mechanism
Edge Compute Nodes



Modular Composable

Global Platform®

Automotive Profiles Roadmap

- SAE J3101-5 PP – Gaps TEE & SE (Q3 2026?)
  - Public Review
- J3101 Baseline SESIP Profile (Q3 / Q4 2026?)
  - Pending Initial Draft (June ?)
- AIST CMOS Image Sensor PP *(Q4 2026 or Q1 2027)*
  - 2nd Draft Published (April 17th)
- Baseline Profile for ECUs (Q1 2027?)
  - 1st Draft - Comments period

Global Platform®

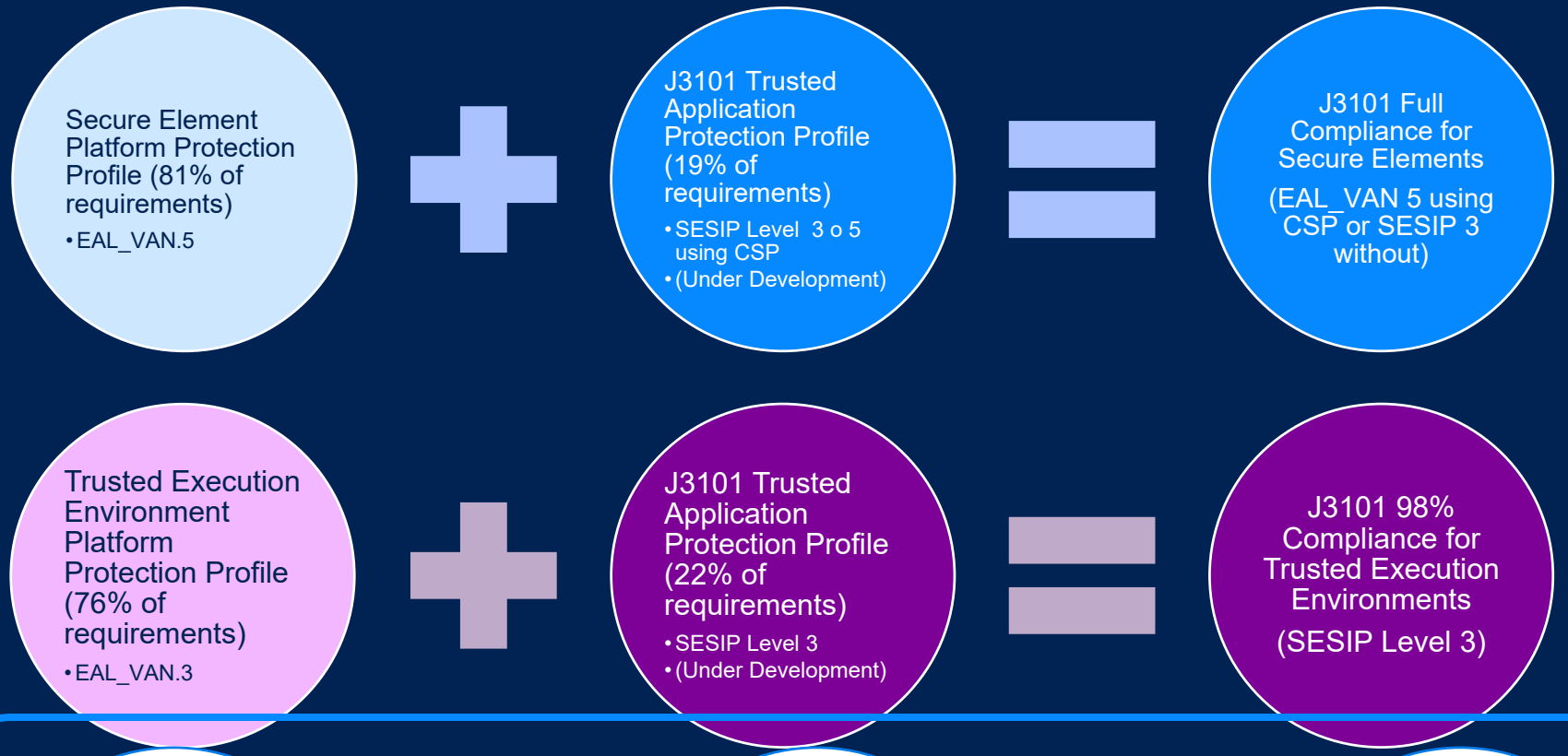
SESIP Technical Automotive SG

J3101 Base Profile

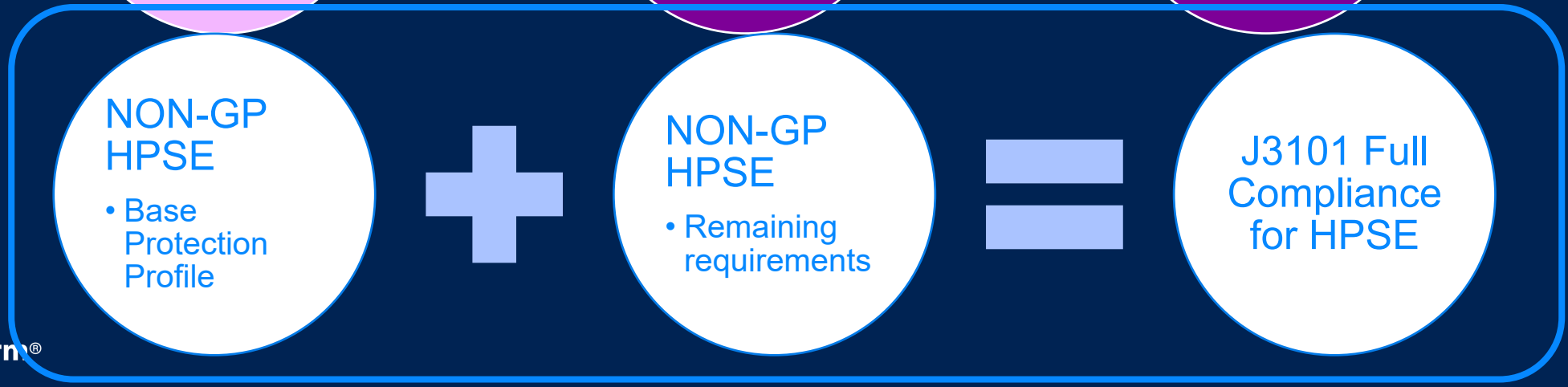
SAE J3101 – Hardware Protected Security Environment (HPSE)

- Defines a hardware-based security framework for automotive / ground-vehicle electronic systems.
- Protects critical assets such as cryptographic keys, secure code execution, and sensitive in-vehicle data.
- Establishes common requirement areas: key protection, crypto algorithms, random number generation, secure nonvolatile storage, interface control, secure execution, and self-tests.
- Typical use cases include secure boot, secure software update, secure in-vehicle messaging, diagnostics, data logging, and IP protection.
- Serves as a useful foundation alongside ISO/SAE 21434 and broader vehicle cybersecurity efforts.

J3101 SESIP Baseline Profile

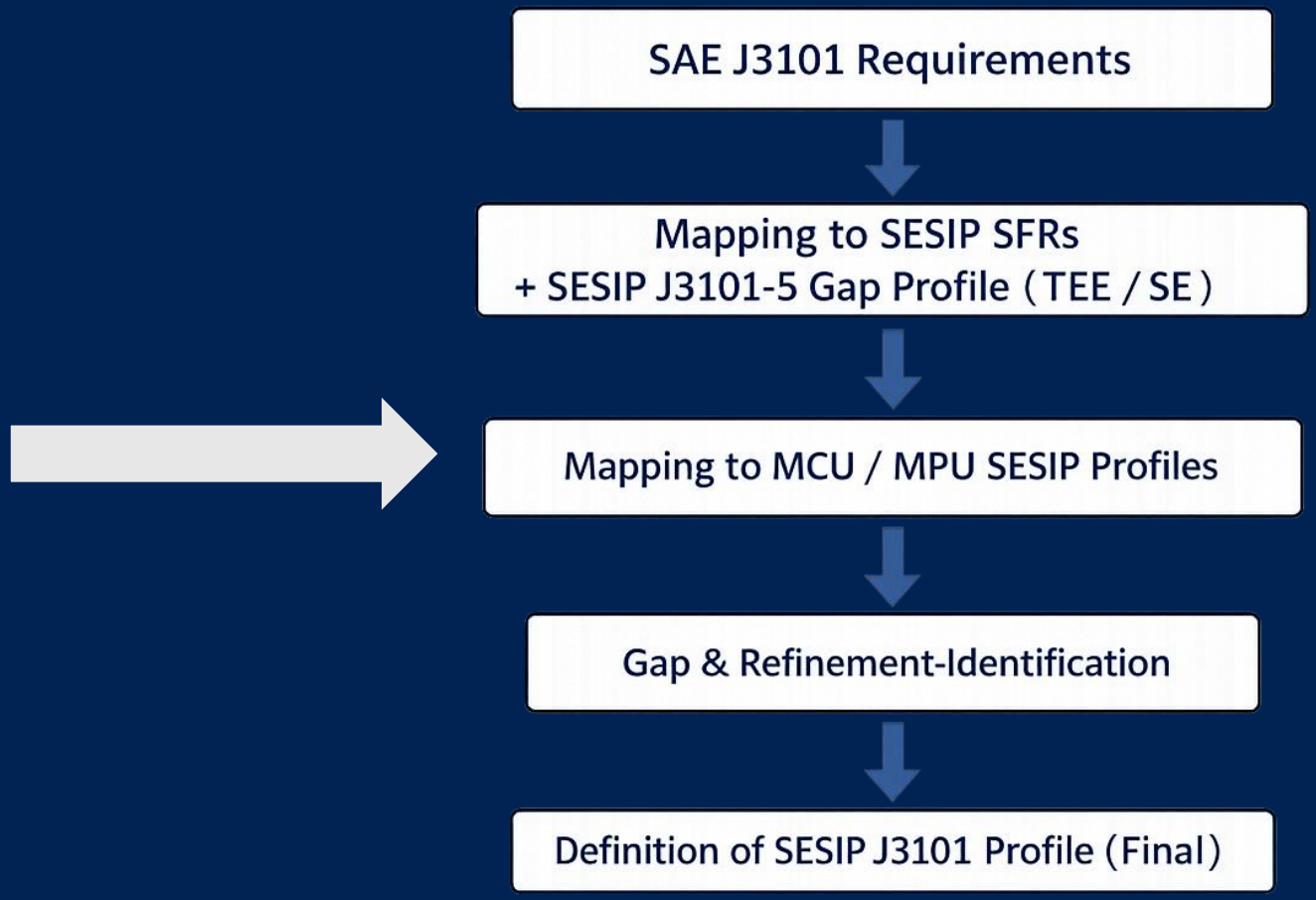


Security Target of Non-GP HPSE



Global Platform®

J3101 Profile



Global Platform®

SESIP Technical Automotive SG

Automotive CMOS Image Sensor Profile

AIST – CMOS Image Sensor

- AIST is actively addressing **security challenges** in CMOS Image Sensors
- Developed a structured **security problem definition**, including:
  - **Assets**: Image data, sensor configurations, control logic, firmware
  - **Threats**:
    - Unauthorized access or control of sensor
    - Data leakage or covert exfiltration
    - Tampering with captured image content
  - **Potential Vulnerabilities**:
    - Insecure interfaces (e.g., test/debug ports)
    - Unprotected memory or firmware regions
    - Lack of authentication in communication protocols
  - **Security Functional Requirements** under development:
    - Secure boot and firmware update
    - Access control and interface protection
    - Integrity checks for image and configuration data

AIST – CMOS Image Sensor – 2nd Draft

- Automotive CMOS Image Sensor Profile
  - Image array considered out of scope
  - SESIP Levels 1,2 and 3
  - Packages: Secure Update & Physical Resistance
  - Mapping to MPU/MCU Profile

SESIP SFR	MCU / MPU Profile	ACIS Profile
Verification of Platform Identity	Base SP	Mandatory
Verification of Platform Instance Identity	-	Mandatory
Secure Initialization of platform	Base SP	Mandatory
Secure Communication Support	-	Mandatory
Secure Communication Enforcement	-	Mandatory
Attestation of Platform Genuineness	-	Optional
Secure Debugging	Base SP	Optional
Secure Data Serialization	Package 'Secure Storage'	Optional
Secure Trusted Storage	Package 'Secure Storage'	Optional
Secure Confidential Storage	Package 'Secure Storage'	Optional
Secure Encrypted Storage	Package 'Secure Storage'	Optional
Cryptographic Operation	Package 'Security Services'	Optional
Secure Update of platform	Base SP	Package 'Secure Update'
Limited Physical Attacker Resistance	Package 'Secure Enclave'	Package 'Hardware Protections'

Global Platform®

ECU Profile

Base Protection Profile

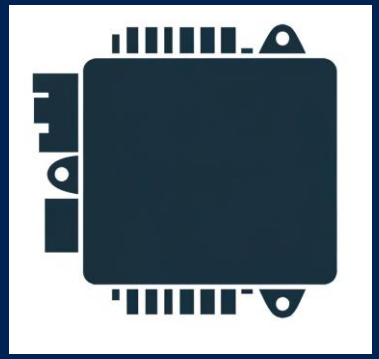
- **Assumptions**
  - Functionality not defined
  - Common automotive interfaces (CAN, LIN or Ethernet)
  - ECU running only RTOS (based on AUTOSAR OS)

- **Reuse of Profiles / Certificates**
  - GP TEE / SE
  - SESIP SAE J3101
  - SESIP MPU / MCU
  - …

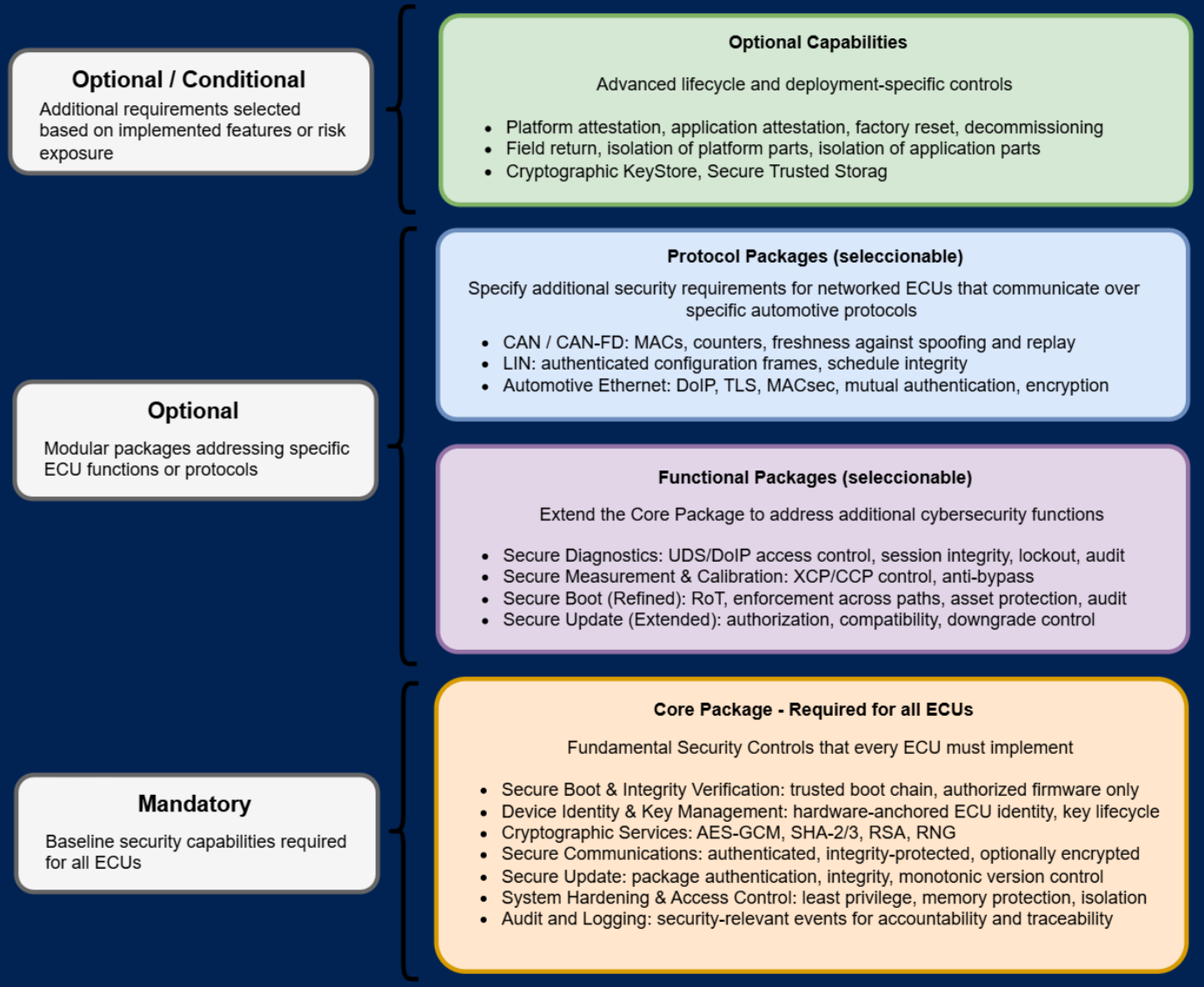
- **Additional Requirements for different SESIP Levels**
  - Potential mapping to CAL
  - Mapping to ASIL levels (?)

Limited Surface

- **ECU with SoC** (AUTOSAR RTOS)
- **Wired Interfaces** (CAN, LIN)
- **Example:** Rear Lamp system integrating one SoC using AUTOSAR OS with 2 x CAN and a LIN interface



Base Protection Profile – General Structure



Typical Configurations Covered

This SESIP Profile is intended to cover a wide range of Electronic Control Units (ECUs) with varying architectures, feature sets, and integration contexts. The Security Target (ST) must indicate in this section the implemented configuration(s) of the ECU platform in order to define which Security Functional Requirements (SFRs) are applicable in subsequent sections. The descriptions below shall be adapted and replaced by the specific details of the TOE).

Typical ECU configurations covered by this SESIP Profile include:

Config ID	Description	Mandatory Packages	Optional Packages	Intended SESIP Level
CFG-BASE	Standard ECU implementing the Core Package only.	Core Package	None	SESIP Level 2
CFG-EXT-SEC	ECU with enhanced security services such as Secure Diagnostics, Secure Logging, or Secure Storage.	Core Package	Functional Packages	SESIP Level 2–3
CFG-PROT	ECU implementing additional network security measures for CAN, Ethernet, or DoIP communications.	Core + Protocol Packages	Functional (optional)	SESIP Level 2-3
CFG-HIGH-ASSURANCE	ECU including recommended requirements anti-rollback, secure manufacturing, or OTA client capabilities,	Core + Optional Capabilities	Functional / Protocol	SESIP Level 3–5

Global Platform®

Questions ?