Global Platform®

Cybersecurity Vehicle Forum

Audi Conference Center - Munich

21st October 2026

Jorge Wallace, Chair of SESIP Automotive SG

© GlobalPlatform 2026

Agenda

Automotive Domain

SAE J3600

SESIP Profiles

Global Platform™

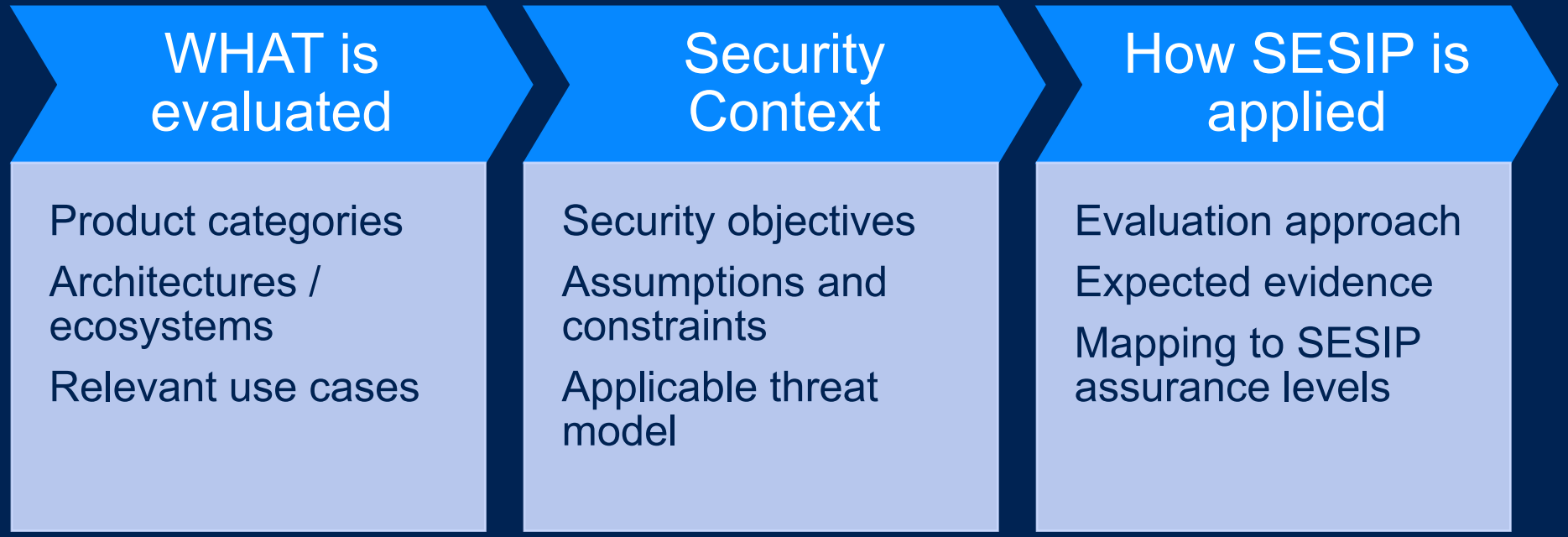
Global Platform®

SESIP Domains

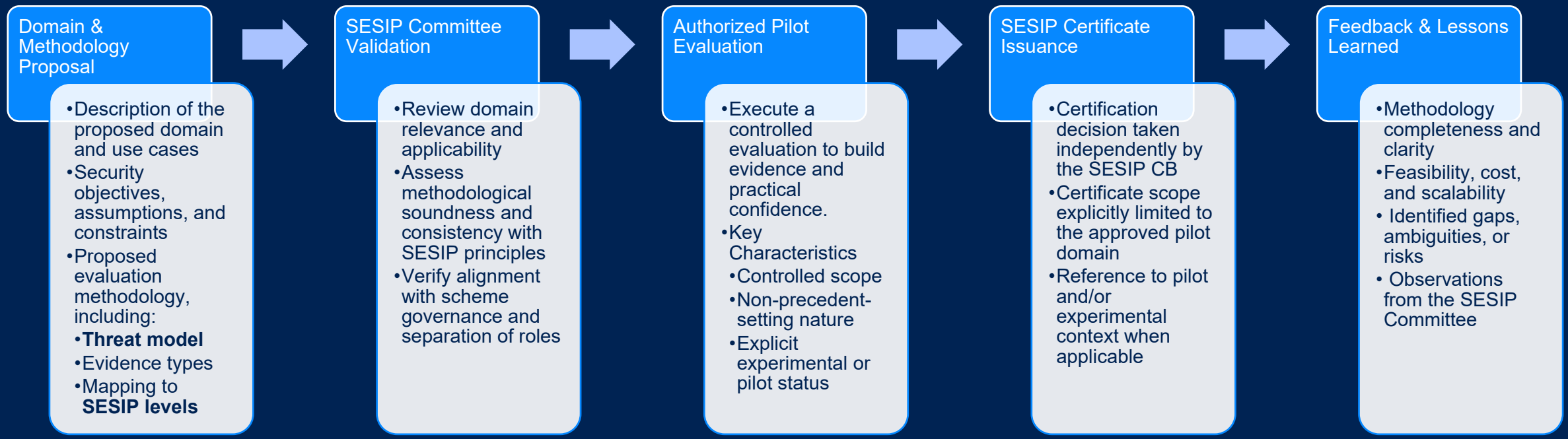
SESIP Domain

A SESIP domain defines the context in which SESIP is applied to a particular class of products, architectures, ecosystems or use cases.

It establishes the boundaries and context needed to apply SESIP consistently



SESIP Domains – Process Description



Why a SESIP Automotive Domain?

GlobalPlatform has requested the creation of a dedicated SESIP Automotive Domain.

- Common framework for applying SESIP consistently across automotive use cases, architectures and component types.
- Allow automotive-specific security concepts and evaluation practices to be incorporated directly into SESIP.
- Automotive-specific test methods, evidence expectations and attack scenarios can be defined at domain level instead of being recreated independently for each profile.

Improved alignment with ISO/SAE 21434, including concepts such as:

- Threat Analysis and Risk Assessment (TARA)
- Cybersecurity goals and claims
- Risk-based security requirements
- Verification and validation activities

The Automotive Domain turns SESIP from a generic component-security methodology into a framework that can directly reflect automotive risks, engineering processes and regulatory expectations.

From Automotive Profile to an Automotive Domain

Original Approach

Automotive Profiles

- **Extend the SESIP Profile structure with automotive-specific sections**
- Include common automotive concepts directly in each Profile
- Add generic automotive material through Profile annexes
- Examples considered:
- CAL mapping
- TAF / Threat Attack Trees
- Verification & Validation activities
- UNECE R155/R156 threats and mitigations
- Automotive attack-tree / attack-method guidance
- **Risk**: common methodology and guidance may be repeated across multiple Profiles

Automotive Domain + Lean Product Profiles

Automotive Domain

- Automotive terminology and common assumptions
- Automotive threat / risk framework
- TARA / TAF interpretation and methodology
- CIA / Supply Chain considerations
- Generic attack methodologies and testing principles
- Automotive interpretation of SESIP assurance levels (including L4 / L5)
- CAL / assurance mapping methodology
- Common V&V expectations
- UNECE threat mappings and regulatory references
- Generic evidence expectations
- Common rules for evaluation reuse and composition

Specialized Profile

- Product / component type
- Intended use cases
- Security boundaries and lifecycle
- Assets and security objectives
- Specific CAL Mapping
- Product-specific threats
- Security functional requirements
- Applicable assurance level
- Specific evaluation activities or adaptations
- Profile-specific rationale and exceptions

Better Alignment with TARA, CAL & TAF

Domain + Specialized Profiles = Automotive-native SESIP

A dedicated **Automotive Domain**, combined with specialized SESIP Profiles, allows SESIP to align much more closely with established automotive cybersecurity methods.

The **Domain** can contain the generic, reusable methodology, while **Profiles** can specialize that methodology for particular product categories.

TARA

Domain: common rules for how TARA outputs are interpreted and used in SESIP

Profile: product-class-specific threats, assets, assumptions and attack scenarios

Evaluation: product/project TARA outputs may be used as input or supporting evidence

CAL

Domain: generic methodology for relating CAL expectations to SESIP assurance and evaluation depth

Profile: expected assurance level or rigor for a specific product category

Evaluation: project-specific CAL information may help justify the selected assurance approach

TAF

Domain: generic attack methodology, attack-potential concepts and rules for deriving test activities

Profile: attack trees or attack paths tailored to the specific product class

Evaluation: those attack paths can drive concrete penetration-testing activities

Why domains matter for SESIP Level 4/5

- Domains allow sector-specific evaluation methodologies
- Methodologies can define threat model, evidence and mapping to SESIP levels
  - Enables high-assurance SESIP evaluations without forcing a CC-only approach for Level 4 / 5
    - Committee Approval required (*)
- Automotive can incorporate TARA, attack methodology including automotive test methods and tailored evidence expectations

Domains are the enabler for SESIP Level 4 and 5 while keeping a structured and credible assurance framework.

Cybersecurity Interface Agreement & Supply Chain considerations

- Automotive cybersecurity is inherently shared across multiple organizations and supply-chain levels.

- SESIP evaluations should make clear which cybersecurity responsibilities belong to:
  - the evaluated component,
  - its integrator,
  - the operational environment, and
  - other suppliers or dependent components.
- Existing SESIP artifacts such as the **Security Target, SESIP Profiles and certificates** can already provide relevant information to support cybersecurity interface agreements.

- The Automotive Domain can also define common principles for documenting and communicating these dependencies.

Cybersecurity Interface Agreement Considerations

- Allocation of cybersecurity responsibilities between supplier and integrator/OEM
- Definition of security assumptions and environmental dependencies
- Identification of security functions provided by the component versus those expected externally
- Required integration and configuration conditions
- Identification of inherited security objectives / requirements

- Definition of cybersecurity evidence to be exchanged between parties including the use of existing SESIP artifacts as supporting evidence, for example:
  - Security Target: security claims, assumptions, objectives and evaluated scope
  - SESIP Profile: product-class security requirements and expected assurance
  - Domain-level guidance: common automotive assumptions, methodologies and supply-chain principles
  - Evaluation reports / certificates: evidence of evaluated security properties and assurance level

Supply Chain Security considerations

- **Objective**: Enable reuse of SESIP evaluation and certification results further up the automotive supply chain
- Clearly identify:
  - evaluated component and version
  - security claims and assurance level
  - assumptions and dependencies
  - applicable configuration
  - limitations of the evaluation
- Support composition of evaluated components into larger automotive systems
- Establish rules for when existing evidence can be reused and when additional evaluation is required
- Use SESIP outputs as part of the supplier assurance package, alongside other relevant evidence

Next Step: Automotive Domain Documents

The objective is to collaboratively develop the material required for the Automotive domain.

Work will focus on defining:

- Automotive domain scope and relevant use cases
- Applicable product categories and architectures
- Automotive-specific security objectives, assumptions and constraints
- Initial threat model / TARA integration approach
- Relevant evaluation and testing methodologies
- Expected evidence and mapping to SESIP assurance levels
- Candidate profiles and areas where existing SESIP material may need adaptation

Global Platform®

SAE J3600

SESIP, Cybersecurity Assurance Level (CAL), and Targeted Attack Feasibility (TAF) Assessments – Information Report

First Draft

SAE J3600: SESIP for Automotive

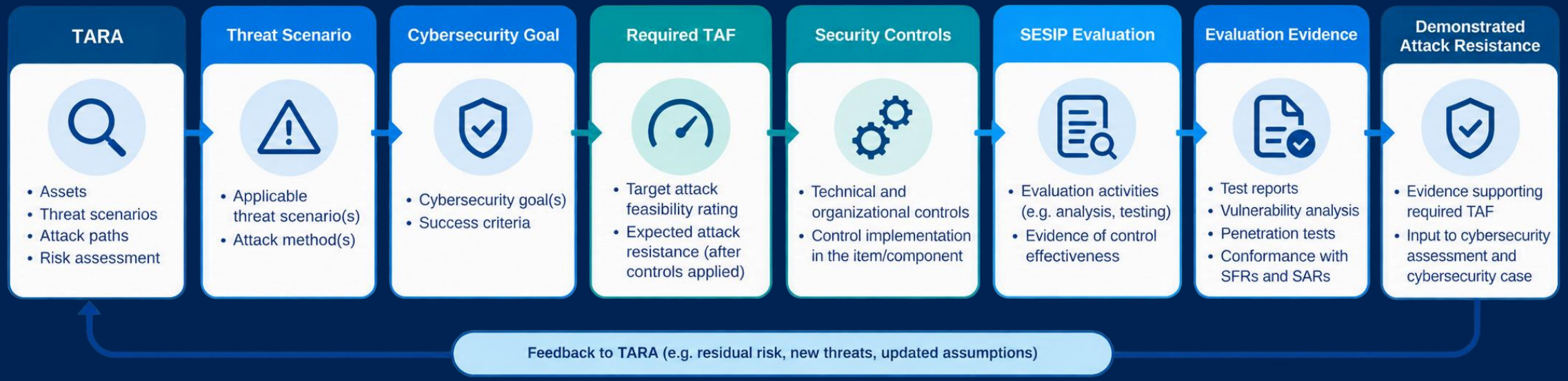
- SAE J3600 provides guidance on how the **Security Evaluation Standard for IoT Platforms (SESIP)** can be applied in the automotive domain and how SESIP evaluation results can support automotive cybersecurity engineering and assurance activities at item and component level.

SAE J3600: Connecting SESIP with CAL

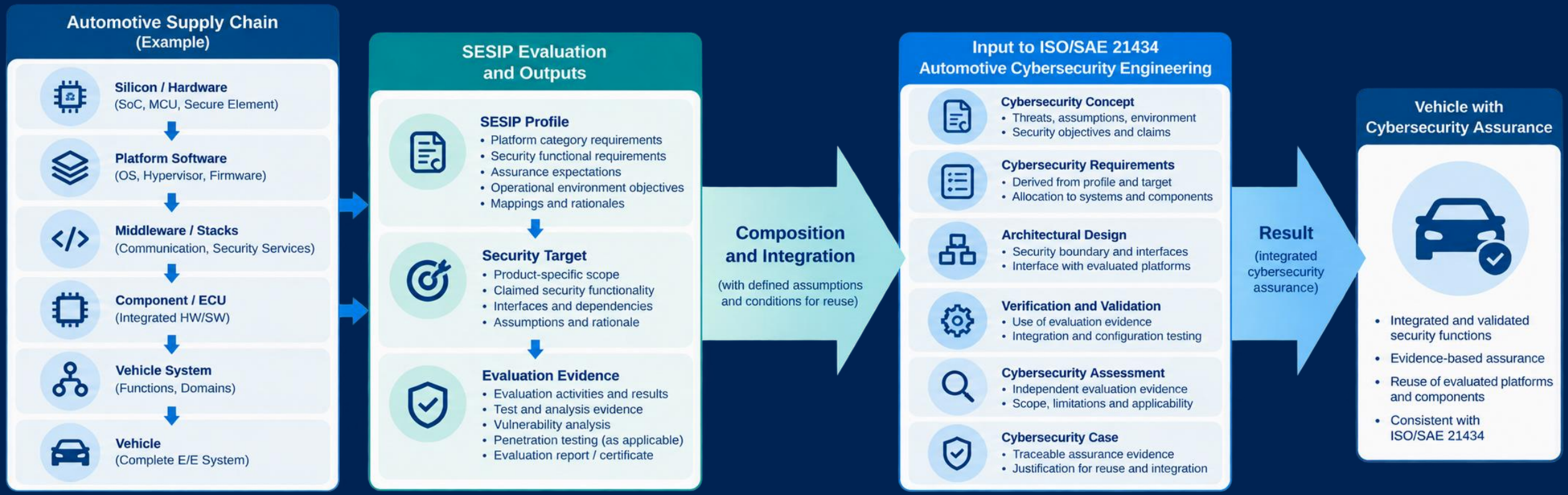
- ISO/SAE 8475 establishes three levels of cybersecurity assurance rigor:
  - CAL1 — Basic rigor
  - CAL2 — Intermediate rigor
  - CAL3 — Advanced rigor
- CAL determines the expected depth and breadth of cybersecurity activities, rather than selecting the cybersecurity controls themselves.

SAE J3600: Connecting SESIP with TAF

- Where CAL addresses development rigor, **TAF addresses the attack resistance expected after cybersecurity controls have been applied**.



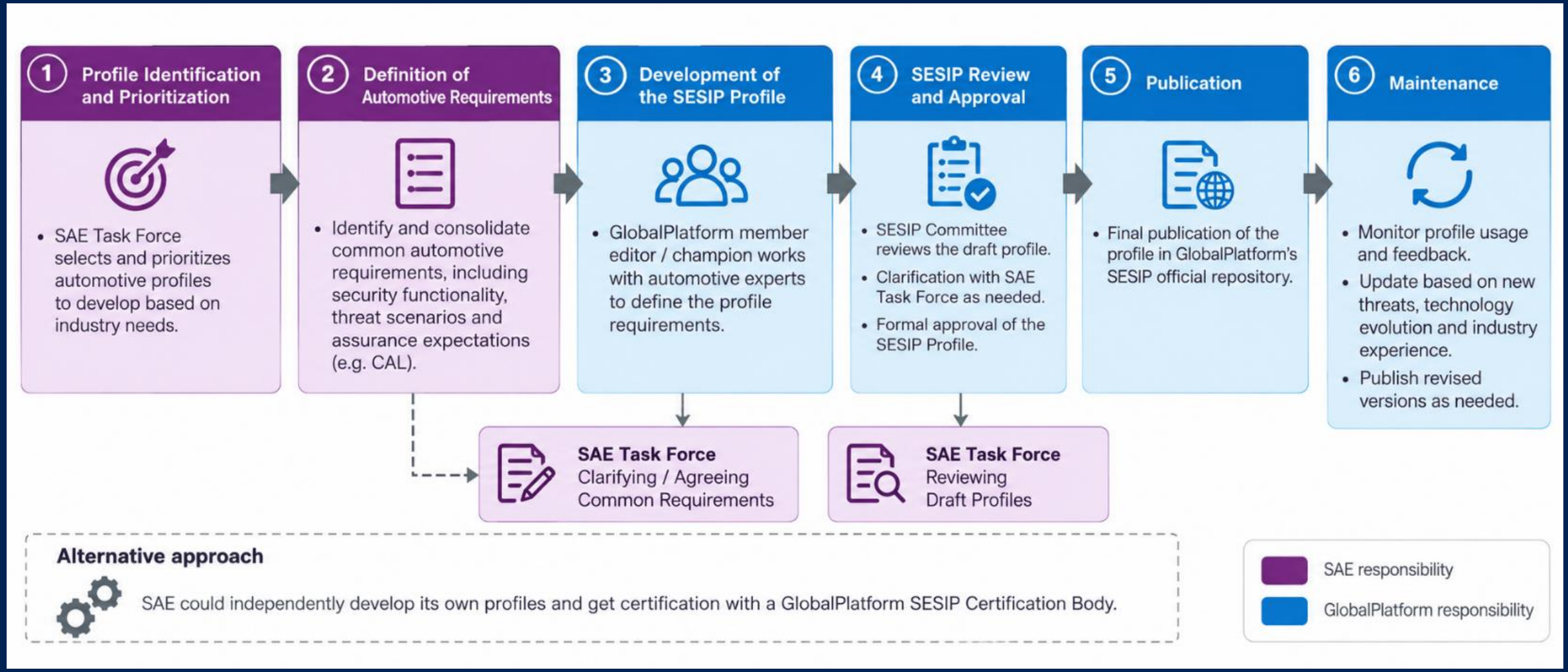
SAE J3600: From component evaluation to Vehicle Assurance



Open Questions

- Profile Development
- Automotive domain
- Delta Certification (ACL_FLR)
  - Software updates
- Annexes

SESIP Profiles - Process



Global Platform®

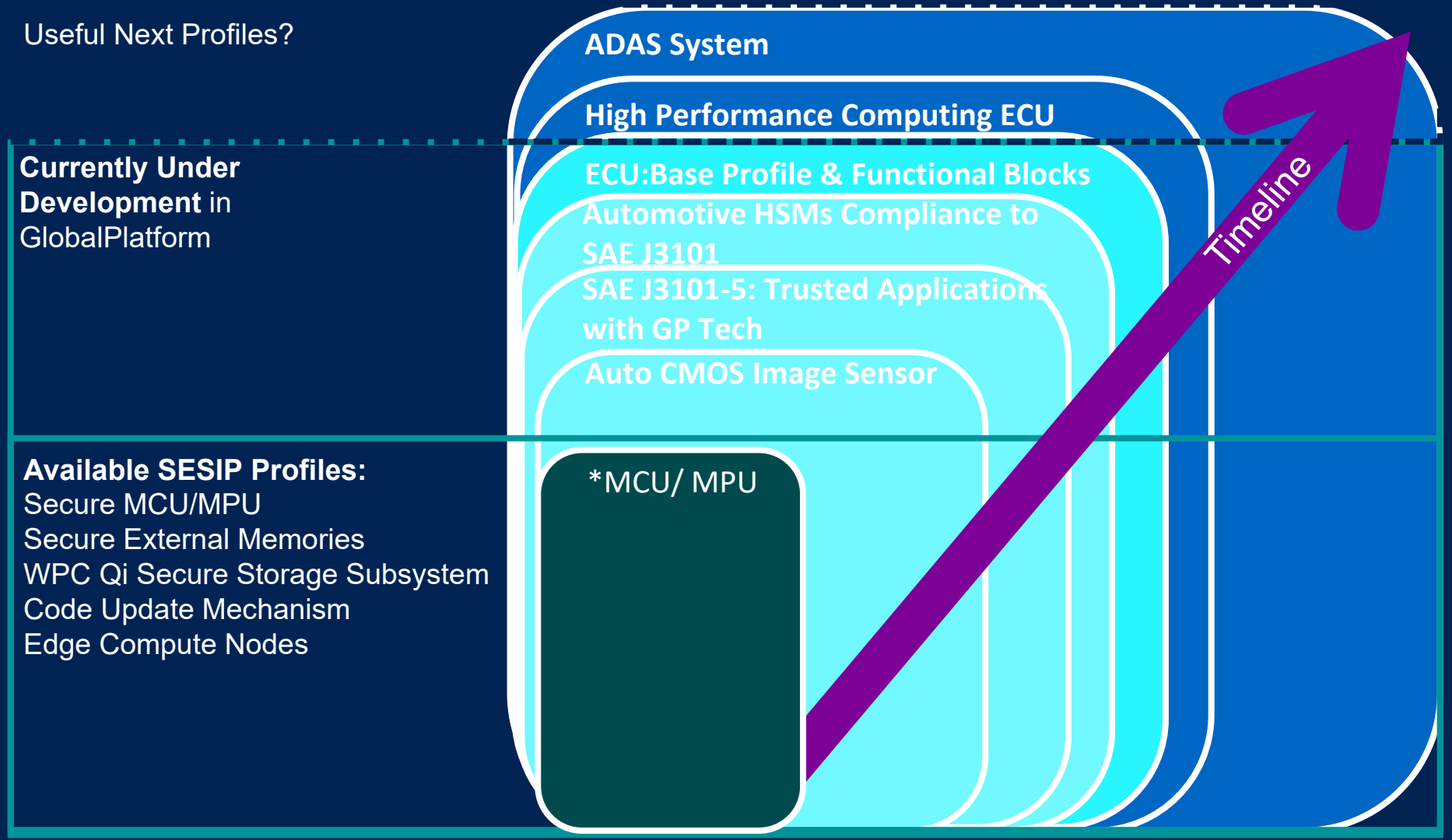
SESIP Profiles

SESIP Automotive Profiles Roadmap: Reusable Building Blocks for Automotive

Useful Next Profiles?

Currently Under Development in GlobalPlatform

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



Modular Composable

Global Platform®

Status of GlobalPlatform Automotive SESIP Profiles

Auto CMOS Image Sensor Profile	SAE J3101-5 Profile	Automotive HSM Compliance with J3101 Profile	Baseline Profile for ECUs
Current Status: 2nd Draft Published in Auto WG	Trusted Application Aspects levering TEE & SE	Proprietary HSM Evaluation of Compliance for J3101	Current Status: 1st Draft - Comments period
Final Publication: Q1 2027	Current status: Soon to be in Public Review	Current Status: Pending Initial Draft (September)	Final Publication: Q1 2027?
	Final Publication: Q4 2026?	Final Publication: Q1 2027?	

https://members.globalplatform.org/discussion/threats-mapping-for-acis-and-un-155-uploaded

Global Platform®

ECU Profile

© GlobalPlatform 2026

Base Protection Profile

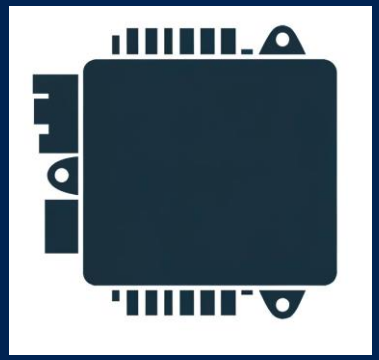
- **Assumptions**
  - Functionality not defined
  - Common automotive interfaces (CAN, LIN or Ethernet)
  - ECU running only RTOS (based on AUTOSAR OS)

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

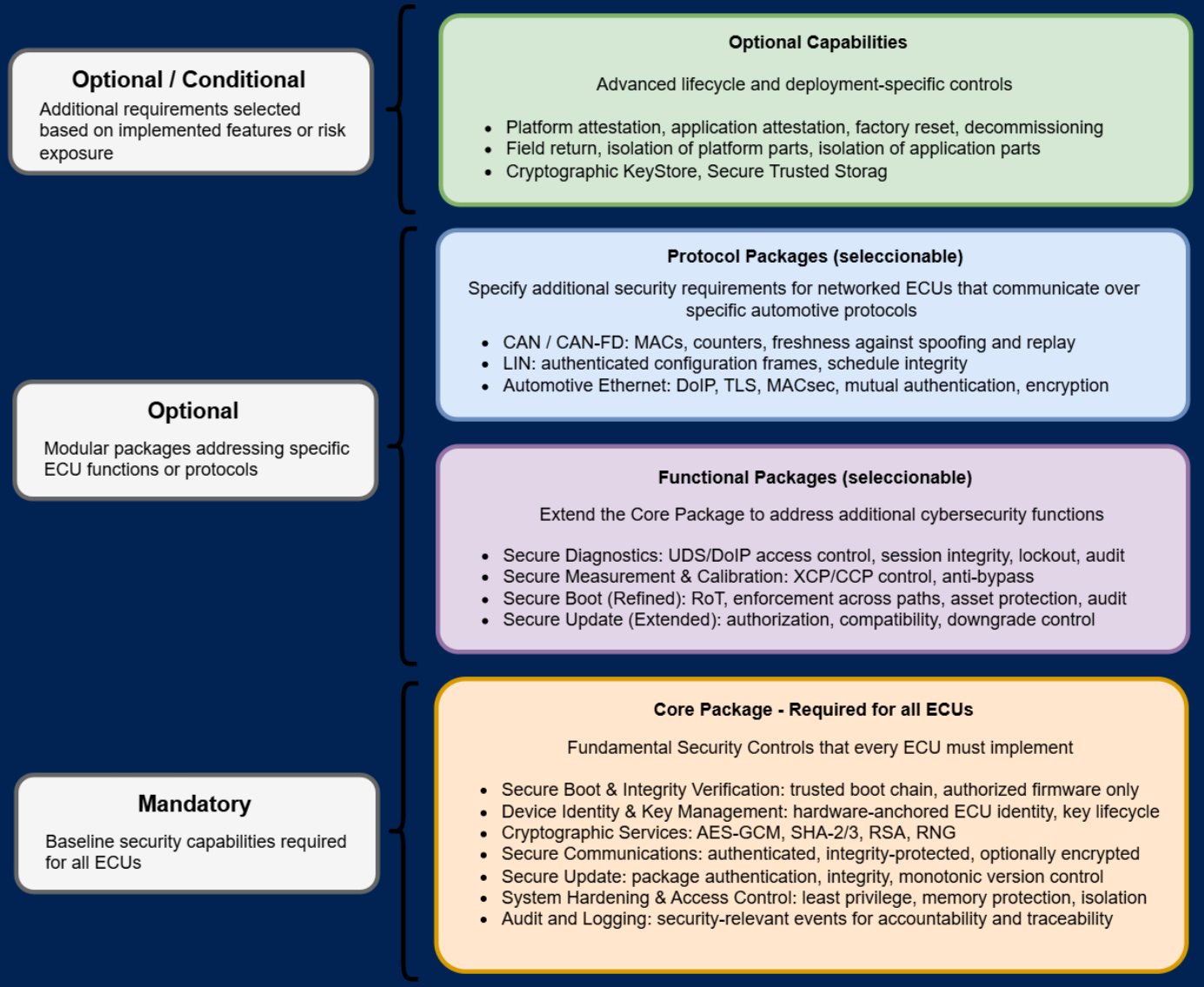
- **Additional Requirements for different SESIP Levels**
  - Potential mapping to CAL
  - Mapping to ASIL levels (?)

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



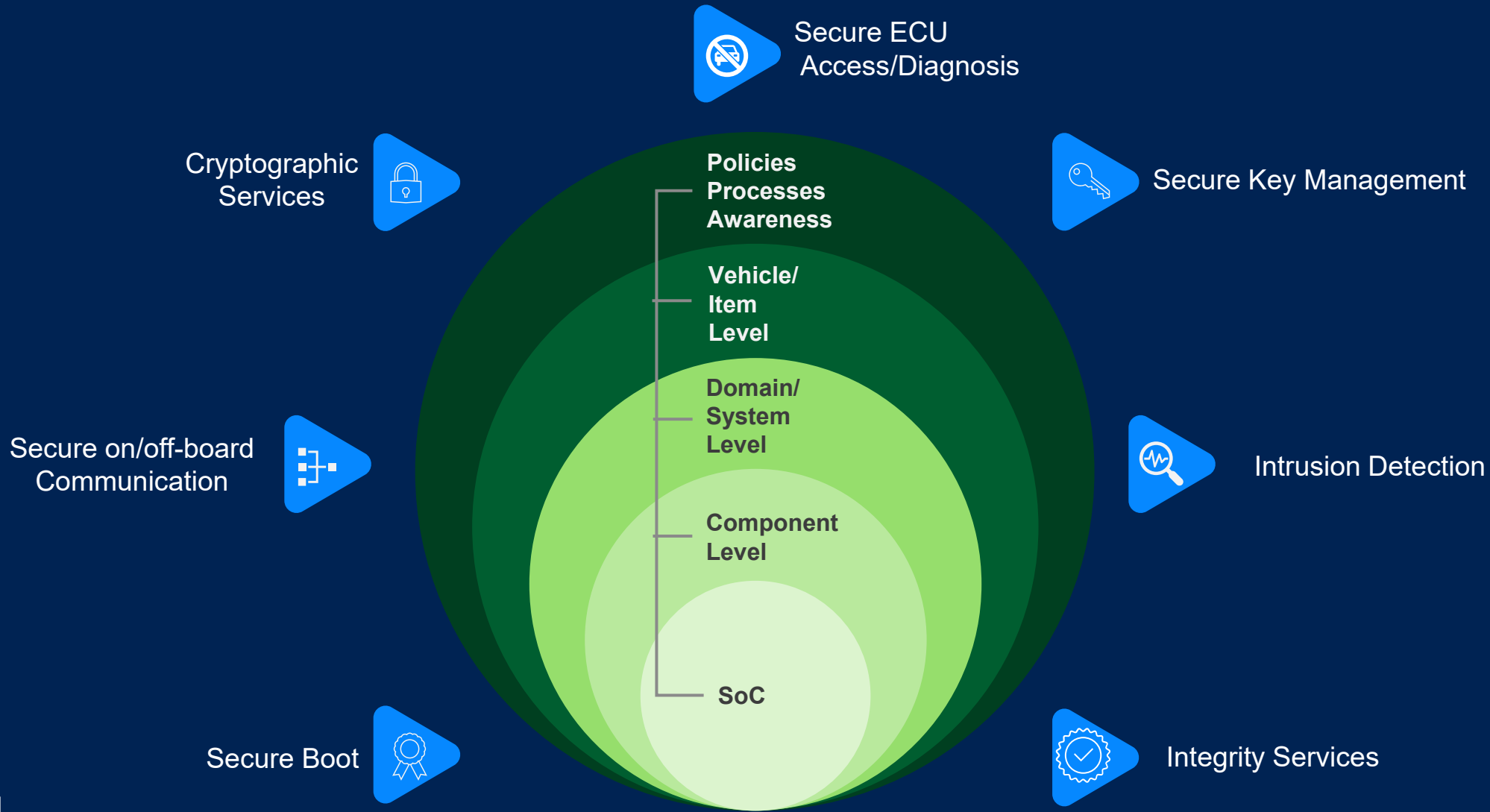
Typical Configurations Covered

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

SESIP Layered Approach



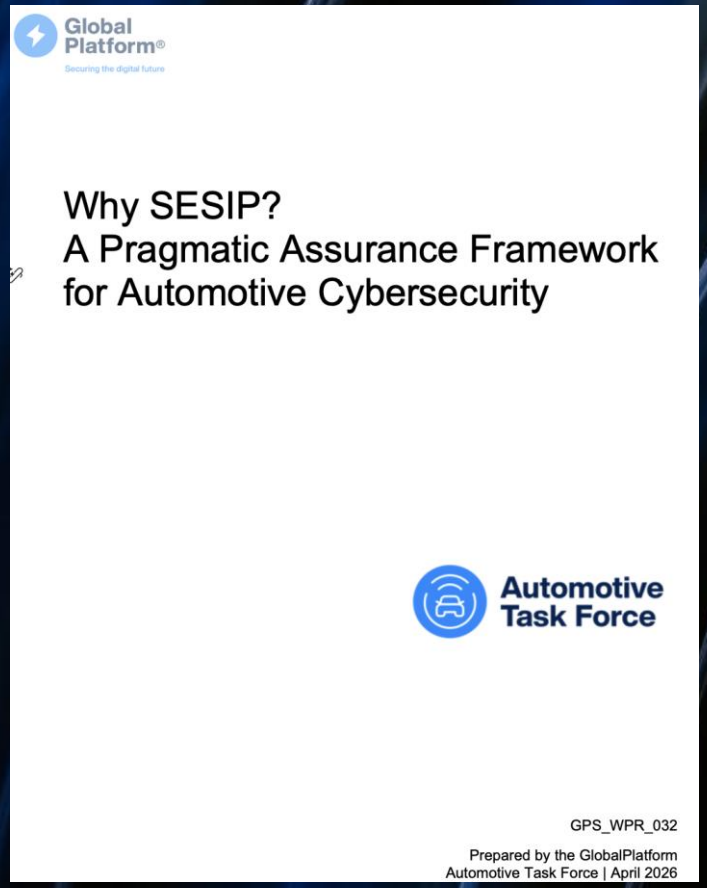
Global Platform®

Questions?

Come Join in the Fun…
Your Voice Needs to be Heard!

automotive@globalplatform.org

Or Develop Your Own Profile!



For additional information, please read our SESIP Whitepaper: https://globalplatform.org/resource-publication/

→globalplatform.org

→globalplatform.org