Global Platform®

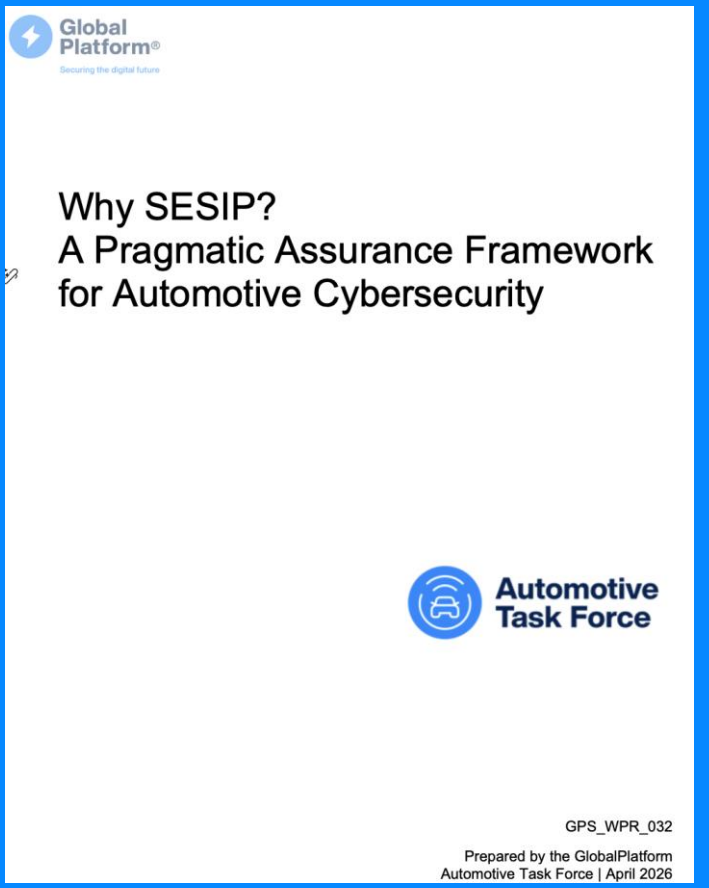
SESIP

May 2026

Francesca Forestieri, GP Head of Automotive
Jorge Wallace, DEKRA, Chair of Auto SESIP WG

Global Platform®

What is SESIP?



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

Measurable Assurance & Reusable Evidence

SESIP

Elements

- SESIP Security Evaluation Methodology
- SESIP Profiles for standard classes
- SESIP Certification for Products
- SESIP Mappings to Existing Regulations and Standards

Status

- Developed within GlobalPlatform by Industry
- Ecosystem Relevance
  - Widely adopted by semiconductor leaders
  - A European CENELC Standard (EN 17927)
  - Future work planned for ISO recognition

Motivation for SESIP Creation

Provide measurable assurance levels to products to meet industrial market needs

Focus on testing and limit bureaucracy aspects

Desire to create a composable solutions

- Reduce redundancy
- Costs
- Time to market

Leverage information used during the product development documentation

Create repeatable assurance method

- not dependent upon single tester

Optimize certification resources:

- completing SESIP certification months vs. years with CC

Scalable Evaluation = Stronger Supply-chain Evidence

SESIP Provides

Supports functional security interoperability

Across the whole development process

Give Security Assurance Levels (SESIP1–SESIP5)

Leverages

Existing Industry Definitions

- Security Assurance Levels (AVA_VAN) (ISO/IEC 15408)
- Security Functional Requirements

Leverages Profiles to enable specificity and comparability across classes of products

Automotive Benefits

Relevant for reusable certified components (e.g. ECUs, HSMs, SEs, TEEs, MCUs)

Reduced time-to-market and certification costs

Transparent, repeatable evidence-based assurance across supply chain

Alignment with Auto Standards

Simplified alignment with CSMS and type approval requirements

Means to deliver on ISO/SAE 21434 CAL/TAF objectives

Directly addresses V&V methods from ISO/SAE 8477 and Testing methods from SAE J3322

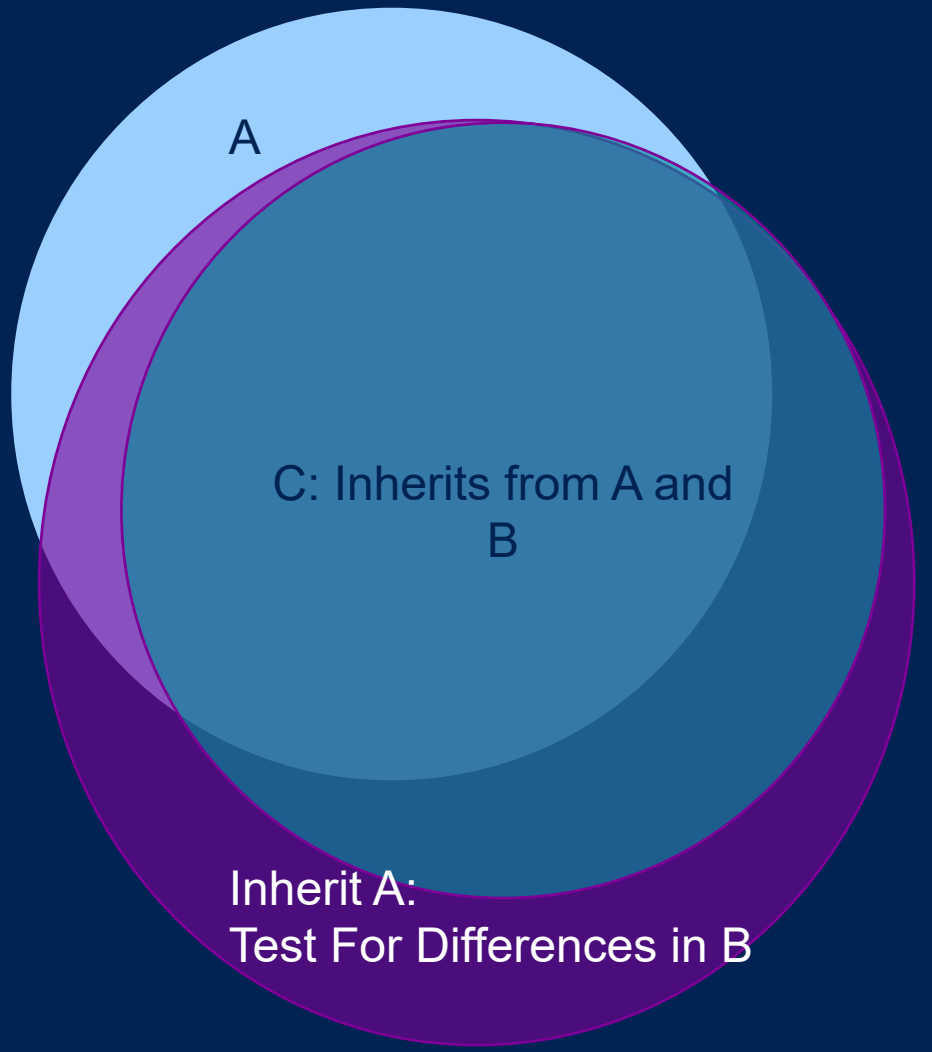
Certify Once & Reuse Many Times: SESIP Composition For Platforms And Devices

Composition Can be Done:

- Side to Side &
- Up and Down

Reuse Mechanisms

- Previously evaluated components reduce testing scope
- Certification evidence transferred to new evaluations
- Common security requirements catalogue enables consistency
- Mapping to vertical standards (ETSI, ISO/IEC, NIST)



Extending GlobalPlatform SESIP Ecosystem

Certification Bodies

TRUSTCB

SGS brightsight

2 potential new certification bodies under review

SESIP Industry Adoption

cen

CARCONNECTIVITY consortium

csa connectivity standards alliance

DTSec

GSMA

psacertified™

ETSI

qi

SESIP Labs

Applus+

BCTC 国家金融科技测评中心 National FinTech Evaluation Center 银行卡检测中心 Bank Card Test Center

brightsight By SGS

DEKRA

OPLS Lab

ESEC LABORATORY

INSTITUTE FOR INFORMATION INDUSTRY

KEYSIGHT

SERMA SAFETY & SECURITY

THALES

SESIP Regulatory Alignments

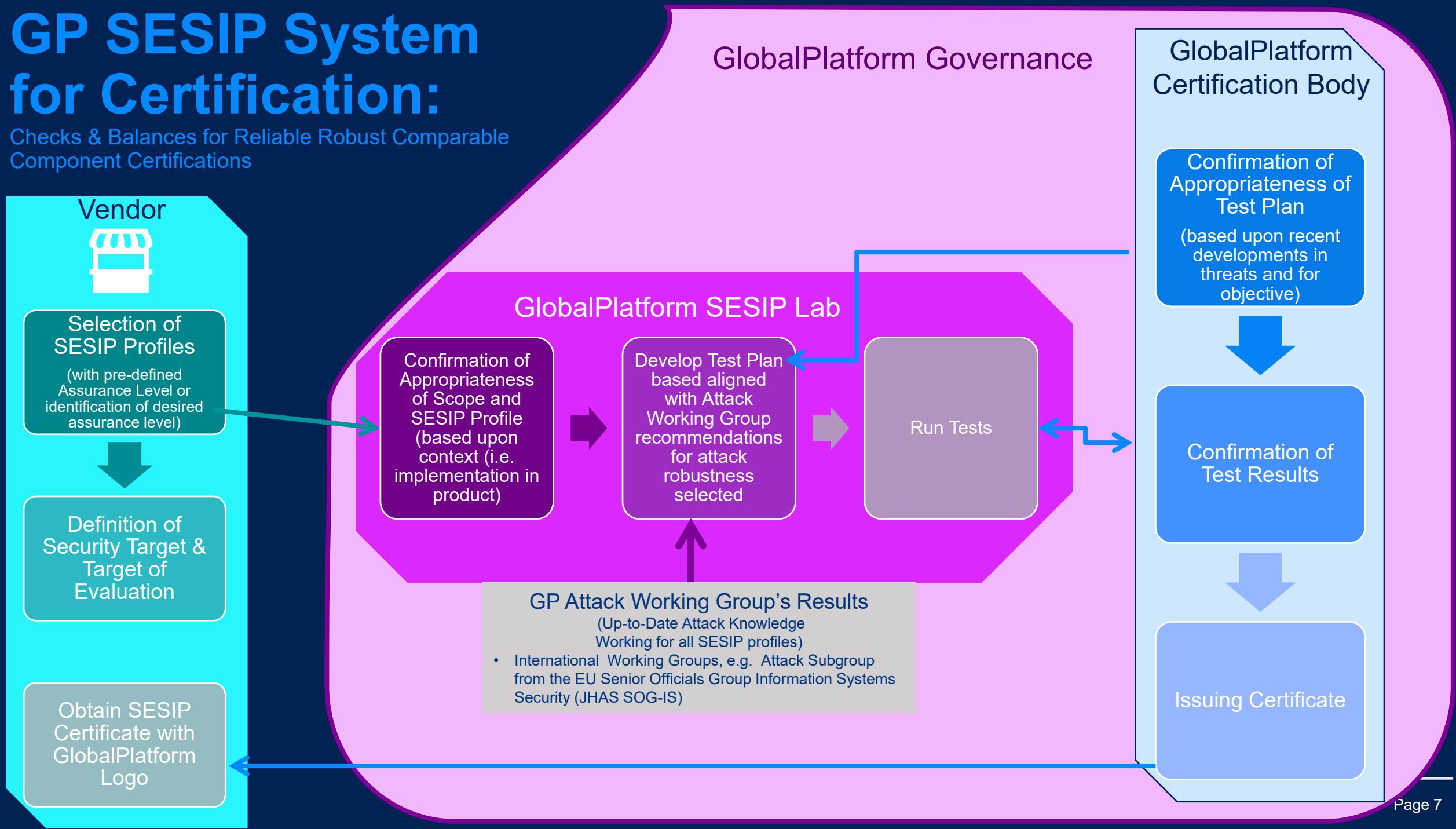
Cyber Resilience Act, US Cyber Trust Mark

Existing Industry Profiles

- Secure MCU/MPU
- Secure External Memories
- WPC Qi Secure Storage Subsystem
- Edge Compute Node
- Code Update Mechanism

GP SESIP System for Certification:

Checks & Balances for Reliable Robust Comparable Component Certifications

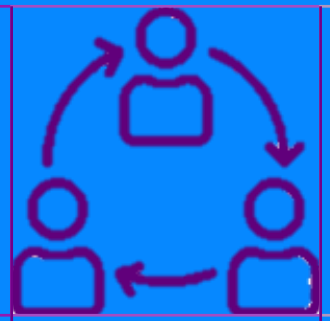


GlobalPlatform Oversight

Governance Roles

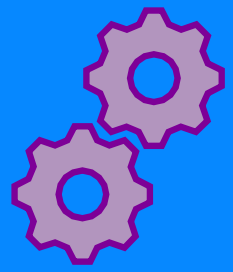
Defining and agreeing requirements of knowledge of labs and CBs to qualify

Supporting the implementation of the mutual recognition agreements between CBs



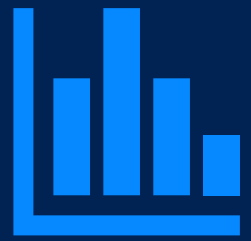
Keeping the Collaboration Effective

- Clarify the requirements for being a SESIP Lab
- Clarify the requirements for being a SESIP CB
- Maintain Collaboration Groups for Labs and CB
- Support Development & Implementation of Mutual Recognition Framework



Single Interface for Interpretation and Alignment on the Implementation of SESIP

SESIP Tools



Develop Guidelines for Methodology Usage

Development of Protection Profiles

Development of Mappings between SESIP, Regulations and Other Standards

Global Platform®

Security Target

ST Introduction

- Identifies the Target of Evaluation (TOE) e.g. an ECU, telematics unit, connected car platform
- Platform reference, functional overview and description

Security Objectives

- Operational Environment technical or procedural
- Inherited Objectives for the Operational Environment for composite paltforms that include platform parts under SESIP

Security Requirements and Implementation

- Assurance requirements (SESIP 1-5 Levels)
  - Flaw Reporting Procedure
  - Vulnerability Survey
- Functional requirements (SFRs) for
  - Verification of platform identity
  - Secure update of the platform
  - Eventual additional SFRs
    - a description of the implementation proposed in the platform
    - assessment manner for implementation appropriateness

Mapping and Sufficiency Rationals

- explains how the assurance requirements are addressed in the Security Target or planned to be addressed in the evaluation

SESIP Security Assurance Requirements (Source: Document Reference: GP_FST_070 v1.2)

Please note that the SESIP 4 & 5 Level definitions were first used for common criteria products and hence reference how to leverage these certificates. Currently, The SESIP Committee is updating the methodology and decisions on SESIP 4 & 5 levels for products that do not have already cc certificates is under assessment

SESIP 1 - Basic Assurance (Self-Assessment)

- Objective: Developer self-assessment with minimal evaluator verification
- Key Requirements: Simplified Security Target, compliance rationale, vulnerability survey, flaw reporting procedures
- Evaluator Role: Check consistency and clarity only - no independent SFR implementation verification
- Attack Resistance: Basic (0-15 rating)

SESIP 2 - Moderate Assurance (Black-box Testing)

- Objective: Black-box penetration testing without source code access
- Key Requirements: Complete functional specification, independent testing, vulnerability analysis
- Evaluator Role: Penetration testing with Basic attack potential
- Attack Resistance: Basic (0-15 rating)

SESIP 3 - Substantial Assurance (White-box Analysis)

- Objective: Source code analysis combined with penetration testing
- Key Requirements: Complete implementation mapping, configuration management, focused vulnerability analysis
- Evaluator Role: Source code review + penetration testing
- Attack Resistance: Enhanced-Basic (0-20 rating)

SESIP 4 - Extended-Substantial Assurance

Methodical vulnerability analysis + independent testing to demonstrate resistance against attackers with a moderate attack potential

Stronger evidence & lifecycle controls:

full functional spec + implementation representation, plus dev environment controls, tooling definition, secure delivery, and site security procedures.

- Attack Resistance: Moderate (0-24 rating)

SESIP 5 - High Assurance

- Advanced methodical vulnerability analysis + independent testing to demonstrate resistance against attackers with a high attack potential

Highest rigor assurance intent: aligned to high-assurance components (e.g., secure elements)

Stronger lifecycle/CM expectations at this level (e.g., production support/automation, problem tracking CM coverage, sufficiency of security measures)

- Attack Resistance: High (0-30 rating)

Currently the SESIP Levels considered most relevant for Automotive Applications

Security Functional Requirements for Connected Platforms: Catalogue of 34 in 8 Categories

- **Platform Optimized**: Each SFR covers complete security purpose for Connected Platforms
- **Accessible**: Readable by security developers without evaluation expertise
- **Composable**: Supports reuse across different platform evaluations
- **Extensible**: Allows platform-specific SFRs when needed

Mandatory SFRs

Verification of Platform Identity (all platforms)

Secure Update of Platform (unless justified why updates not applicable)

Identity & Attestation (7 SFRs)

Platform identity verification and attestation

Application genuineness and state attestation

Secure boot and initialization

Life Cycle Management (7 SFRs)

Secure install/update/uninstall of platform and applications

Factory reset, decommission, field return

Anti-rollback SESIP

Secure Communication (2 SFRs)

Secure channel support with specified protocols

Enforcement of secure communication usage

Attacker Resistance (5 SFRs)

Physical attack resistance (limited and comprehensive)

Software isolation (platform, platform parts, application parts)

Cryptographic Functions (4 SFRs)

Standard crypto operations, key generation, secure key storage

Cryptographically secure random number generation

Compliance Features (11 SFRs)

Storage: Trusted, confidential, encrypted storage; data serialization

Data SESIP: Residual information purging, audit logs, reliable indexing

Operations: Secure debugging, recovery, backup/restore

Generic: Custom security features

Access Control (2 SFRs)

Privileged access control (context-based)

Authenticated access control (role-based)

Availability (2 SFRs)

Resource constraint management

Denial-of-service SESIP

Profiles Make Security Requirements Comparable

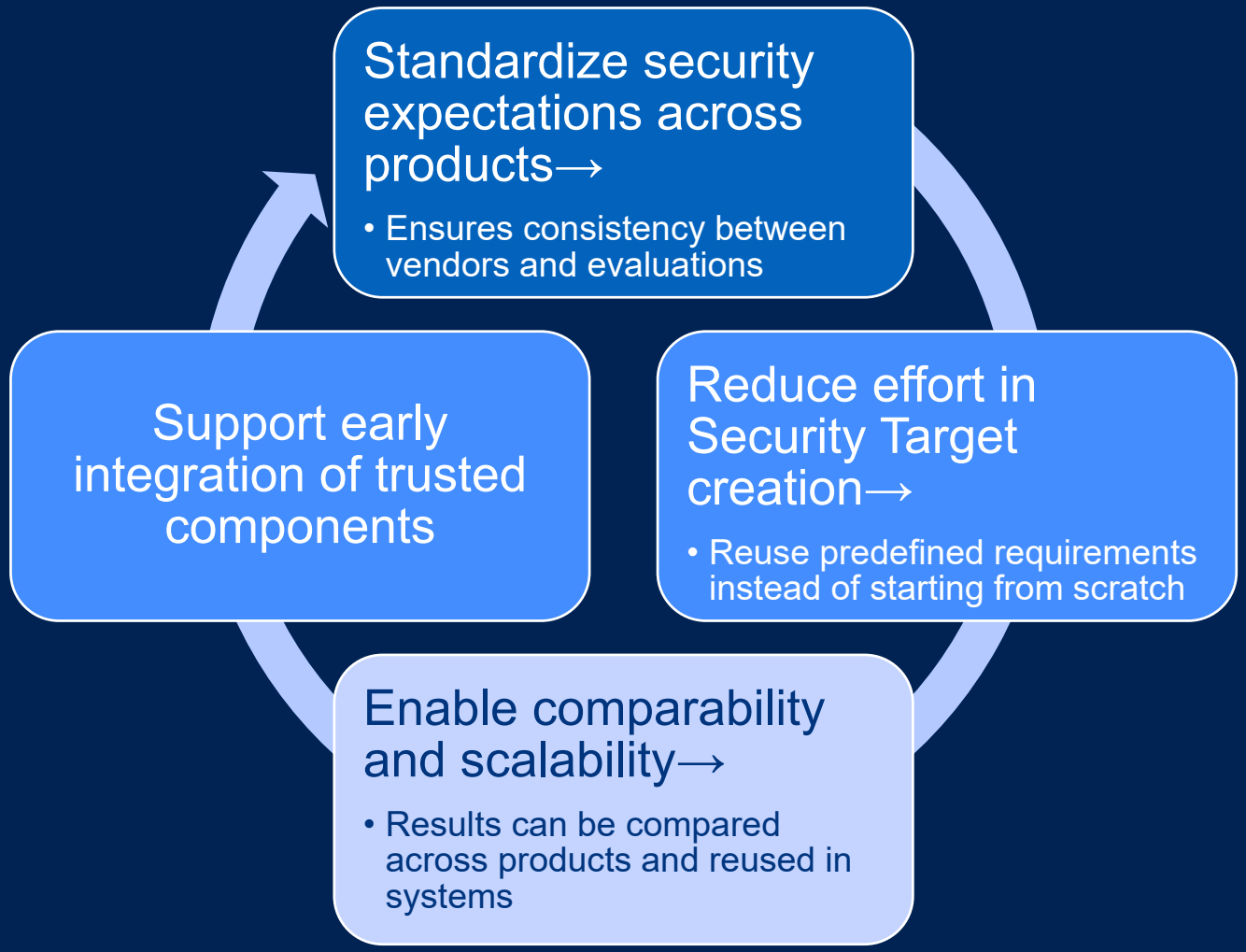
What is a SESIP Profile?

A predefined set of Security Requirements

Tailored for a specific type of platform or component

Defines expected security capabilities and assurance level

Why is it Useful?



What does a SESIP Profile Contain?

- Scope of Evaluation
- Security Functional Requirements
- SESIP Assurance levels (1-5)
- Assumptions and Environment
- May include detail on testing methods
  - Functional testing →
  - Vulnerability analysis →
  - Fuzzing →
  - Penetration testing →

GlobalPlatform Process for Profile Development

GP Member Editor / Champion of SESIP Profile works with Automotive SESIP WG committee members to define common requirements

SESIP Committee

- Works internally on agreeing contents of:
  - Scope of certification
- Coordinates with eventual external parties
- SESIP Committee formally approves SESIP Profile
- Language English

Final Publication of Profile in GP's SESIP official repository

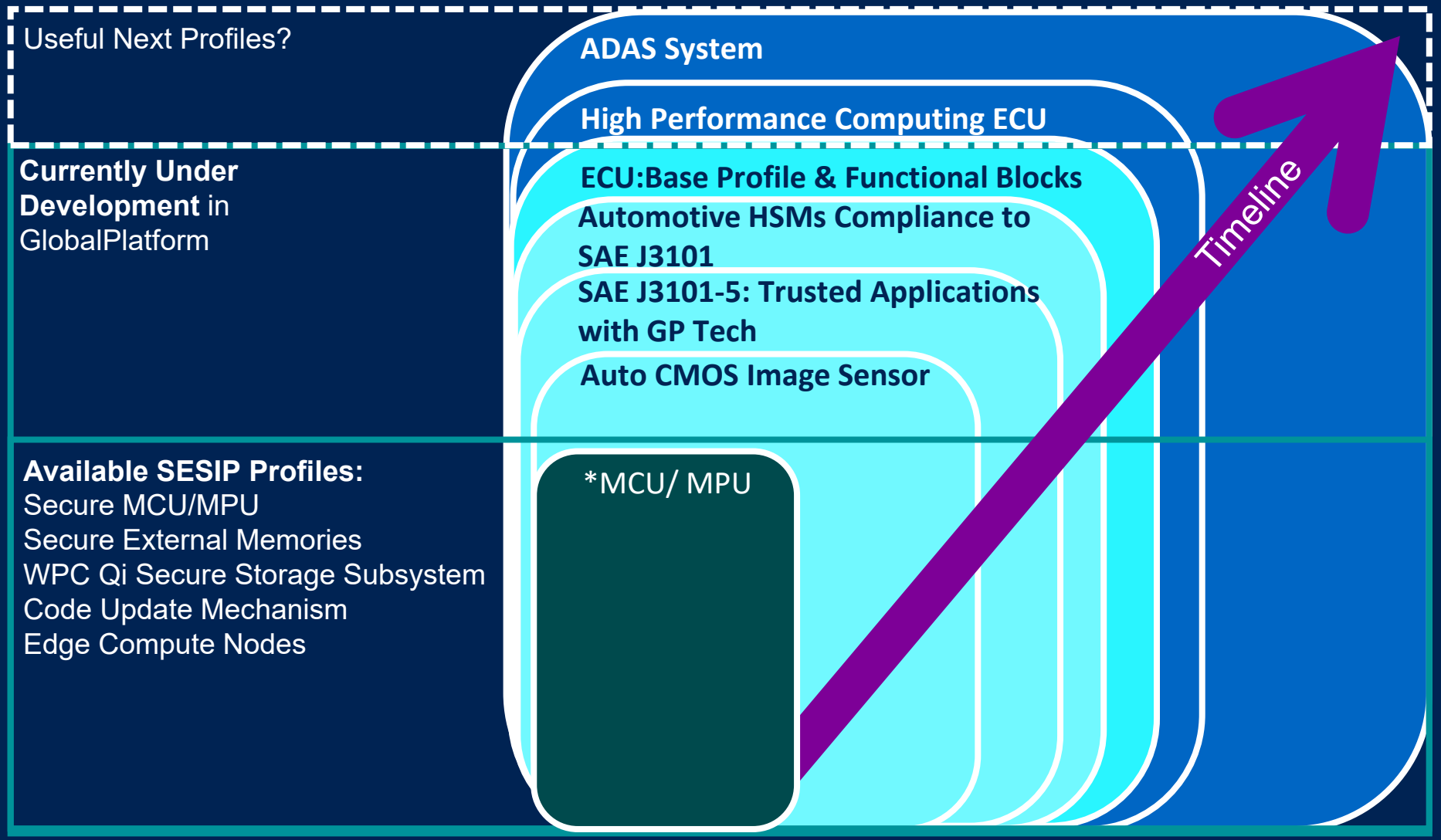
Ongoing Maintenance

- Monitor
- Update based upon expiration date

Global Platform®

Work in Progress for SESIP in Automotive

SESIP Automotive Profiles Roadmap: Reusable Building Blocks for Automotive

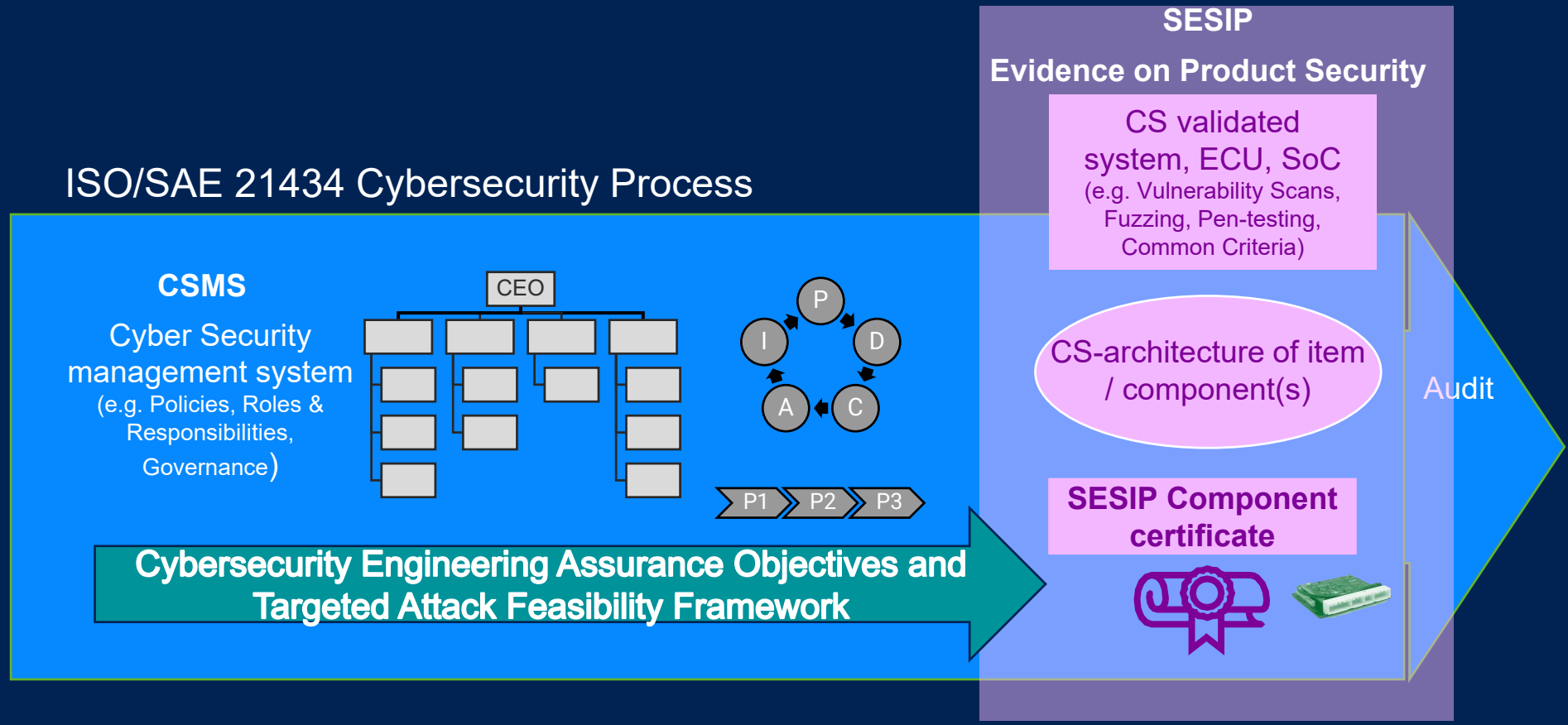


Modular Composable

Status of GlobalPlatform Automotive SESIP Profiles

SAE J3101-5 PP	J3101 Baseline SESIP Profile	Auto CMOS Image Sensor Profile	Baseline Profile for ECUs
Trusted Application Aspects levering TEE & SE	Proprietary HSM Evaluation of Compliance for J3101	Current Status: 2nd Draft Published (April 17th) in Auto WG	Current Status: 1st Draft - Comments period
Current status: Soon to be in Public Review	Current Status: Pending Initial Draft (June ?)	Final Publication: Q4 or Q1 2027	Final Publication: Q1 2027?
Final Publication: Q3 2026?	Final Publication: Q3 / Q4 2026?		

SESIP for Product Level Security Supporting ISO/SAE 21434 Compliance Process



- CS assessment (of 21434 Work Products)
- Post-dev. Report

SESIP Turns CAL Rigor Into Component Evidence

TARA as part of the ISO/SAE 21434:
Cybersecurity Management System Process

TARA inputs → Impact rating → Attack feasibility rating → CAL Determination → Cybersecurity Case

Cybersecurity Assurance Levels:
Rigor of cybersecurity activities (breadth, depth) to achieve engineering ASSURANCE

SESIP:
Assurance Evaluation and Certification Products

SESIP Profile → Product Evaluation Evidence

Method to demonstrate Assurance Levels in Components

- *Final assurance results in product (result of CAL process)*
- *Targeted Attack Feasibility has been Reached*

Why use SESIP together with CAL & TAF Efforts?

COMPARABILITY across components during procurement:

- Ease vendor selection
- Objective evidence to back-up choices made
- Provide artefacts of best-practice decisions (in line with UNECE 155/156)

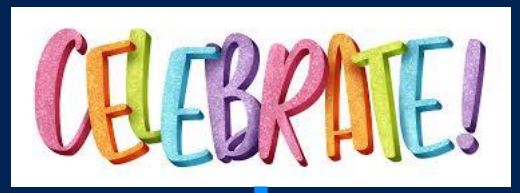
Early INTEGRATION of certified components in development process :

- Cost Benefits: Reduction in Non-Recurring Engineering Costs
- Time to Market: Able to fix problems earlier in the V model

Reduce overall Verification and Validation COSTS with certified components

- Technical Assistance centers recognize validity of certification in scoping their V&V activities (so less V&V on certified components)
- Achieve depreciation of Certification Costs across the Supply Chain (everyone does their own part and for multiple customers)

SAE & GlobalPlatform Moving Forward



Potential Future Areas for Cooperation between GP and SAE

SESIP: Tool Supporting CAL?

- GP & **SAE Vehicle Cybersecurity Systems Engineering Committee**

Decision to Create SAE WIP

- **Vehicle Cybersecurity Systems Engineering Committee**
- **SAE Vehicle Electrical System Security Committee**

Admin opening of SAE 3600 WIP

- Come Join Us!
- Will be held on alternating Wednesday's 9:00-11:00 in **SAE Vehicle Electrical Hardware Security Task Force**

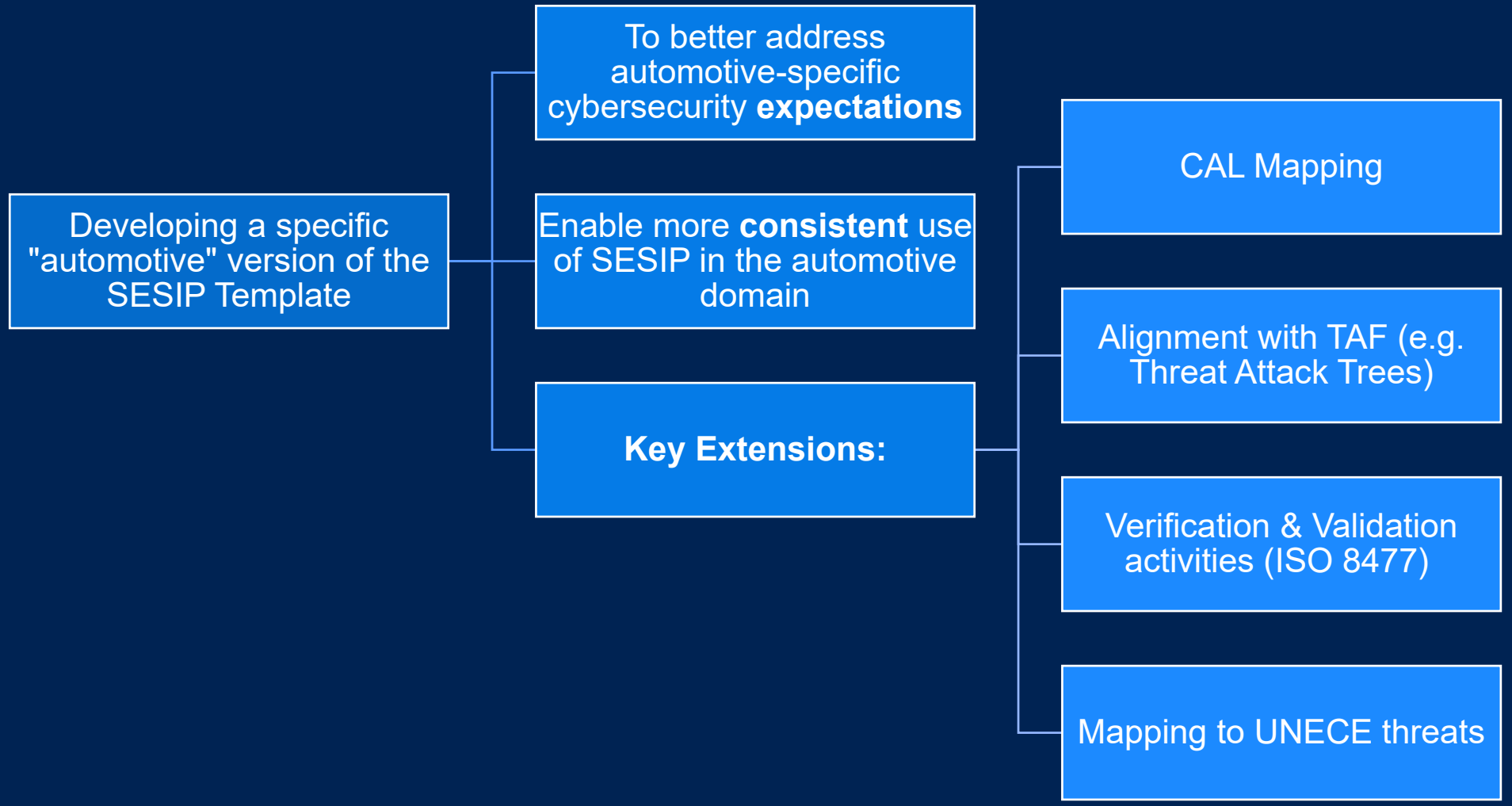
SAE to develop based upon LS from GP:

- Informative / Recommendation on SESIP for ISO/SAE 21434 which contains the alignment between SESIP and CAL Levels

SAE Task Force to provide input to GP

- Clarifying / Agreeing Common Requirements for SESIP Profiles
- SAE to suggest Priority Profiles to develop
- SAE to review draft GP SESIP Auto Profiles
- Others?

New Work Areas SESIP AUTO WG



Extending SESIP for Automotive?

Under Discussion

Introduction	Platform Component Functional Overview	Security Objectives for the Operational Environment	Security Requirements & Implementation	Mapping and Sufficiency Rationales
SESIP Profile Reference	Platform type, Architecture, Components	Platform Objectives	Assurance Requirements	For each identified security threats and objectives.
Platform Type	Functionality	Inherited Objectives (composition evaluation)	Security Functional Requirements	Demonstrates compliance with SESIP standards
Security Targets Claimed	Intended use cases		Secure Processing Package	Ensures assessment of platform's security posture
CAL Mapping Reference?	Security boundaries			Implications from CAL Level?
	Lifecycle			
	Pre-existing certifications or compliance efforts			

Annex:
UNECE 155/156 Threats, Mitigations
Threat Attack Tree

Key Takeaways

Standardization is essential for scalable cybersecurity certification

- Without it, results are not comparable or reusable

ISO/SAE 21434 defines risks and requirements, but not measurable assurance

- Requires a structured evaluation framework

SESIP transforms requirements into testable and certifiable security claims

- SFRs (what) + SARs (how) + Levels (confidence)

SESIP Profiles enable reuse and consistency across the automotive supply chain

- Same requirements, same evaluation, same expectations

SESIP enables component-level assurance for secure composition

- Avoids costly late-stage fixes by addressing vulnerabilities early in the lifecycle

Global Platform®

→globalplatform.org

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