

SESIP Certification:

A means to generate artefacts for
UNECE 155 & ISO 21434 compliance

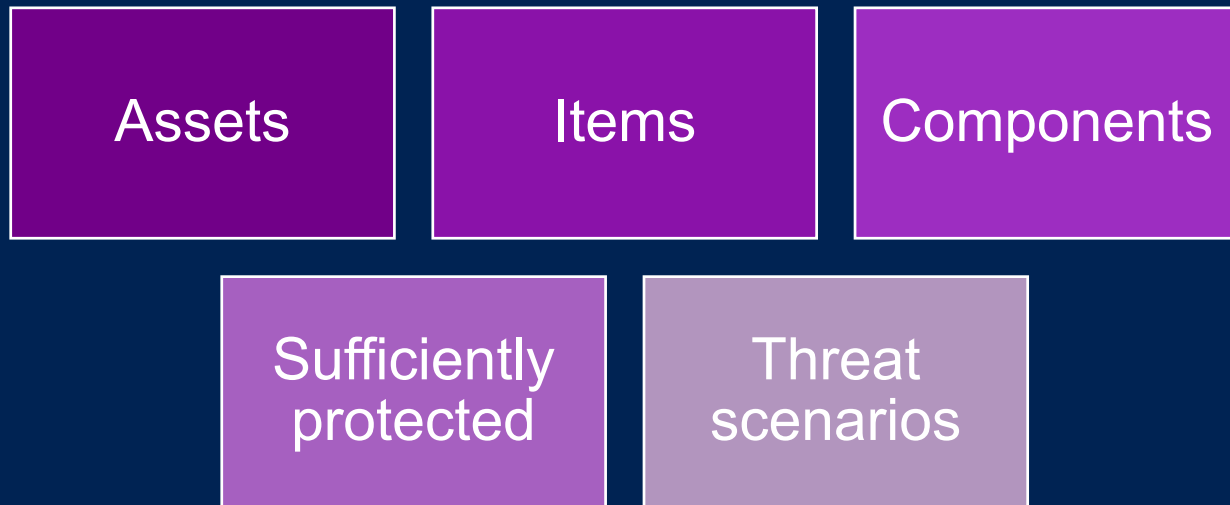
Jorge Wallace Ruiz

4 December 20224

Cybersecurity (ISO 21434)

Cybersecurity: the condition in which ASSETS are SUFFICIENTLY PROTECTED against THREAT SCENARIOS to ITEMS of road vehicles, their functions and their electrical or electronic COMPONENTS.

Relevant definitions



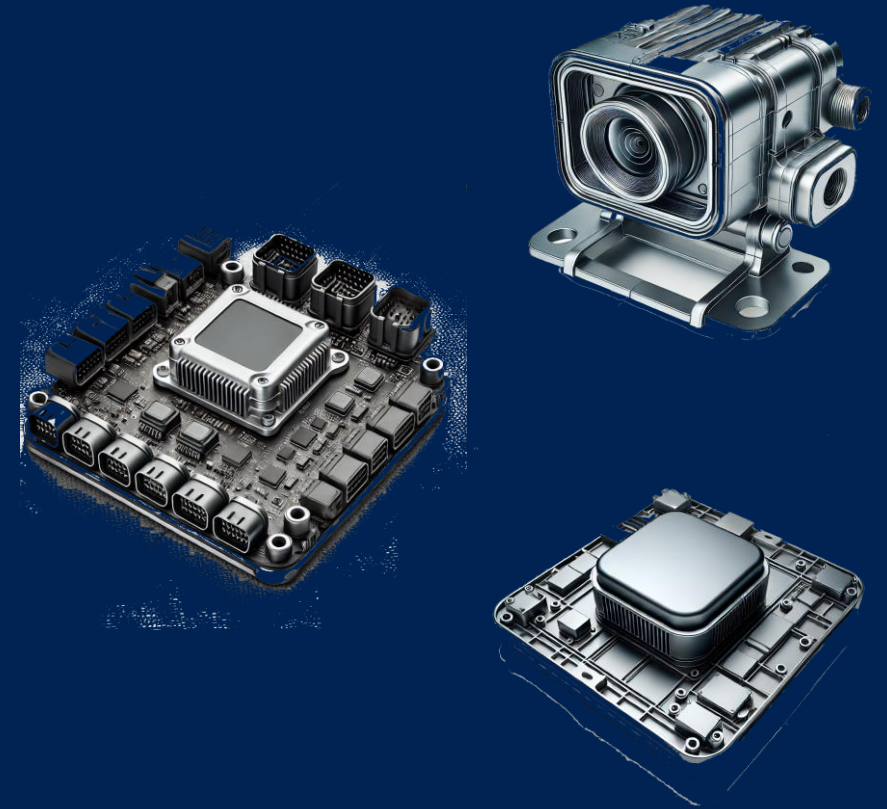
ADAS System

Item – ADAS system

Components –
Radar sensor,
camera systems,
ECUs...

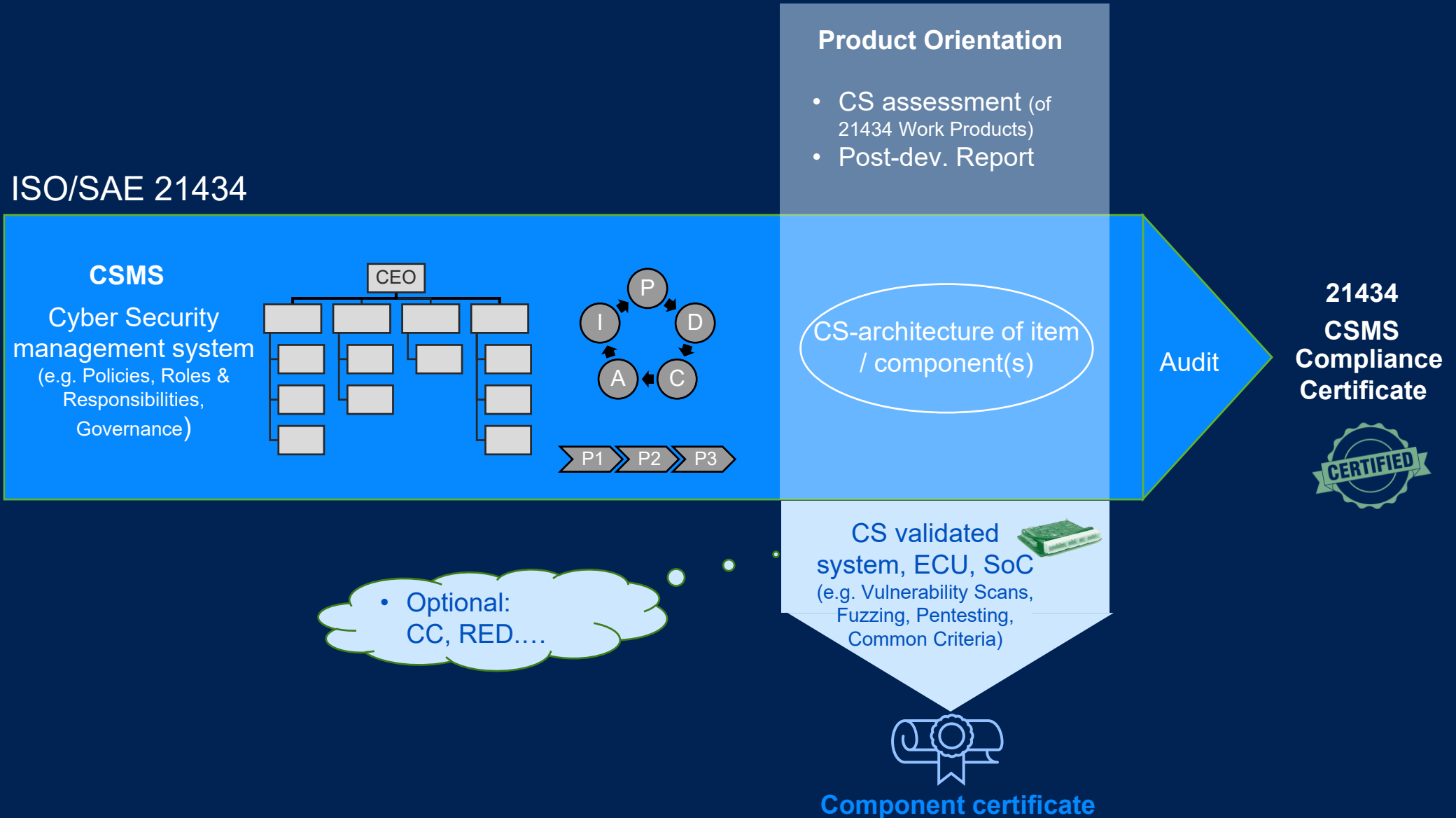
Assets – Radar
sensor data, camera
data,
communication
channels

Threat scenarios –
Radar sensor
spoofing, camera
system tampering,
ECU communication
interception

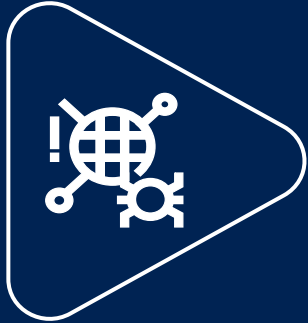


Certification Framework

ISO/SAE 21434



Cybersecurity Relevant Testing Methods



Vulnerability scanning

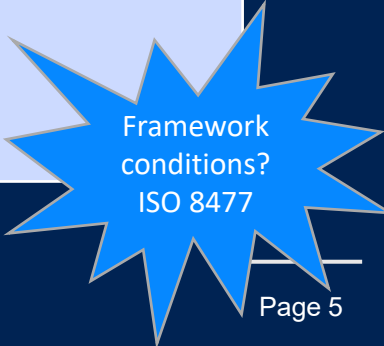


Fuzz Testing



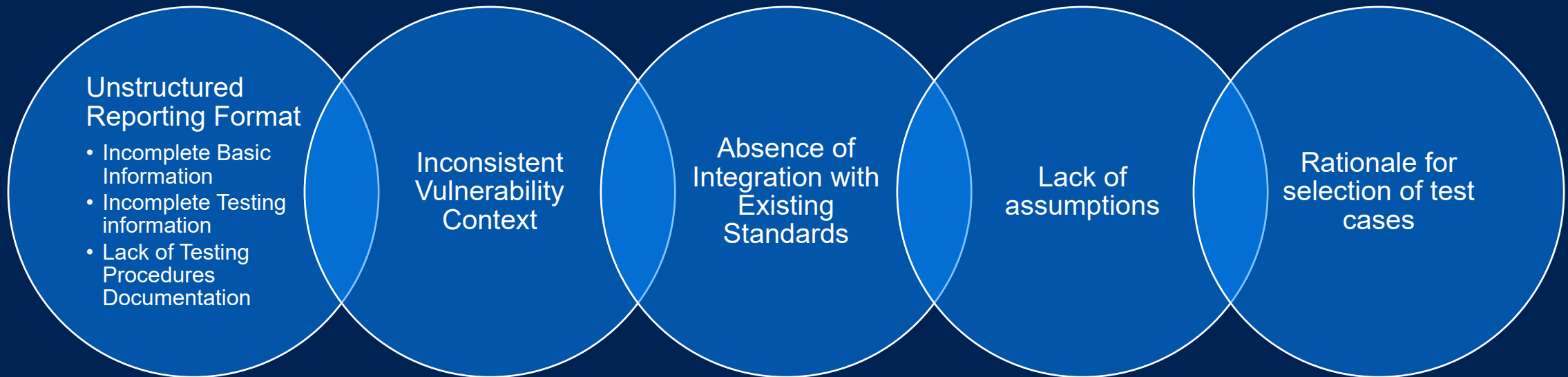
Penetration Testing

General evaluation of the level of security – performed continuously	Can be performed relatively early in the validation phase	Component and system level testing
<ul style="list-style-type: none"> ▪ Identification of known vulnerabilities in different components <ul style="list-style-type: none"> ▪ Software components ▪ Hardware components ▪ Vulnerability scanning <ul style="list-style-type: none"> ▪ BOM based ▪ Network scanning tools ▪ Software Composition Analysis 	<ul style="list-style-type: none"> ▪ Fuzz testing is an “automated” software testing technique ▪ Massive amounts of “random” data, called fuzz, to crash or break the system ▪ Find “software” bugs in code ▪ Exploits systems vulnerabilities, so it can be fixed in due time 	<ul style="list-style-type: none"> ▪ Penetration testing is a form of ethical hacking to find vulnerabilities ▪ Pen-testing can also be referred to as a simulated cyber attack. ▪ Find vulnerabilities

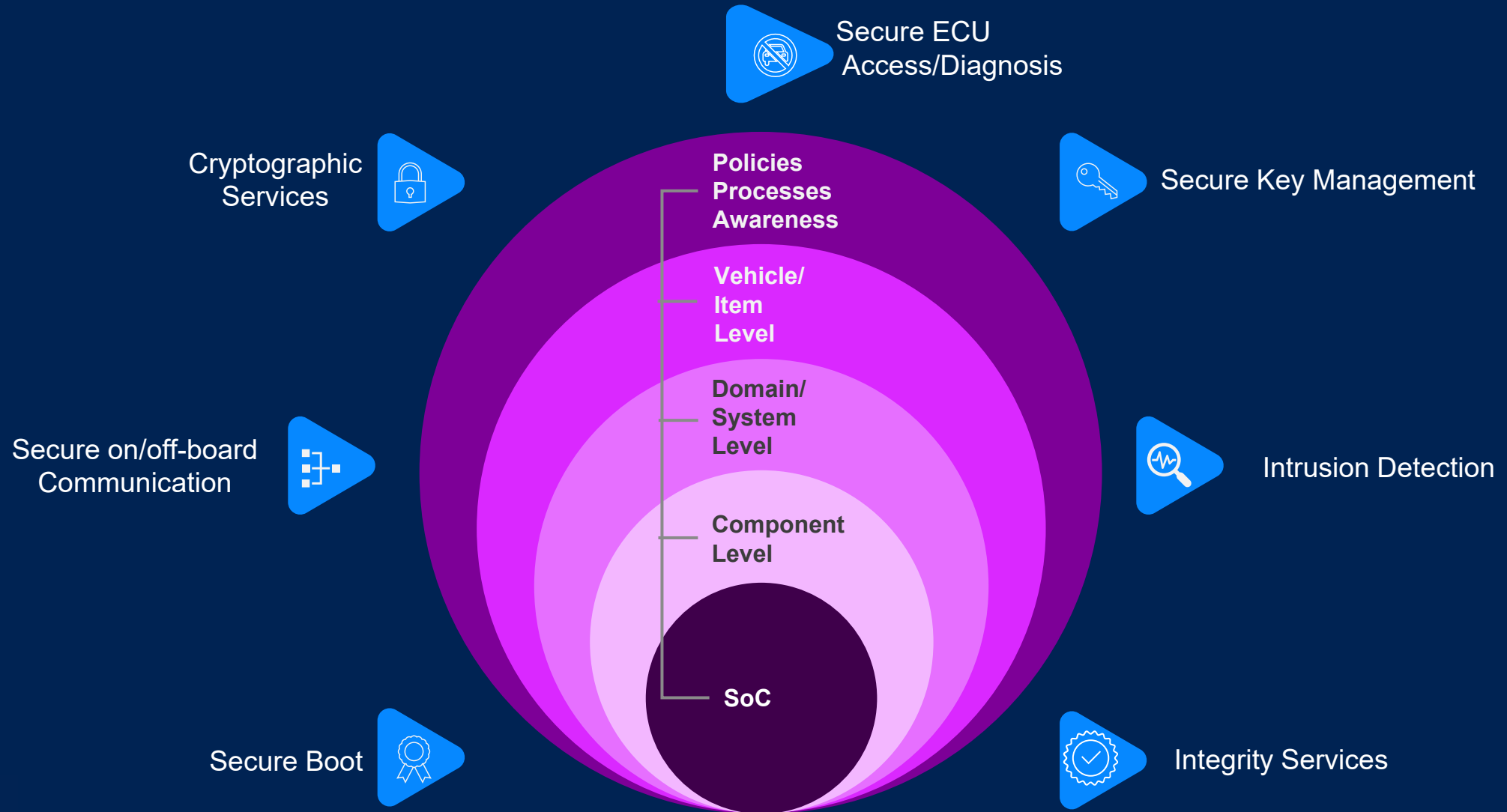


ISO/SAE 21434 Testing Method Challenges: Cybersecurity Evaluations

Reports rejected by OEMs and/or Technical Services



Cybersecurity Layered Approach



Potential Approach for Security Evaluations

Certification scheme for components

Covering ISO 21434 Testing Methods

- Functional testing (*)
- Vulnerability scanning
- Fuzz testing
- Penetration testing

Risk based approach

- Aligned with CALs (*)

Layered approach

- Component
- Item
- Vehicle

CSMS Activities Review (?)

- Working Packages Review
- Processes and procedures

Base Protection Profile

Assumptions

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

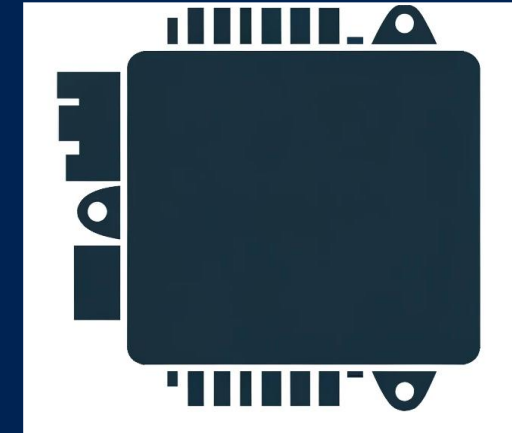
SoC Characteristics

- Secure Boot based on HW Root of Trust
- Supported TEE
- ...

Challenges

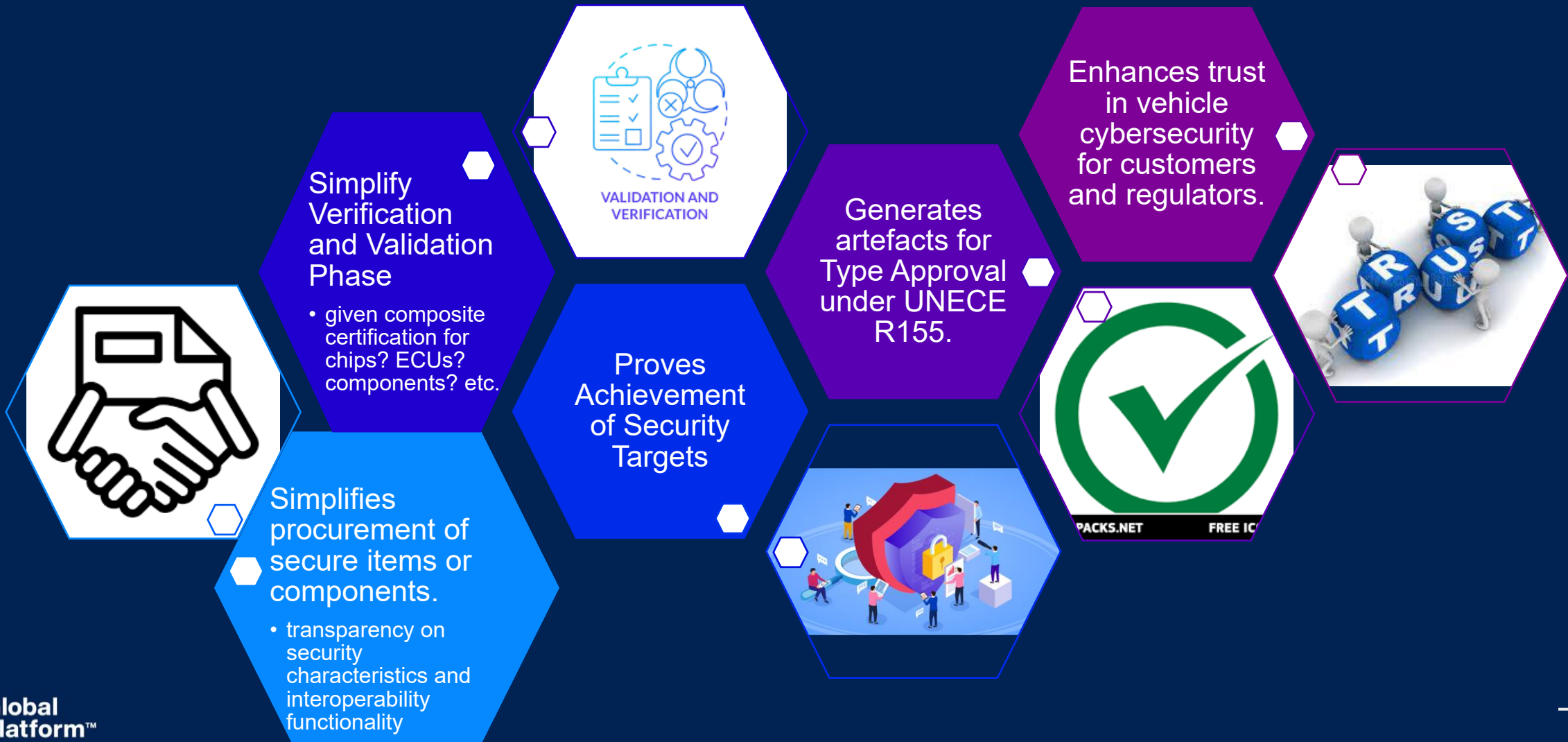
- ISO 21434 vs SESIP / CC
- Certification updates (ISO 24089 ?)

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

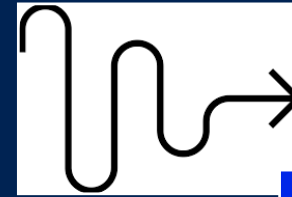
SESIP Certification Benefits: OEMs



SESIP Certification Benefits: Tier 1 & 2s



Transparency on security targets achieved



Streamlines collaboration with OEMs through reusable 3rd party certifications

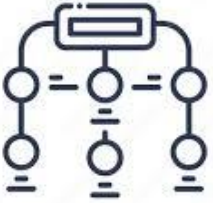

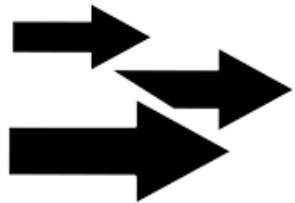


Reduces duplication in testing and evaluation.



Demonstrates compliance with global standards

SESIP Certification Benefits: For Regulators and Certification Bodies

 <p>Framework ICON</p>		
<p>Provides a consistent framework for evaluating security of products (not just processes)</p>	<p>Verifies comparability of security levels</p>	<p>Accelerates compliance assessments and approvals</p> <ul style="list-style-type: none">• Leveraging known standards and methodology speeds up the review and approvals



SESIP: SAE HPSE

J3101 Protection Profile?

SAE J3101: Application-Level Protection Profile

Scope

Clearly define :

- scope of the protection profile to cover application-specific requirements
- Those not met by current hardware or platform-level protection profiles (e.g., TEE or SE).

Ensure the profile addresses both:

- mandatory and
- optional application-layer requirements

Challenges

- Application nature (boundaries, granularity, ...)
- Lifecycle management
- Composition
- Self test vs Crypto validation



Questions?

Open discussion



Global Platform™

The standard for
secure digital services
and devices

→ globalplatform.org

SAE J3101: Current gaps (I)

Requirement	Condition	Description	SE	SE Mapping	TEE	TEE Mapping
REQ_6.2.3.1_10	Mandatory	The hardware protected security environment shall support digital certificates if public keys (asymmetric cryptography) are employed. The digital certificates should be X.509 or IEEE 1609.2 compatible formats.	Partial	X.509 is supported. IEEE 1609.2 is supported through an Application / Configuration.	Partial	X.509 is supported. IEEE 1609.2 is supported through An Application/ Configuration
REQ_6.2.3.2.3_50	Optional	The hardware protected security environment shall support a defined lifetime and a means of rekeying for symmetric keys	Partial	to be managed on a per applet level.	Partial	Supported through an Application (TA)/Configuration.
REQ_6.2.3.4.1_20	Mandatory	The hardware protected security environment, if a keystore is specified to manage keys from multiple owners (either end product owners or supply chain entities), shall check the authorization of any entity which requests to install or invalidate a key within the keystore as a part of the requesting transaction.	Partial	Yes, if owners are internal managed by the platform. to be managed on a per applet level for external owners	Partial	Supported through an Application (TA)/Configuration.
REQ_6.2.3.4.3_10	Mandatory	The hardware protected security environment shall verify usage or validity rules (e.g., validity periods, geo-fence constraints, frequency of use, etc.) as required by internal or external applications according to the key management plan.	Partial	To be managed on a per applet level for external owners	Partial	Supported through an Application (TA)/Configuration.
REQ_6.2.3.5_10	Mandatory	The hardware protected security environment shall manage the validity of all keys according to policies established in the hardware protected security environment's key management plan.	Partial	Supported through an Application policy via the GP SE API	Partial	Supported through an application (TA) along with the TEE Core API.

SAE J3101: Current gaps (II)

Requirement	Condition	Description	SE	SE Mapping	TEE	TEE Mapping
REQ_6.2.3.7_120	Mandatory	If the hardware protected security environment requires a common time as an input as a pre-condition to the security of any key management operation, the authenticity of the time signal and the authorization of its source must be confirmed within the hardware protected security environment before it is valid for use	Partial	Supported through an Application or a Configuration.	Partial	Supported through an Application (TA)/Configuration
REQ_6.2.3.7.1_60	Mandatory	If the hardware protected security environment performs key derivation and supports a policy restricting the number of updates (derivations) that may be performed with a key without rekeying, then the hardware protected security environment shall track and associate the number of updates with the key.	Partial	Supported through an Application or a Configuration.	Partial	Supported through an Application (TA)/Configuration
REQ_6.2.3.7.3_10	Mandatory	While this document does not mandate allowed key agreement protocols, the hardware protected security environment shall employ authentication in all supported key agreement protocols.	YES	Supported through an SE Secure Channel Communication – Secure Channel Protocols	Partial	Supported through an Application (TA)/Configuration.
REQ_6.2.3.7.4_30	Mandatory	The hardware protected security environment shall support update of key derivation algorithms during the lifetime of the hardware protected security environment, unless the product is stated to be of limited use (see 7.6).	Partial	Yes, if present in the product Or with OS update or new application	Partial	Yes, if present in the product Or with OS update or new application