Application of **Common Criteria** in **Cooperative Intelligent Transportation Systems**

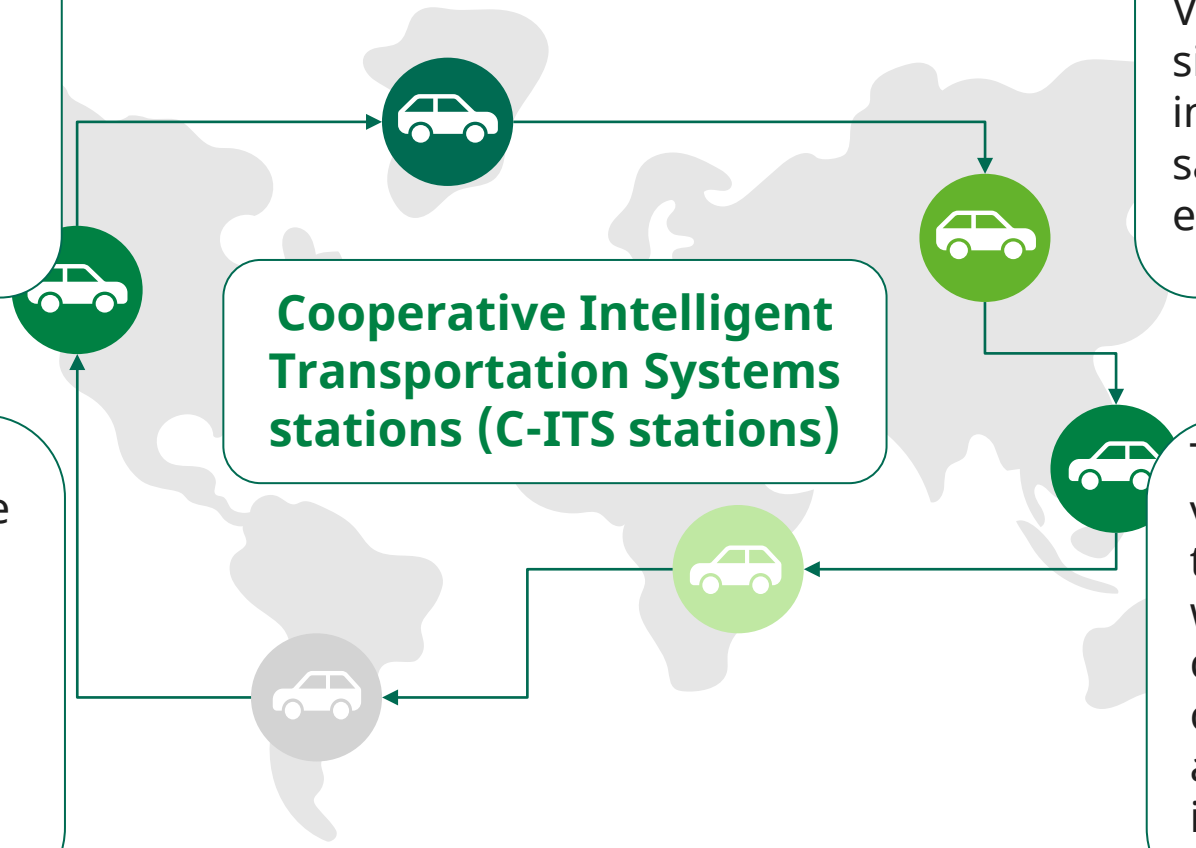
ICCC 2023
NOVEMBER 2023
Washington DC, US

Background

Transportation

Transportation plays a crucial role in our daily routines. There were **1.446 billion vehicles** on Earth in 2022 mainly distributed between Europe, America and Asia.

Vehicles on the road poses significant **challenges**, including traffic congestion, safety concerns, and environmental issues.



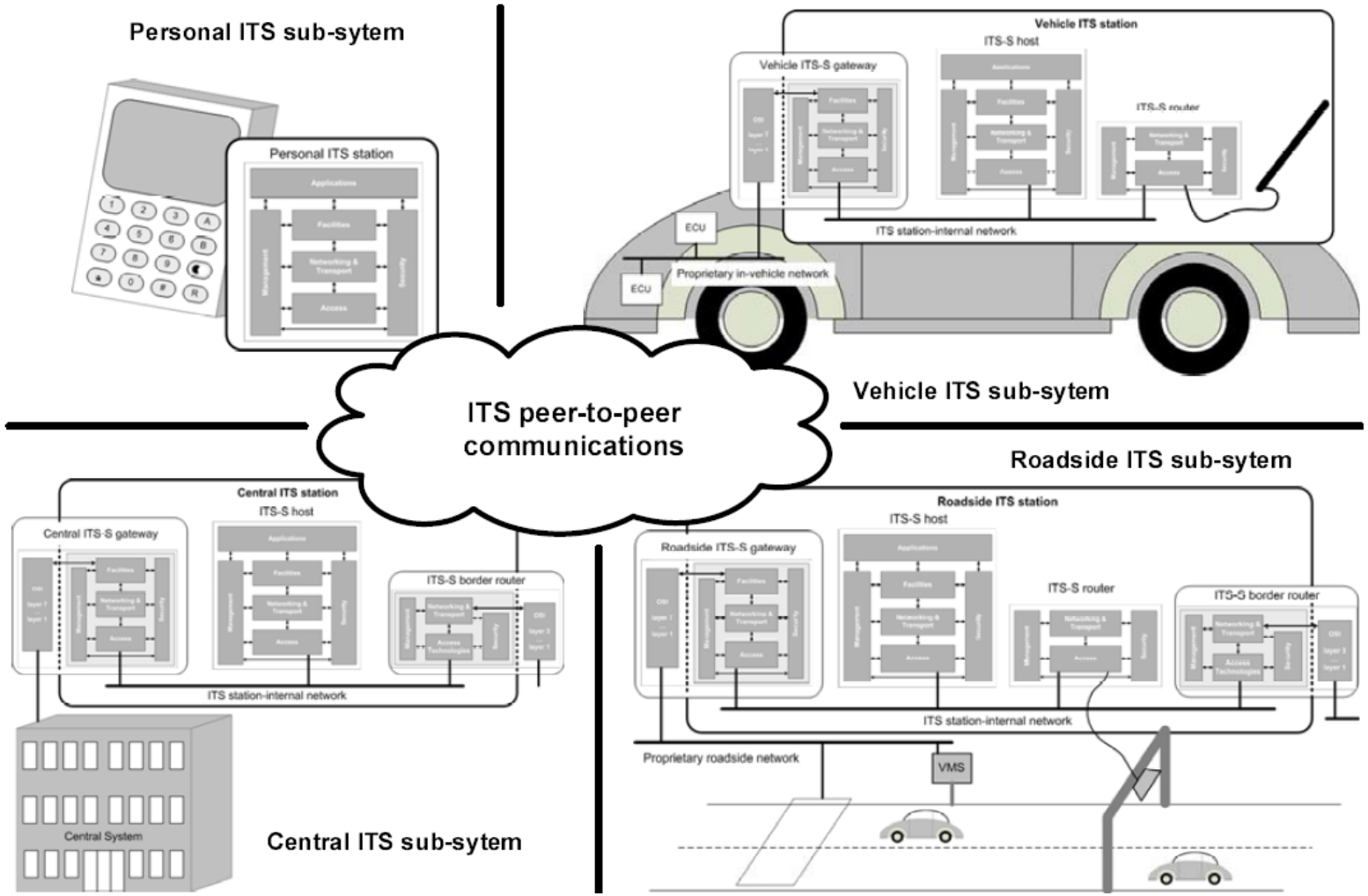
Cooperative Intelligent Transportation Systems stations (C-ITS stations)

Intelligent Transportation Systems (ITS) aim to provide services related to different modes of transport and traffic management, enable users to be better informed and make secure, more coordinated, and 'smarter' use of transport networks.

The emphasis in intelligent vehicle research has turned to **Cooperative ITS (C-ITS)** in which the vehicles communicate with each other, with pedestrians and/or with the infrastructure through **C-ITS stations.**

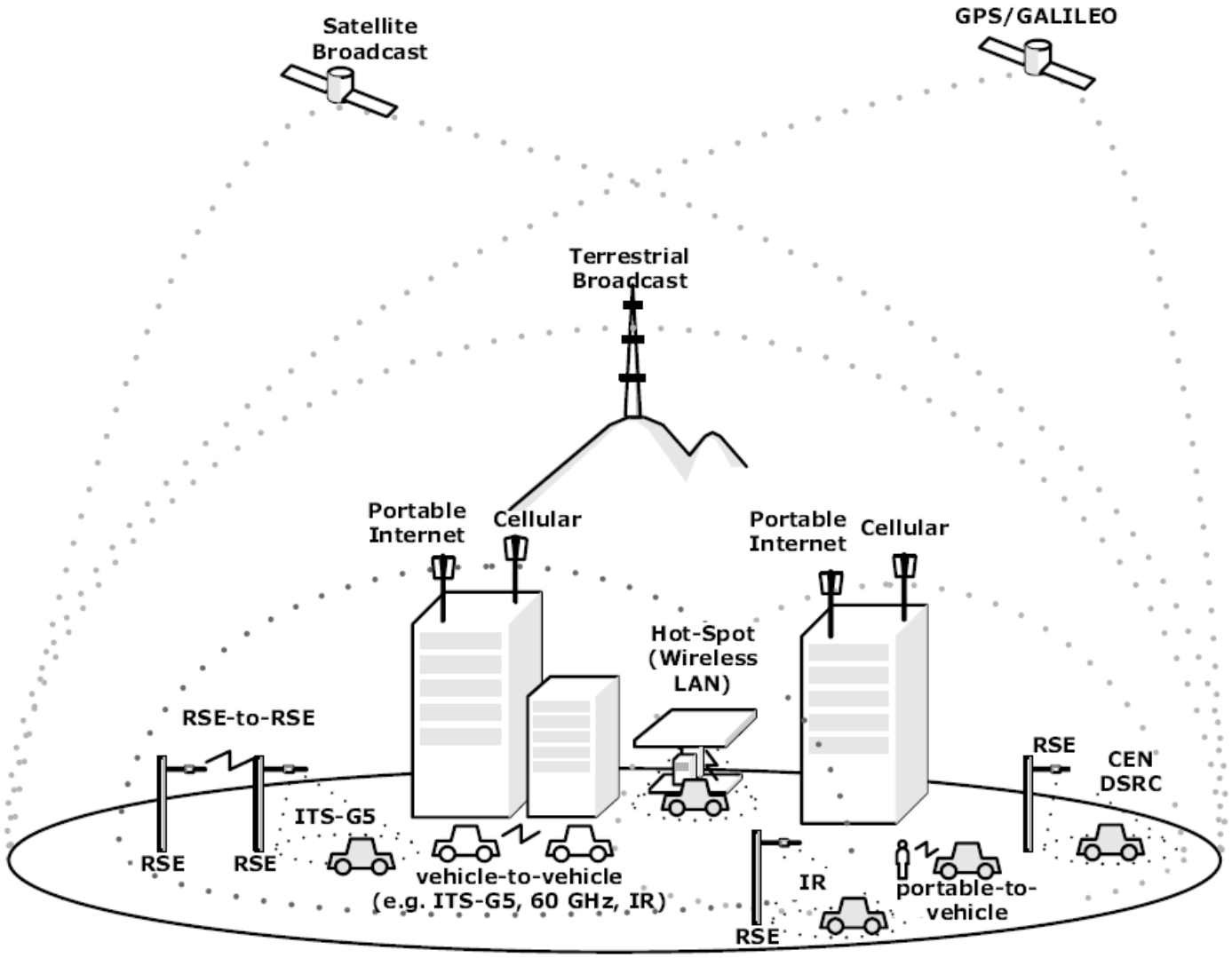
C-ITS Stations

ETSI 302 665



C-ITS Stations

ETSI 302 665



C-ITS Stations

Concerns

C-ITS introduces new potential threats and vulnerabilities that need to be addressed by adequate **security measures**.

One of the challenges to secure C-ITS will be the determination of the level of assurance required to demonstrate compliance with those requirements and the justification of the need to use an independent 3rd party that provides this assurance.

The most appropriate method for demonstrating that a product meets technical specifications would be to conduct an **evaluation by an accredited independent third party.**

CPOC Protocol

European Union C-ITS Security Credential Management System (EU CCMS)

European Commission is focus on the design and the implementation of a *European Union C-ITS Security Credential Management System (EU CCMS)*

Such goal is achieved through the **C-ITS Point of Contact of the European Commission (CPOC)** and portrayed in its protocol *"Description of the CPOC protocol in the EU C-ITS Security Credential Management System CPOC protocol"*

CPOC protocol is going to support the deployment of C-ITS systems and technologies in Europe. In order to create the European Certificate Trust List (ECTL), there **are three scenarios associated with three levels (L0, L1, L2)**

Preliminary testing of C-ITS stations

C-ITS stations which are **not** fully compliant yet, in a ramp-up phase of C-ITS deployment in the EU CCMS

C-ITS stations **fully** compliant in a full productive environment

CPOC Protocol

C-ITS Stations, CC Certification

No evaluation is required.

An evaluation of the C-ITS station shall be performed by a SOG-IS recognized test lab.

The test lab shall evaluate that the C-ITS station is protected against an attacker **with basic attack potential**.

Security certificates for C-ITS stations shall be **issued under the common criteria** certification scheme.

Only as long as C-ITS station protection profiles certified against ‘common criteria’ / ISO 15408 are **not yet available**, C-ITS station operators shall be allowed to have their C-ITS stations assessed and certified against a security target with a similar or higher evaluation assurance level **(EAL 2+ or higher)**

Challenges

- End-users
- Updates
- Specialized tools and teams
- Testing platform
- Tiers/developers
- Automotive regulations
- Certificates/PKI
- **Assurance level**

Challenges

C-ITS Station, CC Certification

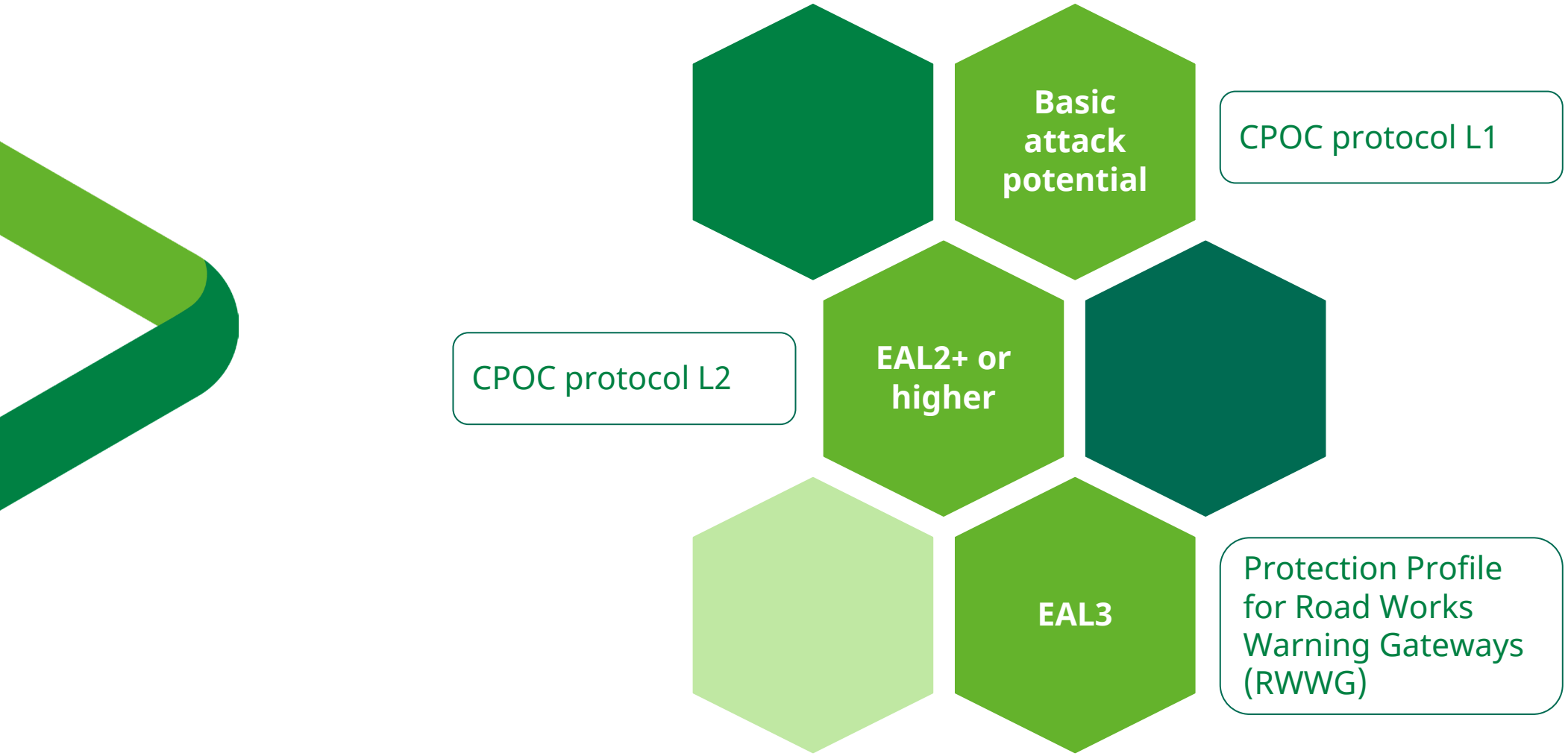
In the development of such protection profiles, the scope of the security certification of the C-ITS station may be defined by the manufacturer, subject to assessment and approval of the CPA and SOG-IS conformity assessment body.

The goal of the presentation is to discuss:

- The open window regarding the minimal assurance level that the C-ITs station shall meet in L2 in the absence of protection profiles.
- The assurance level considered by **DEKRA** after studying the feasibility constrains.

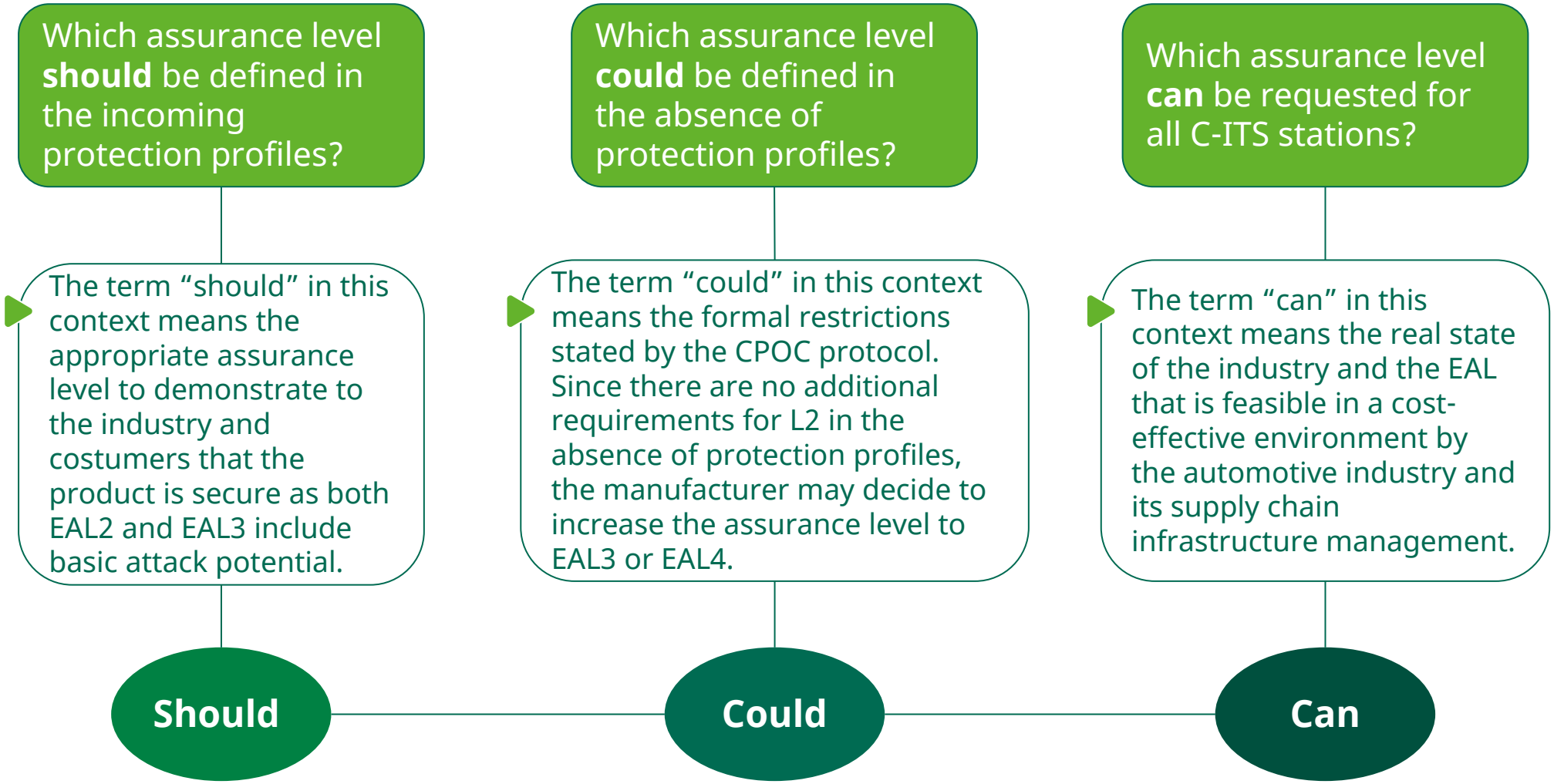
Assurance Level

Precedents



Protection Profiles

Questions



Assurance Levels for C-ITS Stations

Different Approaches of Assurance Levels of C-ITS Stations

This analysis does not consider the reduction to AVA_VAN.1 (and therefore EAL1) as most audiences would agree that the security provided at this level is not enough for the type of product and its intended functionality.

Different approaches of assurance level of C-ITS stations can be considered given the attack potential “basic” determined by AVA_VAN.2.

AVA_VAN.2 -> EAL3

Augmentation of the security concerns during the development

AVA_VAN.2 -> AVA_VAN.3

Augmentation of the security concerns of the TOE

AVA_VAN.2 -> EAL2

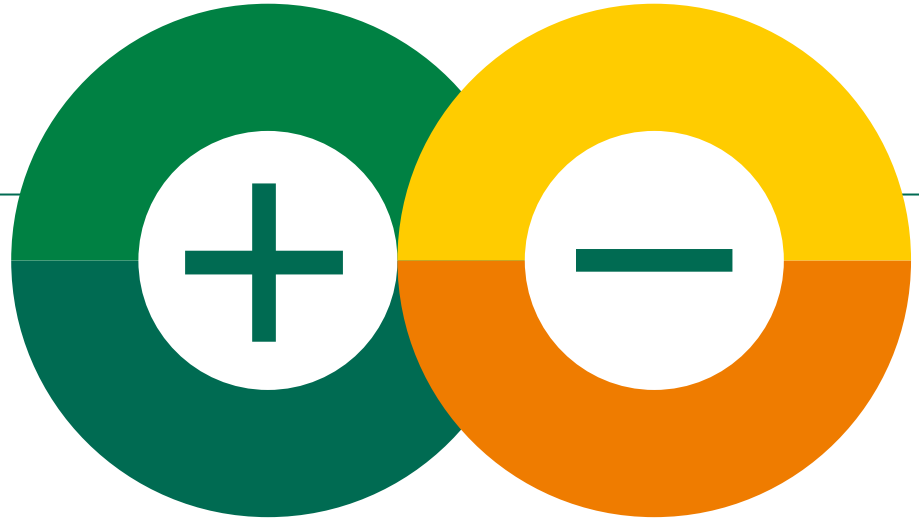
Maintaining the security concerns to EAL2 level

Assurrance Levels for C-ITS Stations

Augmentation of the Security Concerns if the TOE

The C-ITS stations have to be resistant to more complex, sophisticated attacks that can involve more personnel, expertise, equipment, etc.

AVA_VAN.2 -> AVA_VAN.3



The increase in attack potential from AVA_VAN.2 to AVA_VAN.3 poses a challenge regarding the availability and control of the **implementation representation** of each C-ITS station component.

In addition to including specific implementation review activities that require more time and effort.

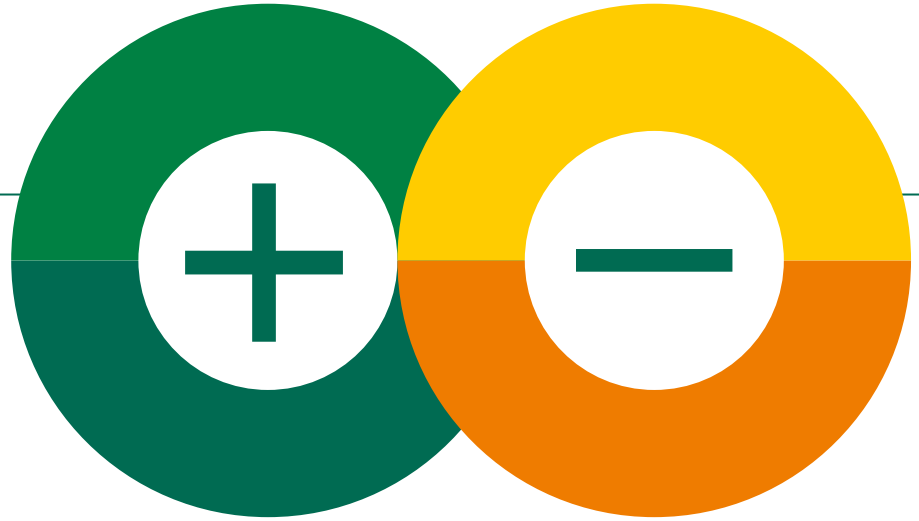
Assurrance Levels for C-ITS Stations

Augmentation of the Security Concerns during the Development

Same attack potential (basic)

Include life-cycle support evaluation activities to verify the development and maintenance.

AVA_VAN.2 -> EAL3



One of the major challenges is carrying out quality reviews in the acceptance and integration of the configuration items that make up the product and come from different manufacturers.

Another challenge is the need of **site visits** that are required to verify the security measures put in place in every area in which a component is developed and/or integrated.

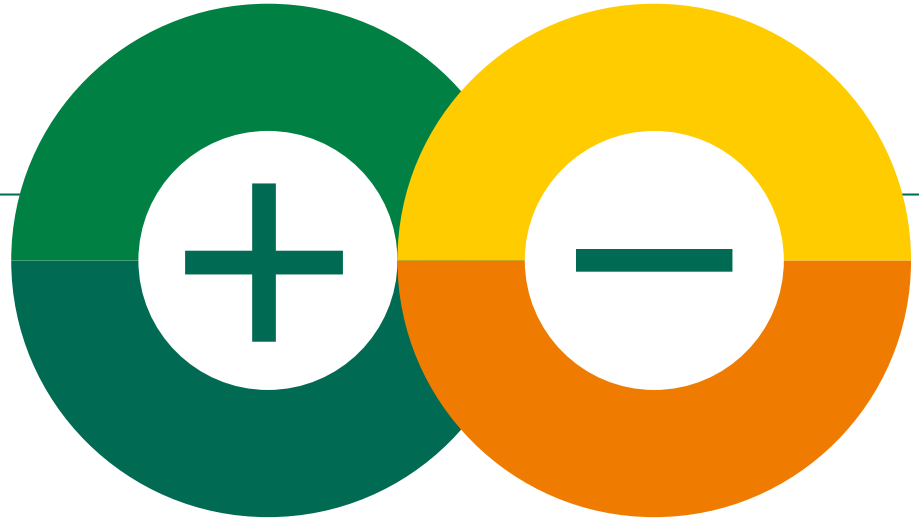
Assurrance Levels for C-ITS Stations

Maintaining the Security Concerns at EAL2

AVA_VAN.2 -> EAL2

Same attack potential (basic).

Low effort evaluation.



No strong security requirements are defined for the lifecycle support and supply chain

Defining the Best Approach

Considerations

To determine the optimal certification appr
C-ITS stations, an analysis has been perfor
based on three critical characteristics that
be ignored

The security provided by the product must be tested at a level **commensurate** with the type of the product and its intended use

The industry must be **prepared** to comply with the CC/ISO 15408 certifications that are required of them

Supply chains are a characteristic of the automotive industry, and the entire vehicle is composed of different scaled elements developed by a large variety of vendors.

This is applicable for C-ITS stations or any automotive component. OEMs do not necessarily develop the C-ITS stations that they deploy in vehicles.

Defining the Best Approach

Vultnerability Analysis

In AVA_VAN.3 scenario the availability of the **implementation representation** (usually source code) is a mandatory input for the evaluation.

It is not enough for the main developer to make available its own source code that they control but the laboratory should also have access to the source code of the parts that have been acquired.

However, this is resolved if we consider that AVA_VAN.2 seems to be an adequate component for the C-ITS stations **as long as the cryptographic operations have been assessed with a higher assurance.**

The critical cryptographic features upon which the C-ITS stations rely are usually delegated in the C-ITS secure elements (HSM). **Cryptographic assets** are crucial for the secure operation of the connected vehicles and this is the reason why C-ITS secure elements have to have their own CC/ISO 15408 certificate including **AVA_VAN.3 or even AVA_VAN.5.**

Accordingly, for C-ITS station itself no augmentations with respect to AVA_VAN.2 component have been considered by the regulations or the available protection profiles.

Defining the Best Approach

Vultnerability Analysis

In EAL3 scenario of a C-ITS stations evaluations, the site visits that the laboratory carries out during the evaluation process need to be **extended to all additional vendors** from which the main developer acquired some parts.

This process can be time-consuming and labor-intensive, which can be a significant burden for the automotive industry in terms of cost and time-to-market.

However, this industry characteristic is important from the perspective of security regarding the acceptance and integration between the different tiers of the various components that constitute the product.

Hence, it would not be appropriate to disregard the review of the life cycle associated to EAL3 without proposing some compensatory measures.

It is suggested to address this issue through extended evaluation activities (**extended SARs**) that enable manufacturers to demonstrate, through the corresponding records and without the need of site visits, how the intergration process is performed throughout the entire supply chain.

These extended SARs could be related with ALC_CMC and ALC_CMS families and based in ALC_CMC.4-8.

Conclusions

It should be noted that the inclusion of augmentations like **EAL3 or AVA_VAN.3 would change the entire landscape.** All tier developers of C-ITS stations would need to be involved in the CC evaluation process as well and should agree to share their internal information in the form of

EAL2 together with integration records is the assurance level that fits the scenario in a **more adequate/cost-effective** manner for Automotive industry/C-ITS manufacturers. Considering the challenges to have all the internal information of the developers in a time-manner of ready availability where access to the different tier level developers can be limited.

Extended SAR to verify the security of the supply chain without the need of onsite visits.

C-ITS secure element (HSM) in charge of cryptographic assets evaluated high assurance.

Questions?

https://www.dekra.com/en/common-criteria-whitepaper/

Thank you!