Whitepaper

Challenges in Common Critiera Evaluation in the Automotive Industry

Author: Diego Sierra Liras

1 Background

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 [1]. However, the escalating volume of vehicles on the road poses significant challenges, including traffic congestion, safety concerns, and environmental issues. Thankfully, modern information and communication technologies present innovative solutions to alleviate these transportation issues.

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. There are many examples of their benefits, from improvements in health and safety, helping to save fuel by using smart motorways or reducing the average road speed with speed cameras to economic savings thanks to efficient traffic and congestion management.

Over recent years, 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**.

The cooperation between two or more C-ITS stations (personal, vehicle, roadside and central) enables and provides an ITS service that offers better quality and an enhanced service level, compared to the same ITS service provided by only one of the ITS sub-systems. However, such cooperation between two C-ITSs stations will introduce new threats for attackers who want to compromise the ITS application data shared by the devices, the security of communications and the certificates they rest on, or the security and privacy of the geo-localization of a vehicle and its occupants.

Within this framework, global standardization activities are underway to determine the security requirements that should be met by deployers of connected vehicle technologies, including deployment of C-ITS stations supporting a PKI trusted model. Deployers may not always be developers of the C-ITS stations, but they can act as manufactures and integrators of technologies acquired from different vendors.

[1] https://hedgescompany.com/blog/2021/06/how-many-cars-are-there-in-the-world/

2 Cybersecurity Risk Threats and Challenges on C-ITS

Collaborative Intelligence transport systems (C-ITS) is a new paradigm of intelligent transportation that enable vehicles to communicate with each other and with the infrastructure, as well as to leverage data from various sources to optimize traffic efficiency and safety. However, C-ITS also introduce **new potential threats and vulnerabilities that need to be addressed by adequate security measures**.

A very detailed analysis of the risks and threats landscape is developed by ENISA in the "ENISA good practices for security of Smart Cars" [2] where threats and assets are identified according to a proposed high-level reference model for smart cars architecture, and relevant security measures are mapped to the relevant threat(s). These security measures cover general policies for security by design, organisational practices for security and incident management and technical practices that would lead to product-specific requirements. 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. Such method has been recommended by the United States Department of Transportation [3] as a best practice for deployers. These evaluations are independent assessments of the security properties and performance of a system or product by a trusted entity. They can provide assurance and confidence to stakeholders that the system or product meets certain security standards and requirements. Sometimes these evaluations are included in the framework of certification schemes that support compliance with specific regulations.

One example of these schemes in EU is the SOG-IS (EUCC under the CSA in the future) which is based on the ISO/IEC 15408 or Common Criteria. Common Criteria (CC) is an international standard for evaluating the security of ICT products. CC defines a set of criteria for security functionality, assurance levels, protection profiles and evaluation methods. This scheme has been proven to be a good solution to provide an adequate risk-based level of assurance for products to be deployed in infrastructures. It is also considered adequate to cover the cybersecurity needs of C-ITS products, with pros and cons.

[2] https://www.enisa.europa.eu/publications/smart-cars

[3] https://www.pcb.its.dot.gov/documents/OBU_LessonsLearned_Report.pdf

2 Cybersecurity Risk Threats and Challenges on C-ITS

Some pros of CC evaluations are:

1. They can provide a common language and methodology for describing and comparing security features and objectives across different systems or products.

2. They can facilitate interoperability and compatibility between different C-ITS components or services that have been evaluated against the same specs (protection profiles) or assurance level.

3. They can increase trustworthiness and transparency among stakeholders by providing evidence-based certification reports that document the evaluation process and results.

4. CC provides a mechanism that allows assigning different guarantees in the same deployment or product according to the risk analysis, providing a comprehensive holistic assurance of the solution.

Some cons of CC evaluations are:

1. They can be costly and time-consuming, especially for higher assurance levels that require more rigorous testing and analysis, complicating the time-to-market of the solutions

2. They can be inflexible or outdated, as they may not cover all aspects or scenarios relevant to C-ITS security or reflect the latest technological developments or threats.

3. They can create a false sense of security, as they may not guarantee absolute protection against all possible attacks that may affect C-ITS security. However, this is „cybersecurity“ by definition: it cannot be guaranteed that a product is secure, the assessment can only offer certainties based on the level of assurance.

CC evaluations are not easy in any framework and less when it comes to the automotive reality, where the supply chain is it very complex and with many parts involved. It involves multiple stakeholders such as manufacturers, suppliers, integrators and OEMs.

One challenge is that each stakeholder may have different security objectives, requirements and capabilities, which may create conflicts during the evaluations of C-ITS systems. Moreover, each stakeholder may have different incentives or disincentives to provide the evidence and information required in a CC evaluation that could be inflexible in some requirements and request collaboration in a timely-manner for some actors of the supply chain. For example, suppliers may want to protect their intellectual property or trade secrets by limiting access to their components design, source code, etc; Eventually, Tiers might not accept 3rd parties site visits associated to assessments activities that in turn make the evaluation cost higher. In addition, participants in the OEM´s supply chain may not have implemented good security practices in their designs, and may find themselves failing to meet the security requirements of the specifications.

Another challenge is that CC evaluations are not so suitable for products that are constantly being updated. This is because CC certification is fixed to a particular version of the product and subsequent updates would require a minor re-certification that could still go at a slower pace than the updates themselves.

In any case, given its benefits, CC continues to be a methodology chosen for C-ITS stations evaluations as in the case of the CPOC protocol.

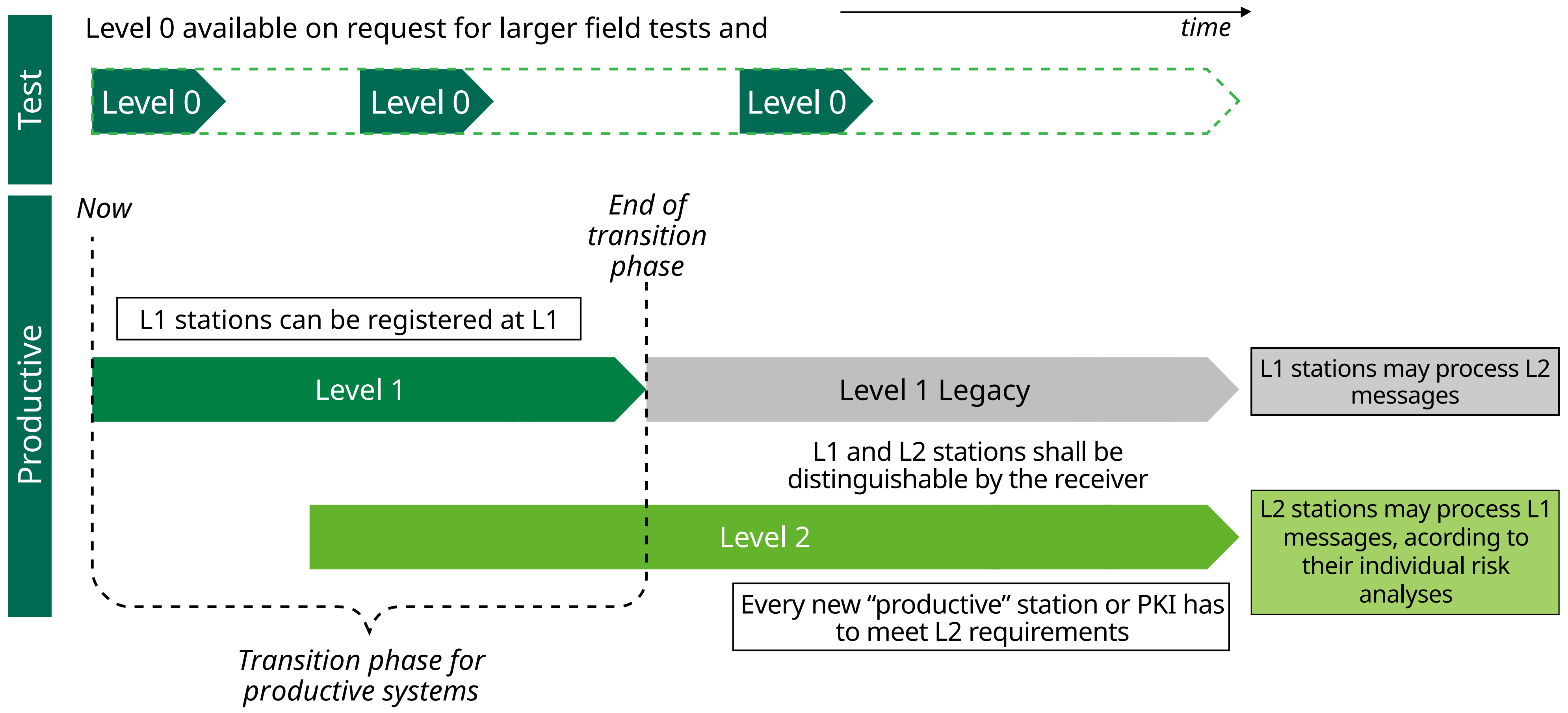
3 Required CC Certification for C-ITS Stations by CPOC Protocol

One of the key actions for the European Commission is the design and implementation of a **European Union C-ITS Security Credential Management System (EU CCMS)** for C-ITS messages.

Such goal is achieved through the C-ITS Point of Contact of the European Comission (CPOC) and portrayed in its protocol “Description of the CPOC protocol in the EU C-ITS Security Credential Management System CPOC protocol” [4].

CPOC protocol is going to support the deployment of C-ITS systems and technologies in Europe by implementing the trust model and providing the necessary security functions. Therefore, in order to create the European Certificate Trust List (ECTL), there are three scenarios associated with three levels (L0, L1 and L2).

While L0 is intended for preliminar testing of C-ITS stations, L1 and L2 provide productive environments. L1 is designed for C-ITS stations which are not fully compliant yet, in a ramp-up phase of C-ITS deployment in the EU CCMS. After the end of the transition phase, L1 stations either move on to the full productive environment L2 once they are fully compliant.



Test

Level 0 available on request for larger field tests and

time

Level 0

Level 0

Level 0

Productive

Now

End of transition phase

L1 stations can be registered at L1

Level 1

Level 1 Legacy

L1 stations may process L2 messages

L1 and L2 stations shall be distinguishable by the receiver

Level 2

L2 stations may process L1 messages, acording to their individual risk analyses

Every new “productive” station or PKI has to meet L2 requirements

Transition phase for productive systems

Overview and timeline of ECTL levels [4]

[4] https://cpoc.jrc.ec.europa.eu/data/documents/EU_CCMS_CPOC_Protocol_Release_1_2.pdf

3 Required CC Certification for C-ITS Stations by CPOC Protocol

For those deployers interested in being compliant with L1, an evaluation performed by a SOG-IS recognised 3rd party laboratory is required. The test laboratory shall evaluate that the C-ITS station is protected against an attacker with **basic** attack potential. For example, performing a man and the middle attack to modify the C2X communication data between two C-ITS stations or modifying on the fly the certificates installed in the TOE during the enrolment process.

Additional requirements for L2 are that the C-ITS stations shall be certified using security assessment criteria as specified in "Common Criteria / ISO 15408" with available **protection profiles**.

In the development of such protection profiles, the scope of the security certification of the C-ITS station may be defined by the manufacturer, with an evaluation assurance level EAL2+ or higher, subject to assessment and approval of the CPA and SOG-IS conformity assessment body.

Although CC/ISO 15408 are defined as the standards for the security assessment due to their flexibility, especially for level 2 (L2) the field is not mature enough yet to have defined the corresponding protection profiles that C-ITS stations shall comply with. In addition, the term EAL2+ is open to interpretation if no additional clarifications about the "+" are provided.

The **goal** of this document is to discuss the following **topics**:

- 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 proposed by DEKRA after studying the feasibility constrains. This information can be considered by main car manufacturers, supply industry representatives, working groups, certification bodies and protection profiles developers.

4 C-ITS Evaluation Assurance Level Analysis

Understanding the Assurance Level for C-ITS Stations

Although there are protection profiles in development (such as that of the CAR 2 CAR consortium), no protection profiles have been certified yet for all kind of C-ITS stations (personnel, vehicle, roadside and central).

The BSI released in 2019 the protection profile “Protection Profile for Road Works Warning Gateways (RWWG)” [5]. Although this protection profile could be considered related to the C-ITS roadside units, road works working gateways and C-ITS roadside units are not necessarily the same.

Even so, the CPOC Protocol has used the information provided in this protection profile as a basis for forming the security features that C-ITS stations shall meet in a L1 scenario and it can be also useful to consider in a L2 scenario.

The evaluation assurance level (EAL) of this protection profile has been built from the vulnerability analysis component AVA_VAN.2 covering the assurance required according to the security problem defined in the PP. This means that the authors of the protection profile have analysed, first, the attack potential for which the C-ITS station has to provide security measures and, second, the overall EAL that includes the component (AVA_VAN.2).

[5] https://www.commoncriteriaportal.org/files/ppfiles/pp0106b_pdf.pdf

4 C-ITS Evaluation Assurance Level Analysis

In terms of CC, there are two different EALs that include the component AVA_VAN.2: EAL2 and EAL3. Considering that the EALs are hierarchical as each EAL represents an increasing assurance with respect to all lower EALs, the authors of protection profile chose EAL3 for their purpose.

The component AVA_VAN.2 is associated to the attack potential "**basic**". The reader may notice that, at the moment, no other attack potential different to "basic" has been mentioned or identified in the throughout this paper and the associated references. For L1 scenarios, "basic" is the attack potential in certifications of C-ITS stations required by the CPOC Protocol and, for L2 scenarios, no additional requirements have been described. The available protection profile for RWWG does not increase the potential to Enhanced-Basic or others.

Although the BSI protection profile seems to have provided an answer to the question of what should be the minimal assurance level for C-ITS stations (EAL3), new questions arise regarding other C-ITS stations (or even roadside units) according to the security problems defined for both levels, EAL2 and EAL3.

For other C-ITS stations, which assurance level **should** be defined in the incoming protection profiles?

The term "should" in this context means the appropriate assurance level to demonstrate to the industry and costumers that the product is secure. As both EAL2 and EAL3 include basic attack potential, an analysis on the need of either levels shall be performed.

For other C-ITS stations, which assurance level **could** be the allocated in the absence of protection profiles?

The term "could" in this context means the formal restrictions stated by the CPOC protocol. Since there are no additional requirements for L2 in the absence of protection profiles, the manufacturer may decide to increase the assurance level to EAL3 or EAL4.

In general, which assurance level **can** be requested for all C-ITS stations?

The term "can" in this context means the real state of the industry and the EAL that is feasible in a cost-effective environment by the automotive industry and its supply chain infrastructure management.

4 C-ITS Evaluation Assurance Level Analysis

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:

- **Augmentation of the security concerns during the development: AVA_VAN.2 → EAL3**
- **Augmentation of the security concerns of the product: AVA_VAN.2 → AVA_VAN.3**
- **Maintaining the security concerns at EAL2 level AVA_VAN.2 → EAL2**

4 C-ITS Evaluation Assurance Level Analysis

Different Approaches of Assurance Levels of C-ITS Stations

Augmentation of the security concerns during the development: AVA_VAN.2→EAL3

While both EAL2 and EAL3 assurance levels have the same basic attack potential, the assurance components pertaining to EAL3 include life-cycle support evaluation activities.

Life-cycle support is an aspect of establishing discipline and control in the processes of refinement of the TOE during its development and maintenance [6]. Accordingly, the laboratory conducts a site visit to the developer facilities where the different software and hardware parts of which the product is composed of are developed in order to verify on-site organizational, procedural and physical security measures.

This increase in the evaluation level from EAL2 to EAL3 brings very complex consequences. 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.

[6] https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf

4 C-ITS Evaluation Assurance Level Analysis

Different Approaches of Assurance Levels of C-ITS Stations

Augmentation of the security concerns of the product: AVA_VAN.2→AVA_VAN.3

If the vulnerability analysis component is increased to AVA_VAN.3, the C-ITS stations have to be resistant to more complex, sophisticated attacks that can involve more personnel, expertise, equipment, etc. Therefore, the laboratory will design its penetration test plan considering this. Manufacturers shall make available a mandatory input to the laboratory, known as the „implementation representation“, Implementation representation is the least abstract representation of the C-ITS station. Source code that is then compiled or a hardware drawing that is used to build the actual hardware are examples of parts of an implementation representation.

The increase in attack potential from AVA_VAN.2 to AVA_VAN.3 poses a challenge regarding the availability and control of the implementation of each C-ITS station component. In addition to including specific implementation review activities that require more time and effort.

4 C-ITS Evaluation Assurance Level Analysis

Different Approaches of Assurance Levels of C-ITS Stations

Maintaining the security concerns at EAL2 level AVA_VAN.2 → EAL2

In this case the attack potential for the product is “basic” and no strong security requirements are defined for the lifecycle support. As described by the CC standard:

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such, it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation can arise when securing legacy systems or where access to the developer can be limited.

4 C-ITS Evaluation Assurance Level Analysis

Defining the Best Approach

To determine the optimal certification approach of C-ITS stations, an analysis has been performed based on two critical characteristics that cannot be ignored. First, that the security provided by the product must be tested at a level commensurate with the type of the product and its intended use. Second, the industry must be prepared to comply with the CC/ISO 15408 certifications that are required of them.

For those interested in approaching an EAL3 or AVA_VAN.3 scenario, the following issues should be taken into consideration. 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. Subsequently, C-ITS stations developers usually do not develop the entire source code that conforms the product by acquiring some security parts to an additional tier level vendor.

a. Vulnerability 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 resolve 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. This is mainly because this level is appropriate for analysing the exploitable vulnerabilities of the C-ITS stations, which handle V2X communications and associated data.

b. Life cycle assessment

In EAL3 scenario of a C-ITS stations evaluations, the site visits that the laboratory carries out during the evaluation process where the life cycle support is analysed is not be restricted to the facilities of the main developer of the product. It needs to be extended to all additional vendors from which the main developer acquired some parts meaning that the evaluators will perform site visits to these vendors as well.

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 simultaneously renders it expensive to assess and 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. In this case, it is suggested to address this issue through extended evaluation activities (extended SARs) explicitly designed for these evaluations 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:

The configuration management plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

5 Conclusion

Given the corresponding explanations, they lead to the conclusion that the most convenient approach for CC security certifications of C-ITS stations should target evaluation assurance level EAL2 as the minimum assurance level that the products must comply with in order to be deployed in real scenarios as long as it is completed with extended SARs that cover the integration of the product parts throughout the supply chain. This is a level commensurate with the current state of the art of automotive industry and useful for the analysis of the V2X communications while the cryptographic mechanisms rely on a secure element certified with high assurance protection profiles.

It should be noted that the inclusion of augmentations like EAL3 or AVA_VAN.3 would change the entire landscape and would add difficulties and restrictions to the supply chain that might not be affordable. It would not be enough for suppliers to deliver functional solutions, for example in the form of compiled libraries, they would need to be involved in the CC evaluation process as well. All tier developers of C-ITS stations should agree to share their internal information in the form of source code or in the form of an invasive site visit.

Therefore, 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.

6 Bibliography

- **European Commission:**
https://cpoc.jrc.ec.europa.eu/

- **Common Criteria Portal:**
https://www.commoncriteriaportal.org/cc/

- **Car 2 Car Communication Consortium:**
https://www.car-2-car.org/about-c-its/

- **European Commission:**
https://transport.ec.europa.eu/index_en

- **European Telecommunications Standards Institute:**
https://www.etsi.org/technologies/automotive-intelligent-transport

- **Intelligent Transportation Systems Joint Program Office:**
https://www.itskrs.its.dot.gov/benefits

- **Hedges Company:**
https://hedgescompany.com/blog/2021/06/how-many-cars-are-there-in-the-world/

- **Intelligent Transportation Systems:**
https://www.pcb.its.dot.gov/CV_deployer_resources.aspx#opensrc

DEKRA **Contact**

About Digital & Product Solutions
Innovating safety and security by creating the intelligent testing solutions that contribute to making the digitalized and connected world a safer place.
We are the experts in testing and certifying products and new digital technologies.We deliver solutions from Cybersecurity, Artificial intelligence, Big Data, to Connectivity, Product Safety, Electromagnetic Compatibility & Radiofrequency, Product Certification, Medical Devices and Automotive Testing.
Through a global network of 48 state-of-the-art test laboratories and facilities, we offer a broad portfolio of product testing services based on national and international standards as well as industry and customer requirements

www.dekra-dps.com

Would you like more information?

Contact

© 2023 DEKRA. All rights reserved. All trademarks are the property of DEKRA reg. U.S. Pat. & Tm. Off.; reg. OHIM and other countries as shown on our website.