C-ITS Platform Phase II
Working Group Compliance Assessment

Final report

12 July 2017

Contents

1. Executive summary

C-ITS is based on vehicle to vehicle communication and communication between vehicle and physical and/or digital infrastructure. To ensure that this works, it is important to ensure interoperability. It is well-known from other systems that a way to ensure this is through compliance assessment. The objective of this report is to evaluate and issue recommendations on how this compliance assessment can be achieved, with a specific focus on C-ITS stations.

Main recommendations:

- Need to set up an appropriate common EU legal and technical framework defining the functional, technical and organisational provisions to implement the proposed roles and compliance assessment requirements and process, which is summarised on the figure on the overview of the compliance assessment process.
- Main roles in relation to C-ITS compliance assessment are governance (C-ITS Governing Body), operation (Compliance Assessment Body) and supervision (C-ITS Supervision Body). Main decision body is the C-ITS Governing Body.
- Any new C-ITS station must fulfil the compliance assessment criteria to be part of the C-ITS security trust model.
- Considering the challenging time schedule of setting up a final organisation as described by the Compliance assessment Working Group, progressive development of this organisation should allow for deployment in a relatively short timeframe (2019).
- After 2019, the proposed compliance assessment organisation should be able to also address and ensure interoperability of existing services and future C-ITS service extensions and technology deployments.
- The proposed organisation shall have the capability allowing the introduction of new services and/or new technologies in a backward compatibility manner with already deployed services.
- Need to finalise by second half of 2018 the standards and profiles necessary to support the compliance assessment process for Day 1 services.
- Need to maintain consistency with other validation frameworks having an impact on connected and automated vehicles and road infrastructure, e.g. in the future, evolution of data quality requirements may be needed for higher levels of automated vehicles.
- Further work is needed to elaborate a common EU framework to cover the roles defined by all WGs (in particular compliance assessment, privacy/data protection, security).

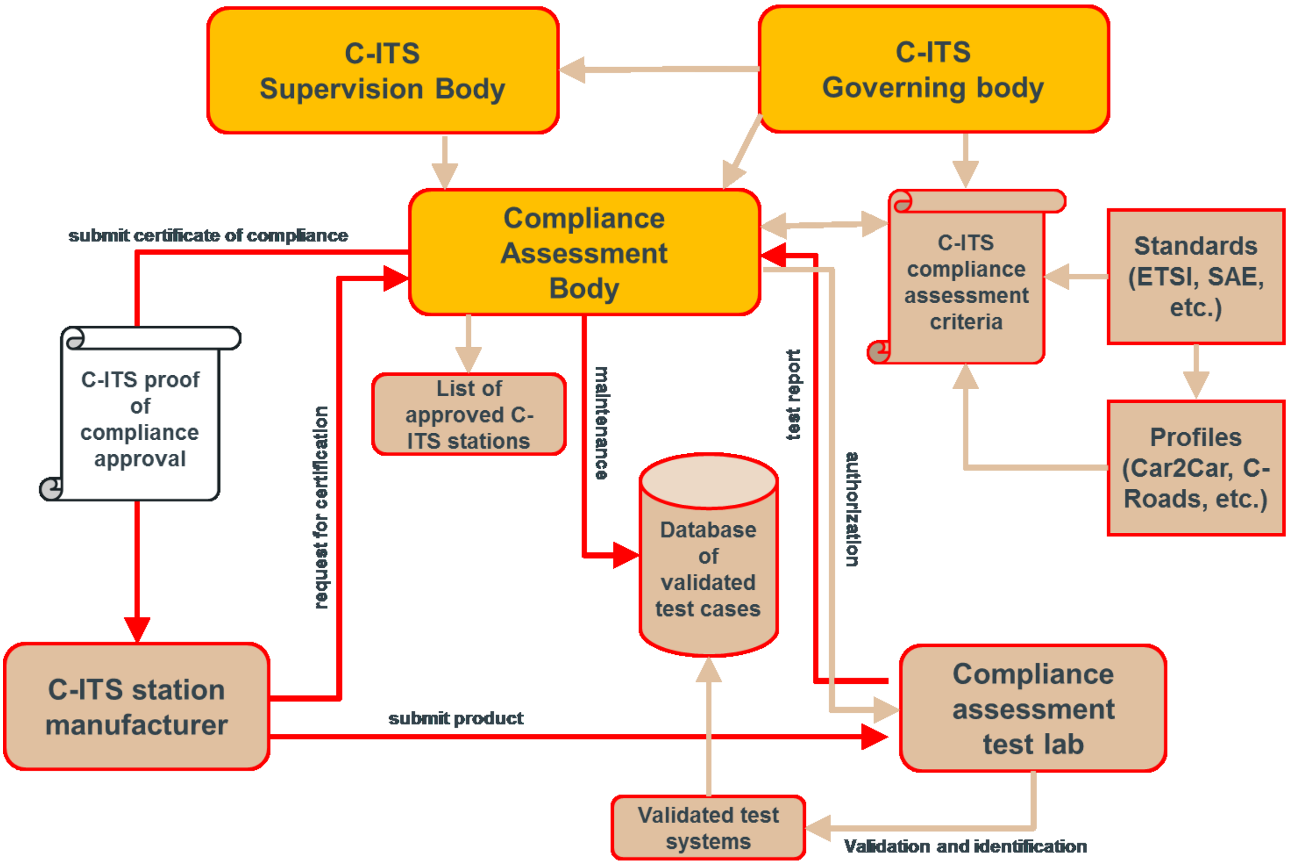

C-ITS Supervision Body
C-ITS Governing body
Compliance Assessment Body
C-ITS compliance assessment criteria
Standards (ETSI, SAE, etc.)
Profiles (Car2Car, C-Roads, etc.)
submit certificate of compliance
C-ITS proof of compliance approval
List of approved C-ITS stations
maintenance
test report
authorization
request for certification
Database of validated test cases
C-ITS station manufacturer
submit product
Compliance assessment test lab
Validated test systems
Validation and identification

Figure: overview of the compliance assessment process

Organisation of Work

The organisation of work was based on regular Working Group meetings (with a total of 12 meetings in Brussels from July 2016 to July 2017 in the course of the second phase of the C-ITS platform) and also on some phone conferences to deal with specific sub-topics.

All results, outputs and expert recommendations of the C-ITS Platform Working Group Compliance Assessment have been prepared and discussed by the nominated experts representing the organisations and countries listed in Annex "Phase II – Compliance Assessment – Annex 1". This report of the C-ITS Platform Working Group Compliance Assessment has been approved by the Working Group on 12 July 2017.

2. Overall scope of the work group report

2.1. Methodology and approach for deploying interoperable C-ITS services on all C-ITS stations in the EU

In this report, that has to be understood as a guidance document for further work at EU level, we define an approach and a methodology to assess all different C-ITS stations to allow collection and delivery of information enabling deployment of C-ITS services in Europe and how this compliance assessment should be organised. These processes of a single C-ITS station as member of the overall C-ITS Network are independent from the time, the place, the network connections, the C-ITS station they are using, and the traffic environment they are involved in. Overall the report defines also the objectives to achieve with a compliance assessment procedure for C-ITS roll out in Europe and the further developments to extend the applications in the future.

The approach is based on the standard C-ITS messages (including CAM, DENM, SPAT/MAP and IVI) for day one applications as a starting point, but will also take into account future extensions of them linked to day 1.5 or day 2 services and beyond, in the direction of supporting cooperative movements of vehicles and automation.

The methodology for validation should make it possible that C-ITS services are perceived by the end user the same way for the same C-ITS application, and at the same time efforts for testing and validation are minimal for all C-ITS station operators / manufacturers and service providers involved.

In this context, the generic overarching term “compliance assessment” is used, since other terms such as “type approval” or “certification” might lead to pre-conclude on specific forms of compliance assessment (which might already be established in the road transport sector).

The aim of this report is to define a top-level approach and methodology for testing and validation. This includes making recommendations on the necessary legal and organisational frameworks for the setup and the operational phase of the C-ITS network.

The scope of this compliance assessment report includes the distribution of C-ITS messages via different communication technologies in the future and distinguishes between the following two basic options now in the introduction phase of C-ITS. One possibility is a cloud based messaging service to single users via different generations of cellular networks with direct connections and platforms able to handle standards based information input and network handover for their customers.[1] The second option is a message based C-ITS service with standard communication messages including communication security provisions at message level. The latter option is the basis for the compliance assessment procedure in this report and will be defined in the chapters to follow.

This will be a first set of recommendations for a compliance assessment process which supports the setup phase for all day one applications launched and the operational phase of a C-ITS Network in Europe and takes into account the further international links in terms of countries and regions, but also the future extension to additional C-ITS Stations or communication technologies and networks. At the same time the setup phase with currently available technologies will form a core part of this section.

Develop intentions in terms of recommendation for:

- Validation for a successful introduction of C-ITS in the setup and launch phase, and
- A procedure to extend the C-ITS (Applications, stations, technologies, stakeholders) in the future with indications for future end to end testing of the C-ITS Message chain for day 1.5 and day 2 application groups

The following chapters of the report will define the basic elements and targets to be included in the later chapters of the document in a more detailed level of information.

Overall in the report the roles and responsibilities of actors will be described for the C-ITS context followed by the legislative framework and an introduction to compliance assessment in the following chapters, based on examples from several application areas and types of equipment.

---

[1] Different cloud-based solutions with different characteristics exist currently, with different performances, which require clear specifications and capabilities assessments with regard to applications requirements.

From this point on the definition of the minimum performance of C-ITS Systems and the following requirements to reach interoperability are described, together with the concrete proposal of the validation methodology for C-ITS Stations. These chapters include testing of communication aspects between C-ITS stations, laboratory and on road testing and end to end testing of complete C-ITS service delivery chains.

Finally important additional aspects for the future aspects for C-ITS introduction at a larger scale are mentioned and described in further details, this includes security and data protection, but also system scalability, before the report concludes with the recommendations for C-ITS Compliance assessment in the introduction phase of C-ITS day one applications in Europe.

2.2. Existing common elements of C-ITS testing

In the scope of this document the overall purpose of C-ITS compliance assessment is to ensure that implementations are interoperable across Europe and across manufacturers. To do this several types of testing can be performed and include different levels or parts of the C-ITS Network e.g. single C-ITS applications, modules, C-ITS stations, or complete service chains. The different ways of C-ITS network validation can be defined as interoperability testing, conformance assessment and end to end testing.

Conformance testing

Conformance testing aims to determine whether a C-ITS Station complies with the relevant standards and reference specifications. Conformance testing can be executed based on a specific set of a test equipment or a test system to test a C-ITS -Station to verify that it is implemented in accordance with the relevant standards and reference specifications. This approach will normally lead to reproducible results, but will at the same time also depend on the number of functions defined in the standards and implemented in the test equipment. For part of the tests a device known to be compliant can be used as test equipment. These types of tests then become similar to interoperability testing, see next paragraph. Not all types of tests, however, can be executed by using a compliant device: error handling testing, for example, is not possible in this way, as a compliant device would not trigger error conditions in the system under test.

To make conformance testing work it is necessary to have a set of well-defined and verified test cases that test what is specified by the relevant standards and reference specifications (communication, applications, security), i.e. what is considered to be typical configurations under normal operating conditions of the equipment with the basic set of applications, i.e. what is specified by the relevant standards and reference specifications (telecom, applications, security). The set of test cases that is to be passed by a C-ITS Station are known as the test criteria. It is important to notice that the specific test criteria might vary depending on the type of C-ITS station (Vehicle, Roadside Unit etc.) and on the services the C-ITS station supports. Clearly, the triggering of messages might be quite different between e.g. a vehicular C-ITS station and a Roadside C-ITS station. As the general procedure of conformance testing for stations foresees a sequence of test cases according to the supported C-ITS applications, the “interdependencies between applications” are not covered.

It is important to note that conformance testing will a priori not guarantee interoperability between all systems that pass the same conformance tests, because the underlying standards and reference specifications do not guarantee interoperability.

Interoperability testing

Interoperability testing aims to test two or more implementations of a set of standards and reference specifications at C-ITS station level in their communication capabilities against each other and see if they work as expected. This type of testing has been done for C-ITS in a laboratory environment in the ETSI plug tests, and is also performed in live traffic environments and public roads in the different Pilot projects such as, e.g., SCOOP@F, EcoAT etc. When using interoperability testing, the testing shows that at least two different implementations can work together and provide the intended functions of the systems. Interoperability testing is often performed in a more dynamic traffic environment on open roads than conformance testing and thus results for all C-ITS stakeholders involved may not be a 100% reproducible.

Especially in the earlier stages of the development of the standards and reference specifications, interoperability testing plays an important role in improving the quality of those standards and reference specifications, as inconsistencies and parts that can be interpreted in multiple ways are identified and can be fixed.

In some case Interoperability testing and conformance testing might be supplemented with additional volunteer testing of single C-ITS stations or applications in a certification scheme. Such test could cover validation aspects not strictly needed for interoperability but for instance related to the applications towards the users or to interdependencies between applications and certain traffic environments.

End to end functional testing

For end to end functional testing procedures other settings of the validation scheme and expected outcomes apply which need to be discussed with the main stakeholders in the C-ITS domain and need to make sure that the initial start of C-ITS introduction is according to the users expectations and takes into account the future extensions of applications and C-ITS units in operation. This will be achieved within the C-ROADS platform were the single work groups can elaborate a set of common documents for the national implementations and take into account mutual acceptance. For this purpose the actors in C-ITS and their roles are briefly described in the next chapter of this report.

2.3. Actors in the C-ITS

- **Communication network: Cellular or ad-hoc**

    Cellular: Mobile Network Operator – Mobile Virtual Network Operator

    Ad-Hoc Network: All stakeholders that transmit on the network

- **Information Providers:**

    Road operators

    Individual C-ITS stations, e.g. vehicles, RSUs

    Service providers (e.g. brokering, information market places

- **Application Providers:**

    Vehicle Manufacturer

App developers, e.g. smartphone apps

Aftermarket and nomadic device manufacturers

- **End Users**

    Road users (e.g. driver, automated vehicle, pedestrian etc.)

    Road operators (e.g. traffic managers)

- **Service providers of Security and trust**

    The different elements in PKI (CPOC - Central Point of Contact)

    Compliance assessment

    Governance and supervision board

- **Preparation of the technical and legal framework**

    C-Roads and associated projects

    Car2Car

    ESOs

    Member States experts

    European Commission

Short range communication portion of the communication in C-ITS is designed to work without presence of infrastructure and is based on ad-hoc networking. This means that on contrary to cellular communication there is no central operator, who is operating the network and ensures correct configuration of the network and correct usages of the resources.

In the ad-hoc network the role as network operator is distributed to all the actors, who must follow the laid-out principles for the network. As an example, it is up to the Vehicle manufacturer and the Road operators to ensure not only that their C-ITS stations are compliant to the Compliance Assessment Criteria, but also that the resource of the ad-hoc network is not misused.

This of course means it that both manufacturers of C-ITS stations and C-ITS station operators have a role in C-ITS than goes beyond just putting the products in the field. Also, there is a need for a governance and/or supervision organisation to set the operational rules and to monitor the performance of the ad-hoc network. In addition, information providers and C-ITS Service providers will have a role in the overall C-ITS. For the Compliance Assessment, some more specific roles will exist and is described later in this document.

3. References

[1].	Global Compliance assessment Forum (GCF) http://www.globalcertificationforum.org/
[2].	ISO/TS 16949 Quality management standard for suppliers to the automotive sector
[3].	EN ISO/IEC 17065:2012

[4].	European Type Approval for Automotive Systems and Components by Vehicle Compliance assessment Agency (VCA), UK Government http://www.dft.gov.uk/vca/additional/files/vehicle-type-approval/vehicle-type-approval/vca004.pdf
[5].	DIRECTIVE 2007/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 September 2007 on establishing a framework for the approval of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles.
[6].	DIRECTIVE 2014/53/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC
[7].	UNECE "1958" Type approval. http://www.unece.org/trans/main/wp29/wp29regs.html
[8].	Regulation (EC) No. 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0030:0047:en:PDF
[9].	ETSI EN 302 665, Intelligent Transport Systems (ITS); Communications Architecture http://www.etsi.org/deliver/etsi_en/302600_302699/302665/01.01.01_60/en_302665v010101p
[10].	Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport Text with EEA relevance http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32010L0040
[11].	Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC Text with EEA relevance
[12].	Common Criteria v3.1. Release 4 Part 1: Introduction and general model at https://www.commoncriteriaportal.org/cc/.
[13].	ISO DIS 17427-1 Intelligent transport systems – Cooperative ITS Part 1: Roles and responsibilities in the context of co-operative ITS architecture(s)

[14]	**Day 1 C-ITS services list**
	Hazardous location notifications:
	– Slow or stationary vehicle(s) & traffic ahead warning;
	– Road works warning;
	– Weather conditions;
	– Emergency brake light;
	– Emergency vehicle approaching;
	– Other hazards.
	Signage applications:
	– In-vehicle signage;
	– In-vehicle speed limits;
	– Signal violation / intersection safety;
	– Traffic signal priority request by designated vehicles;
	– Green light optimal speed advisory;
	– Probe vehicle data;
	– Shockwave damping (falls under European Telecommunication Standards Institute (ETSI) category 'local hazard warning').

[15]	**Day 1.5 C-ITS services list** – Information on fuelling & charging stations for alternative fuel vehicles; – Vulnerable road user protection; – On street parking management & information; – Off street parking information; – Park & ride information; – Connected & cooperative navigation into and out of the city (first and last mile, parking, route advice, coordinated traffic lights); – Traffic information & smart routing.

4. Definitions

The objective of this section is to describe the different terms frequently used in the area of compliance assessment:

Compliance Assessment	Compliance assessment is an activity that helps to directly or indirectly identify the extent, to which vehicle or its constituent parts comply with the set of technical requirements, which must be validated to make the C-ITS station operational. From an operational point of view, compliance assessment is an equipment authorization issued by a compliance assessment body based on representations and test data submitted by the applicant.
C-ITS station	ITS station: functional entity specified by the ITS station (ITS-S) reference architecture (from [9])
Conformance assessment	Conformance assessment means checking that products, materials, services, systems or people measure up to the relevant reference specifications and standards.
Conformity assessment	Conformity assessment shall mean the process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled. In this report this term can be considered a less stringent synonym of compliance assessment.
Conformity / Compliance Testing	Conformance testing is the process used to determine whether a product or system complies with the requirements and/or functional reference specifications.
Declaration of Conformity	Declaration of Conformity is the conclusive step of a procedure where a responsible party makes measurements or takes other necessary steps to ensure that the equipment complies with the appropriate technical standards.
Homologation	Automotive homologation is the process of certifying vehicles or a particular component in a vehicle that it has satisfied the requirements set by various statutory regulatory bodies. Homologation is usually a synonym of type approval for vehicle related matters.
Individual approval	Approval of an individual vehicle instead of a type approval. On the basis of [5], individual approval can only be applied to specific categories of vehicles like vehicles designed and constructed for use by the armed services, civil defense, fire services and forces responsible for maintaining public order.
Type approval	Type approval is the confirmation that production samples of a design (i.e., the type of vehicle or simply the model of a vehicle) will meet specified performance standards. The specification of the product is recorded and only that specification is approved.

Verification	Verification is a procedure where the manufacturer makes measurements or takes the necessary steps to ensure that the equipment complies with the appropriate technical standards.
Whole Vehicle Type Approval	European Community Whole Vehicle Type Approval (ECWVTA) is the type approval of a specific type of vehicle.
	To be completed if necessary

5. Process, roles and responsibilities of actors

5.1. Existing certification frameworks

5.1.1. EU accreditation and conformity assessment frameworks

Regulation 765/2008 provides an independent and authoritative attestation of the competence, impartiality and integrity of conformity assessment bodies, which the objective to ensure one accreditation certificate for the whole territory of EU. There is a single national accreditation body per Member State, within the Framework for the formal recognition of the European co-operation for accreditation (each accreditation body is member of EA) as the official European accreditation infrastructure. EC can mandate to develop sectorial accreditation schemes.

The lightest administrative act to nominate an accredited body is notification (Notified Body), for specific legislative area, to assess products. The Notified Body has to produce a report with tests, and takes legal responsibility.

Decision 768/2008, lays down the "horizontal menu" of conformity assessment modules and the ways procedures are built of modules. The sectorial legislator selects from the menu of conformity assessment modules/procedures the most appropriate ones for the concerned sector.

Overview of the Modules:

A Internal production control

B EC type examination

C Conformity to type

D Production quality assurance

E Product quality assurance

F Product verification

G Unit verification

H Full quality assurance

As an example, type-approval (see infra) is a combination of modules B and C.

Manufacturers remain responsible for products placed on the market, all procedures lead to CE marking.

5.1.2. Radio Equipment Directive (2014/53/EU)

'New Approach' Directive, aligned with the New Legislative Framework (Decision No 768/2008 /EC). It lays down the regulatory framework for making available radio equipment on the market. It ensures health and safety, electromagnetic compatibility and coexistence and interoperability.

The application of harmonized standards or other standards remains voluntary action and the manufacturer is always free to apply other technical specifications. The manufacturer is responsible for assessing the conformity of the product and is subject to a series of obligations, together with the economic operators.

The Directive provides three ways to assess the conformity with the essential requirements:

Radio equipment which is in conformity with harmonised standards published in the Official Journal of the European Union shall be presumed to be in conformity with the essential requirements of the Directive (Article 16). In this regard, a standardization request (536) has been addressed to ETSI and CENELEC and to prepare harmonized standards to support the Directive.

Where the manufacturer has not applied or has applied only in part harmonised standards, radio equipment shall be submitted with regard to those essential requirements to either of the following procedures (Article 17):

- EU-type examination that is followed by the conformity to type based on internal production control (Annex III),
- conformity based on full quality assurance (Annex IV).

Compliance with the harmonised standard ensures, in the case of C-ITS, an harmonised usage of the assigned 5.9 GHz ITS spectrum. However, it does not check the correct usage of the different bands of this frequency by the different applications, in particular between safety critical or non-critical applications.

5.1.3. Vehicle Type-Approval

Technical harmonisation in the EU is based on the Whole Vehicle Type-Approval System (WVTA)[2]. Under the WVTA, a manufacturer can obtain certification for a vehicle type in one EU country and market it EU-wide without further tests. The certification is issued by a type-approval authority and the tests are carried out by the designated technical services.

Directive 2007/46/EC sets out the safety and environmental requirements that motor vehicles have to comply with before being placed on the EU market. The Directive makes the EU-WVTA system mandatory for all categories of motor vehicles and their trailers. A large number of UNECE regulations are also made mandatory. These replace 38 Directives previously in force.

National approval authorities must send a copy of the vehicle type-approval certificate for each approved, refused, or withdrawn vehicle type to the approval authorities in other EU countries.

The Directive requires EU countries to take measures at two stages:

- before granting type-approval - the approval authority must verify that the type of vehicle complies with the safety and environmental requirements, and that production is in conformity with the rules;

---

[2] https://ec.europa.eu/growth/sectors/automotive/technical-harmonisation/eu_en

- after having granted type-approval - the approval authority must verify that the conformity of the manufacturer’s production arrangements continue to be adequate.

5.1.4. Common Criteria approach

Common Criteria (CC) for Information Technology Security Evaluation (ISO 15408) permits systems and devices to be evaluated against a specific Protection Profile (PP). The Protection Profile (PP) expresses an implementation-independent set of security objectives for a type or category of ICT product. It also specifies the security requirements and assurance measures which fulfil those objectives.

The CC defines different levels of evaluation called Evaluation Assurance Levels (EAL) from 1 to 7. The CC contains criteria to be used by evaluators when forming judgements about the conformance of systems and devices to their security requirements. The CC describes the set of general actions the evaluator is to carry out. Note that the CC does not specify procedures to be followed in carrying out those actions.

This CC approach is the basis for the evaluation and certification of the Digital Tachograph (see https://www.commoncriteriaportal.org/files/ppfiles/pp0057b_pdf.pdf for the vehicle unit, and https://www.commoncriteriaportal.org/files/ppfiles/pp0070b_pdf.pdf for the smart card).

5.1.5. Global Certification Framework (GCF)

GCF is a 3GPP Partner Organisation supported by mobile phone Operators, device Manufacturers and the Test Industry worldwide. Its aim is to ensure products (phones but also connected devices, IoT devices and M2M) are interoperable with Operator networks. It is a member-led and financed scheme (nearly 300 members from across the globe). ~ 500 certified devices per year.

It enables the mobile industry to define a common certification process for mobile devices implementing 3GPP radio access technology. GCF’s Test scope is agreed by its members in quarterly meetings.

GCF Certification is based on conformance, IOP and live network Field Trials.

Assessment Capable Entities (ACEs) have the competence to:

- Identify the range of tests required to certify a device.
- Assess the test results and determine if the device satisfies all the relevant certification criteria.

Manufacturers can use their own in-house ACE or may use the services of a third party ACE.

All testing in GCF must be performed by a Recognized Test Organization (RTO).

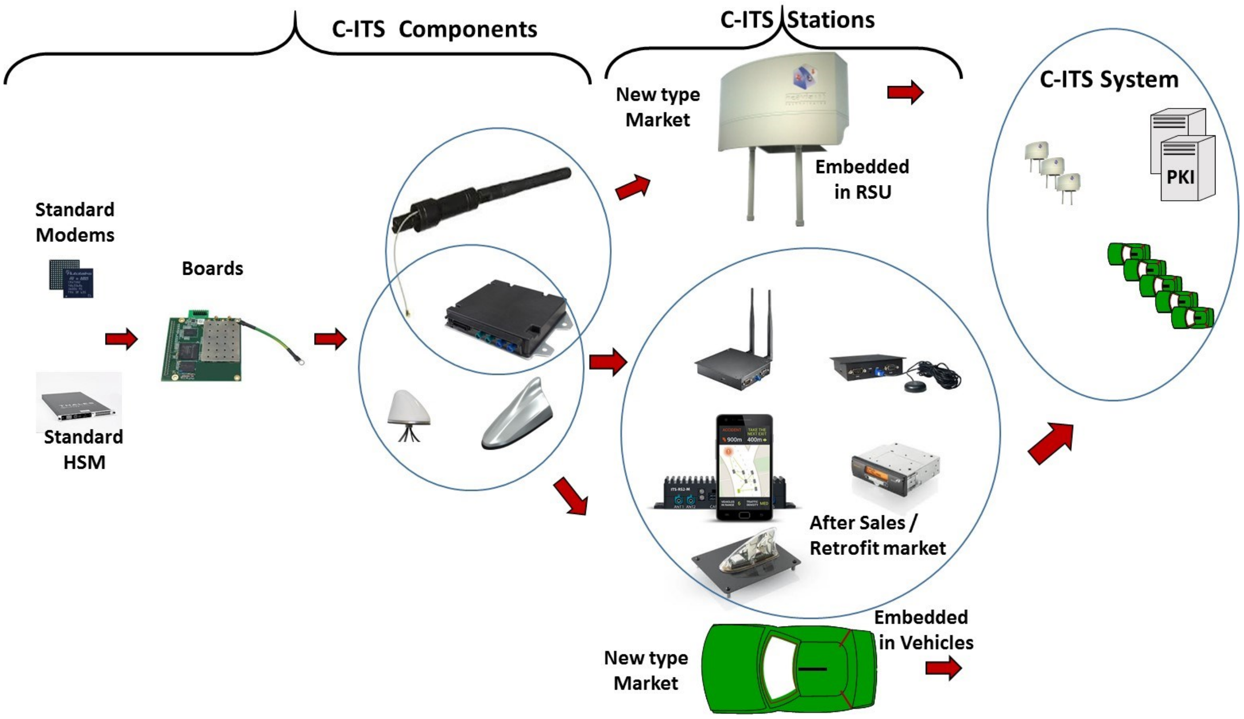
Manufacturers may use their own RTO or a Third Party RTO.

5.2. Legal framework for C-ITS

The upcoming legal framework for C-ITS has to ensure that there is a European legal basis for the C-ITS Governing Body and its sub-ordinates (Compliance assessment body, C-ITS Supervision body, etc.) to perform their functions as outlined in this document.

5.3. Compliance assessment process

The supply chain of a C-ITS system is summarized on the following figure:



Three levels can be distinguished:

- The C-ITS components starting with the provision of key integrated circuits (chips) such as C-ITS HSM (Hardware Security Module) and C-ITS modems which are then integrated in C-ITS boards (printed circuits) and then packaged in C-ITS units. Antennas, cables and HMI will be added to constitute a complete C-ITS Station.
- The C-ITS Station which can be sold on the after sales / retrofit market and be mounted by accredited agents in vehicles or road side units being already in-service. But, in most of the cases, the C-ITS Station will be directly embedded in new types of vehicles / RSU by OEMs.
- The complete C-ITS system which is composed of many C-ITS Stations which are cooperating and are supported by C-ITS servers especially for the system security management (PKI) and the delivery of customers' services.

The scope of the C-ITS Compliance Assessment process being described here below is only considering the C-ITS Station level including isolated C-ITS Stations for the after sales and retrofit, and C-ITS Station being embedded in vehicles and RSU.

However, this does not mean that C-ITS components and systems will not be validated, but their compliance assessment is out of the scope of the proposed organisation and is left to the private industries and Member States.

The following picture is based on the overview of the phase 1 proposed organisation at EU level supporting the compliance assessment process and its evolutions. This initial picture has been slightly changed to replace the word "certified" with "approved" and completed with the standards' profiles.

It is underlined that there will be a potential need for interim regime until "everything is perfect", in terms of criteria, test cases, organization, as deployment should start in a relatively short timeframe (2019). Moreover, there is a need for process to check if the enrolment of new services and/or new technologies has no bad interference with Day 1 services.

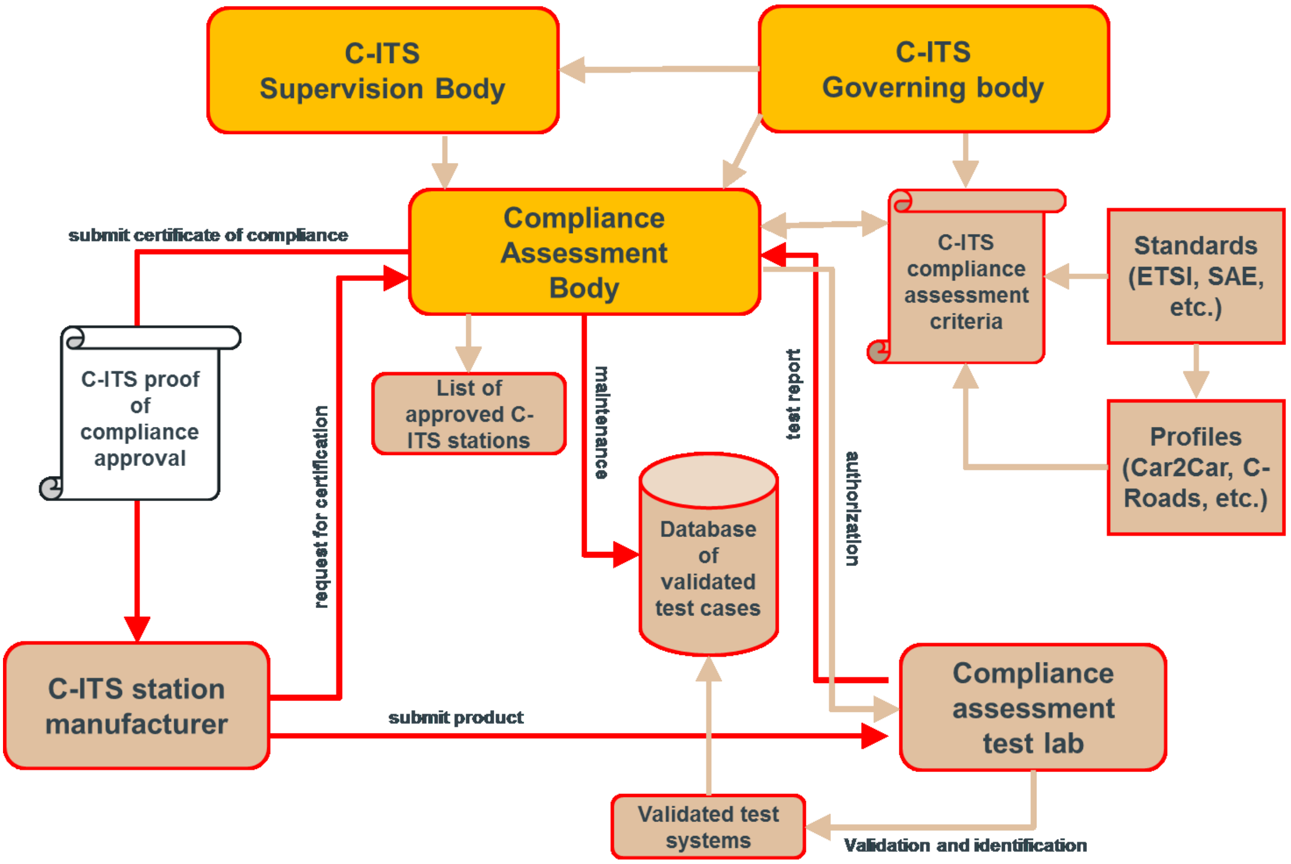

C-ITS Supervision Body
C-ITS Governing body
submit certificate of compliance
Compliance Assessment Body
C-ITS compliance assessment criteria
Standards (ETSI, SAE, etc.)
C-ITS proof of compliance approval
List of approved C-ITS stations
maintenance
test report
authorization
request for certification
Profiles (Car2Car, C-Roads, etc.)
Database of validated test cases
C-ITS station manufacturer
submit product
Compliance assessment test lab
Validated test systems
Validation and identification

Figure: overview of the compliance assessment process

Initially, a C-ITS Compliance Assessment Reference Framework is developed by the C-ITS Governing Body which is including all relevant C-ITS stakeholders. This reference framework includes:

- C-ITS assessment criteria which shall be used during the compliance assessment process by testing laboratories and other assessment organizations.
- C-ITS Reference Specifications, including basic and test standards, which shall be used during the different steps of the assessment process.
- C-ITS system profiles, which are the selections of particular options or parts of standards to be used.

This C-ITS Reference Framework shall be used by the Compliance assessment body and all compliance assessment labs and assessment environments as a reference for testing and assessing against it the conformity of C-ITS stations.

The C-ITS Governing Body shall manage the evolutions (change management process) of this compliance assessment reference framework so enabling necessary corrections (corrective maintenance) and evolutions (evolutive maintenance). Evolutions will be necessary for the inclusion of new technologies and new customers' services / applications. Agile and flexible organisation for quick corrective maintenance (minor corrections) will be paramount.

The C-ITS Governing Body shall then be able to update the C-ITS Compliance Assessment Reference Framework in such a way to maintain the interoperability of C-ITS legacy systems and so enabling a smooth migration of them toward new technologies / profiles / applications. Such evolutions will likely need some synchronised changes at the level of already operational systems.

With the objective of assisting the C-ITS Governing Body in preparation of important evolutions (technical, service-related etc.), some pilot projects could be started to provide validated initial reference C-ITS assessment criteria and specifications for an important evolution (e.g. new technology, new deployment phase applications).

If necessary, the C-ITS Governing Body may propose to the European Commission the initiation of a request for standardisation to European Standard Organisations for the development of missing standards.

Pilot project should also include the development of test systems and test cases to be validated by test laboratories and other compliance assessment organisation with the objective to be ready when a new version of the C-ITS Compliance Assessment Reference Framework is published.

As soon as a new version of the C-ITS Compliance Assessment Reference Framework is released and the required validated test system and test cases are available, the operational compliance assessment process for this new version can be started and then opened to C-ITS stations suppliers. The C-ITS Governing Body may decide on a transition period.

When a C-ITS station (e.g. vehicle, RSU…etc.) is ready for the validation against the released C-ITS compliance assessment reference framework, the manufacturer shall issue a request for compliance approval firstly to the Compliance Assessment Body and then select the necessary authorised test laboratories and assessment organisation which have the capability to cover all the required assessment criteria.

A supplier organisation may operate itself the required test / assessment if authorised.

C-ITS stations shall be provided to selected test labs and assessment organisations when a request for compliance approval is sent to the Compliance Assessment Body.

Each selected test lab, assessment organisation achieves the required tests / assessments accordingly to the C-ITS Compliance Assessment Reference Framework version consistent with supplier certification request.

Each selected test lab, assessment body sends to the Compliance Assessment Body its test / assessment report. A station can only be put on the market once this report is positive.

Once the Compliance Assessment Body has received all required test / assessment report, it shall analyse all the results and consolidate a global decision to deliver or not a certificate of compliance to the requesting supplier. In case of negative response of the Compliance Assessment Body, this one shall provide the rational for such a result and guidance for changing the result in an optimised way.

When the Compliance Assessment Body is delivering a C-ITS proof of compliance approval, the approved station is added in the list of C-ITS stations and the supplier shall ask to be part of the security framework.

The C-ITS Supervision Body shall be surveying the C-ITS deployment and market. It shall be maintaining some statistics on the deployment speed and collect incidents being reported by suppliers which products have been approved and deployed. It is responsible for the detection of problems in the deployment phase, which can be reported to C-ITS Governing Body and Compliance assessment body for further analysis and action.

The C-ITS Supervision Body shall be statistically monitoring the performance of deployed systems, especially in areas approaching saturation and in areas where new technologies, new applications are deployed.

5.4. Detailed Roles and responsibilities

This chapter lists the stakeholders involved in the different entities of the compliance assessment process, as well as the needs that a future organisation of these entities should fulfil. Future organisations involved in the process could play several roles. Any future organization should be defined in synergy with the organisation of the security part.

C-ITS Governing Body

The C-ITS Governing Body defines the requirements to the C-ITS Station, that fulfil the policy needs. The C-ITS Governing Body defines the operational and security requirements, which drive the definition of the compliance assessment test and procedures, which are coordinated by the Compliance Assessment Body, and defines rules (including conflict resolution process) for the resolution of issues detected by the C-ITS Supervision body. It is also its responsibility to maintain consistency with any other certification schemes.

Stakeholders:

European Commission

Member States

Infrastructure (road & communication) operators

Manufacturers and suppliers

Organisational needs:

European organisation.

Formal decision is needed to set it up and to define its main tasks (including the right to set compliance assessment criteria).

Steering board for decision-making.

Need for experts sub-groups e.g. to draft compliance assessment criteria.

Should be combined with the policy authority from the security part, and potentially with data protection part.

Compliance Assessment body

The central operational body in the compliance assessment process, it oversees the overall process, and manages the day to day Compliance Assessment operation. It defines the governing rules and procedures for the compliance assessment tests and procedures. It issues the C-ITS proof of compliance approval. It maintains the list of approved C-ITS stations.

Stakeholders:

C-ITS Governing Body ("owner" of the process)

Test houses

Notified bodies

Organisational needs:

Centralised functions: list of approved stations, list of validated test cases (including validation rules)

Daily operation could be decentralised.

C-ITS Supervision Body

The C-ITS Supervision Body is responsible for the detection of problems in the deployment and operational phase, which can be reported to the C-ITS Governing Body and to the Compliance Assessment Body for further analysis and action, on the basis of rules defined by the C-ITS Governing Body. This requires a hierarchical organisation to be able to solve issues at appropriate level and/or report them to the appropriate level.

Stakeholders:

European Commission

Member States

Infrastructure operators

Manufacturers and suppliers

Organisational needs:

Central supervision board (EU wide)

National supervision boards

Industry supervision board(s) e.g. for vehicles

Standardisation bodies

Responsible for drafting the standards for communication and testing.

Stakeholders:

ETSI, CEN/ISO, IEEE, SAE

European Commission (for possible mandates)

Organisational needs:

Already existing

European profiles managers

Define communication profiles and test specifications. Propose profiles to the C-ITS Governing Body which decides to take them on board.

Stakeholders:

Car2Car (vehicle OEMs)

C-Roads (infrastructure operators)

Organisational needs:

Existing

Compliance assessment test labs

Execute the compliance assessment tests and procedures.

Stakeholders:

Independent test houses

Manufacturers (In-house labs for self-testing)

Organisational needs:

Already existing

The following roles have been identified as related to security aspects, and should be confirmed and defined by the security WG. Once this is done, both organisations have to be integrated, in order to avoid repetition of similar organisation parts.

Enrolment authority

This entity is responsible to perform the enrolment of a C-ITS station based on a positive test outcome of a compliance assessment test lab. The enrolment is related to the recording of the ID and features of a C-ITS station before deployment in the field.

Stakeholders:

To be defined by WG security

Organisational needs:

To be defined by WG security

Authorisation authority

This entity is authorized to perform the authorization of a C-ITS station. This is a security function in comparison to the enrolment authority, which is specific to the recording of the ID and features of a C-ITS station before deployment in the road.

Stakeholders:

To be defined by WG security

Organisational needs:

To be defined by WG security

Trust model manager

To be defined by WG security.

Stakeholders:

To be defined by WG security

Organisational needs:

To be defined by WG security

----

6. Guidelines to compliance assessment

As a general principle, the compliance assessment process can only check what is defined in reference specifications and standards, therefore its scope may be limited initially to requirements relating to existing standards, without precluding additional requirements as soon as standards are made available. As the requirements are also based on the profiling of set of standards (such as the C-Roads Harmonised communication profiling for C-ITS pilot services across Europe), there is a need to formalize these profiles.

6.1. Compliance Assessment process requirements

The purpose of the compliance assessment process detailed in this document is to support the achievement of key public policy goals. The overall goal of the C-ITS platform is to accelerate the deployment of interoperable C-ITS in the EU. The key aspects for a technical framework to achieve these goals have been described in the results of the first phase of the C-ITS platform, and are summarized below:

1. Support for Day-1 services. Also, a list of Day 1'5 services have been defined that are highly desired by the market, for which reference specifications or standards might not be completely ready (this issue is also valid for applications beyond Day 1,5)
2. Realize one common standardised C-ITS trust model and certificate policy all over the EU, based on a Public Key Infrastructure (PKI) and defined in an appropriate regulatory framework, shall be urgently deployed to support full secure interoperability of C-ITS Day 1 services at the European level.
3. a hybrid communication concept is needed in order to take advantage of complementary technologies. It is therefore essential to ensure that C-ITS messages can be transmitted independently from the

underlying communications technology (access-layer agnostic) wherever possible. The first communication standards have been validated for ITS-G5 ad-hoc networks, similar validation work still remains to be done for other technologies. For short-range communications in the 5.9 GHz band initially the communication system currently available is IEEE802.11p/ETSI ITS-G5. It is to be studied whether geographical coverage obligations can be introduced to increase coverage of C-ITS services through existing cellular communications infrastructure.

4. Standards being used within current C-ITS deployment initiatives are a starting point to discuss how profiles can and have to be defined for EU-wide deployment. This includes also the standard for DCC.
5. A set of five guiding principles that shall apply when granting access to in-vehicle data and resources was agreed upon and served as a basis for all agreements and discussions.

These aspects can be translated into key requirements for the conformance assessment process

1. The CA process is explicitly seen in the scope of the common standardised C-ITS trust model. It should be **sufficient** for any device or system to pass the CA process successfully to be granted access to the technical implementation of the trust model. That means that the CA process should cover all requirements necessary to be granted access to the PKI infrastructure. Note, however, that this does not make any statement on how compliance with those requirements should be proven: that needs to be defined in detail based on those requirements as part of the definition of the compliance assessment process.
2. Vice versa, it should also be **necessary** for any device or system to pass the CA process successfully to be granted access to the technical implementation of the trust model. It should not be possible to be granted access to the PKI infrastructure if the CA process has not been completed successfully. This will require well defined procedures on how to handle cases where systems *do* fulfil all requirements, but cannot pass the implementation of the test cases due to (technical) reasons. This could for example be caused by assumptions on the implementation of systems in the design of the test cases, which are not required and not fulfilled by specific devices.
3. The scope of the CA process should be day-1 services based on standards currently being used in deployment initiatives in Europe, but should already take into account that more services will be included in the process in the (near) future.
4. IEEE802.11p/ETSI ITS-G5 should be covered by the compliance assessment process. However, other communication technologies, such as cellular communication, should also be taken into account. Where possible, test cases should be defined technology agnostic as much as possible.
5. The CA process should ensure interoperability of systems that have passed the CA process successfully. However, the requirement for interoperable systems should not be interpreted as only being limited to technical interoperability on the protocol level. It should also be interpreted on the application level, where it can be interpreted as a requirement on the usability of the information being exchanged. This means that the CA process should also assess the correctness (i.e. timeliness, completeness, accuracy, reliability, etc.) of all information being exchanged.
6. The goal of accelerating the deployment of systems means that the CA process should also be efficient. A balance need to be found between completeness of the process to fulfil the first 5 requirements, and the time and costs it will require to complete the detailing of the process, the definition and implementation of test cases and test setups, and finally the time and costs related to the actual execution of the process for a specific implementation of a C-ITS device.

The different requirements are to some extend at odds with each other. The most obvious is the balance that needs to be found between the completeness of the test cases that will be part of the CA process, and the costs and time related to the definition, implementation and execution of them.

Also requirement 1 and 2 (sufficient and necessary to be granted access to the PKI) are at odds with requirement 5 (interoperability). Requirement 1 and 2 will make it necessary that the CA process can be completed by a single device (which is common in most compliance assessment schemes), and cannot be based on interoperability tests of multiple systems. This is also recognized e.g. in the plug tests organized by ETSI, where the interoperability tests and conformity tests are treated separately: the interoperability tests are executed with devices from multiple vendors combined, whereas the conformity tests are executed based on separate test cases, against a test system. Interoperability tests of a single device under test and a reference implementation can be seen to some extend as a conformance assessment. Note, however, that implementations aimed at deployment are commonly implemented with resilience against implementation errors of the systems from which information is received. Therefore, if such implementations are used as reference systems, they do not guarantee conformity of the system under test if interoperability tests are passed successfully. However, even if full reference specifications conformance is proven based on dedicated conformity tests, that does not guarantee interoperability if the reference specifications itself do not guarantee interoperability. Standards in general contain options and/or do not give a full system specification, and therefore do not guarantee interoperability. Therefore, additional profiling is required to limit interoperability issues, but even than it does not guarantee interoperability. Therefore both standards conformance testing and interoperability assessment are required.

6.2. Architectural scope

The conformance assessment process is limited to C-ITS stations. C-ITS stations are defined as devices or systems that implement the C-ITS reference architecture, as defined by ETSI and ISO [ref]. A high level overview is given in the figure below:

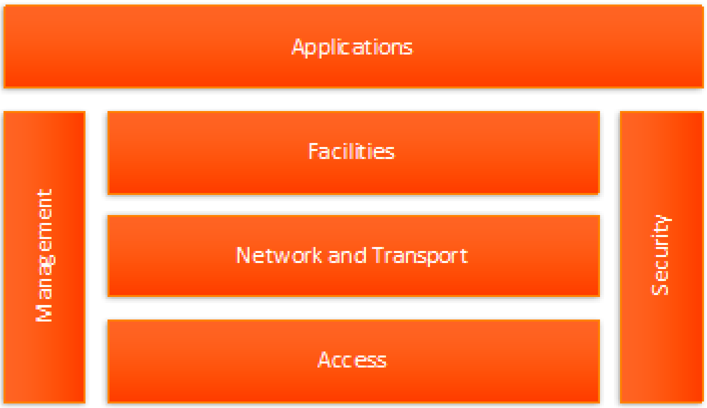


Figure: High level functional architecture of a C-ITS reference station.

The requirements and CA test cases will be structured based on this architecture. This facilitates easy linking to existing standards and test cases, which are also based on this structure. In addition to requirements and test cases relating to these functional building blocks, also requirements and test cases will be defined that related to the system as a whole.

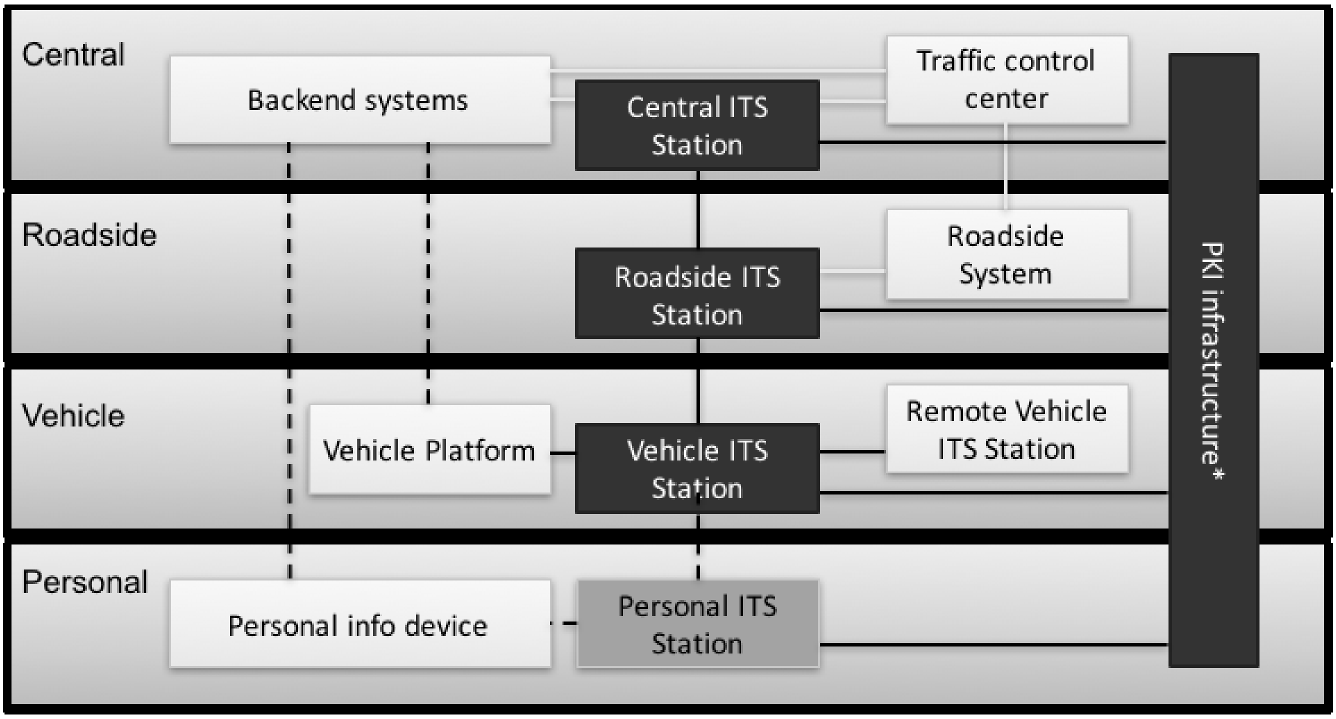


*Figure: General system overview for C-ITS. Black blocks and lines are part of the conformance assessment process, white boxes and lines are out of scope. Grey boxes and dashed lines are currently out of scope, but could be added in the future. *The exact scope of the PKI infrastructure is described by the Security WG.*

An informative overview of the overall system architecture for C-ITS is presented in the figure above. This overview is only included to facilitate the description of the scope of the conformance assessment process. Some details are left out, and not all possible implementation solutions are covered. In this overview, four different components implement the C-ITS Station reference architecture: Central, Roadside, Vehicle, and Personal C-ITS Station. The vehicle C-ITS Station specifies the cooperative functionality in the vehicle. This function obtains its (sensor) information from the Vehicle platform, and uses the HMI of the Vehicle system to interact with the driver. The Vehicle C-ITS station in another vehicle is indicated as Remove Vehicle system. The roadside C-ITS Station obtains its information from either Roadside system like loop detectors or traffic light controllers, or via a Central C-ITS Station from a Traffic control centre or backend systems from service providers. In current implementations, the R-ITS Station and V-ITS station implement the ETSI Geonetworking/BTP and ITS G5 protocol, in addition to facilities and application layer functionality. The Central C-ITS Station in general do not implement the Geonetworking/BTP and/or ITS G5 protocol stack, but use other network and access layer technologies to communicate with the roadside systems.

In current implementations, also cellular communication is used to communicate with vehicles, or personal devices (smartphones, personal navigation devices, etc.) Cellular communication is also included in the C-ITS Reference station, so could also be used for the communication between the C-ITS Stations and or the C-ITS station and other components. However, no standardized communication profile exists yet (ongoing work at ETSI to define a communication profile for cellular networks (ETSI Work Item DTS/ITS-00135)**,** and therefor this has been left out of the conformance assessment for the time being. Also personal C-ITS Stations are not specified in detail, and are currently out of scope of the conformance assessment.

The main focus of the conformance assessment is on the interfaces between the V-ITS Station and V-ITS Station, and on the interface between vehicle C-ITS Station and roadside C-ITS Station. However, the correctness of the information being transmitted by those C-ITS Station is largely determined by the input from the Vehicle platform or Roadside systems/Traffic control centre, respectively. For the V-ITS system, it is therefore proposed to include the Vehicle Platform as part of the conformance assessment, at least where it influences the correctness of the information. In practise, this means that the conformance assessment of the information contents needs to be done in a real or reference vehicle context.

Also for the roadside C-ITS Station this argument is valid. However, it is deemed the responsibility of a road operator to ensure correctness of the information transmitted, and therefore is considered out of scope for the conformance assessment. For example, it is not considered part of the conformance assessment of a R-ITS Station to validate the correctness of the output of a traffic light controller, whereas it is considered as part of the conformance assessment to validate the accuracy of the position of a vehicle, as used in the various cooperative messages and in the geo-networking protocol.

6.3. Technology agnostic conformance assessment

The conformance assessment should be implemented agnostic of the specific technology as much as possible. This improves the reusability of the test reference specifications in case of changes in or extensions of the reference specifications. Furthermore, it can improve (cost) effectiveness of the whole CA process, because a smaller number of variants of test cases need to be defined, implemented, and executed. On the other hand, it is preferable to implement the test cases such, that the device under test can be treated as a black box, meaning that no modifications to a production system need to be made to use it for the conformance process. That means that the test cases can only make use of the standardized interface protocols, which are always technology specific. This leads to the following principles for the definition of the conformance assessment process:

- At the highest level of abstraction, generic, technology agnostic requirements need to be defined. These will help as a guide to define the technology dependent requirements. Furthermore, these can be used when other technologies are added to the conformance assessment. Requirements at this level should include e.g. a requirement to adhere to all relevant legal requirements, to adhere to applicable standards, and to make use of radio resources effectively. No actual testing is done against these requirements, but they can be considered as a basis for the detailed requirements, and corresponding test cases.
- At the next stage, the high level requirements are translated into concrete technical requirements. Although these will be technology specific, by defining them focussed on the layers in the C-ITS Station reference architecture, they can be defined independent of the other components. It is expected that in addition to the requirements that can be attributed to a specific layer, also overall system requirements will exist.
- The actual conformance assessment will be done by defining test cases based on the technical requirements. To allow black box testing, these test cases will have to be defined based on the interfaces that are expected for the systems under test. As long as those interfaces are part of the (required) reference specifications, that is not an issue. For example, if Geo-networking/BTP over ITS-G5 is required for every C-ITS Station, then this interface (upper tester) can be used (after being conformance assessed) to assess the correctness of the facilities layer (e.g. message formats and information contents). However, if no standardized interface definition exists, this makes it more difficult to define a black box testing methodology. If de-facto standard interfaces are used (e.g. GNSS signals as part of the positioning subsystem), then it is still possible to define black box test cases for, as

long as solutions are also provided for systems that do not implement those de-facto standard interfaces.

As discussed in the previous section, different types of C-ITS Stations exist. Part of the reference specifications is identical for different types of C-ITS Stations. This fact will be used to define test cases independent for the type of C-ITS Station. Typical examples are the Geonetworking specifications that are identical for vehicle and roadside C-ITS Stations, and the message definitions. Note, however, that for the message definitions, some messages are only transmitted by R-ITS Stations (MAP, SPAT, IVI), and only received by V-ITS Stations. So although the messages are the same for both stations, a minimal conformance assessment process could limit the conformance testing to only encoding or only decoding of those messages, respectively. Especially on the application layer, the different C-ITS Stations are expected to implement different reference specifications, and therefore the test cases will need to be defined separately for the different C-ITS Stations.

In summary, high level requirements need to be defined in a technology agnostic way, and further detailed based on specific technologies. Requirements for a specific layer should be defined agnostic of technologies used on other layers, and further converted into test cases. Black box testing is preferred, but does require technology dependent implementations. This needs special attentions if interfaces required for testing are not fully specified. Furthermore, requirements and test cases are made C-ITS Station variant agnostic, if possible.

7. Interoperability and minimum performance of C-ITS Systems

The elements in this chapter apply to mature technologies which has been already tested and validated for a long time in many European research projects, FOTs and pre-deployment projects, and for which profiles of standards are being adopted. Now, for the start-up phase of C-ITS in Europe on first infrastructure networks and in vehicle stations further steps are needed to validate the compliance of new C-ITS stations in regular traffic operating environments for all “day one applications” at infrastructure and at vehicle side. This is the reason to define the minimum requirements for all C-ITS stations and their data communication in the following chapter, and elaborate the first future steps in the direction of a full-fledged C-ITS certification scheme later in this report. The complete elaboration of the certification scheme needs to take into account the main stakeholder views of the C-ITS network, the roadside operators and public authorities and the vehicle manufacturers and mobile station operators.

7.1. Minimum requirements for conformance and performance

7.1.1. Physical and Access layer

Minimum requirements should be based on following standards:

EN 302 571 v2.1.1[3] Intelligent Transport Systems (ITS); Radiocommunications equipment operating in the 5 855 MHz to 5 925 MHz frequency band; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU

This harmonized standard covers the requirements of the ECC Decision (08)01 and recommendations (08)01 for using the 5.9 GHz frequency band. All ITS-Stations using the ITS-G5 frequency bands are required to comply

---

[3] Published in the OJEU on 8 June 2017 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=uriserv:OJ.C_.2017.180.01.0005.01.ENG

with this document which provides definitions, limits and equipment tests, thus ensuring that these stations comply with the Radio Equipment Directive for this frequency spectrum.

This harmonized standard covers also the mitigation to avoid of interfering with tolling[4].

ETSI TS 102 792 v1.2.1 Intelligent Transport Systems (ITS); Mitigation techniques to avoid interference between European CEN Dedicated Short Range Communication (CEN DSRC) equipment and Intelligent Transport Systems (ITS) operating in the 5 GHz frequency range

This technical specification provides various mitigation techniques which are to be employed between ITS equipment and CEN DSRC station (Tolling-Systems). The usage of mitigation is a mandatory requirement for using the ITS-G5 frequency bands and this document is normatively referenced by the EN 302 571 and required by the ECC Decision (08)01.

EN 302 663 v1.2.1 (2013-07), Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band

This European norm provides the necessary information on the access layer configuration of ITS-Stations using the 5.9 GHz frequency bands in Europe. In order to enable inter-operability between all ITS-Stations active in the same frequency bands, it is of utmost importance that the same configuration of the access layer is used, as specified in this document. Access layer specification for Intelligent Transport Systems operating in the 5.9 GHz frequency band has fixed the bands to use for communications.

ETSI TS 102 687 v1.1.1 Intelligent Transport Systems (ITS); Decentralized Congestion Control Mechanisms for Intelligent Transport Systems operating in the 5 GHz range; Access layer part

This technical specification provides the guidelines for the De-Centralized Congestion Control (DCC) mechanism which enables every ITS-Station using the 5.9 GHz frequency bands to get a fair usage of the spectrum. The DCC mechanism shall be implemented by all ITS-Stations in order to prevent an irrational usage of the communication resources and considerable reduce the number of packed errors due to collisions.

TS 102 724 v1.1.1 Intelligent Transport Systems (ITS); Harmonized Channel Specifications for Intelligent Transport Systems operating in the 5 GHz frequency band

This technical specification provides additional information on how the DCC concepts are to be applied over all ITS-G5 channels defined inside the 5.9 GHz spectrum in order to maximize the performance of the ITS-Stations and prevent or minimize any congestion on the communication channels.

7.1.2. Networking

An ITS-station should respect the geo-networking protocol standard specified on the document EN 302 636 (part 1 to part 6). Part 1 defines the requirements to be fulfilled by any ITS-station.

Geo-Networking basically provides two, strongly coupled functions:

- geographical addressing: The ability to identify each station
- geographical forwarding: The ability to transfer packet from a node to another node or to a specific

---

[4] C-ITS applications and protection of tolling station
CEN DSRC (not to be confused with the USA DSRC), being used at the level of tolling stations for Electronic Toll Collection, has been deployed before the assignment of the C-ITS band (5.875 – 5.905 Gigahertz) by the European Commission. The CEN DSRC tolling band is around 5.8 Gigahertz and some experts are considering that it exists some risk of interference between these two bands in spite of a large gap of more than 100 megahertz between them. This risk is due to the fact that, for economical reasons, some CEN DSRC equipment are not staying in the CEN DSRC assigned frequency band and so could be disturbed by C-ITS broadcasting especially when the density of equipped vehicles will become important.
Taking into account this concern from road operators, ETSI has been developing a standard specification (TS 102792) describing several mitigation technics reducing drastically this risk of interference. It is then recommended to V C-ITS S to adopt at least one of these mitigation technic when approaching a tolling station which may be signalled by various means.

area through some intermediate node.

The conformance testing of such a protocol is described in the following document:
ETSI TS 102 871 Conformance test specifications for Geo-Networking ITS-G5 (revision on-going at ETSI to address remaining issues such as listed below).

GN Scenarios are planned in these test cases. The conformance testing is run in laboratories but geo-networking has to forward packets from the source station to a destination station which could be outside of the radio range of the source node. Then the forwarding process should be handled properly. But when these test cases are run in a laboratory, the nodes are in the same radio range. The effective testing of forwarding could not be checked without any additional conditions our specific material (Faraday boxes to reduce radio propagation).
The actual test cases for geo-networking are not able to test some part of the behaviour of the networking layer into the ITS protocol stack. For this reason, if one needs to guarantee a correct behaviour of geo-networking of a C-ITS station, test field testing as well as open road testing are needed. In addition to these flaws, geo-networking could have some troubles when a greedy forwarding is launched to reach the next closest station to the destination. Indeed, if the selected one from the station neighbours has moved and is not reachable, the message will not be delivered.

Another sensitive issue is about the forwarding algorithms to use. Three algorithms could be used:

- Simple forwarding algorithm (SIMPLE)
- Contention based forwarding algorithm (CBF)
- Advanced forwarding algorithm (ADVANCED)

The interoperability of these three protocols is quite sensitive. If fact in a network if a node can only use a SIMPLE forwarding algorithm and other nodes use an algorithm different from the SIMPLE one, then all other nodes cannot take advantage of their algorithm since they will behave as a SIMPLE one.

7.1.3. Facilities
(Adherence to communication standards/protocols)

The basic standards for testing communication capabilities in C-ITS stations are defined in ETSI for the following aspects:

<u>For communication access in ITS G5</u>

List of services CAM, DENM; SPAT MAP, IVI and standards

EN 302 637-2 v1.3.2 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service

This European norm provides the specification of the Cooperative Awareness Basic Service, the first ITS service mandatory for all ITS-Stations. The structure of Cooperative Awareness Messages (CAMs) is provided, the quality requirements of the data elements as well as the message generation rules. Inside this document the interfaces and SAPs required for communication with the other layers of the ITS protocol stack are also described.

EN 302 637-3 v1.2.2 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service

This European norm provides the specification of the Decentralized Environmental Notification Basic Service, the second ITS service mandatory for all ITS-Stations. The structures of various Decentralized Event Notification

Messages (DENMs) are provided as well as the quality requirements of the data elements. Inside this document the interfaces and SAPs required for communication with the other layers of the ITS protocol stack are also described.

ETSI TS 103 301 v1.1.1 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services

This European specification provides the specification of the various infrastructure oriented C-ITS services. The structures and generation rules for different messages, like Signal Phase And Time (SPAT), Topology (MAP) and In-Vehicle Information (IVI) are provided, as well as mechanism detailing how these messages can use the ITS-G5 communication stack.

ETSI TS 102 894 – 2 V1.2.1 Intelligent Transport Systems (ITS); Users and applications requirements; Part2: Applications and facilities layer common data dictionary.

This technical specification provides the structure and definition of the various data elements used by the Cooperative Awareness and Decentralized Environmental Notification Basic Services and it is therefore required in conjunction with the previous two European norms.

Test suite for CAM, DENM, SPAT, MAP, IVI

ETSI TS 102 868-1/2/3 Conformance test specification for Co-operative Awareness Messages (CAM)

ETSI TS 102 869-1/2/3 Conformance test specification for Decentralized Environmental Notification Messages (DENM)

ETSI TS 103 191-1/2/3 Conformance test specifications for Signal Phase And Timing (SPAT) and Map (MAP)

For Networking: GeoNetworking

ETSI TS 102 859 Conformance test specifications for Transmission of IP packets over GeoNetworking (GN6)

ETSI TS 102 870 Conformance test specifications for GeoNetworking Basic Transport Protocol (BTP)

ETSI TS 102 871 Conformance test specifications for GeoNetworking ITS-G5 (GN)

For the application profiles: ETSI/CEN Message definitions and

For the selection of standard sets of release one

7.1.4. Applications

List of application requirements standards being applicable:

ETSI TR 102965 v1.1.1. Intelligent Transport Systems (ITS); Application Object Identifier (ITS – AID); Registration list.

ETSI TS 101539-1 v1.1.1 Intelligent Transport Systems (ITS); V2X Applications; Part 1: Road Hazard Signalling (RHS) application requirements.

ISO TS 17425 Intelligent transport systems – Cooperative ITS – Data exchange specification for in-vehicle presentation of external road and traffic related data.

ISO TS 17426 Intelligent transport systems (ITS) – Cooperative ITS – Contextual speeds.

On the application layer in C-ITS, many parts could be implemented. But for effective deployment of Road Hazard Signalling, we should first focus on the verification of triggering conditions which are mainly automatic. The second part deals with manual data send by drivers. In order to take in consideration these data, data quality should be evaluated in order to know if the data is serious enough to be considered by receiving C-ITS station.

(a) triggering conditions

A mobile ITS-station is able to send automatically messages triggered by the vehicle if some conditions are satisfied. These conditions are denoted “triggering conditions” which are mainly defined by the C2C (Car to Car consortium) as a part of the C2C-CC Basic system Profile.

On a C-ITS station, it is required to check if these triggering conditions are properly implemented. Two stages to do so:

- Stage 1: Check if the station is able to send the appropriate message when the conditions are satisfied. This issue is achieved by extending the ETSI upper tester with the required primitives. This part is done only with the computing unit (CU) of the ITS.

- Stage 2: Check if the rules defining a combination of conditions are respected for the triggering of the standard message broadcasting by ITS-CU, this last one provides the appropriate automatic message.

(b) quality of data

Addressed in chapter 8. End to end service test´s - Quality of service assessment

7.1.5. Cross-applications interaction and possible consequences for testing and validation

For Day 1 applications, the interaction is limited, and consequences are deemed not to be critical. This will need more investigation for Day 2 applications

7.1.6. Particular requirements for roadside C-ITS stations

Application Profile: sending specific roadside messages and/or receiving specific vehicle messages

Vehicle Probe data application:

A compliant Roadside C-ITS Station shall be capable of receiving and decoding standard messages (CAM and DENM) broadcasted by Vehicle C-ITS Stations via the standard communication and security profiles retained for C-ITS phase 1 deployment. This Roadside C-ITS station shall be capable of using collected standard messages for providing safety and traffic information to road users. However, it is left to the road operator to decide if the collected data can be immediately used by Roadside Units to inform road user or, if in the contrary, these collected data shall be forwarded to a traffic management centre for consolidation before being used to inform road users.

Road Hazard Signalling application:

A compliant Roadside C-ITS Station shall be capable of signalling consolidated (high level of confidence) road hazard such as: -roadwork, stationary vehicles (breakdown or accident), traffic jam ahead, hazardous location, bad weather condition. For this purpose, the roadside unit shall broadcast standard DENM messages associated to C-ITS standard communication and security profiles selected for C-ITS phase 1 deployment. A Roadside C-ITS Station can be fixed, movable or mobile. DENM messages shall indicate the dissemination area and the relevance area.

Particular case: Shockwave Damping application:

A compliant Roadside C-ITS Station shall be capable of transmitting standard IVI messages containing speed advice data targeting the prevention and/or mitigation of shockwave traffic jams. The certificate used to sign these messages by the Roadside C-ITS Station shall allow C-ITS Stations to identify and authenticate these messages as being transmitted on behalf by the responsible road operator. For the IVI transmission purpose, the Roadside C-ITS Station shall be capable of managing standard C-ITS communication and security profiles selected for C-ITS phase 1 deployment.

In-Vehicle signage application:

A compliant Roadside C-ITS Station shall be capable of providing safety and traffic information using variable message signs (VMS). For this purpose, the roadside unit shall broadcast standard IVI messages associated to C-ITS standard communication and security profiles selected for C-ITS phase 1 deployment.

In-Vehicle speed limits application:

A compliant Roadside C-ITS Station shall be capable of providing contextual and permanent speed limits applicable in identified relevant areas. For this purpose, the roadside unit shall broadcast with a high level of confidence standard IVI messages conform to contextual speed application requirements. IVI messages shall be broadcasted using C-ITS standard communication and security profiles selected for C-ITS phase 1 deployment.

Green Light Optimal Speed Advisory (GLOSA) application:

A compliant Roadside C-ITS Station associated to a traffic light shall be capable of providing Signal Phase & Timing (SPAT) and MAP (map of the area controlled by the traffic light) enabling the standard Vehicle C-ITS Station to adapt dynamically their speed with the objective to cross synchronized traffic lights when being green without having to change abruptly their speeds. For this purpose, the roadside unit shall broadcast SPAT & MAP standard messages using C-ITS communication and security profiles selected for C-ITS phase 1 deployment.

Signal Violation at intersection application:

A compliant Roadside C-ITS Station shall have the capability to detect a signal violation and signal it to others vehicle C-ITS Stations moving near the intersection. For this purpose, the roadside unit shall broadcast standard DENM messages associated to C-ITS standard communication and security profiles selected for C-ITS phase 1 deployment. The detection of a signal violation can be achieved by the Roadside unit either following the reception of CAM messages (position of the vehicle and its velocity) from standard C-ITS vehicles or by the use of sensors (e.g. radars) able to detect a signal violation from non-C-ITS standard vehicles.

Vehicle priority application:

A compliant Roadside C-ITS Station shall have the capability to analyse received CAM messages with the objective to identify priority vehicles (emergency vehicles in activity, public transport in activity…etc.). According to local operator policy and consecutive to the detection of a priority vehicle, the Roadside unit may have the capability to act on the traffic lights to give priority to detected vehicles. For this purpose, the Roadside unit shall have the capability to decode CAM messages associated to C-ITS communication and security profiles selected for C-ITS phase 1 deployment.

7.1.7. Particular requirements for vehicle C-ITS stations

Application Profile: sending specific vehicle messages and/or receiving specific roadside messages

Road Hazard Signalling application:

A compliant Vehicle C-ITS Station shall be capable of signalling to others Vehicle C-ITS Stations detected road hazard and be capable of signalling to its driver received road hazard signalling. The road hazards which shall be detected and signalled are: - Emergency Electronic Brake Light, emergency vehicle approaching, slow/stationary vehicles (breakdown or accident), traffic jam ahead, hazardous location, bad weather condition. For this purpose, the Vehicle C-ITS Station shall be capable to broadcast triggered standard DENM messages associated to C-ITS standard communication and security profiles selected for phase 1 deployment. A compliant Vehicle C-ITS Station shall also be capable of receiving standard DENM messages associated to communication and security profiles selected for C-ITS phase 1 deployment. Compliant receiving Vehicle C-ITS Stations shall have the capability to check the relevance of received standard data with the objective to minimize false positive and false negative information provided to drivers.

Particular case: Shockwave Damping application:

A compliant Vehicle C-ITS Station shall be capable of receiving standard IVI messages containing speed advice data targeting the prevention and/or mitigation of shockwave traffic jams. Then, it shall be capable of verifying the relevance of data (relevance check) and assess the safety situation, before signalling a speed advise to the driver. For the IVI reception purpose, the Vehicle C-ITS Station shall be capable of managing standard C-ITS communication and security profiles selected for C-ITS phase 1 deployment.

Roadwork warning application:

A compliant Vehicle C-ITS Station shall be capable of receiving and processing standard DENM messages signalling a roadwork. Then it shall be capable of verifying the relevance of data (relevance check) before signalling this event to the driver. For the DENM reception purpose, the Vehicle C-ITS Station shall be capable of managing standard C-ITS communication and security profiles selected for C-ITS phase 1 deployment.

In-Vehicle Signage application:

A compliant Vehicle C-TS Station shall be capable of receiving and processing standard IVI messages transporting In-Vehicle Signage data. Then it shall be capable of checking the relevance of received data before providing the information to the driver. For the IVI reception purpose, the Vehicle C-ITS Station shall be capable of managing standard C-ITS communication and security profiles selected for C-ITS phase 1 deployment.

In-Vehicle Speed Limit application:

A compliant Vehicle C-ITS Station shall be capable of receiving and processing standard IVI messages providing contextual or permanent speed limits. Then it shall be capable of checking the relevance of received data relative to its trajectory and speed before providing the information to the driver or acting on the speed regulator. For the IVI reception purpose, the vehicle C-ITS Station shall be capable of managing standard C-ITS communication and security profiles selected for C-ITS phase 1 deployment.

Green Light Optimal Speed Advisory (GLOSA):

A compliant Vehicle C-ITS Station shall be capable of receiving and processing standard SPAT and MAP messages with the objective to provide to the driver the optimal speed to follow to pass all traffic lights at green without abrupt changes of speed. For this purpose, the Vehicle C-ITS Station shall be capable to manage C-ITS standard communication and security profiles selected for C-ITS phase 1 deployment.

Signal Violation at intersection application:

A compliant Vehicle C-ITS Station shall have the capability to detect that is will be violating a signal and then signal it to others Vehicle C-ITS Stations moving near the intersection. For this purpose, compliant Vehicle C-ITS Stations shall be capable to broadcast and receive standard DENM messages associated to C-ITS standard communication and security profiles selected for C-ITS phase 1 deployment. The relevance of a signal violation warning received in a standard DENM message shall be checked before presentation to the driver. According to the criticality of the situation, upon decision of the OEM, an alert can be provided to the driver or an emergency brake can be triggered.

7.2. Compliance assessment methodology

ITS Station device testing, based on ETSI CA test cases (NOT Interop testing)

ETSI (standards, test specs), CEN/ISO

End to end test for day one applications

The general compliance assessment methodology is represented on the figure here below.

- Conformance to product specification can be, in large part, achieved in test laboratories. Product specification shall include the identification of C-ITS standard communication, security and application profiles applicable to each application which are supporting C-ITS phase 1 deployment. So the standard conformance testing and interoperability testing can be achieved in reference to ETSI C-ITS plug tests.
- Performance of C-ITS system shall be tested in close environment between implemented C-ITS Stations (Vehicles, Roadside unit, Central (PKI) station) before being assessed in open environment. This performance testing includes the radio system (G5) performances (minimum radio coverage, PER, EMI…etc.) for each complete system under test (SUT).

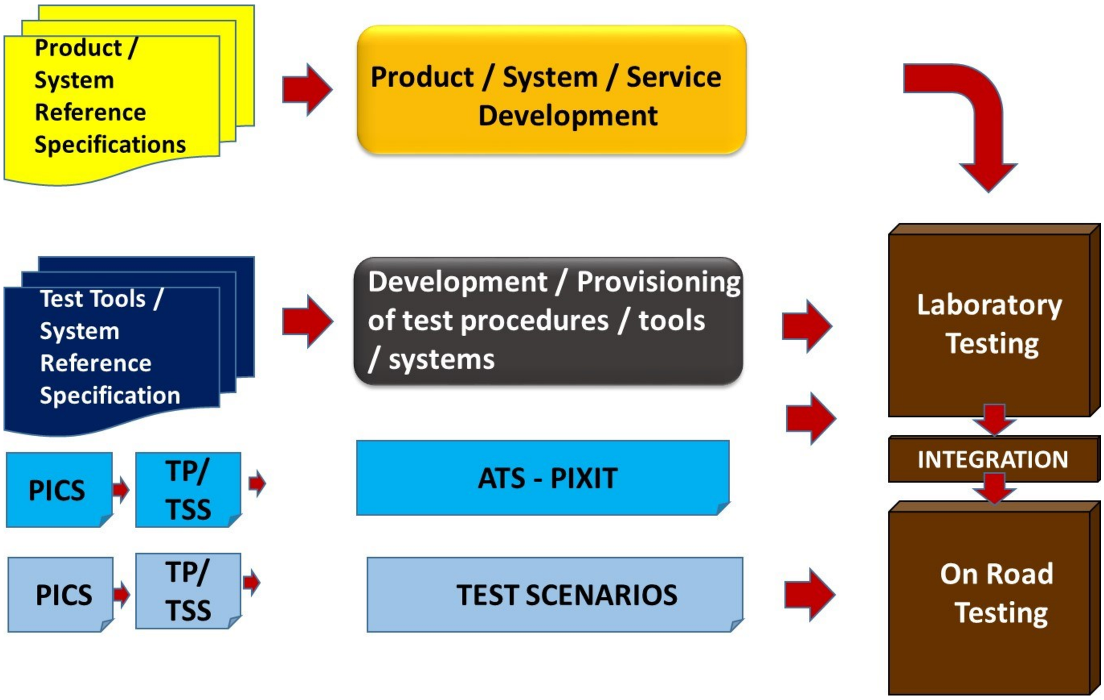

Product / System Reference Specifications
Product / System / Service Development
Test Tools / System Reference Specification
Development / Provisioning of test procedures / tools / systems
PICS
TP/ TSS
ATS - PIXIT
PICS
TP/ TSS
TEST SCENARIOS
Laboratory Testing
INTEGRATION
On Road Testing

Figure: Overview of the compliance assessment methodology

End to end test´s for future C-ITS applications:

The End to End testing for future C-ITS applications is depending of evolutions (differences) existing in comparison to C-ITS phase 1 deployment. If we keep the same G5 technology, communication protocols and security profile, then the difference will be mainly residing in application profiles (new message set required to support new applications). In such case, it will be only necessary to achieve end to end testing for each new application using new message standards. It has to be noted that in the communication profile we specify the technology to be used (e.g. G5), but also the required frequency channel (e.g. CCH, SCH1, SCH2…etc.) being assigned to each application (e.g. CCH for critical road safety). Consequently, if new applications use different channels of CCH, radio test shall be achieved also for these new channels. End to End performances shall be achieved to verify the compliance of the product to the performance requirements to be developed for each new application.

Additionally to the C-ITS application level the following applies:

For conformance assessment and end to end testing procedures other settings of the validation scheme and expected outcomes apply which need to be discussed with the main stakeholders in the C-ITS domain and take into account the future extensions of applications and C-ITS units in operation. This may be achieved within the C-ROADS platform were the single work groups can elaborate a set of common documents for the national pilot implementations and take into account mutual acceptance.

7.2.1. Specific methodology for roadside C-ITS stations

As identified in section 6.2, it is considered that roadside C-ITS Station compliance to standard specification (conformance testing) and interoperability testing will be achieved at accredited test laboratory level on the basis of ETSI plug tests.

End to end test for day one applications:

For the roadside minimum performance compliance assessment, it will be necessary to achieve it on close circuit representing the various environments where Roadside Unit will be installed (motorway, urban, suburban, departmental / regional roads). In such case, reference Vehicle C-ITS Stations shall be installed in vehicles moving at different speeds on scenario relevant test circuits.

Assessment scenarios shall be specified for each application and derived use case to be deployed in C-ITS phase 1. These scenarios purpose is to verify that the roadside under assessment is satisfying all minimum performance requirements stated in reference standards and specifications. All the specified scenarios assessment results shall be registered on PICS (Protocol Implementation Conformance Statement) like administrative documents indicating if the roadside unit under assessment has satisfied the minimum performance requirements stated in reference standards / specifications.

7.2.2. Specific methodology for vehicle C-ITS stations

As identified in section 6.2, it is considered that Vehicle C-ITS Station compliance to reference specifications (conformance testing) and interoperability testing will be achieved at accredited test laboratory level on the basis of ETSI plug tests.

In such case, it is not necessary to have a completely equipped vehicle under test, however, an upper layer tester and some simulators (CAN BUS and GPS simulation) may be required.

End to end test for day one applications

For the vehicle C-ITS Station minimum performance compliance assessment, it will be necessary to achieve it on close circuit representing the various environments where vehicles will be evolving (motorway, urban, suburban, departmental / regional roads). In such case, reference Vehicle C-ITS Stations and reference roadside C-ITS Station shall be used for V2V and V2I assessment of targeted C-ITS phase 1 applications. Vehicle under test and reference vehicles shall be moving at different speeds on scenario relevant test circuits.

Assessment scenarios shall be specified for each application and derived use case to be deployed in C-ITS phase 1. These scenarios purpose is to verify that the vehicle under assessment is satisfying all minimum performance requirements stated in reference standards and specifications. All the specified scenarios assessment results shall be registered on PICS (Protocol Implementation Conformance Statement) like administrative documents indicating if the vehicle under assessment has satisfied the minimum performance requirements stated in reference standards / specifications.

7.3. Beyond Day 1 services

To get C-ITS operational on the field it is important that the compliance assessment ensures a proper level of testing for the Day 1 services. However, it is at least as important to have a good understanding how the compliance assessment can be rapidly upgraded to ensure new functionality can be included to avoid that new untested functionality enters the field before these new functionalities can be a part of the compliance assessment scheme.

7.4. Standardisation status

In this chapter, the current status of the required standards for phase 1 deployment is described, and missing standards are identified. This status is based on the knowledge of participating experts and may need update as some standards are still being developed. Moreover, organisations like C2C-CC and C-Roads are currently consolidating the set of standards included in profiles which will be the reference for deployment and compliance assessment.

7.4.1. Architectural standards

Several standards available, but not directly relevant for compliance assessment.

- ETSI TS 103 301 v1.1.1
- Recommendation ITU-T X.691/ISO/IEC 8825-2 (1997-12): "Information Technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)".

7.4.2. Interface specification standards

Physical and Access layer

See 7.1.1. for details. Relevant standards are:

- EN 302 571 v2.1.1[5]
- ETSI TS 102 792 v1.2.1 (DSRC Mitigation)
- (OPTIONAL) EN 302 663 v1.2.1
- (OPTIONAL) ETSI TS 102 687 v1.1.1 (DCC)
- TS 102 792 V1.1.1 (Interference mitigation with CEN DSRC)
- EN302663 v1.2.1: Intelligent Transport Systems (ITS); Access Layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band.

No additional standards are required for day-1 services.

Transport and Networking layer

See 7.1.2 for more details. Relevant standards are:

- EN 302 636

No additional standards are required for day-1 services.

Facilities layer

Relevant standard are:

- EN 302 637-2 v1.3.2 Part 2 (CAM) Intelligent Transport Systems (ITS); Vehicular Communications;Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service
- EN 302 637-3 v1.2.2 Part 2 (DENM) Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service
- TS 102 894-2 v1.1.1 (CDD)
- ISO / TS 19091: 2017 (EN) Intelligent Transport Systems-Cooperative ITS – Using V2I and I2V communications for applications related to signalized intersection.
- ISO/TS 19321: 2015 Intelligent Transport Systems – Cooperative ITS – Dictionary of in-vehicle information (IVI) data structure.
- ETSI TS 103301 v1.1.1 Intelligent Transport Systems (ITS); Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services.

---

[5] Published in the OJEU on 8 June 2017 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=uriserv:OJ.C_.2017.180.01.0005.01.ENG

Security layer

Relevant standards are:

- TS 102 940 v1.1.1 (architectural overview)
- TS 102 941 v1.1.1 (specifications of authorities)
- TS 103 097 v1.2.1 (security headers)

Status and versions to be further updated and clarified by the Security Working Group.

Management layer

No relevant standards for compliance assessment exist, and are not required either.

Application layer

Interoperability compliance assessment does not need standards for application layers (performance requirements are addressed in §9).

7.4.3. Common profiles (define how a set of standards is implemented in a coherent way)

Common profiles define how a set of standards is implemented in a specific C-ITS station in order to support a group of services/ applications and enhance service interoperability also by defining additional requirements. Therefore, the compliance assessment process should ultimately be based on common profiles adopted by all participants of the C-ITS Network.

Profiles for Vehicle-ITS Stations

The C2C CC has developed and maintains the C2CCC Basic System Profile. It focusses on safety related use cases. The following vehicle-vehicle use cases are fully supported:

- Emergency Vehicle Warning
- Dangerous Situation
- Stationary vehicle warning
- Traffic Jam Ahead Warning
- Collision Risk Warning
- Adverse Weather Conditions

Infrastructure-to-vehicle use cases are partly covered for:

- Road Work Warning
- Traffic Jam Ahead Warning

Some other Day 1 services, such as GLOSA or Probe Vehicle Data, still need to be fully specified. The profile needs to be extended, or an additional profile needs to be developed, for the Day-1 services that are not included at the moment. The profiles used at the infrastructure level shall be consistent with the one being used at the vehicle level. Action has been taken by C-Roads and C2C-CC through the signature of a MoU on cooperation for C-ITS introduction in the EU and on sharing and alignment of profiles[6].

---

[6] https://www.c-roads.eu/platform/about/news/News/entry/show/c-its-cooperation-between-c2c-cc-and-c-roads-platform-1.html

Profiles for Infrastructure based Roadside-ITS Stations

At project level several use case based communication profiles have been developed and harmonised in bilateral work between partners of different projects, but especially in the cooperative corridor NL-DE-AT a first infrastructure based harmonized communication profile has been developed, published in several releases and validated and tested together with industry and external stakeholders. Harmonization of the infrastructure communication profile is currently on-going in the context of C-Roads for all participating members and pilots, as a contribution to large scale European wide deployment of day one applications.

Profiles for Personal-ITS Stations

Up to now no project related detailed communication profile and no European wide profiling has been started or announced for Personal-ITS Stations. A compliance assessment of P-ITS Stations can only be done when such a common profile has been developed and adopted.

7.4.4. Test specifications

Physical and Access layer

Testing Physical layer is not specified by the ETSI.

Networking

Available test specifications

- ETSI TS 102 871 (Geonetworking): Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking ITS-G5 (part 1, part 2 and part 3)
- ETSI TS 102 870 (BTP): Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking Basic Transport Protocol (BTP) (part 1, part 2 and part 3)

ETSI TS 102 859 (GN6): Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Transmission of IP packets over GeoNetworking (part 1, part 2 and part 3)

Facilities

Available test specifications

- ETSI TS 102 868-1/2/3 (CAM) : Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Cooperative Awareness Basic Service (CA);
- ETSI TS 102 869-1/2/3 (DENM): Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Decentralized Environmental Notification Basic Service (DEN);
- ETSI TS 103 191-1/2/3 Conformance test specifications for facilities layer protocols and communication requirements for infrastructure services. This is including SPAT /MAP and IVI.

Missing: IVI test specifications.

Applications

Interoperability compliance assessment does not need testing specifications for application layers (performance requirements are addressed in §9).

Security

To be further updated and clarified by the Security Working Group.

Management

As no relevant standards are required for the interoperability, no test specifications are required either.

7.4.5. Profile based test specifications

The compliance assessment process should ensure interoperability. The interoperability is not provided directly by the adopted standards, but by the profiles that describe how they are to be used. Therefore, the compliance assessment also needs to be based on test specifications for those profiles. Note that these will refer partly to the test specifications for the relevant standards, in the same way as the profiles themselves refer to the relevant standards.

Test specifications for Vehicle ITS Station profiles

The test specifications for the Basic systems profile of the C2C CC is still work in progress.

Test specifications for Roadside ITS Station profiles

No complete set of test specifications have been released for the Roadside ITS Station profiles under development, although some test specifications are available.

Test specifications for Personal ITS Station profiles

As no personal ITS Station profiles exist, no test specifications exist either.

8. Emerging solutions

This section is looking into on-going technology developments and assessing potential compliance assessment procedures for deployment.

8.1. Cloud based solutions

Vehicular Cloud Computing (VCC) is a promising solution for C-ITS deployment. VCC is a hybrid technology that has an interesting impact on traffic management and road safety by instantly using vehicular resources, such as computing, storage and internet access for decision making. In such solutions, a group of vehicles (VC : Vehicle Cloud) which corporates computing, sensing, communication and physical resources can be coordinated and dynamically allocated to authorized users. In these networks,

Efficiency: event detection is achieved efficiently close to the occurred event,

Autonomy: there is more autonomy: for the decision of each vehicle to participate in the VC,

Agility: ability of VCs to tailor the amount of shared resources to the actual needs of the situation in support of which the VC was constituted.

All protocols currently used for these solutions are proprietary protocols, characteristics of these solutions are not public and compliance assessment of these solutions is excluded from this document.

The communication from C-ITS station is typically based on cellular technology. The compliance of the communication link can therefore generally be assumed to be covered by the GCF certification scheme.

8.2. LTE V2X

LTE V2X is being developed by 3GPP who primarily have worked on providing an access layer for the V2X. The design is relying on the fact that the higher layers of the stack for C-ITS are access layer agnostic and thus the higher layers described in the previous sections can be reused over LTE V2X. The 3GPP LTE V2X is a part of 3GPP Release 14 (and beyond) and the first complete version being completed in 2017.

Three different options that can exist either in isolation or in combination are offered in the 3GPP specifications. One is known as LTE sidelink link using the so called PC5 interface which is direct communication between C-ITS stations similar to ETSI G5. The two other modes are server based solution where the C-ITS establish a cellular connection over (Uu interface) to a network based server that then performs the distribution of the messages in the relevant geographic area. The distribution will in one solution be performed via a peer to Peer cellular link between the server and the relevant C-ITS stations. In the other solution the distribution will be performed by eMBMS which is a cellular broadcast service (one to many).

8.2.1. LTE sidelink

For LTE Sidelink there are two high level deployment configurations currently defined, and illustrated in the figure below.

Both configurations use a dedicated carrier for V2V communications, meaning the target band is only used for PC5 based V2V communications. Also in both cases GNSS is used for time synchronization.

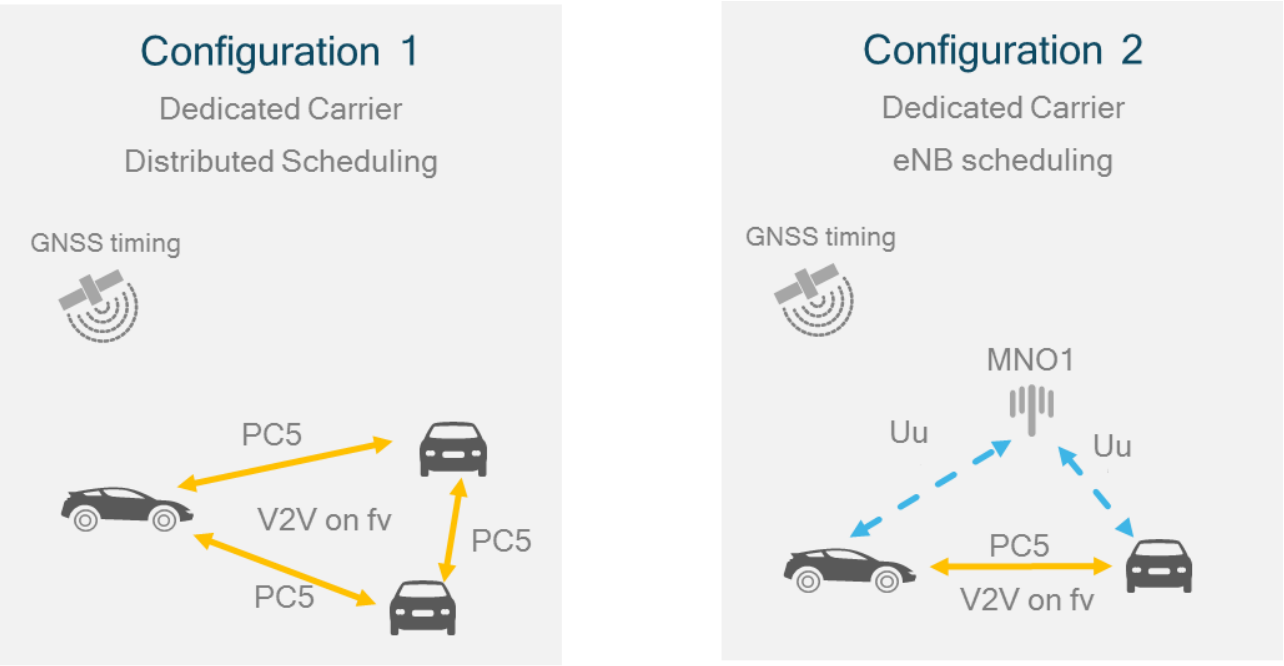


Figure: LTE Sidelink

In “Configuration 1” scheduling and interference management of V2V traffic is supported based on distributed algorithms (Mode 4) implemented between the vehicles. As mentioned earlier the distributed algorithm is based on sensing with semi-persistent transmission. Additionally, a new mechanism where resource allocation is dependent on geographical information is introduced. Such a mechanism counters near far effect arising due to in-band emissions.

In “Configuration 2” scheduling and interference management of V2V traffic is assisted by eNBs (a.k.a. Mode 3) via control signalling over the Uu interface. The eNodeB will assign the resources being used for V2V signalling in a dynamic manner.

8.2.2. Initial thoughts on Compliance assessment for LTE V2X

Compliance assessment of modes using cellular uplink

For the two modes of LTE V2X that uses a cellular uplink to a server that is responsible for the distribution of the messages, it is assumed that for the communication part the RED combined with the GCF certification scheme would be sufficient to assure compliance of the communication.

For the performance requirements, only part of the delay requirement can be seen at the C-ITS and its communication. Thus the performance requirements discussed in the previous sections cannot be used directly, as part of the performance is dependent on the performance of the server that does the distribution as well as the downlink transmission. Therefore it is likely it would be necessary to split the performance requirements between the different elements. E.g. for the delay/latency an overall delay budget is required, so the requirements for end to end delay is split between the different parts of the overall connection, and a resulting measurable performance requirement for the C-ITS station from triggering event to transmission on the cellular interface can be measured.

Compliance assessment of modes using LTE sidelink

LTE sidelink uses a direct communication link between two C-ITS stations similar to what is the case for ETSI G5, thus for the general performance requirements on the higher layers as described in previous sections can most likely just be reused from independent of whether ETSI G5 or LTE sidelink is used.

As described above LTE sidelink have two deployment configurations – with or without eNB scheduling assistance. There will need to be some basic rules in place on which resources can be used if there is no cellular coverage, to avoid that if in coverage the eNB do not allocated a resource already used by a C-ITS station not in coverage. This type of requirements and associated test appears to be likely to be in the framework of the RED.

At this point in time, a first assumption would be that the main difference in terms of compliance for ETSI G5 and LTE sidelink would be covered by the requirement associated with the RED and all compliance assessment criteria above the access layer can be common.

9. End to end service test´s - Quality of service assessment

9.1. Minimum requirements for conformance and performance

9.1.1. Particular requirements for roadside C-ITS stations

A Road Side C-ITS Station has typically two categories of customers (users): road users and road operators, or traffic managers.

The quality of C-ITS service is not only specific to the Road Side C-ITS Station but also from the distribution chains from the TMC to the R-ITS-S or the mobile trailer.

Generally, we could focus on the following requirements partly under the responsibility of the Road Side C-ITS Station:

Minimum requirements on the level of confidence to be associated to the information provided by the RSU to vehicles. In some case (e.g. contextual speed limit), this level of confidence shall be near 100%.

Minimum requirements on the MTBF (Mean Time Between Failure) and MTTR (Mean Time To Repair) which are both related to the service availability.

The RSU receives data elements contained in standard messages which are broadcasted by vehicle C-ITS stations (considered as probe vehicles). For deployment phase 1, these data elements will be collected and partly analysed by the RSU and then transferred to traffic management centres for the development of traffic management and safety services targeting road users. CAM data elements will be fused with other data elements coming from other sources with the objective, after analysis, to derive traffic management services. CAM data elements will also be used to identify priority vehicle being in-mission with the objective to give them the priority at traffic lights. DENM data elements will be immediately used for consolidating (increasing the confidence level) detected road hazards data elements, so triggering the broadcasting of signalling information from RSUs to vehicles and initiating road operators' vehicle intervention to secure the hazardous locations. Some CAM data elements are also used to identify priority vehicles being in-mission.

SCOPE: The scope of minimum performance requirements compliance assessment at receiving RSUs level, for deployment phase 1, is to verify that the quality of received data elements is sufficient for the development of road users' services which are targeted by road operators. As road operators are not the end users of these services, but their providers, the quality of the services being delivered by road operators is relative to the detailed specification of these services which need to be developed before engaging some compliance assessment activity. This is true for PVD (Probe Vehicle Data), however, for giving priority to some categories of vehicles being in-mission, it will be necessary to classify them (e.g. priority of emergency vehicles with regard to Public Transport vehicles) and verify the veracity (trust the road operators can put on them) of the CAM data elements which are used for deciding to act on the traffic lights.

9.1.2. Particular requirements for vehicle C-ITS stations

Minimum requirements on the level of confidence to be associated to the provided information.

Minimum requirements on the maximum acceptable false negative information provided by the receiving vehicle, consecutive to a properly transmitted information.

Minimum requirements on the maximum acceptable false positive information provided by the receiving vehicle, consecutive to a properly transmitted information.

Minimum requirements on mode of presentation (audio and visual[7]) and timing of the presentation (e.g. at least 10 seconds before reaching the relevance area, duration of the presentation of at least 4 seconds, suppression of the presentation for road hazard at least 3 seconds before reaching it to leave the possibility of replacing an information by an alert for collision avoidance in the future).

At the vehicle level, the situation is different as the receiving vehicle is the one which is directly providing the service to the road user. So the quality of service is related to the quality of the data elements received from others C-ITS S (Vehicles and RSU), the reliability of the G5 communication link between C-ITS Stations (typically

---

[7] Here we don't specify the HMI, but requiring the use of both audio and visual to signal an event. Audio to attract the attention of the driver and visual in case of noise problem and to maintain a minimum the info giving more visual precision.

its PER), but is also related to the performances of the receiving vehicle. In particular, the received data elements will be compared to the receiving vehicle data elements (e.g. in terms of relative velocity, relative positioning, relative movements) to decide about the action to start (doing nothing, issue a cooperative awareness signalling to the driver, issue an alert to the driver, trigger an automatic action (e.g. emergency brake), request a contextual speed adjustment…etc.). Indeed, an important function is the "relevance checks" which decide if the received messages are relevant or not to the receiving vehicle and if yes enable the service supporting application(s) to take the required action.

SCOPE: The scope of the minimum performance compliance assessment at the receiving vehicle level, for the deployment phase 1, is to verify that the receiving vehicle has the capability and minimum performances required to deliver an efficient service (fulfilling the service objectives under specified conditions) to its road user. Such requirement is of prime importance for services which are directly related to road safety like road hazard signalling and contextual speed adaptation. The quality of service shall be characterized in terms of veracity (trust the road user can put on received information) and timeliness of the information, which are both relying on data quality (latency, accuracy, confidence level) provided by both cooperative ITS-S elements (transmitting and receiving ones) and the communication network enabling their cooperation. This is particularly important for road safety, because it exist a strong continuity (depending on relative distances, trajectories and velocity of both vehicles), between the cooperative awareness information, the human collision avoidance and the automatic collision avoidance services (see the figure below).

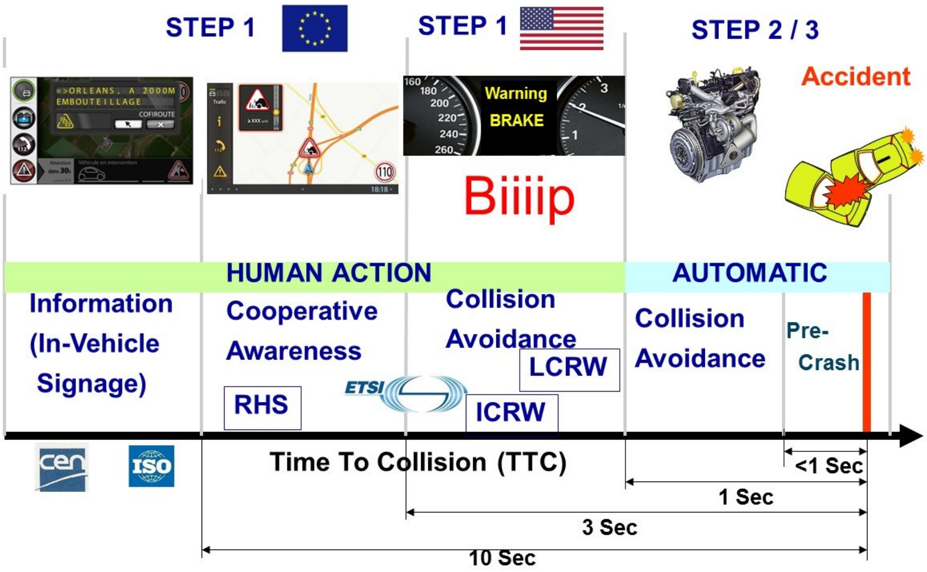


Figure: Continuity between phase 1 and phase 2 services

So even if focusing on cooperative awareness information (e.g. road hazard signalling), it is required, at the receiving vehicle level to be able to estimate properly the criticality of the situation to start the right action (e.g. not providing a signalling information if an immediate action is required and vice versa). Moreover, the information shall be provided at the optimum time to the end user (when its vigilance level is still sufficient after receiving a cooperative awareness), to enable him to start quietly some action to secure its driving.

9.2. Compliance assessment methodology

For the quality of service’ assessment it is preferable to use / assess the actual elements of the targeted system in a nominal (without a particular loading of the system) operational mode. This could be achieved in an open environment or in a private environment exhibiting a diversity of traffic and road topographic situations.

HMI Ergonomic assessment (figure 1a):

Verification that the HMI provides a confidence level associated to the information which is given to the driver, uses audio and visual presentation modes and respect the start and stop timing requirements for the presentation of the information.

An object on the road (e.g. an immobilized vehicle or an RSU) broadcast some information. The subject vehicle (vehicle under assessment) receives the information, achieve a relevance test and present the information to the driver according to the minimum requirements being set.

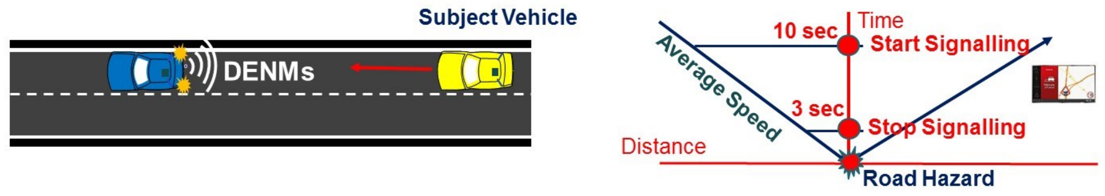


Figure 1a : HMI Ergonomic Assessment

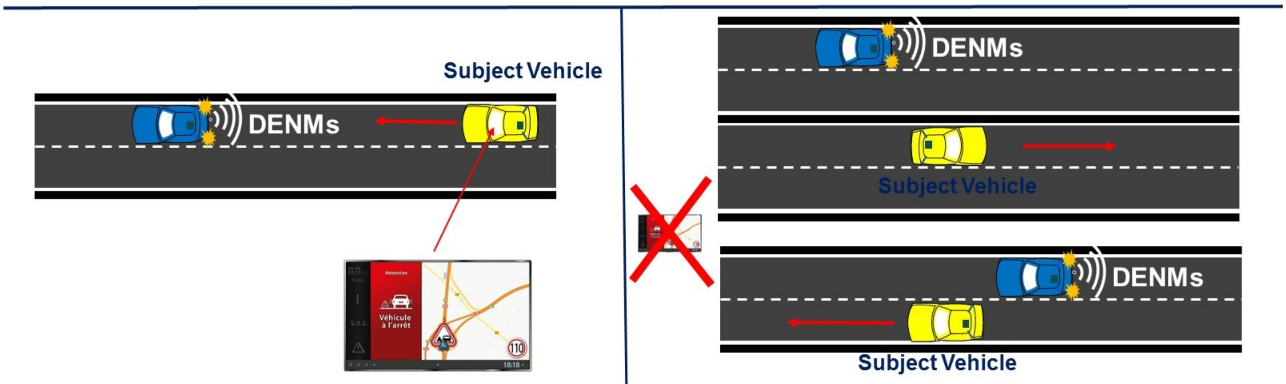


Figure 1b : No false negative signalling

Figure 1b : No false positive signalling

Figure: Vehicle Quality of Service Assessment (ex: Road Hazard Signalling)

<u>False Negative information assessment (figure 1b)</u>:

Verification that the information being received by the vehicle is really presented to its driver under the two following conditions (relevance check):

The subject vehicle (or vehicle under assessment) is moving on the same road that the object (e.g. immobilized vehicle) which is broadcasting an information. If the information is broadcasted by an RSU, the subject vehicle is moving on the road of the relevance area provided by the DENMs.

The subject vehicle (or vehicle under assessment) is heading toward the object which is broadcasting an information or toward the relevance area provided by DENMs being broadcasted by an RSU.

This could be achieved a certain number of time at different speed and in different environment. The information shall be delivered to the driver as required for all achieved testing.

False Positive information assessment (figure 1b):

Verification that an information being received by the vehicle is not presented to its driver under one or the other two following conditions:

The subject vehicle (or vehicle under assessment) is not moving on the road where the object (e.g. immobilized vehicle) broadcasting an information is located. If the information is broadcasted by an RSU, the provided relevance area provided by DENMs is not located on the road on which the subject vehicle is moving.

The subject vehicle (or vehicle under assessment) is not heading toward the object (e.g. immobilized vehicle) broadcasting an information or toward the relevance area provided by DENMs being broadcasted by an RSU.

9.2.1. Specific methodology for roadside C-ITS stations

Roadside C-ITS Stations are providing information to Vehicle C-ITS Stations. The assessment methodology being used shall verify the following aspects at the level of a reference vehicle C-ITS Station being heading in the direction of the RSU and the relevant road:

- The R C-ITS S is authorized to broadcast the information. The level of authorization shall be verified according to the criticality of the information (e.g. level of the road operator or level of the legal public authority).
- The relevance area is correctly provided in relation to the applicability of it or of the positioning of the event (case of a road hazard signalling).
- A level of confidence shall be provided for the receiving vehicle being able to give priority to simultaneous identical information (e.g. provided on its digital map, received from another vehicle, received from the cloud or received from a Roadside C-ITS S).
- A dissemination area shall be provided and verified in term of consistency with the provided relevance area. The driver shall have the possibility to have adapted its vehicle speed / trajectory when entering the relevance area.
- The category and nature of the provided information shall be verified as far as possible (Road hazard, speed limit…etc.).
- The radio coverage of the R C-ITS S shall be verified in terms of consistency to the information being provided (e.g. minimum time or distance between the dissemination area and relevance area). Then, the radio coverage of the R C-ITS S shall be greater than the dissemination area.

9.2.2. Specific methodology for vehicle C-ITS stations

Most of the methodology to be used for vehicle C-ITS Stations is already provided in section 9.2 of this document. However, the following situations shall be considered at the vehicle level:

- Even if the HMI shall be left to the discretion of the vehicle manufacturer or equipment supplier (after sales solutions), it is desirable that a minimum of common HMI characteristics be respected in order to facilitate the driver adaptation when changing vehicle (e.g. car sharing, vehicle renting). Such HMI adaptation would be facilitated through some recommended common practices for the presentation of information / alerts in terms of audio and visuals. This aspect shall be part of the ergonomic judgement.

- Some European guidance may be provided. The European Statement of Principles on human-machine interface (ESOP) issued on 26 May 2008 refers to ISO standards has a focus on avoidance of driver distraction. It is suggested to develop rules for Day 1 applications, and reminded that ISO TC 204 (Intelligent transport systems) WG 14 (Vehicle/roadway warning and control systems) works on similar issues for ADAS.
- In case of simultaneous information / alerts received from several different sources, the HMI support shall be considering their respective priorities and the level of trust to be given to these sources. The assessment methodology will consist to generate simultaneously several events from different sources and then verify that the HMI is presenting them according to their priority and level of trust.

9.3. Standardization state

Until now, in the C-ITS domain, the standardization bodies have just dedicated a minimum of time to the writing of minimum performance requirements as putting their first priority to interoperability and conformance testing.

Minimum performance requirements are particularly important for road safety applications and in particular collision avoidance (human or automated). If one element of the cooperating system does not meet some performance requirements (e.g. maximum latency time, data element accuracy, level of trust in received data…etc.), the result can be catastrophic as not enabling the right action to avoid the collision.

Even for critical time information, the driver shall have the level of confidence in the provided information to trust them and use them. If it is not the case, the driver will quickly ignore the provided information leading to not using the service and so reducing the benefits expected from the whole community.

9.3.1. Road Hazard Signalling Requirements

This is typically a road safety service which purpose is to provide in real time cooperative awareness information with the objective to increase the human driver vigilance relatively to a signaled road hazard which is on its way ahead at a time distance of about 10 seconds. ETSI has been developing the TS 101539-1 V1.1.1 (2013-08) -Intelligent Transport Systems (ITS); V2X Applications; Part 1: Road Hazard Signalling (RHS) application requirements specification.

This TS considers the main road hazard use cases which are part of the C-ITS phase 1 deployment (Emergency vehicle approaching, Emergency Electronic Brake Light, slow or stationary vehicle (breakdown or accident), traffic jam ahead, hazardous location, bad weather condition).

This TS considers the two elements which are cooperating together to increase the driver awareness of a road hazard:

- The originating C-ITS Station Unit,
- The receiving C-ITS Station Unit.

The TS 101539-1 specifies that: *The main function provided by the RHS application at the receiving level is the notification of a road hazard to the driver based on the processing of received standard messages (CAM, DENM, others). These messages can originate from vehicle and roadside ITS-S.*

In particular, this TS is providing the following generic (applicable to all use cases) Functional Requirement for the application (FRA) which targeting the receiving vehicle:

FRA05: For a Vehicle ITS-S, the RHS application shall be capable of taking action (e.g. trigger driven information) of a **valid and relevant** road hazard based on received messages. The **validity and relevance** of the received road hazard signaling shall be established when the subject vehicle is positioned as being heading toward the road hazard and being at a given minimum distance of it.

This requirement is completed by the following operational requirement which indicates that the HMI design is left to the responsibility of the vehicle manufacturer.

FRR02: Received road hazard information shall be generating an action in the receiving vehicles if being judged relevant. This action is for example the notification of a "driver awareness indication" signalling the road hazard (cause and sub cause) being at the origin of the DENM. In this case, the way of presenting it to the driver and the presentation instant according to determined TTC is left at the discretion of the vehicle manufacturer or equipment supplier in case of an after sales installation.

Others requirements are provided also for the originating ITS Ss.

Such requirement is focusing on “false positive” signaling (the road hazard shall be signaled only if the vehicle is heading toward it). It indicates also that the road hazard shall be signaled when the vehicle is at a given minimum distance of the road hazard (rising the driver vigilance at the right time to take the best action).

However, we don’t have requirements about “false negative” signaling (not signaling an existing road hazard on time) which will certainly occur when using cellular technologies due to their latency time.

Then for each use case this TS specifies:

- The use case specific function which shall be fulfilled by the originating vehicle.
- The event triggering conditions for the originating vehicle.
- Some specific use case vehicle ITS – S state and condition.
- The relevance area determined by the originating vehicle and used by the receiving vehicle for its relevance check.
- The event termination conditions for the originating vehicle.
- Use case specific data elements to be provided.

In terms of the minimum performance requirement, only the maximum end to end latency time is specified: **Max 2 seconds** for class B vehicles (vehicles not implementing collision avoidance applications).

This minimum performance requirement will likely never be fulfilled by cloud based systems.

9.3.2. Contextual Speed

The contextual speed is the recommended or limited speed to be applied in some particular contexts (e.g. high level of pollution, road work, accident, bad weather conditions, traffic regulation…etc.). The ISO / CEN standard “TS 17426 – Intelligent Transport Systems (ITS) - Co-operative systems – Contextual Speed” is focusing on contextual speed signaling to a human driver.

- Provision of mandatory speed limit information into vehicle – for driver awareness purpose.
- Provision of advisory speed information into vehicle – for driver awareness purpose.

Contextual speed can be considered as covering the two domains of – Road Safety – Traffic management.

Consequently, for road safety, the quality of the provided information shall be of high level if we want that the driver trust and apply the contextual speed.

Contextual speeds are broadcasted by road side unit ITS S or are communicated by a Central ITS-S. One of the main requirements for the user to trust the provided information is to clearly identify the source and in particular, for speed limit the legal authority authorized to provide contextual speed limits.

The maximum latency time is depending on the flow type (type of used network technology). It shall be between 100 milliseconds (in my opinion it is too optimistic for end to end?) for direct V2X to 1 minute for point to point cellular.

What is important is that the contextual speed be provided to the driver in a sufficient time for him to adapt its speed before entering the relevance zone (requirement SDR013).

However, the standard is not considering requirements about the relevance check of the contextual speed verifying that the contextual speed provided to the driver is true (not false positive or false negative due to bad relevance check). This is the same situation as for RHS.

9.3.3. In-Vehicle signage (IVS)

In-vehicle signage consists to provide directly on the driver HMI the Fixed and Variable Message Signs (VMS) which are actually provided by physical panels. This is covering several categories of information from road safety to traffic management and mobility information.

The ISO / CEN standard “TS 17425 – Intelligent Transport Systems – Cooperative ITS – Data exchange specification for in-vehicle presentation of external road and traffic related data” is focusing on what is currently named “In-Vehicle Signage”.

Generally, the IVS service expected is to provide information to road users from an authorized content provider presented in the vehicle in a manner that is consistent with that of VMS and road signs.

Again, an important function of the receiving vehicle is the “relevance checks” and “plausibility checks” verifying that the source of the data elements is an authorized source.

The standard classifies the IVS service in two categories with respective priorities from 1 to 5):

- **Primary services:** 1. Immediate danger warning messages, - 2. Regulatory messages: Prohibition, restriction, obligation or special regulation.
- **Secondary services:** - 3. Traffic related information messages, - 4. Pollution messages, - Not traffic related messages.

Several requirements related to data quality are dedicated to the receiving vehicle:

MR130: The IVS receiver C-ITS station shall check the relevance of information contained within any received IVS message and check the current time in the IVS receiver C-ITS station is not greater than the Validity End Time of that IVS message.
MR140: The IVS receiver C-ITS station shall present valid and relevant received IVS message content to the HMI unit.
MR170: The IVS receiver C-ITS station shall update the retained IVS message information when an IVS message having the same identifier and later message generation time is received. Only the last version of an IVS message is stored.
…etc.

9.3.4. Signal Violation at Intersection

Signal violation at intersection is a critical use case as for example the EEBL. This use case is currently under specification at ETSI (verify its current status) in the draft DTS 101539-2 – Intelligent Transport Systems (ITS); V2X Application; Part 2: Intersection Collision Risk Warning application requirement specification.

The development of this standard has been slowing down due to the lack of the SPAT / MAP standard which is required for one of its implementation (the V ITS SU is detecting a risk of signal violation by reference to its position / velocity relatively to the current phase and timing of the traffic light.

Another solution which is under development at least in France (in PAC V2X project) is the detection of an intersection signal violation by a R ITS SU integrating a specific sensor (radar) and then the broadcasting of DENM (signal violation warning).

The difficulty for this use case and some others which are similar (e.g. EEBL) is that the receiving vehicle shall be able to establish, according to the distance separating it from the moving road hazard and their relative velocity, if it is an information (cooperative awareness) or an alarm (warning) which shall be given to the driver. In example when being at about three second of the spot of collision risk, the receiving vehicle shall send an alarm to the driver which shall react immediately by an emergency braking to avoid the collision.

Three seconds takes into account the reaction time of the driver (1 to 2 seconds according to its level of vigilance) and the time necessary to stop the vehicle (according to its speed and the state of the road).

The DTS 101539-2 specifies that the total end to end latency time shall be less than 300 milliseconds (including the possibility of one packet lost (adding 100 ms).

It shall be existing an ISO standard focusing also on this use case (from TC 204 WG14).

So this use case quality of service requirements shall be investigated in light of the current statuses of ETSI TC ITS WG1 and ISO TC 204 WG14 actual situations.

9.4. Way forward

In all cases we have for a few applications targeted for C-ITS phase 1 deployment some application requirements related to the data quality (mainly for safety related applications). But we don’t have currently existing conformance testing standards which should be specifying how to verify the conformity of products (transmitting vehicles, receiving vehicles, road side units) to the reference specifications (development of PICS, TP, TSS, ATS and PIXIT). It is then recommended to ask European SDOs to develop the missing conformance testing standards.

In all cases we shall verify the source of the information being received and associate to it some confidence level. High level of confidence when coming from a certified authority or triggered automatically, lower levels for semi-automatic (e.g. start of the windscreen wipers / fog lights) or human triggering). This should be integrated in existing standards revisions or future standards.

Likely, the level of quality of data elements related only to traffic management is less important to the level of quality of the safety applications especially when related to collision avoidance. Decision should be taken about the level of quality to be mandated for traffic management applications. According to such decision, it could be necessary to develop missing applications requirements and associated conformance testing standards (e.g. GLOSA, PVD…etc.).

The transition from cooperative awareness to collision avoidance is completely under the responsibility of the receiving vehicle when comparing its trajectory and speed to the ones of the transmitting vehicle. So we shall be clear to manage this transition in such a way to not disturb the action which shall be taken for a collision avoidance (see what is regulated at the level of the emergency braking for trucks). This issue shall be considered by relevant SDOs if not yet done.

Safety data quality shall be clearly associated to the nature of the service to be provided to the user (Cooperative awareness or alert service) which exhibit differences in terms of HMI and criticality level. The C2C-CC is not clear on this subject in its MoU as talking to "warning". Does it mean a road hazard signaling (information or a Road hazard alert (immediate action)? A clear terminology should be developed to identify the criticality of the considered service.

The trust in provided data elements shall be considering the reality of the provided data (eliminating false positive and false negative data) as well as their timeliness (rising at the right time the driver awareness / Alert). Recommendations should be provided to SDOs especially for road safety applications to take into account these quality elements in the development of their application requirements.

Investigate about the states of developing standards (ETSI / ISO) related to "signal violation warning".

10. C - ITS – System Scalability

10.1. Minimum scalability requirements

V and R C-ITS Stations have a long life cycle (at least 10 years for vehicles and several 10 years for Road Side Equipment). During this long life cycle, we will be facing two major evolutions:

- The standards will be up dated to correct mistakes and add new useful features.
- During deployment, the system will be growing with more and more equipped vehicles and road side equipment cooperating together.

It is then required that Vehicle (V) and Road Side (R) C-ITS Stations be developed with some particular capabilities to adapt to standardization evolutions and to sustain a continuous increase of their processing / storage load without any disturbance of their operations.

Both types of C-ITS Stations (vehicles and Road Side) shall have the following capabilities:

- Be reconfigurable to be up-dated with the latest standard versions. This shall be achieved in a coordinated manner with the objective to maintain the interoperability between cooperating elements (Vehicles, Road Side Equipment, Central stations) of the cooperating system. The reconfiguration procedure is left to vehicle manufacturers and road managers, however, they shall minimize their impacts on customers (e.g. avoid vehicles' owners to be obliged to bring their vehicles in a shop to have them up-dated) and enable a quick evolution with the objective to, as much as possible, reduce the time obtaining a fully up-dated operational system.
- Process and decode a minimum number of received standard messages with the objective to maintain the system performances and quality of service specified in nominal load (see chapters 5 and 6).

10.1.1. Particular requirements for roadside C-ITS stations

A new standard version shall lead to a new compliance assessment of Roadside C-ITS Station products being delivered on the market. This new compliance assessment step shall verify that the new standard version can cohabit and run together with the former version without disturbance of an operational cooperating system.

In-Service Roadside C-ITS Stations shall be remotely reconfigurable through the downloading of a new software configuration to be installed and started in operational RSUs. The previous configuration shall be kept at least until the new version has been tested and activated. The two versions shall be maintained running together at least during a minimum of time taking into account Vehicle C-ITS Stations which are not yet updated and those which have been updated.

For a Road Side C-ITS Station it is less crucial to receive and decode all CAMs. For example, they can only be able to receive about 10% of them to obtain a good perception of the road traffic. This means that if a V C-ITS Station shall be able to receive and process a minimum number of 1000 messages per second, a Roadside C-ITS Station shall have the capability to receive and process a minimum number of 100 messages per second. However, a Roadside C-ITS Station shall be able to extract form its CAMs flow all other messages (e.g. DENM) necessary to achieved deployed services with their associated Quality Of Service level.

The latency time specified for the exchanges of a Roadside Equipment C-ITS Station and other C-ITS Stations (Vehicles and Central) shall not be increased by more than 10% compared to a nominal operation whatever the level of increased load in the limits specified below.

10.1.2. Particular requirements for vehicle C-ITS stations

A new standard version shall lead to a new compliance assessment of Vehicle C-ITS Station products being delivered on the market. This new compliance assessment step shall verify that the new standard version can cohabit and run together with the former version without disturbance of an operational system.

In-Service Vehicle C-ITS Stations shall be remotely reconfigurable through the downloading of a new software configuration to be installed and started in operational one. The previous configuration shall be kept at least until the new version has been tested and activated. The two versions shall be maintained running together at least during a minimum of time taking into account Vehicle / Roadside C-ITS Stations which are not yet updated and those which have been updated.

In-service Vehicle C-ITS Stations shall be able to receive and process a minimum of 1000 messages per second. This is corresponding to 100 vehicles transmitting CAMs at a frequency of 10 hertz (periodicity of 100 milliseconds). At the receiving level, the critical function is the authentication of messages.

In-service vehicle shall be equipped with a DCC (Decentralized Congestion Control) function which has the capability to reduce the transmit power in order to reduce the size of the ad-hoc local area network and then, consequently the number of Vehicle C-ITS Station sharing it.

In-service vehicle shall be equipped with a DCC function which has the capability to increase the periodicity of non-critical CAM messages. Non-critical CAM messages are those having the lowest priority level.

10.2. Compliance assessment methodology

Capacity to adapt to new standard versions:

The assessment methodology may consist to initially configure the assessed C-ITS Stations with a given software configuration, verify that the tested system is working properly and then reconfigure the C-ITS Station under test (e.g. adding some optional containers in broadcasted messages) to verify that the whole system will remain operational.

Capacity to sustain a system load increase:

A progressive increase of the system load can be achieved by introducing progressively more and more V C-ITS Stations in the system. At least three possibilities exist:

- Introducing test vehicles which have the capacity to generate and broadcast CAM messages at a higher frequency (e.g. 100 hertz). In such case, with 10 test vehicles we simulate 100 vehicles.
- Use test Roadside C-ITS Stations having the capability to generate CAM messages at a frequency of 100 hertz. About 10 to 20 RSE can be used to simulate 100 to 200 vehicles.
- Use fleets of mini-drones equipped with standard V2X controllers and then having the capability to simulate moving terrestrial vehicles. Such low cost vehicle (1 to 2 K€) is enabling a more dynamic configuration as representing fleets of vehicles which itineraries can be programmed to represent a realistic road traffic.

10.2.1. Specific methodology for roadside C-ITS stations

Capacity to adapt to new standard versions:

The assessment methodology may consist to initially configure the assessed roadside C-ITS Stations with a given software configuration, verify that the tested system is working properly and then reconfigure the roadside C-ITS Station under test (e.g. adding some optional containers in DENM broadcasted messages) to verify that the whole system will remain operational.

Note: A remote reconfiguration of the roadside C-ITS Station from a traffic management center is certainly the best approach, however, as roadside C-ITS Stations number will be limited per km², a local reconfiguration could be acceptable.

Capacity to sustain a system load increase:

A progressive increase of the roadside C-ITS Station load shall be achieved by introducing progressively more and more reference Vehicle C-ITS Stations in the system. A mix of real or simulated vehicle C-ITS Stations can be introduced, some mini-drones implementing V2X can also be used for this purpose. However, whatever the solution being selected, this one shall be homologated and be reproducible in different assessment accredited centers with the objective to enable a cross recognition of compliance assessment results obtained at an EU member state level by all other EU member states (so avoiding to achieve the same tests in all EU member states).

Assessment scenarios shall be developed for each application supported by roadside C-ITS Station to verify that the required performances are still met whatever the increased load.

All the specified scenarios assessment results shall be registered on PICS (Protocol Implementation Conformance Statement) like administrative documents indicating if the roadside under assessment has satisfied the minimum performance requirements stated in reference standards / specifications even during the specified increase of the system load.

Note: It is not necessary at the roadside C-ITS Station level to implement the DCC (Distributed Congestion Control) under the condition that only one roadside C-ITS Station is present at the level of a G5 ad-hoc local area network.

10.2.2. Specific methodology for vehicle C-ITS stations

Capacity to adapt to new standard versions:

The assessment methodology may consist to initially configure the assessed Vehicle C-ITS Stations with a given software configuration, verify that the tested system is working properly and then remotely reconfigure the Vehicle C-ITS Station under test (e.g. adding some optional containers in CAM broadcasted messages) to verify that the whole system will remain operational.

Capacity to sustain a system load increase:

A progressive increase of the Vehicle C-ITS Station load shall be achieved by introducing progressively more and more reference Vehicle C-ITS Stations in the system. A mix of real or simulated vehicle C-ITS Stations can be introduced, some mini-drones implementing V2X can also be used for this purpose. However, whatever the solution being selected, this one shall be homologated and be reproducible in different accredited compliance assessment centers with the objective to enable a cross recognition of compliance assessment results obtained at an EU member state level by all other EU member states (so avoiding to achieve the same tests in all EU member states).

At vehicle C-ITS Station level, the DCC shall be assessed even if not required for C-ITS phase 1 deployment. This test is required because the necessity for in-service vehicles to have the capability to adapt when the deployed number of C-ITS vehicles will be reaching some threshold leading to some risk of G5 channel saturation.

DCC shall take into consideration the messages' priorities (CAM and DENM) which are associated to the criticality of the road safety situations. For example, the messages' frequency or the transmission power shall not be reduced for the broadcasting of messages having the highest level of priority associated to a collision avoidance or collision mitigation (post-crash mitigation).

Note: Generally, only a few vehicles are in a critical road safety situation especially when we approach a saturation of the ad-hoc network reflecting a huge traffic with a low velocity. This means that only a few vehicles shall not apply fully the DCC rules, all others with lower priority messages shall apply them.

Assessment scenarios shall be developed for each application supported by Vehicle C-ITS Station to verify that the required performances are still met whatever the increased load.

All the specified scenarios assessment results shall be registered on PICS (Protocol Implementation Conformance Statement) like administrative documents indicating if the vehicle under assessment has satisfied the minimum performance requirements stated in reference standards / specifications even during the specified increase of the system load.

11. SECURITY - trusted members of the European PKI Trust Model

--- addressed by the Security WG ---

12. DATA PROTECTION & PRIVACY

--- addressed by the Data Protection & Privacy WG ---

13. CONCLUSIONS AND RECOMMENDATIONS

The scope of the C-ITS Compliance Assessment process being described is this report is considering the C-ITS Station level including isolated C-ITS Stations for the after sales and retrofit, and C-ITS Station being embedded in vehicles and RSU.

However, this does not mean that C-ITS components and systems will not be validated, but their compliance assessment is out of the scope of the proposed organisation and is left to the private industries and Member States.

It is important to note that the described CA process/organisation does not remove the need for the stakeholders to perform end-to-end and system testing.

Main recommendations:

- Need to set up an appropriate common EU legal and technical framework defining the functional, technical and organisational provisions to implement the proposed roles and compliance assessment requirements and process, which is summarised on the figure on the overview of the compliance assessment process.
- Main roles in relation to C-ITS compliance assessment are governance (C-ITS Governing Body), operation (Compliance Assessment Body) and supervision (C-ITS Supervision Body). Main decision body is the C-ITS Governing Body.
- Any new C-ITS station must fulfil the compliance assessment criteria to be part of the C-ITS security trust model.
- Considering the challenging time schedule of setting up a final organisation as described by the Compliance assessment Working Group, progressive development of this organisation should allow for deployment in a relatively short timeframe (2019).
- After 2019, the proposed compliance assessment organisation should be able to also address and ensure interoperability of existing services and future C-ITS service extensions and technology deployments.

- The proposed organisation shall have the capability allowing the introduction of new services and/or new technologies in a backward compatibility manner with already deployed services.
- Need to finalise by second half of 2018 the standards and profiles necessary to support the compliance assessment process for Day 1 services.
- Need to maintain consistency with other validation frameworks having an impact on connected and automated vehicles and road infrastructure, e.g. in the future, evolution of data quality requirements may be needed for higher levels of automated vehicles.
- Further work is needed to elaborate a common EU framework to cover the roles defined by all WGs (in particular compliance assessment, privacy/data protection, security).