C-ITS Platform

WG5: Security & Certification

Final Report

ANNEX 4: Compliance assessment in Cooperative ITS (C-ITS)

An analysis of the challenges, potential approaches and processes for compliance assessment in C-ITS

v1.0

1 Contents

2 Scope

The objective of this document is to give a comprehensive, high level overview on the process definition for the compliance assessment for C-ITS systems or stations and C-ITS enabled vehicles.

The term "compliance assessment" is used in this report to describe the process by which a C-ITS station is validated through a set of tests to be deployed in the market. In this context to C-ITS, the generic overarching term "*compliance assessment*" is used, since other terms like for instance "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). On the basis of this assumption, all the cases formulated in this report do not include type approval because there is no planned (at the time of writing this report) regulation in C-ITS, which would require type approval. For additional details on this aspect, see also section 7.

Please, see section 4 for a definition of various terms used in the road transport sector for testing.

For the achievement of key public policy goals, C-ITS stations require compliance assessment before being placed on the EU's internal market. This report will briefly look at which technical aspects are required to achieve public policy goals, such as road safety, protection of health, environmental protection, energy efficiency, protection against unauthorised use, non-discriminatory market access, etc. Then, this report discusses, in which cases compliance assessment procedures are necessary.

This report identifies and refers to other documents or reports for product/system validation and certification for deployment of C-ITS. This document points to existing procedures wherever possible, and includes outlooks on missing parts for the C-ITS domain.

The subjects for C-ITS compliance assessment based on the policy goals of C-ITS deployment will most likely include:

- Interoperability of C-ITS stations and groups of applications (based on minimum system requirements)
- Security (e.g., Common Criteria)
- Performance (minimum/nominal system performance)
- Reliability (over time, over environmental, over application categories,…)
- Backward compatibility procedures, migration path, extendibility of applications
- Categories for integration levels (component, C-ITS station, etc.)
- Categories of test locations (laboratory, vehicle, etc.)

This report shall provide input to all stakeholders involved in the compliance assessment. The identified risks, deduced conclusion and recommendations within the document shall support decision making process. The ambition is to provide lean, practicable and economically feasible procedures.

Existing structures and procedures (e.g. for the vehicle ITS station the UN ECE WP.29, CE) are well recognised and any process for compliance assessment shall not invent new procedural bodies/structures without clear justification. On the other side, some features of C-ITS may require extension of existing procedures.

The requirements for compliance assessment might differ for:

- regulatory applications

- commercial applications and
- road safety related applications.

Further, C-ITS compliance assessment can be addressed at different levels (technology, system or ITS station level, group of applications, …). These points are recognised and in general considered in the conclusions or recommendations of this report. The conclusions and recommendations do **not** favour whether the certificate of conformity shall be issued by **an independent third party** or through **self-compliance assessment** by industry stakeholders, C-ITS station operators or a combination hereof. This report will discuss different options including pros and cons for each option

To summarize, the objectives in this report are:

1. To identify the main phases in the compliance assessment process in C-ITS for the different categories of applications
2. To identify risks and challenges for these processes
3. To identify the main stakeholders involved
4. To define a feasible approach for compliance assessment of the C-ITS network both from the organizational and technology point of view.

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.pdf
[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/.

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 specifications of a relevant standard.
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 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.

5 Context description

5.1 Policy Framework

Within Europe, two systems of type approval have been in existence for over 20 years for road transportation. One is based around EC Directives (see [5]) and Regulations, and provides for the approval of whole vehicles, vehicle systems, and separate components. The other is based around UN Regulations and provides for approval of vehicle systems and separate components, but not whole vehicles. In addition for C-ITS, the Radio Equipment Directive (RED) (see [6]) will apply because of the Short Range Communications (ITS-G5) devices used in C-ITS stations. The RED directive also includes cellular networks used in C-ITS.

As described in [5], type approval can be both for vehicle systems or separate components. Note that the directive also includes the case where a component can be approved only in conjunction with other parts of the vehicle, thereby making it possible to verify compliance with the requirements only when the component or separate technical unit is operating in conjunction with those other vehicle parts.

Because the term type approval is mainly used for current deployment in the market of conventional vehicles and it is mostly related to mechanical, environmental testing, in this report it has been decided to use the term **compliance assessment for C-ITS stations**. Another reason why this term has been chosen is because C-ITS station does not only represent the vehicle, but also roadside equipment and possibly personal ITS Stations in the future. This is also in line with the ITS Directive [10], where conformity assessment procedures are used for ITS roadside equipment.

In this report, the term compliance assessment and conformity assessment from [10] are synonym.

5.2 Regulatory and standardization frameworks

5.2.1 UN ECE WP.29

The UN 1958, 1997 and 1998 agreements [7] provide the legal framework to assure road safety, health protection, environmental protection, energy efficiency and the protection against unauthorised use for the contracting parties to establish regulatory instruments concerning motor vehicle and motor vehicle equipment. UN ECE World Forum for Harmonization of Vehicle Regulations aims at providing a harmonized regulatory framework supporting innovations for safe and environmental friendly vehicles. The regulatory framework developed by WP.29 allows the market introduction of innovative vehicle technologies and is facilitating cross-border trade, since provisions established under the 1958 Agreement include the reciprocal acceptance of approvals of vehicle systems, parts and equipment issued by other Contracting Parties.

5.2.2 Radio Equipment Directive

Self assessment procedures. The report will link the analysis with the recent Radio Equipment Directive (RED) 2014/53/EU [11] for telematics equipment.

The RED directive is applicable to C-ITS. In particular, as described in [11], we note the following clauses:

- (10) In order to ensure that radio equipment uses the radio spectrum effectively and supports the efficient use of radio spectrum, radio equipment should be constructed so that: in the case of a transmitter, when the transmitter is properly installed, maintained and used for its intended purpose it generates radio waves emissions that do not create harmful interference, while unwanted radio waves emissions generated by the transmitter (e.g. in adjacent channels) with a potential negative

impact on the goals of radio spectrum policy should be limited to such a level that, according to the state of the art, harmful interference is avoided; and, in the case of a receiver, it has a level of performance that allows it to operate as intended and protects it against the risk of harmful interference, in particular from shared or adjacent channels, and, in so doing, supports improvements in the efficient use of shared or adjacent channels.

- (11) Although receivers do not themselves cause harmful interference, reception capabilities are an increasingly important factor in ensuring the efficient use of radio spectrum by way of an increased resilience of receivers against harmful interference and unwanted signals on the basis of the relevant essential requirements of Union harmonisation legislation.

5.2.3 Common Criteria for security assessment

One of the elements of the compliance assessment process is the validation of the security requirements. This can be achieved by different approaches. One of the most known approaches is based on Common Criteria (CC).

As defined in [12], the CC permits comparability between the results of independent security evaluations. The CC does so by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. These IT products may be implemented in hardware, firmware or software. The evaluation process establishes a level of confidence that the security functionality of these IT products and the assurance measures applied to these IT products meet these requirements. The evaluation results may help consumers to determine whether these IT products fulfil their security needs.

Common Criteria can be applied to C-ITS but to ensure an adequate level of security assurance for the C-ITS station.

5.2.4 EU Product rules

- Regulation 765/2008 accreditation & market surveillance
- Decision 768/2008 common framework on marketing products

5.3 Stakeholders or Roles

The main stakeholders involved in the compliance assessment process and lifecycle of the C-ITS station, especially in the setup (and decommissioning) but also in the regular operational phase of the C-ITS network are the following:

Central organizations:

- **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 governing body.
- **Compliance assessment governing body**: the central governing body in the compliance assessment process, defines the Common Criteria (if this process is accepted by the C-ITS community) for the compliance assessment labs and the governing rules and procedures for the compliance assessment tests and procedures. It issues the C-ITS certificates of compliance.

- **Trust model manager**: This is the entity responsible for managing the trust model infrastructure (e.g., PKI) according to the requirements of the C-ITS Governing Body.
- **C-ITS Supervision Board**, who is responsible for the detection of problems in the deployment phase, which can be reported to Compliance assessment governing body for further analysis and action.
- **Standardization bodies**: responsible for drafting the standards for communication and testing (e.g., EN ISO/IEC 17065:2012).

Setup and decommissioning phase of C-ITS stations and networks:

- **Compliance assessment lab:** executes the compliance assessment tests and procedures.
- **Workshop for mobile C-ITS stations**: for the setup and decommissioning of the mobile C-ITS station.
- **Workshop for roadside C-ITS stations**: for the setup and decommissioning of the roadside C-ITS station.
- **Manufacturer** of the C-ITS Station. Responsible for production and performance of the compliance assessment procedure for the single C-ITS stations in the related market segment.
- **Enrollment authority**: This entity is responsible to perform the enrolment of a C-ITS station based on a positive test outcome of a compliance assessment lab. The enrolment is related to the recording of the ID and features of a C-ITS station before deployment in the field.
- **Authorization 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.
- **Member state authority**: responsible for the distribution of cryptographic material for public safety related C-ITS station network, if required by security policy.

Operational Phase of the C-ITS network:

- **Operator** of the C-ITS Station (e.g. vehicle manufacturer or road operator)
- **Workshop for mobile C-ITS stations** (as above) for maintenance and periodic inspection**.**
- **Workshop for roadside C-ITS stations** (as above) for maintenance and periodic inspection.
- **User**: This is the driver of the C-ITS vehicle.
- **Service provider**: This is the servicing entity of C-ITS stations for regular tasks on behalf of users, operators, manufacturers or other organisations.
- **Law enforcement organization:** It represents a law enforcer organization, which must ensure conformance to the regulations and to the specific public policies of the C-ITS governing body.

These stakeholders and roles must not be fully defined at the beginning of the C-ITS roll-out, but respective tasks should be defined by the stakeholders involved and be planned to enable a future extension of the roles.

5.4 Categories of C-ITS Stations

This section describes the different categories of C-ITS Station based on the basic architecture described in ISO 21217/EN 302 665.

The following groups of C-ITS stations can be identified for compliance assessment processes:

- Roadside C-ITS station: C-ITS station in a roadside ITS sub-system.
- Vehicle C-ITS station: C-ITS station in a vehicular ITS sub-system.
- Central C-ITS station: C-ITS station in a central ITS sub-system.
- Personal C-ITS station: C-ITS station in a personal sub-system

6 Compliance Assessment process

6.1 Introduction

This section describes an envisaged C-ITS compliance assessment process and how the stakeholders identified in 5.3 are involved or responsible for the different phases.

The overall workflow is based on the concept that a **C-ITS station** must pass the compliance assessment phase to be enlisted in a "**List of Certified C-ITS Stations**".

6.2 Compliance assessment process overview

The proposed compliance assessment framework is intended to certify compliancy and suitability of a C-ITS station.

The compliance assessment framework would need to be coordinated by an independent organisation, representing the relevant stakeholders. The following C-ITS compliance assessment scheme is based on the existing and well-established mobile terminal compliance assessment scheme from the Global Compliance assessment Forum (GCF) [http://www.globalcertificationforum.org/]. However, for C-ITS, the compliance assessment processing must for instance also take safety aspects in consideration, which are not the main focus in the compliance assessment scheme from GCF.

Figure 1 provides an overview of the compliance assessment process.

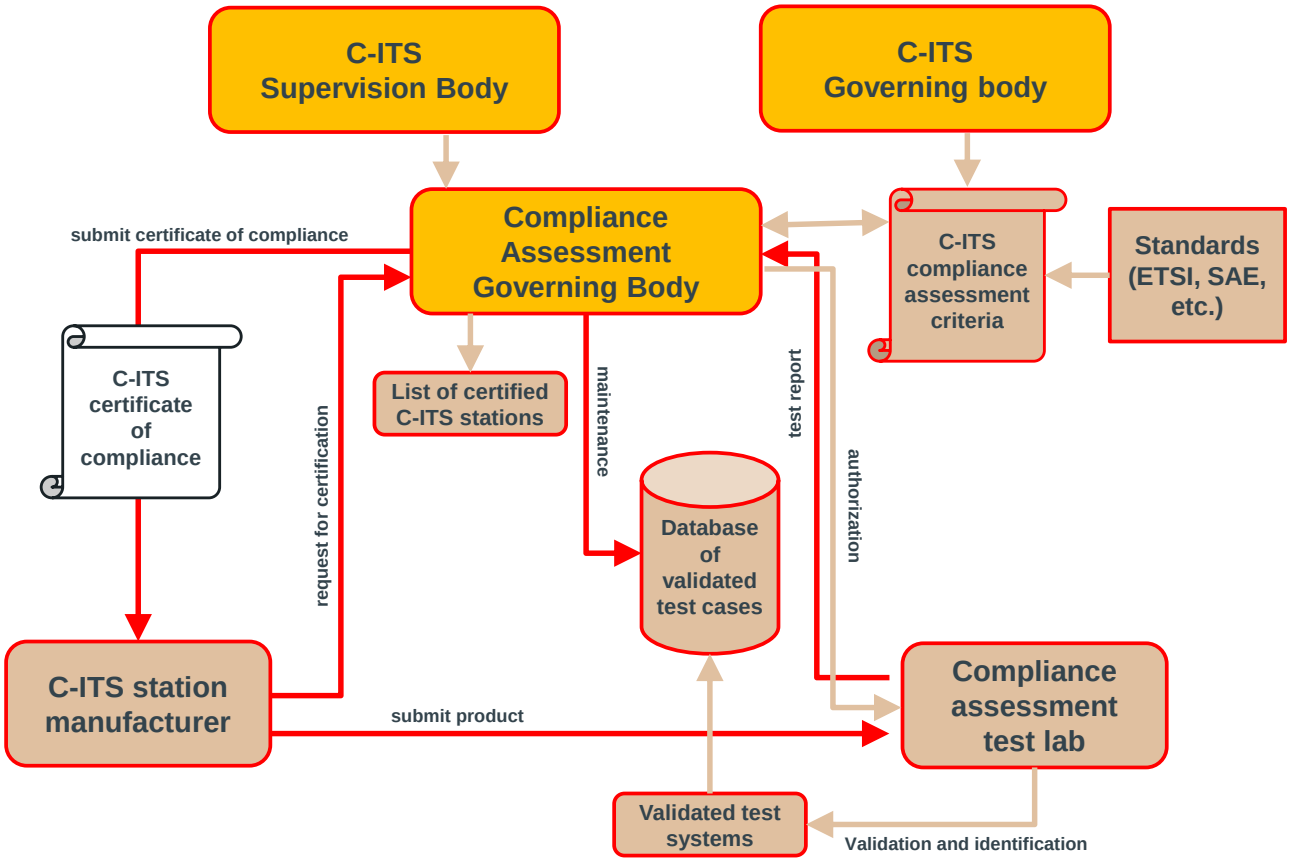

Figure 1 Overview of the Compliance Assessment Process

The **compliance assessment governing body** is a centralized entity responsible for:

- Definition of compliance assessment criteria, which are compliant to and using the C-ITS Governing Body's input documents for operational and security requirements and the standards.
- handling of compliance assessment requests of C-ITS manufacturers
- definition of test scope for the compliance assessment (based on the C-ITS station type and functionality)
- definition of the minimum set of test criteria for the compliance assessment of every C-ITS station in order to be an interoperable node of the C-ITS Network
- submit certificate of compliance after successful C-ITS compliance assessment.
- maintenance of the list of certified C-ITS stations.
- authorization of ISO17025 accredited test labs (e.g., independent test labs)
    - based on frequent repetition of the accreditation in strict accordance on not yet defined certain criteria, but in accordance of the valid EU wide C-ITS Trust Modell and the respective procedures
    - nomination of qualified lab auditors
- maintenance of a database, which lists and stores validated test cases and validated test systems, which must be used for the execution of the test procedures for compliance assessment.

The Compliance assessment Governing Body can be accredited according to to the following standard:

- EN ISO/IEC 17065:2012 - Conformity assessment – Requirements for bodies certifying products, processes and services

The **Compliance assessment test lab** is responsible for:

- execution of test cases according to the C-ITS compliance assessment criteria
- testing will be performed:
    - by qualified persons
    - only on validated test systems
    - in a shielded lab environment
- validation of test cases on selected and validated test systems
- creating test reports and submission to the Compliance assessment Governing Body

The Test Lab should be accredited according to the following standard:

- EN ISO/IEC 17025:2005 - General requirements for the competence of testing and calibration laboratories.

The details of the main elements of the compliance assessment process are described in the following sections.

6.3 Authorization

The purpose of this section is to look at the requirements for moving from the design and production to make a C-ITS station a part of the trusted C-ITS system and manage it during its life time. It is a prerequisite for being a part of the C-ITS system that a C-ITS station is authorized in the C-ITS security system. The basic C-ITS security which is based on security certificates allows a receiving C-ITS station to verify that the transmitting C-ITS station is trustworthy. However, on its own the security mechanism only verifies that the transmitting C-ITS station is using a valid certificate. Therefore there must be some rules for who administrates the certificates (**Authorization Authority**) and on what principles they are located. As part of these rules it appears reasonable to set some minimum requirements for conformance of the C-ITS stations. Clearly these conformance requirements should ensure a level of interoperability, but also ensure that not only the security certificate but also the content of the information sent by the C-ITS station has a certain level of trustworthiness.

Looking at the **Authorization Authority** function and its needs, it is clear that on one side it needs to be authorized to allocate long term certificates to the requester (OEM, Supplier, road authorities, enforcement agencies as described in chapter 5.3.) - this topic is considered part of the security framework, and therefore not considered in this document. Secondly the Authorization Authority needs information about whether the C-ITS station in question is fulfilling the minimum requirements of conformance. To keep roles separate in this description it is requested that there exists a Database of models of C-ITS stations that fulfil the minimum requirements of conformance for each type of C-ITS stations (**List of Certified C-ITS stations**). This means that when certificates are requested by a requester the Enrolment Authority for the conformance and performance aspects simply will check in the database (List of C-ITS station) whether the C-ITS station model is on the list for the given type of C-ITS stations or not before starting the process of allocating certificates.

6.4 Compliance assessment function and test cases definition

6.4.1 Basic elements of compliance assessment - the Compliance assessment Function

In order to build and operate the databases of C-ITS stations a **Compliance assessment Function** is needed. To operate the database the minimum requirements for conformance and performance needs to be established and maintained. This will typically consist of the following elements:

- Set of test cases per C-ITS station
- Compliance assessment Criteria for each type of C-ITS station (list of subset of test cases required to be passed for a given type of C-ITS station, and the minimum criteria for every validated C-ITS station in the network)
- Database of verified test cases and test implementations
- Rules for declaration of conformance

6.4.2 Development of set of test cases

Test cases are often developed by the same Standards Setting Organisations, which develop the basic specification for a system. Test cases aim to ensure the interoperability, performance and conformance with the underlying standard. Often this is an iterative process where the parties using the test cases identify the need for additional test cases. Test cases are often developed to cover multiple options and different types/variants of equipment and thus not all test cases will be applicable for all different types/variants of equipment. Therefore test specifications will normally be supplemented with documents that identify which test cases are relevant for which types/variants of equipment.

For C-ITS, the test specifications can be based on a black box approach. However, for some aspects of the security, e.g. protection of credentials other well defined methods and compliance assessment schemes (e.g., common criteria) exist and can be used.

Beyond black box testing for communication only, interoperability tests will also be needed to complete the compliance assessment process.

6.4.3 Compliance assessment Criteria

To set the Compliance assessment criteria, it will be necessary for any given type of C-ITS station to select the set of identified tests that needs to be passed in order be put on the List of Certified or C-ITS stations.

As a C-ITS station is containing radio parts, it will have to fulfil the Radio Equipment Directive (RED) 2014/53/EU for telematics equipment. As radio equipment cannot be put on the market in Europe without fulfilling the Radio Equipment Directive (RED) all C-ITS equipment will have to pass the corresponding tests. Even though these tests might belong to other approval regime, one can argue that passing the RED relevant tests should be a part of the Compliance assessment criteria. However, it is clear that inclusion of these in the Compliance assessment Criteria should be done in such a way that the testing do not add any additional burden to that caused by the RED. Similar it is clear that the legal status, responsibilities etc. still is regulated by RED.

For selection of other tests to be part of the Compliance assessment criteria considerations should be given to the trade-off between cost and complexity of performing the relevant test versus the value added of a given test. The current standardisation of C-ITS have focused on the transmitted signals and not specifying the behaviour of actual applications. This is the case since the applications may involve other input than just the

data that is received from other C-ITS stations. Therefore testing of such applications is not suited as being a part of the Compliance assessment Criteria, however depending of their nature they can be subject to other specific regulatory frameworks. However for, e.g., a Roadside C-ITS Station it can be considered to test whether it correctly forwards the information received, but this can only be tested if there in the future exist standards for how to aggregate and forward information.

Considering this it is proposed that the test selected to be part of the Compliance assessment Criteria should focus on the transmitted signals compliance with the standards and their content, e.g. triggering of certain type of messages and the timing hereof.

Also it is important to clearly define the boundaries for the Compliance Assessment, e.g., for a Roadside unit it will not be realistic to include the complete backhaul and traffic management in the Compliance assessment Scheme. Also proper considerations need to be given to what is to be a part of the Compliance assessment criteria and what is a part of policies. As an example, certain specific requirements might be identified for C-ITS stations in Emergency Vehicles or public transport, but the right for a given C-ITS station to take on board this role is not a technical issue, but a policy issue that needs to be a part of the rules the Enrolment Authority uses. A possible approach would be that the framework proposed in this report is only for **'generic' C-ITS stations.** The 'specialized' C-ITS station (like an emergency vehicle) will have additional compliance assessment schemes or even type approval schemes if the specialization of the C-ITS station is based on a specific regulation.

One thing is to setup the general rules for the Compliance assessment Criteria, but there needs to be an entity with the responsibility for the Compliance assessment Criteria and the maintenance of the current list of test required test cases. As C-ITS development can change in time, the definition regulatory frameworks is to be discussed. Therefore models of setting up a Compliance assessment Criteria Board with representative for the relevant stakeholders should be considered.

It is important to notice that no set of Compliance assessment Criteria will ever be so complete that it fully can remove the need for Interoperability tests. As said before, interoperability tests must be defined and maintained as part of the compliance assessment process.

6.4.4 Test case availability and validation

In the previous section, the availability of test specifications has been assumed, but this is not sufficient in itself. The actual test cases need to be implemented and verified. In the worst case, a C-ITS station will pass on one test implementation and fail on another and second C-ITS station might fail on the first implementation but pass on the second implementation. This clearly can lead to interoperability issues. It is therefore important to establish a process to validate test case implementations and establish a database of validated test cases and related products. This is clearly another task of the overall Governance and Initialisation function and could be a role of the Compliance assessment Governing Body.

It is important to have procedures and responsibilities established to deal with situations where it is later found that a validated test case is incorrect. The consequences of this might not be as simple as just removing the test case from the database of validated test cases, as C-ITS stations passing the test case might already have entered the market. It is therefore important to define a process for re-testing and re-compliance assessment of C-ITS stations to address faults in the test definitions.

Also situations can occur especially in the start-up phase of C-ITS that the database of validated test cases do not contain a validated test case corresponding to each of the test cases required in the Compliance assessment Criteria.

What are the options in such a case ?

1. Wait with Compliance assessment and deployment until the complete set of tests are available – risk to lead to long delays
2. Introduce an interim Compliance assessment based on available tests. The risk is that equipment will enter the market that might not have been fully tested.

The most feasible option to ensure a smooth and safe deployment of C-ITS in Europe for Day One applications would be to ensure that the set of test is complete as much as possible (Option 1). It is acknowledged that identification of problems in the field (detected by the C-ITS supervision body described below), evolutions of technologies, new C-ITS applications and changes in the regulatory context may anyway require modifications to the compliance assessment criteria and test procedures. As a consequence a process for updating such criteria must be defined.

6.4.5 Rules for the declaration of performance

With clear definition of the Compliance assessment Criteria and well defined validated test cases, one of the main questions is what documentation will be required as proof of compliance with the Compliance Assessment Criteria. There is a question if they should be complete test reports or just signed statements of compliance. Our recommendation is that they should be both, so that the compliance assessment governing body has the details of the test report in case the statement/certificate of compliance was based on invalid results or not properly created.

6.4.6 Supervision

There is always a risk that issues with the system or with equipment is first detected when systems are already deployed in the market. For this reason a regular and consistent monitoring of misbehaving communication messages by all C-ITS stations, including a regular reporting to the respective C-ITS station operator with an analysis and a public summary report is a first step. It is therefore necessary to have a supervision process, e.g. operated by an additional C-ITS Supervision body, where problems can be reported and analysed. It is clear that if the reported problem relate to specific products the manufacturer might need to be invited to participate in the analysis of the reported problem. When the nature and the cause of the problem is identified a clear process for how to identify the actions to be taken needs to exist. Some possible actions could be:

- Addition of tests to the Compliance assessment Criteria for future Compliance Assessments.
- Update/correction of test case(s)
- Update of system specifications with corresponding updates to the Compliance assessment Scheme
- Request to manufacturer of updating future production, possibly new Compliance Assessments.
- Removal for Database of list of C-ITS stations.
- Request for update of equipment in the market
- Etc.

For such a supervision process to function, it is important that it is setup with clear rules and in such a way that it will be considered fair and impartial. Even though resolution of problems in general should be

negotiated to find pragmatic solutions to the issues identified, the Supervision Board needs to have the necessary powers to take actions, e.g. to remove a C-ITS station form the list of C-ITS stations.

Considering the importance of this function how to setup a supervision Board should be carefully examined, but a Supervision Board composed of representatives for the relevant stakeholders should be considered.

6.4.7 Re-execution of Compliance assessment

There may be the need for the re-execution of the compliance assessment in specific situations, which are described here. In re-compliance assessment the elements of the system must be designed to minimize the need for re-compliance assessment or re-alignment, adjustment, and replacement of critical components. When systems or subsystems are "repaired" it is important that any remaining security certificates or be either invalidated immediately, or that there be a trusted process that allows the C--ITS station to be re-validated for compliance assessment and allow the continued use of its security certificates. Regarding re-certification, the following types of issues will need to be addressed:

- Will periodic inspection be required to ensure that a re-compliance assessment is needed?
- What type of failed metrics or errors can cause a re-compliance assessment?
- Should be these metrics be harmonized?
- What is the relationship between the life span of the certificates and the need for periodic inspections?

7 Identification of risks and challenges

Following the discussions of the C-ITS Platform WG5 experts, this section describes the potential issues and challenges to design and deploy an effective compliance assessment process including liabilities. This section aims to summarise the concerns and open discussion points of the proposed compliance assessment process in section.

The following risks/challenges are identified in the compliance assessment process of C-ITS:

1. An approach of compliance assessment based on "Black box" testing can be simpler than "white box" testing but security vulnerabilities may not be identified and discovered before C-ITS station deployment. Black box testing is understood as testing of a C-ITS station on the basis of its functions and not the inner working or structure of the C-ITS station. While "black box" testing is widely used and effective in most cases, it is noted that security testing (e.g., higher level of Common Criteria evaluation) requires "white box" testing. For example, the analysis of the code to identify deficiencies in the design and development, which could be exploited by malicious parties. In addition, it is noted that Black Box testing has limited support for the extension of a C-ITS station towards new or additional applications because Black Box testing is initially performed against a specific application.

2. Compliance assessment should include security and privacy aspects. There are some basic security aspects in compliance assessment, which should be clarified. For example if a Common Criteria evaluation model would be appropriate in C-ITS and up to which level. Lack of security testing in C-ITS can generate security vulnerabilities, which are difficult to address after the design and deployment phases. In addition, if compliance assessment does not include security and privacy aspects, there is the risk that interoperability is not fully supported in C-ITS because the authentication or integrity of the message could be different among the C-ITS stations.

3. An important question is which entity should have the responsibility of the Compliance Assessment board and/or the responsibility for the maintenance of the Compliance Assessment database of test cases at European level.

4. The model presented in this report has a "static" vision of the software components and applications in a C-ITS station. In other words, the components of the C-ITS station are tested for a specific combination of software and hardware against specific functions before deployment in the field, but the possibility of upgrading the software in the field is not addressed. While, it would be preferable not to perform any upgrade of the operational C-ITS stations and its components in the field, the reality is that software errors and subsequence patches or software upgrades may be needed. It is possible that the download and activation of software not properly tested in the components of a C-ITS station can generate security vulnerabilities. In other words, the feasibility of supporting a "static" model for software in C-ITS when software errors and software upgrade (e.g., patching) is often needed in any existing ICT applications should be further discussed. According to some experts' opinion C-ITS stations are composed by hardware and software and every change to hardware or software should require a new compliance assessment even if it is already operational in the field. This may imply to foresee a recall process of the C-ITS stations.

5. Interoperability testing should be part of the compliance assessment process. If the standards and the related conformance tests have deficiencies, there is the risk that the conformance test to specific standards would not automatically guarantee interoperability among the C-ITS stations when operational. Interoperability tests also addresses the support for end-to-end compliance assessment.

6. Considering that some C-ITS applications are safety related, a regulatory framework could be defined in the future to ensure the safety of drivers and passengers. If such a regulatory framework is put in place, the initial assumptions in this report that a type approval is not required may have to be revised.

8 Recommendations

On the basis of the analysis provided in the previous sections, the WG5 experts recommend:

(1) to pursue a compliance assessment process for C-ITS as proposed and described in section 6 for Day One deployment of C-ITS. During the implementation of this process, at least the risks and challenges identified in Section 7 have to be further analysed and discussed with the involved stakeholders in order to ensure a well-functioning C-ITS compliance assessment process. For the definition of the details of this process, the main stakeholders in the C-ITS deployment, e.g. public authorities and road operators, vehicle manufacturers and C-ITS station suppliers and C-ITS station operators, should be directly involved to define the necessary next steps together.

(2) On the basis of the first recommendation, the central entities defined in Section 6 should be selected at European level. For example a governing body must be established which is in charge of defining the C-ITS Station requirements to both realise those technical aspects and meet the stakeholders' needs. Further a compliance assessment authority, which administers the compliance assessment criteria and the timing for the applicability, should be defined.

(3) Need for Legal Certainty: The need for an appropriate legislative framework (e.g. new EU delegated acts or the identification of the amendments to the existing EU regulatory framework) needs to be analysed.

(4) The financing scheme needs to be discussed to identify which parties will support or contribute to the financing scheme to support the compliance assessment process.

(5) A time-plan to endorse the compliance assessment process should be defined. It is important that the first set of C-ITS compliance assessment criteria is available at least 18 months before start of operation of C-ITS (an envisaged goal for the first version of the C-ITS compliance assessment criteria would be in 2017). This time-plan should define the main milestones and dependencies among the different tasks.