C-ITS Platform

Final report

January 2016

This report represents the views of the members of the C-ITS Platform on the subject matter. These views have not been adopted or in any way endorsed by the Commission and should not be relied upon as a statement of the Commission's or DG MOVE's views. The European Commission does not guarantee the accuracy of the data included in this report, nor does it accept responsibility for any use made thereof.

C-ITS Platform

Final report

January 2016

1. Executive summary

Cooperative Intelligent Transport Systems (C-ITS) use technologies that allow road vehicles to communicate with other vehicles, with traffic signals and roadside infrastructure as well as with other road users. The systems are also known as vehicle-to-vehicle communications, or vehicle-to-infrastructure communications.

With alerts generated from the increased information available, these systems have a strong potential to improve road safety and the efficiency of the road transport. Because of these expected benefits and considering the overall relatively moderated costs linked to deployment, there is a strong interest in enabling a fast move at European scale that will translate into market production and early deployment.

The European industry has traditionally held a competitive position on a global scale in the field of intelligent transport systems. Maintaining this privileged position also in the area of cooperative systems is crucial: new business cases arise and more actors at an international level are challenging Europe's competitive edge.

At the same time, though clearly moving from research to large scale pilot deployment, C-ITS has been facing a recurrent "chicken and egg" problem: where should investments start first, how to stimulate the emergence of business cases, how to foster interoperability and on which basis should cooperation amongst public and private stakeholders be pursued.

The Platform for the Deployment of Cooperative Intelligent Transport Systems in the European Union (C-ITS Platform) was created by the European Commission services (DG MOVE) in November 2014 with the clear intention to help addressing this "chicken and egg problem" and support the emergence of a common vision across all actors involved in the value chain. The C-ITS Platform, which gathers public and private stakeholders, represents all of the key stakeholders along the value chain including public authorities, vehicle manufacturers, suppliers, service providers, telecomm companies etc., and delivered in its first phase (November 2014 – January 2016) its contribution towards a shared vision on the interoperable deployment of Cooperative Intelligent Transport Systems in the European Union.

The C-ITS platform addressed the main technical (frequencies, hybrid communications, (cyber-)security and access to in-vehicle data and resources) and legal issues (such as liability, data protection and privacy). Regarding access to in-vehicle data and resources, the work of the Platform was also guided by the recent adoption of the eCall type-approval Regulation, which requests the Commission to "assess the need of requirements for an interoperable, standardised, secure and open-access platform". The Platform also covered standardisation, cost benefit analysis, business models, public acceptance, road safety and other implementation topics, international cooperation, etc.

Within working groups dedicated to these issues, the C-ITS Platform developed policy recommendations and proposals for action for both the Commission but also for other relevant actors along the C-ITS value chain. The progress of the development of work in the

different working groups was however not completely homogeneous, due to the nature of the topics treated in each of them. On most issues a shared vision emerged, including on the common solutions to address these issues, whereas on some others the related working group succeeded on mapping the issues and possible ways to address them but did not yet share a common solution.

Among the outcomes of the C-ITS Platform, which address the issues related to the following aspects:

- the common technical framework necessary for the deployment of C-ITS,
- the legal questions related to C-ITS,
- the "legitimacy" of the deployment of C-ITS, i.e. the fact that the deployment of C-ITS can be justified and fostered at all levels, and
- international cooperation,

the following conclusions can be highlighted:

A common technical framework

- **List of Day 1 services**

The C-ITS Platform agreed on a **list of 'Day 1 services'** which, because of their expected societal benefits and the maturity of technology, are expected to and should be available in the short term (personal benefits, users' willingness to pay, business cases and market driven deployment strategies were not taken into account at this stage):

- ***List of Day1 services***
  Hazardous location notifications:
  Slow or stationary vehicle(s) & Traffic ahead warning
  Road works warning
  Weather conditions
  Emergency brake light
  Emergency vehicle approaching
  Other hazardous notifications
  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 (GLOSA)
  Probe vehicle data
  Shockwave Damping (falls under ETSI Category "local hazard warning")

Furthermore, the C-ITS Platform also agreed on a list of 'Day 1'5 services', considered as mature and highly desired by the market, though, for which specifications or standards might not be completely ready.

- ***List of Day 1'5 services***
  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 (1st and last mile, parking, route advice, coordinated traffic lights)
  Traffic information & Smart routing

- **Security and Certification**

Security is paramount to the deployment of C-ITS in the EU. No security, no C-ITS.

The main security aspects in C-ITS, which must be addressed to support a secure and safe deployment across Europe, have been identified and discussed within the C-ITS platform.

The recommendations of the C-ITS platform are very clear: **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**. Beyond the Day 1 phase, C-ITS may be extended with multiple interoperable trust domains if deemed necessary to take the variety of stakeholders and the responsibilities for private and public entities involved into account. There is also a definite **need for international cooperation beyond the EU to discuss how interoperability of other domains (outside Europe) with the single EU trust domain can be realised**. This topic is even more relevant for the future where the emergence of multiple trust domains in Europe may occur.

All related aspects (e.g. standardisation, revocation of trust, compliance assessment, identification and involvement of actors regarding the governance of the PKI) must take part in a **clear time plan for the secure deployment of C-ITS**. It is emphasised that the **C-ITS compliance assessment process should be discussed at an international level**, in order to identify areas where harmonisation is needed.

- **Radio frequency and hybrid communication**

The C-ITS platform concluded that currently neither ETSI ITS-G5 nor cellular systems can provide the full range of necessary services for C-ITS. Consequently a hybrid communication concept is therefore 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 C-ITS Platform recommends that **for short-range communications in the 5.9 GHz band initially the communication system to be used is IEEE802.11p/ETSI ITS-G5**, and to study whether geographical coverage obligations can be introduced to increase coverage of C-ITS services through existing cellular communications infrastructure, and therefore foster uptake of C-ITS services.

Another **major achievement of the C-ITS platform has been to agree on mitigation techniques to ensure coexistence between 5.8 GHz tolling DSRC and 5.9 GHz ITS**

applications. The approach that was developed to ensure this coexistence is reflected in the forthcoming update of the relevant Electronic Communications Committee (ECC) Regulations and ETSI Technical Specifications. Other co-existence issues (e.g. with urban rail) need to be studied and mitigated.

Risks related to possible WAS/RLAN expansion in the 5 GHz band have been identified. **The C-ITS Platform recommends that the 5855-5875 MHz, the 5905-5925 MHz and the 63-64 GHz band are designated to C-ITS services to cope with future capacity demand.**

The C-ITS platform recommends also to **seek international cooperation**, e.g. via joint studies and positions, towards the protection of the 5.9 GHz and the allocation of additional spectrum in the 63 GHz frequency band.

- **Standardisation**

In addition to standardisation needs dealt with in each working group of the C-ITS platform, an overview of the standards being used within current C-ITS deployments initiatives in the EU has been collected. This is the first important starting point which will help to lay the necessary foundation to further discuss in a second phase how profiles can and have to be defined for EU-wide interoperable C-ITS deployment in the near future.

- **Decentralised Congestion Control (DCC)**

DCC has been developed to handle network stability in the absence of an access point or base station, when faced with an increasing number of C-ITS messages being emitted, in order to avoid interference and degradation of C-ITS applications. It has been standardised in the approved ETSI Technical Specification 102 687 V1.1.1. **This current specification is deemed sufficient for early deployment of Day 1 applications** , i.e., no short term actions need to be taken. ETSI TC ITS is currently making its first steps towards addressing DCC supporting an increased penetration of C-ITS. Supporting further work at ETSI level to also include future requirements such as the introduction of C-ITS for vulnerable road users (VRU) in particular pedestrians is deemed necessary by the C-ITS Platform.

- **Access to in-vehicle data and resources**

This topic had a rather specific position within the C-ITS platform, as its scope was well beyond purely C-ITS and included existing and possible future in-vehicle applications or services. Specific was also the link to existing legislation, in particular the eCall type-approval Regulation, which requests the Commission to "assess the need of requirements for an interoperable, standardised, secure and open-access platform" (article 12(2) of Regulation 2015/758).

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:

(a) Data provision conditions: Consent

The data subject (owner of the vehicle and/or through the use of the vehicle or nomadic devices) decides if data can be provided and to whom, including the concrete purpose for the use of the data (and hence for the identified service). There is always an opt-out option for

end customers and data subjects. This is without prejudice to requirements of regulatory applications.

(b) Fair and undistorted competition

Subject to prior consent of the data subject, all service providers should be in an equal, fair, reasonable and non-discriminatory position to offer services to the data subject.

(c) Data privacy and data protection

There is a need for the data subject to have its vehicle and movement data protected for privacy reasons, and in the case of companies, for competition and/or security reasons.

(d) Tamper-proof access and liability

Services making use of in-vehicle data and resources should not endanger the proper safe and secure functioning of the vehicles. In addition, the access to vehicle data and resources shall not impact the liability of vehicle manufacturers regarding the use of the vehicle.

(e) Data economy

With the caveat that data protection provisions or specific technologic prescriptions are respected, standardised access favours interoperability between different applications, notably regulatory key applications, and facilitates the common use of same vehicle data and resources.

Three technical solutions have been identified for this access to in-vehicle data and resources: the on-board application platform, the in-vehicle interface and the data server platform.

In addition to the guiding principles, standardisation needs were also agreed as an input to the 2015 Rolling Plan for ICT Standardisation as well as a technical solution for the in-vehicle interface, and progress in the identification of possible use cases and related data needs was made.

It is thus recommended to always base the access to in-vehicle data and resources on the five guiding principles, and to further investigate standardisation needs and start standardisation work at appropriate level(s), including also possible retrofit solutions.

Nevertheless, strong disagreements between vehicle manufacturers and the independent operators/service providers remained on several important topics, in particular: different views on how data can be accessed, different strategies towards on-board application platform, different governance of the data server platform, different views regarding concrete implementation and possible legislation.

As many of these issues were not only technical issues, but also concerns linked to the lack of trust between direct competitors, exploring new ways to improve cooperation are recommended.

In order to further progress and also to help answering legislators request (cf Article 12(2) of the eCall type-approval Regulation), and on the basis of the five guiding principles, all

elements approved or identified within the working group should now contribute to and benefit from a scenario-based analysis on legal, liability, technical and cost-benefits aspects.

Legal questions

- **Liability**

Many actors may be involved in the provision of C-ITS information and services. Day 1 applications being for information purposes only, the driver always remains in control of the vehicle, and therefore **there are no changes concerning liability compared to the current situation** and the current amendment to the Vienna Convention (Amendment Article 8, paragraph 5) will be sufficient.

However, two aspects must be taken into account:

Firstly, the potential of consumers "trusting technology", this effect being even stronger with information provided by public authorities. It is therefore recommended that vehicle manufacturers, service providers and public authorities use the appropriate level of information (e.g. disclaimers) to **raise the user's awareness of the limitation of the information provided**, in particular regarding safety critical messages and/or information provided in the absence of physical traffic signage.

The second aspect is related to the trends towards **higher levels of connectivity and automation**, where information provided via C-ITS may trigger subsequent action from the vehicle. It is **recommended to re-evaluate the question of liability for these cases** in the second phase of the C-ITS platform.

- **Data protection and privacy issues**

As C-ITS equipped vehicles making use of **CAM and DENM** messages are constantly broadcasting data, including their speed and location etc., this raises potential concern as how to guarantee **privacy and data protection**.

After various consultations, in particular with the EDPS and privacy experts, **the C-ITS platform considers these messages as "personal data"** because of their potential of indirect identification of users. Therefore the EU legislation (Directive 95/46/EC) on data privacy and data protection applies.

From the several legal bases listed in this Directive allowing the process of personal data, processing based on consent (article 7(a) of the Directive) is deemed to be the most straightforward, therefore **it is recommended to implement the principle of "informed consent"** by providing the vehicles with ad-hoc technologies allowing to attach "consent markers" to personal data.

An **opt-out possibility should be offered to the drivers, authorising the driver to shut down the broadcast**, while fully informing him about possible adverse consequences.

Other identified potential legal bases are "vital interests of data subject" and "public interest" (resp. articles 7 (d) and 7(e) of the Directive), which could allow the processing of data without drivers explicit consent. For C-ITS road safety and traffic management applications, where a "vital or public interest" is at stake and is demonstrated, a limited

number of applications could process the data without drivers' explicit consent, provided that the legal basis to process the data (according to the legal framework in place) and these applications are strictly defined and the data collected under these conditions are not further processed or re-purposed beyond these applications.

In any case it is recommended to foster the principle of **'Privacy by Design'** and develop systems flexible enough to **guarantee full control of personal data** by the data subject.

Legitimacy of the deployment of C-ITS

- **Road safety issues**

The deployment of C-ITS poses some obvious road safety issues, linked in particular to the driver's lack of knowledge of C-ITS functionalities, false perception, over-reliance on the system etc. Likewise, the simultaneous presence on the same road networks of C-ITS equipped and non-equipped vehicles may create some safety challenges. Therefore the C-ITS Platform proposes several **recommendations related to the revision of the European Statement of Principles on Human Machine Interface, to the coexistence of equipped and non-equipped vehicles and to training and awareness.**

- **Acceptance and readiness to invest**

A major obstacle for C-ITS deployment is that significant upfront investments are required both on the vehicle and the infrastructure level and that enhanced co-operation needs to be established before any benefits will occur. Hence, synchronisation of actions is key, considering existing inter-dependencies.

Therefore the C-ITS Platform **recommends the Commission to continue the on-going financial support of C-ITS deployment projects in the context of the Connecting Europe Facility (CEF)**. Furthermore, it is considered that all the existing, and upcoming projects, should engage in the exchange of results and experiences through stable mechanisms. The second phase of the C-ITS Platform should also consider how to consolidate key stakeholders' engagement in the future. The C-ITS Platform **also recommends the Commission to support public investment, by means of harmonised C-ITS pre-commercial procurement schemes and practical tools such as investment guidelines for infrastructure managers**.

To ensure a strong, simultaneous and fast uptake of C-ITS deployment, clear messages need to be provided to convince private and professional end-users and infrastructure owners or operators to invest in vehicle and infrastructure equipment. Difficulties to develop business models in urban environments were specifically highlighted. Therefore the C-ITS Platform underlined the importance of having 'quick win' cases and ambassadors for C-ITS projects.

The second phase of the C-ITS platform could help better define the measures and messages which i.a. could address the legal and technical certainty for infrastructure owners, reduction of operating costs for fleets, societal benefits (safety, reduction of congestion and emissions), answers to tracking fears, knowledge sharing between stakeholders etc.

- **Costs and Benefits**

A cost-benefit analysis was performed on the basis of the list of Day 1 services. Agreeing on this list has been a crucial step to further develop and commonly identify the most cost/efficient C-ITS deployment scenarios.

Supported by an external study, several additive scenarios based on multiple combinations of services were analysed, taking into account the likely type of communication, different geographical environments and the purpose of the services (road safety, traffic information, freight services, etc).

The timeframe for assessing the impact of deployment was set to 2018-2030, with significant benefits only starting to accumulate between 5 and 10 years after initial investments, depending on deployment scenario and uptake rates. **Ultimately benefits significantly outweigh costs on an annual basis, and - depending on the scenario - by a ratio of up to 3:1 when evaluated over the whole 2018-2030 period**.

An overall conclusion is that **a strong uptake is an essential prerequisite for achieving meaningful benefits, and that services will most probably always be bundled.** Benefits of deploying C-ITS services are very large indeed but they will not necessarily appear in the short-term.

To ensure interoperability and maximise benefits, it is essential to **base this deployment throughout the EU on the list of Day 1 applications and on common standards**. In parallel, as the investments will not be dependent from the number of services, it is necessary to deploy a maximum of services as quickly as possible in order to ensure the quickest possible positive return on investment. The need to have low entry barriers in terms of access to data - and more specifically to in-vehicle data - in order to allow for the deployment of new C-ITS enabled services and applications was also highlighted.

International Cooperation

International cooperation is fundamental for Cooperative Systems as worldwide markets have global players which therefore require global strategies. Areas such as C-ITS security policy and harmonisation of standards have already benefitted from international cooperation with the US and Japan since respectively 2009 and 2011. The huge progress of C-ITS requires a change in activities, moving from research and pilot projects to the stages of early deployment. This was recognised as an important driver to take into account when revisiting aspects and (possibly new) priorities for future international cooperation.

On technical issues, areas identified as critical to continue cooperation are those in which the well-established dialogue has already brought substantial progress, such as communication and spectrum issues, and security and data protection.

Learning from collaborations with partners within the same geographical region or at international level also represents a key asset for future progress. The C-ITS Platform recommends the Commission to encourage the exchange on technical, organisational and political learnings coming out of pilots in different regions, while other aspects more closely

linked to commercial issues could be addressed by the private sector in parallel. **The C-ITS Platform also recommends the Commission to enlarge cooperation on deployment practices at government level with other regions**, such as Canada, Australia, South Korea and other countries, as well as closely follow international developments in this field, in coordination with other initiatives, on-going or to come, in the field of automation.

Conclusion

A first general conclusion to be drawn from the activities of the C-ITS Platform is that a coordinated action for the deployment of C-ITS in the EU is paramount: a unique legal and technical framework is essential and coordinated efforts to ensure quick uptake of C-ITS are requested.

A second general conclusion is urgency: the technology is ready, the industry is already deploying C-ITS equipped vehicles in other parts of the world and announced to be ready to deploy in the EU by 2019, provided that the above-mentioned framework is in place sufficiently in time.

The members of the C-ITS platform welcome the work achieved during this first phase that has benefitted from such an inclusiveness process and suggest following the same methodology when addressing further the remaining issues, implementing the agreed recommendations and start considering vehicle automation and related road infrastructure issues.

The C-ITS platform members are calling the European Commission to build on these conclusions and the outcome of the C-ITS Platform when envisaging further actions and measures in order to, without delay, actively guide the interoperable deployment of C-ITS in the EU with clear timeline, goals, objectives and actions.

This report of the C-ITS platform has been endorsed by nominated experts, representing the organisations and countries listed in the Register of Commission Expert Groups[1]. On an ad hoc basis, individual experts have been invited to participate in the work of specific working groups and are listed in the attendance list of each working group.

[1] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3188

2. The C-ITS platform – Objectives and process

The Platform for the Deployment of Cooperative Intelligent Transport Systems in the European Union (C-ITS Platform) was launched by the Commission in July 2014, and met for the first time in November 2014.

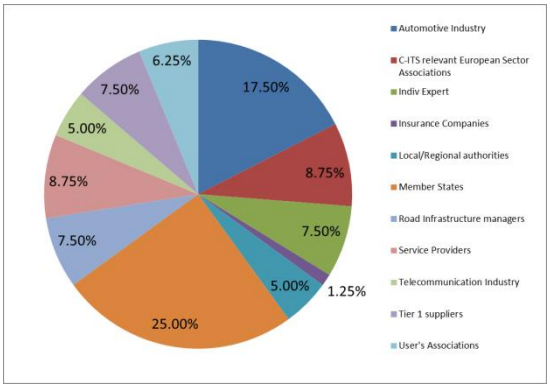
The C-ITS Platform provided an operational instrument for a dialogue, exchange of technical knowledge and cooperation, among the Commission, public stakeholders from Member States and local/regional authorities, and private stakeholders (such as vehicle manufacturers, service providers, road operators, telecomm companies, Tier 1 suppliers, etc.) to cooperate on technical, legal, organisational, administrative and governing aspects. Around 120 experts[2] met on a regular basis in monthly working groups meetings and four plenary meetings of the C-ITS platform were organised in November 2014, May 2015, October 2015 and January 2016.

The objective of the C-ITS platform was to identify and agree on how to ensure interoperability of C-ITS across borders and along the whole value chain, as well as to identify the most likely and suitable deployment scenario(s). These include the first vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) services to be deployed across the EU and their most beneficial geographical environments (long distance corridors, secondary roads and the urban environment).

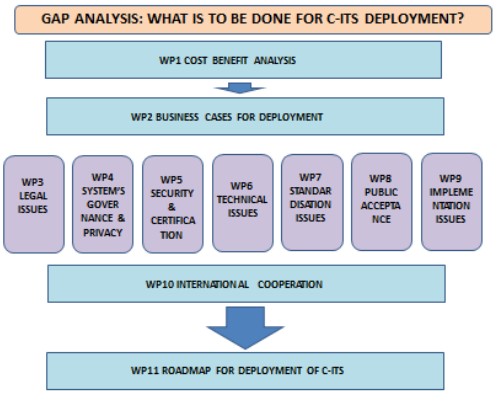
The scope of the C-ITS platform was focussed on the main technical (frequencies, hybrid communications, (cyber-)security and access to in-vehicle data) and legal issues (such as liability, data protection and privacy). It also covered standardisation, cost benefit analysis, business models, public acceptance, road safety and other implementation topics, international cooperation, etc.

These topics were analysed and discussed in 10 working groups of the C-ITS platform. Those working groups were all chaired by DG MOVE representatives in cooperation and with active participation of other Commission services, such as JRC, DG GROW, DG RTD, DG CNECT, DG JUST or institutions such as the European Data Protection Supervisory (EDPS). A 11th working group on roadmap for the deployment of C-ITS has been put on-hold and is expected to build on the achievements of other working groups in order to accompany the implementation phase of the recommendations and make the appropriate link with automation.

[2] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3188



C-ITS platform members



C-ITS platform working groups

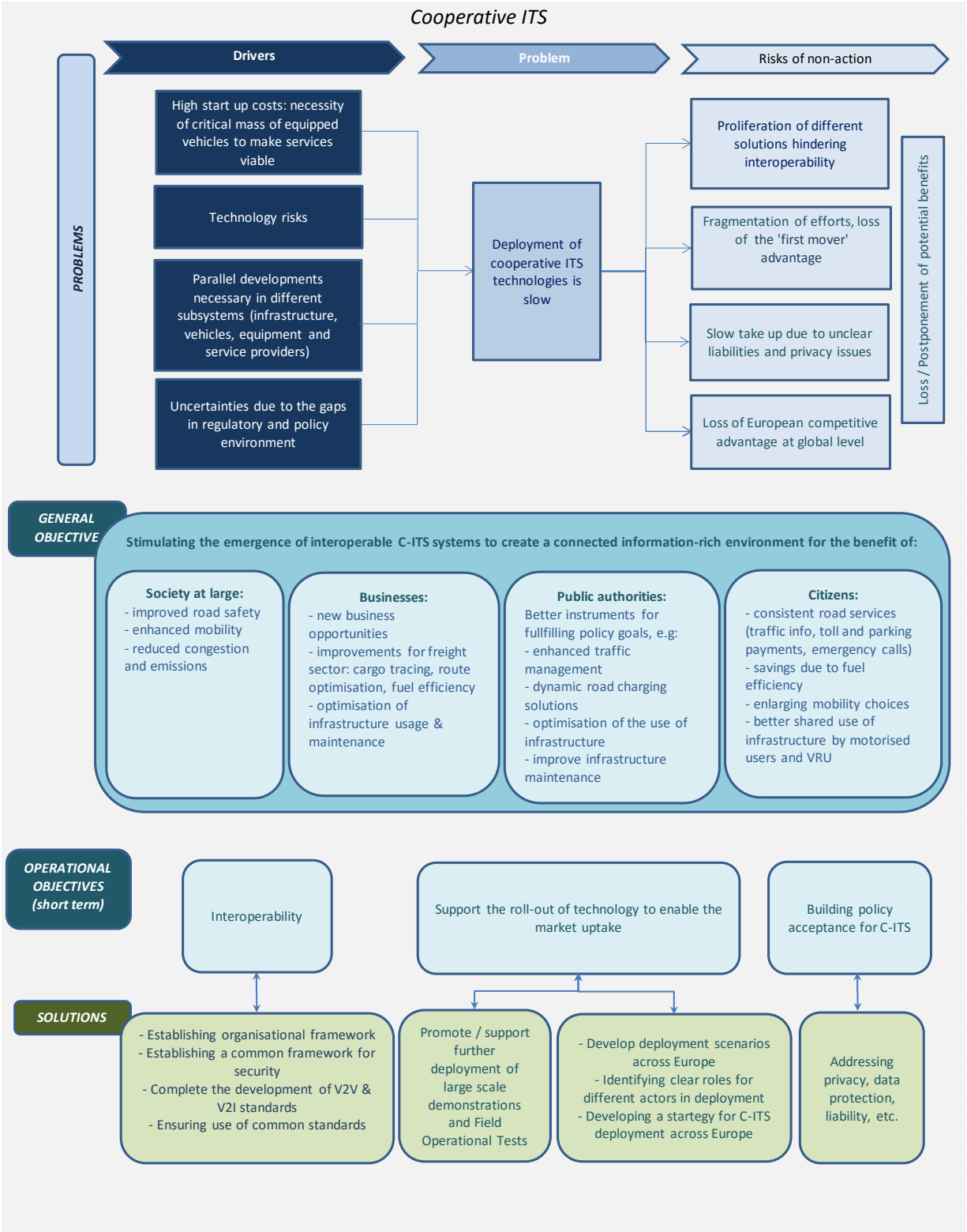
The working groups developed, until the end of 2015, policy recommendations and proposals for action (for the Commission but also for other relevant actors along the C-ITS value chain), endorsed by the C-ITS platform during its plenary meeting on 21 January 2016, which concluded the first phase of the platform.

This report of the C-ITS platform is to be understood as a stakeholders' contribution to the forthcoming Master Plan for the deployment of Interoperable Cooperative Intelligent Transport Systems in the EU.

3. Working Group 1 - Cost Benefit Analysis

3.1. Executive Summary

In a non-paper on a draft "C-ITS Problem Tree" the EC mapped the main problems, identifying causes and effects in order to agree in a first stage on the risks associated to no further action at European level.



The risk of uncoordinated deployment that would in turn restrict interoperability, and the risk to face a slow penetration rate in Europe compared to other regions of the world, hence affecting the competitiveness of our economy, were both identified as major issues. These together with the identified drivers would become part of the Commission's Impact Assessment for a Master Plan on C-ITS.

WG1 "Cost Benefit Analysis" proposes establishing a matrix of different geographical environments and time horizons, in order to identify for each of them the most likely applications to be deployed in different time frames. In addition the cost benefit analysis needs to consider how applications can benefit different categories of users as for many C-ITS applications there is a potential benefit for the user as an individual, as well as a potential benefit for the society, that goes beyond the addition of the individual benefits. The members of the group agreed that the first step would be to identify bundles of services to develop scenarios for the CBA study to be carried out, on behalf the Commission.

3.2. Objectives of the Working Group

The objective of the C-ITS Platform Working Group on Cost Benefit Analysis is to support deployment of C-ITS in Europe by proposing a selected number of scenarios – supported by a large group of public and private stakeholders – that would lead to the widespread and coordinated deployment of interoperable C-ITS services throughout Europe. The analysis studied the costs and benefits of deploying C-ITS enabled services for road transport in the Member States of the European Union in the period between 2015 and 2030.

This process started with agreeing on the main problems to be addressed and creating the foundation layer on the basis of which further Cost Benefit Analysis could be carried out, as well as allowing the various other Working Groups of the C-ITS Platform to examine issues in the light of the identified applications. EU-wide interoperability and continuity of services are core requirements, as well as environmental and safety issues, technological neutrality and achieving sufficient uptake rates. Multimodality is taken into consideration and technological readiness was assessed, amongst others by reviewing existing demonstration projects.

This led to the establishment of – and agreement on – a list of C-ITS services that are likely to be deployed first. The list includes services which have been studied earlier on in the context of European and national research projects, followed by large scale Field Operational Tests. The services rely on available message standards. The list comprises C-ITS services which are supported by the emerging deployment and specification initiatives in various Member States. Having such a list is a key element towards maximizing benefits by making sure there is continuity of services across Member States. Furthermore, each service comes with a definition to remove currently existing ambiguity.

Secondly a baseline scenario was established and agreed upon by the working group, describing the likely deployment roadmap of C-ITS services – without additional EU action,

but including existing Member State and Industry initiatives – and covering the whole of Europe.

In the third step the working group identified the most promising deployment scenarios in terms of rapid and widespread uptake, over and above the baseline, each scenario building on the previous one and together covering not only the whole list of Day 1 and Day 1.5 services but also all relevant vehicle and road types.

Finally, the combined intelligence of the Working Group (consisting of data from European project databases, operational data, research data, etc.) was considered and debated during the working group meetings, to produce the highest possible quality of detailed input data to feed into the cost benefit analysis.

The outputs and conclusions of this CBA will in turn feed into the recommendations - from the working group to the European Commission - to further support C-ITS deployment in Europe and foster the benefits delivered by the commonly agreed scenarios.

3.3. Organisation of Work

The organization of work was based on regular Working Group meetings (WG1 conducted a total of 11 meetings in Brussels from November 2014 – December 2015 in the course of the first phase of the C-ITS platform) and also on some phone conferences to deal with specific sub-topics in the main work items.

Ricardo Energy & Environment, together with their partner TRT Trasporti e Territorio, were commissioned to deliver a "Study on the Deployment of C-ITS in Europe", which supported the work of the working group on CBA and included the whole modelling exercise, as well as a major desk research and consultation and data collection exercises. In addition to the modelling outputs a series of international case studies was carried out to identify best practice and lessons learned elsewhere which could be relevant to the EU.

The members of the Working Group supported this study through the definition of the deployment scenarios, providing where possible the necessary data inputs and being closely and actively involved in the definition of the model and the followed methodology.

DG MOVE as Chair of WG1 took care of maintaining relationships with other Working Groups and informing the WG1 participants of work items, which could be relevant for the Group to consider.

All results, outputs and expert recommendations of the C-ITS Platform WG1 have been produced, discussed and endorsed by the following nominated experts, representing the following organizations and countries:

Table 1: WG1 members and organizations

Organisation	Name
ACEM	Vassileva Veneta
ADAC	Hecht Christoph
Austriatech	Froetscher Alexander
CEDR	Geissler Torsten
Ericsson	Fagerholt Anders
ETSC	Carsten Oliver
	Townsend Ellen
European Cyclist Federation	Woolsgrove Ceri
FEMA	Zee Anna
Finnish Transport Agency	Kulmala Risto
GDV	Lubos Christian
IAV GmbH	Fickel Frank
Independent Expert	Sampson Eric
IRU	Jeftic Zeljko
Member State (AT)	Molin Helge
Member State (BE)	Kenis Eric
Member State (F)	Delache Xavier
	Ollinger Eric
	Patin Nicolas
Member State (NL)	Schuurman Henk
Member State (POL)	Mazur Adrian
	Warda Krystian
Member State (SE)	Biding Torbjörn
	Marton Maria
Member State (UK)	Ferguson Anthony
	Hanson Graham
POLIS	Hoadley Suzanne
PSA Peugeot Citroen	Servel Alain
TISA	Schmidt Andreas
TNO	Malone Kerry
Transport for London	De Estevan Ubeda Natalia
VOLVO Group	Wahlund Jörgen
VTT	Rämä Pirkko
Xerox	Harris Richard

The following European Commission Staff have been involved in WG1:

Table 2: WG1 Commission staff

Services	Name
EC GROW	LAGRANGE Antony
EC MOVE	ALFAYATE Maria
EC MOVE	CARABIN Gilles
EC MOVE	DEPRE Claire
EC MOVE	MENZEL Gerhard
EC MOVE	TZAMALIS Georgios
EC MOVE	VAN DER LINDEN Geert
EC MOVE	VAN GAEVER Alain

3.4. Cost Benefit Analysis

3.4.1 List of defined C-ITS services

An agreed list of Day 1 (and Day 1.5) applications for Europe, to be deployed in the short-term, was supported by all WG1 members and was endorsed by the wider C-ITS community during the C-ITS Platform plenary meetings. Such a list is essential for building agreement on which services to deploy first, aligning funding and investment priorities and (where applicable) innovation activities.

These services were chosen on their importance from policy perspectives or potential to answer major societal needs, such as increasing road safety. A further split was introduced based on technical readiness in the short-term (Day 1 vs Day 1.5). To avoid ambiguity each service was accompanied by a clear definition.

The agreement on this list maximizes the chances of achieving Europe-wide coverage and continuity of C-ITS services as soon as possible, which in turn increases the societal benefits achieved from the said services. Note that having such an agreed upon list does not imply all parties have signed up to deploy all services on that list in exact similar timescales because of the different levels of readiness of budgets, maturity of infrastructure investment, political factors etc. The list also fosters faster deployment by creating a Europe-wide market for C-ITS services and further focusses and increases the need for efforts on ensuring seamless communication between all vehicles and infrastructure and the interoperability of services. The latter addresses both the continuity of services geographically (between member states, regions, cities, on main network corridors or other highways, extra-urban roads and in urban environments) and the compatibility of different services.

The final list of **25** C-ITS services (Day 1 and Day 1.5) can be found in Table 3 and Table 4, more details can be found in **WG1 - ANNEX 1 – C-ITS Service List.xls.**

Table 3: List of Day 1 Services

#	Day 1 Services
1	Emergency electronic brake light
2	**Emergency vehicle approaching**
3	Slow or stationary vehicle(s)
4	Traffic jam ahead warning
5	Hazardous location notification
6	Road works warning
7	Weather conditions
8	In-vehicle signage
9	In-vehicle speed limits
10	Probe vehicle data
11	Shockwave damping
12	Green Light Optimal Speed Advisory (GLOSA) / Time To Green (TTG)
13	Signal violation/Intersection safety
14	Traffic signal priority request by designated vehicles

Table 4: List of Day 1.5 Services

#	Day 1.5 Services
1	Off street parking information
2	On street parking information and management
3	Park & Ride information
4	Information on AFV fuelling & charging stations
5	Traffic information and smart routing
6	Zone access control for urban areas
7	Loading zone management
8	Vulnerable road user protection (pedestrians and cyclists)
9	Cooperative collision risk warning
10	Motorcycle approaching indication
11	Wrong way driving

3.4.2 Scenario Building

The WG agreed very early in the process that when deploying C-ITS it would appear sensible to bundle services for at least two (related) reasons: (1) many services will rely on the same hardware investment – in particular on the vehicle side 92) it will be highly unlikely that many business cases can be found for individual services. In other words as the in-vehicle hardware is essentially identical for all scenarios the marginal cost for adding services is

minimal and the working group looked into the most appropriate ways services could be combined from an operational, investment and technological point of view.

In a first step the working group decided to take two additional criteria into consideration when evaluating the list of 25 C-ITS services, besides the earlier introduced Day 1 and Day 1.5 divide, namely:

1. V2V, V2I or V2X communication (V=vehicle, I=infrastructure, X=anything, e.g. pedestrian)
2. The primary purpose of the service (e.g. road safety, traffic information, freight services, etc.)

These additional dimensions facilitated the working group's concluding on 9 service bundles, each aiming at a particular communication type and purpose. Though not a hard criterion *per se* some bundles have a geographical dimension as well, e.g. parking information has some use on motorways but is mostly relevant in urban environments.

Table 5: List of Day 1 Bundles

#	Day 1 Services			Bundle
1	Emergency electronic brake light	V2V	Safety	1
2	Emergency vehicle approaching	V2V	Safety	1
3	Slow or stationary vehicle(s)	V2V	Safety	1
4	Traffic jam ahead warning	V2V	Safety	1
5	Hazardous location notification	V2I	Motorway	2
6	Road works warning	V2I	Motorway	2
7	Weather conditions	V2I	Motorway	2
8	In-vehicle signage	V2I	Motorway	2
9	In-vehicle speed limits	V2I	Motorway	2
10	Probe vehicle data	V2I	Motorway	2
11	Shockwave damping	V2I	Motorway	2
12	GLOSA / Time To Green (TTG)	V2I	Urban	3
13	Signal violation/Intersection safety	V2I	Urban	3
14	Traffic signal priority request by designated vehicles	V2I	Urban	3

Table 6: List of Day 1.5 Bundles

#	Day 1.5 Services			Bundle
1	Off street parking information	V2I	Parking	4
2	On street parking information and management	V2I	Parking	4
3	Park & Ride information	V2I	Parking	4

#	Day 1.5 Services			Bundle
4	Information on AFV fuelling & charging stations	V2I	Smart Routing	5
5	Traffic information and smart routing	V2I	Smart Routing	5
6	Zone access control for urban areas	V2I	Smart Routing	5
7	Loading zone management	V2I	Freight	6
8	Vulnerable road user protection (pedestrians and cyclists)	V2X	VRU	7
9	Cooperative collision risk warning	V2V	Collision	8
10	Motorcycle approaching indication	V2V	Collision	8
11	Wrong way driving	V2I	Wrong Way	9

Note that all 14 Day 1 services are combined into just 3 bundles, concentrating on safety based V2V services, V2I services typically associated with motorway driving and services concentrating on traffic lights. The Day 1.5 services are more divers and lead to the creation of 6 additional service bundles.

In a second step the working group added two more dimensions, to be combined with the 9 service bundles in a matrix (1) transport type (personal, public, freight) and (2) geographical environment (TEN-T corridor[3], TEN-T core network, TEN-T comprehensive network, extra-urban, urban).

In the third step the working group filled the matrix by valuing the applicability of each segment of the matrix (e.g. GLOSA is not applicable on highways as there are no traffic lights).

The final step consisted of combining all segments into commonly agreed deployment scenarios. The working group decided on scenarios that have 2 properties:

1. They are additive, i.e. scenario B contains all of scenario A, scenario C contains all of scenario B and A, etc.
2. They are to a large extent chronological, e.g. though some small overlap may exist, scenarios A and B will be deployed prior to scenarios D and E.

Clearly, the CBA exercise also benefitted from this, i.e. the impact of deploying each one of these services needed not be modelled individually.

[3] http://ec.europa.eu/transport/themes/infrastructure/index_en.htm

Bundle of services			TEN-T Corridors	TEN-T Core	TEN-T Comprehensive	Non m-way non urban	Urban	Services
Bundle 1 *Day 1 V2V - safety ITS-G5*	V	Personal transport	A	A	A	A	A	Emergency brake light Emergency vehicle approaching Slow or stationary vehicle(s) Traffic jam ahead warning Hazardous location notification
		Public transport	C	C	C	C	C	
		Freight	A	A	A	A	A	
Bundle 2 *Day 1 V2I (mainly applicable to motorways)*	I	Personal transport	B	B	C	C/D	C	Road works warning Weather conditions In-vehicle signage In-vehicle speed limits Probe vehicle data Shockwave damping
		Public transport						
		Freight	B	B	C	C/D	C	
Bundle 3 *Day 1 V2I (mainly applicable to urban areas)*	I	Personal transport				C/D	C	GLOSA/TTG Signal violation/intersection safety Traffic signal priority request by designated vehicles
		Public transport				C/D	C	
		Freight				C/D	C	
Bundle 4 *Day 1.5 V2I - Parking information*	I	Personal transport	D	D	E	E	C	Off street parking information On street parking management and information Park & Ride information Information on fuelling & charging stations for AFVs
		Public transport						
		Freight	E	E	E	E	C	
Bundle 5 *Day 1.5 V2I - Traffic information*	I	Personal transport	A	A	B	C/D	C	Traffic information & smart routing
		Public transport						
		Freight	B	B	B	C/D	C	
Bundle 6 *Day 1.5 V2I - Zone management services*	I	Personal transport					D	Loading zone management Urban zone access control
		Public transport						
		Freight	D	D			D	
Bundle 7 *Day 1.5 - V2X (mainly applicable to urban areas)*	X	Personal transport				E	E	Vulnerable road user protection
		Public transport				E	E	
		Freight				E	E	
Bundle 8 *Day 1.5 V2V - safety*	V	Personal transport	E	E	E	E	E	Motorcycle approaching indication Cooperative collision risk warning
		Public transport	E	E	E	E	E	
		Freight	E	E	E	E	E	
Bundle 9 *Day 1.5 V2I - safety*	I	Personal transport	E	E	E		E	Wrong way driving
		Public transport						
		Freight	E	E	E		E	

Figure 1: C-ITS Service Bundle Matrix

The five resulting scenarios – as defined by the working group and labeled from A through E – can be summarized as follows:

Table 7: C-ITS deployment scenarios

Scenario A	• Deployment of all safety based V2V services (Bundle 1) starts on all roads (as V2V is road independent, the determining factor is the uptake rate in vehicles) • Traffic information & smart routing (Bundle 5) is deployed on TEN-T corridors and core roads first and initially for passenger cars only
Scenario B	• The (mainly) motorway-focused V2I services from Bundle 2 (such as road works warning and shockwave damping) are deployed on TEN-T corridors and core roads • Traffic information & smart routing extends to comprehensive network and now includes freight vehicles
Scenario C	• Urban deployment of the applicable services from Bundle 2 and the very urban focused services from Bundles 3 (e.g. GLOSA, traffic signal priority) and 4

	(Parking information) • Traffic information & smart routing extends to all other equipped roads • Safety based V2V services (Bundle 1) extend to buses • Motorway-focused V2I services (Bundle 2) are further deployed to all equipped roads
Scenario D	• Loading zone management is deployed to freight vehicles and equipped roads
Scenario E	• All additional Day 1.5 V2X services (e.g. motorcycle approaching indication or VRU protection) are deployed across all vehicle types and equipped roads

Note that most services can be provided via both ITS G5 and cellular communication, and most as both V2V and V2I, even though for calculation purposes the services are only allocated to one alternative of each.

The final report with more details on this work item can be found in **WG1 - ANNEX 2 - Summary Report_FV.PDF**.

3.4.3 CBA model and data Input (uptake rates, impact percentages and cost)

After the working group defined 5 additive deployment scenarios these needed to be translated into their environmental, social and economic impacts, a process which requires several steps:

1. Define the uptake rates of C-ITS technology (note that this was not yet part of chapter 3.4.2)
2. Model the effects of the introduction of C-ITS technology (this requires a traffic simulation at European scale, allowing modelling of e.g. reduced accidents, leading to reduced congestion, etc.)
3. Quantify the benefits of the previous step (e.g. reduced fuel consumption, emissions, fatalities, etc.)
4. Translate quantified benefits into costs and compare to required investment
5. Assess secondary effects such as reduced fuel tax revenues, job creation, modal shift

All of these steps need a lot of input data and to date very few 'real' data exist as until very recently there's been little relevant deployment. In order to reach the best possible quality of data the combined experience and knowledge of the whole working group (consisting of data from European project databases, operational data, research data, etc.) was complemented with discussions and live feedback during the working group meetings to make intelligent estimations. Remaining data gaps were filled by an extensive literature review and where necessary by extrapolating from data related to C-ITS services which are expected to operate through a similar mechanism. For clarity the input data were clustered in three different families:

1. ***Uptake rates***, these are essential for the CBA (and as such part of a sensitivity analysis) and concern both vehicle (OEM and aftermarket) and infrastructure equipment. In total 4 sets of numbers were compiled:

    - Baseline includes all existing developments and their likely continuation. IMPORTANT NOTE: this scenario is a shared vision, supported by representatives from industry and Member States, built-up at European scale, of the likely deployment roadmap if no additional EU action is taken.

    - Low sensitivity has moderate uptake in new vehicles and aftermarket devices and relatively lower uptake in infrastructure equipment.

    - Central sensitivity has a more aggressive uptake in new vehicles and aftermarket devices (compared to low sensitivity) and in particular a higher uptake in infrastructure equipment.

    - High sensitivity is identical to Central with added maximum infrastructure coverage due to the introduction of cellular networks for all V2I services.

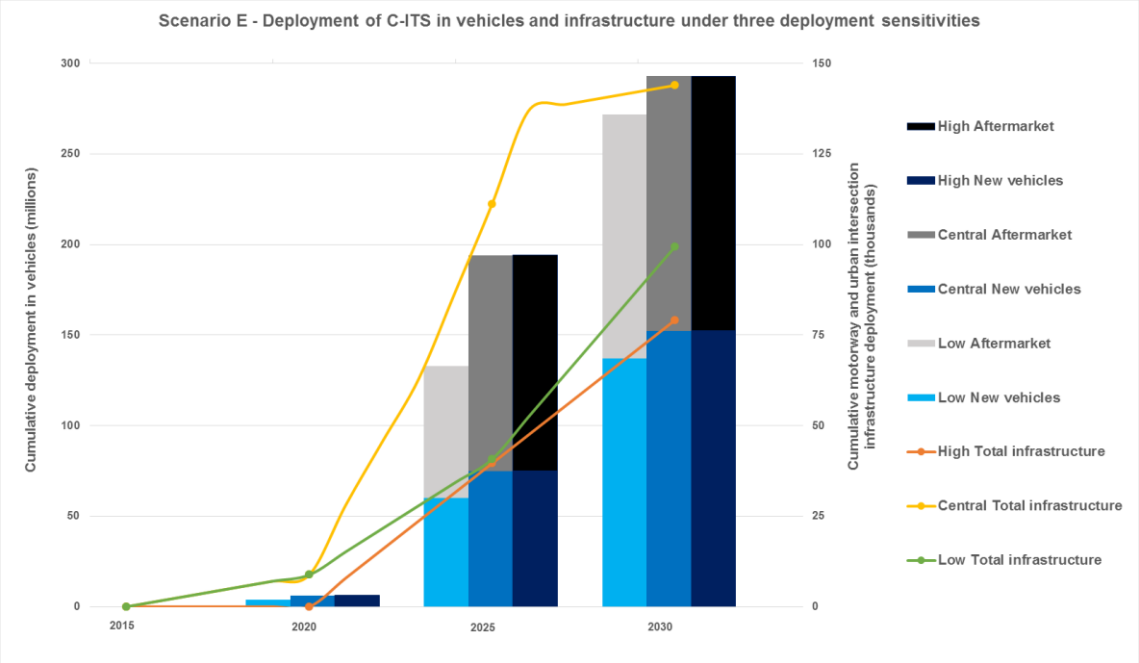


Figure 2: Cumulative deployment of C-ITS equipment in vehicles and infrastructure

2. ***Impact data***, these numbers define the impacts of C-ITS services on both individual vehicles and the environment or economy when installed across different vehicle and road types. For each C-ITS service included in the C-ITS deployment scenarios, data related to the following parameters was collected:

    - Traffic efficiency i.e. the percentage change in average speed for a vehicle equipped with C-ITS services.

- Fuel consumption i.e. the percentage change in fuel consumption for a vehicle equipped with C-ITS services.
- Polluting emissions i.e. the percentage change in NO_x, CO, VOC and PM emissions for a vehicle equipped with C-ITS services.
- Safety i.e. the percentage change in accident rates (classified by fatalities, serious injuries, light injuries and material damages) for a vehicle equipped with C-ITS services.

C-ITS services can have varying impacts depending on the road type and vehicle type in which they are deployed, so this impact data was collected for all applicable geographical environments (see 3.4.2) as well as all vehicle categories (passenger cars, light trucks, heavy trucks and buses).

3. ***Cost data***, contains investment and maintenance cost of hardware/devices and software required for C-ITS services, they are categorised in four types:
   - Central ITS sub-systems, which may be part of a centralised traffic management system. One such sub-system is able to manage C-ITS services for an entire city, or road operator, or national highway system etc.
   - Personal ITS sub-systems such as mobile phones, tablets, personal navigation satnav-type devices, and other hand-held devices not attached to the vehicle's information bus – these can enable V2I communications along suitably equipped roads/regions.
   - Vehicle ITS sub-system, are fitted by the vehicle manufacturer and are attached to the vehicle communication buses – these can enable both V2V communications and V2I along suitably equipped roads/regions.
   - Roadside ITS sub-systems such as beacons on gantries, poles, smart traffic lights, etc. which allow V2I communications along specific stretches of roads.

All details and further background information on all these assumptions can be found in the following annexes:

WG1 - ANNEX 3 - Summary of deployment assumptions 20151022_FV.XLSX

WG1 - ANNEX 4 - C-ITS impacts data overview_FV.XLSX

WG1 - ANNEX 5 - C-ITS impacts data assumptions by service_FV.PDF

WG1 - ANNEX 6 - C-ITS cost data assumptions_FV.xlsx

WG1 - ANNEX 7 - C-ITS cost data assumptions_FV.pdf

3.4.4 Outputs of the CBA

Outputs and conclusions below relate to the central sensitivity case for scenario E (i.e. deployment of all defined services) by 2030. The choice for scenario E is justified by the clear incentive to aim high and deploy as many services as possible as the benefits will increase but the costs remain more or less stable (note however that this does not imply that all services are to be deployed at the same time in this scenario).

The choice for 2030 – the end of the timeframe of this exercise – comes from the relatively long-term nature of this technology, i.e. network effects imply that sufficient uptake is an essential prerequisite for achieving meaningful benefits. Otherwise put, there is a significant delay between the initial investment and the appearance of large benefits.

A first overall conclusion is thus that the benefits of deploying C-ITS services are very large indeed but they will not appear in the short-term.

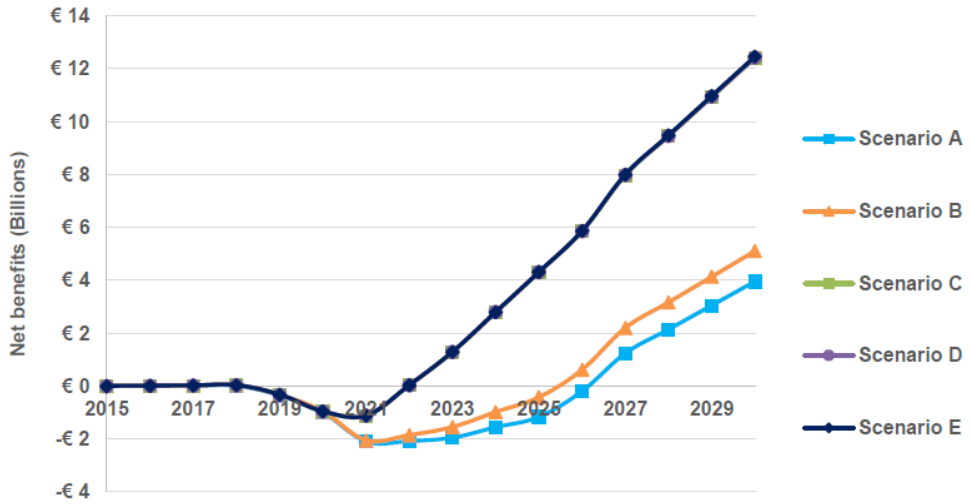


Figure 3: Net Benefits from C-ITS

As can be seen from Figure 3Figure 3 net benefits become positive somewhere between 2022 and 2026. This chart was based on central sensitivity values for the uptake rates, whereas the break-even point is reached earlier in the high sensitivity case, which adds – high – cellular coverage and its related benefits. Note also that in this chart the difference between scenarios C, D and E is barely (or not) visible, this is not a mistake but due to (1) the relatively small number of extra services that come with scenarios D and E (2) these are all Day 1.5 services and their introduction only starts in 2025, meaning high uptake and the maximum potential benefits from these services will not have been achieved by 2030.

A second overall conclusion is that we find benefits are dominated by reduced travel times, reduced accident rates and reduced fuel consumption whilst costs are largely dominated by vehicle equipment, even more so when aftermarket devices are added. Though it is not very clear what form such devices are likely to take they are expected to play a big role initially and phase out when the majority of the fleet and all new vehicles will be connected.

In the following paragraphs the main impacts are illustrated against the timeline 2015 to 2030 to provide some indication on the temporal allocation of costs and benefits.

3.4.4.1 Economic Impacts

In all scenarios connecting new vehicles (i.e. installing in-vehicle communication modules) is by far the dominant cost item (see Figure 4), it is estimated that up to 30 million cars will be connected annually, representing an equipment cost of up to €3Bn per year, with ⅙ of that cost coming from aftermarket devices (though not as abruptly as in the chart, these are expected to phase out as future cars will all be OEM connected).

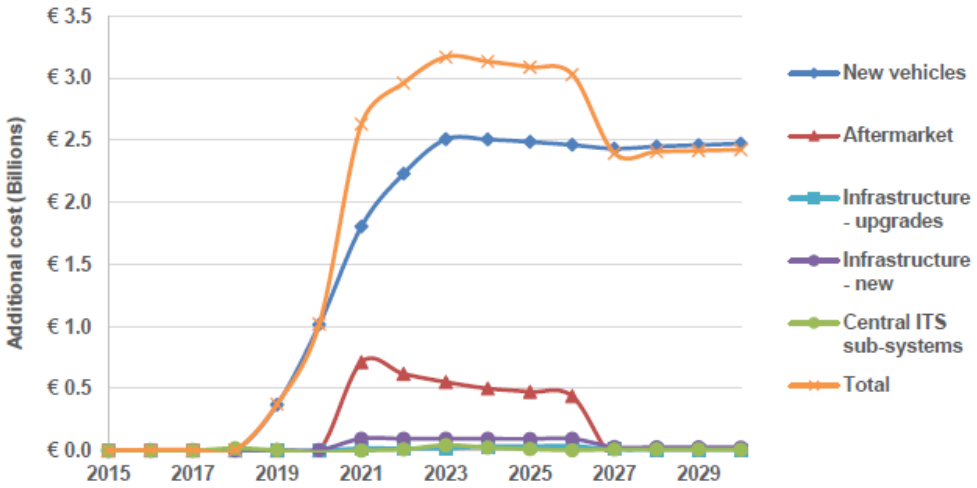


Figure 4: Costs for C-ITS deployment

Infrastructure costs on the other hand are limited to an annual investment of some €95M, so whilst many questions remain on the real cost for infrastructure upgrades, and infrastructure investment might still be a showstopper for some local deployment, it is clear these will not have a big impact on the overall EU-level Cost Benefit Analysis.

On the benefit side time related impacts of 2 billion hours or 3% of total time spend on the road makes up approximately ⅔ of total annual benefits, or €10Bn. Most of these savings are achieved through intersection-related services, parking information and smart routing, which, in particular in an urban environment are not well understood or supported by empirical data. Though there is no doubt about the benefit potential of such services and the positive Benefit Cost Ratio achieved, it is also clear there is range of additional benefits, some small some large, and we cannot quantify all of them yet. For example although learning curves have been applied in this analysis competition may very well push down prices faster than expected (notable past examples of this are ABS and ESC). Also, initial feedback from pilot projects reports that drivers experience less stress but this CBA has not assigned a (monetary) value to this. Another potentially large but unquantified benefit is that improved traffic flows may remove or at least postpone investments in new infrastructure.

3.4.4.2 Social impacts

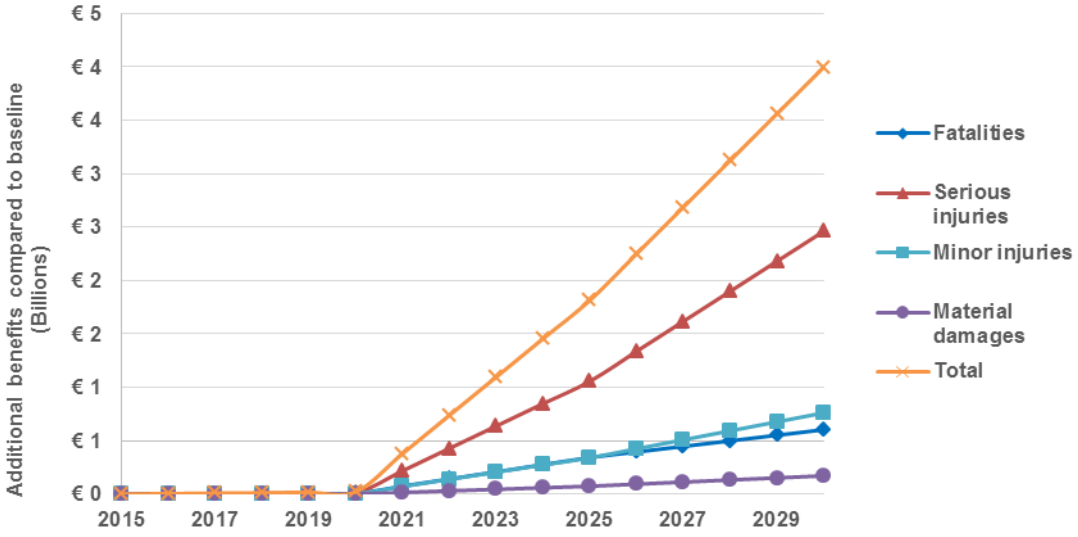


Figure 5: Safety Benefits / cost reductions from C-ITS

Despite a considerable reduction of accidents in the baseline scenario (at +/- 5% per year), specific safety related services such as hazardous location warning, in-vehicle speed limits and intersection safety are expected to bring an additional 7% reduction in fatalities, as well as serious and minor injuries. This constitutes the second largest contributor on the benefit side at up to €3.5Bn saved per year by 2030.

3.4.4.3 Environmental impacts

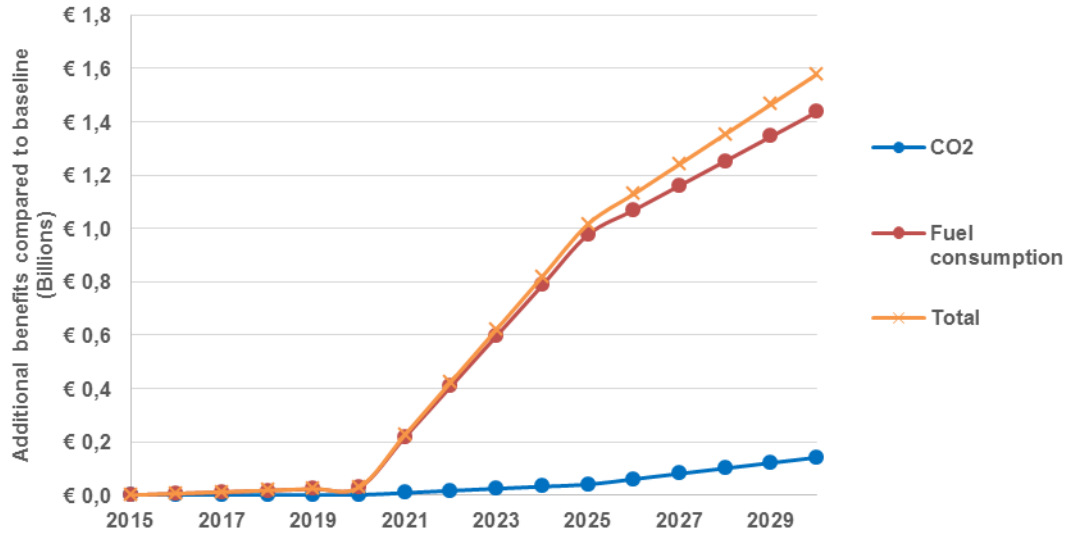


Figure 6: Environmental Benefits / cost reductions from C-ITS

Fuel consumption and CO_2 emissions are expected to drop by 1.2% by 2030 which is the equivalent of €1.6Bn (of which only €0.2Bn is on the emission side, due to the relatively low unit cost of CO_2). Other emissions, such as NOx, CO, VOC and PM, are estimated to drop by +/- 0.5%, yielding an additional benefit of €33M annually by 2030. Though these savings are

rather insignificant when looking at the overall Cost Benefit Analysis they may still have significant local impacts on air quality.

3.4.4.4 Overall Benefit Cost Ratio

With total annual benefits rising to €15Bn and total annual costs estimated at €2.5Bn by 2030 we find a very high Benefit Cost Ratio (BCR) of up to 3 to 1 based on cumulative costs and benefits to 2030. This is in line with earlier studies, provided one takes into account the number of services that were included in those studies.

As can be seen from Figure 7 though, the BCR varies through time, once more illustrating the importance of the network effect (this chart was constructed based on central sensitivity values for the uptake rates, results are even better for the high sensitivity case, which adds – high – cellular coverage and its related benefits).

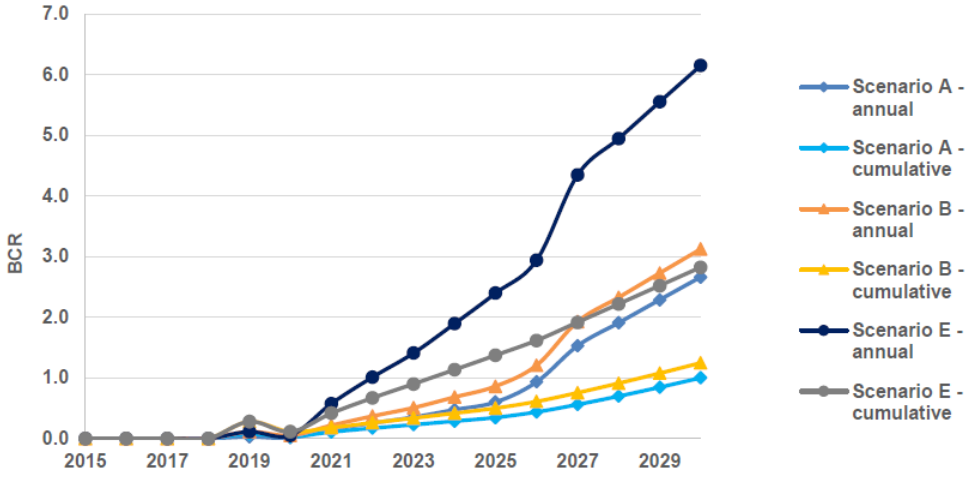


Figure 7: Benefit Cost Ratio

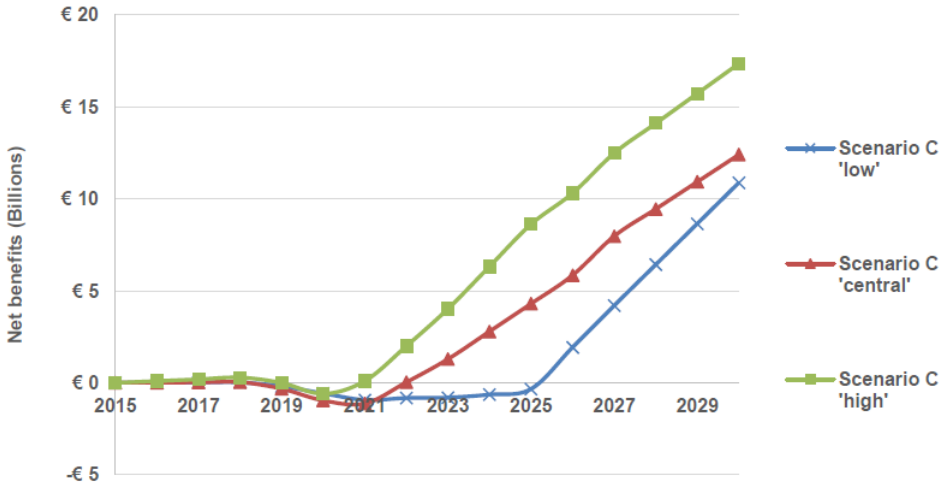


Figure 8: Sensitivity analysis

As can be seen in Figure 8, comparing the Net Benefits of Scenario C in low, central and high sensitivity cases, there is a clear and positive relation between the uptake rates and the net

benefits realized. NOTE: In the studied timeframe scenario C is largely equivalent to scenarios D and E, see also Figure 3.

Further background information and details on additional secondary impacts (e.g. can be found in **WG1 - ANNEX 2 - Summary Report_FV.PDF**

3.5. Recommendations and Follow-Up Actions

This chapter is split into two parts; the first concerns the recommendations from the experts of WG1 to the European Commission; the second lists possible follow-up actions, ways to further detail the CBA and suggestions on the continuation of WG1 in the second phase of the C-ITS platform.

3.5.1 Recommendations

1. When deployed pan-European C-ITS services are cost effective with a Benefit Cost Ratio of up to 3 to 1 based on cumulative costs and benefits to 2030. However significant benefits will only start to accumulate between 5 and 10 years after initial investments, depending on deployment scenario and uptake rates. It is therefore strongly recommended to actively guide the deployment of C-ITS through a Master Plan with clear goals, objectives and actions.

2. The established list of Day 1 (and beyond) services is key to guiding C-ITS funding and deployment initiatives, ensuring interoperability and continuity of services and maximising the Europe-wide uptake of C-ITS. It is therefore strongly recommended that use of this list – which is supported by all WG1 members and endorsed by the wider C-ITS community in the plenary sessions – is taken up by all public and private C-ITS stakeholders, though it might not necessarily happen in the same time frame. To support this it is also recommended that coordination of future deployment activities, both EC and MS funded, is based on this list which should be an integral part of the EC Master Plan. The Working Group also recommends regularly updating the list as new services are developed and deemed mature for deployment.

3. There is clear difference in the nature of Costs and Benefits of C-ITS services. The majority of costs are essentially service independent. This means there is little variation in costs in all scenarios (even when comparing scenario A to E, see Table 7) and in the long term more or less equal to the cost of connecting all vehicles and all relevant stretches of road and installing all required management infrastructure. The benefits however increase with each service deployed and it is therefore recommended to deploy as many services as soon as possible (e.g. deploy all V2V safety related services as a single bundle rather than separately). Furthermore, deployment should be such that adding new services is straightforward and does not require significant hardware changes. This recommendation is rather characteristic for introduction of new technology and not following it would negatively impact the Benefit Cost Ratio.

4. Faster deployment leads to earlier initial investments (though not necessarily higher overall) but also to faster break-even and higher overall benefits. This can largely be attributed to the fact that many impacts depend on sufficient uptake. Hence slow uptake rates would therefore lead to relatively long periods with little benefits. It is thus recommended to align all actors (this includes amongst others vehicle OEMs, aftermarket device manufacturers, infrastructure owners, telecoms and C-ITS service providers) and investments so as to push for a very strong, simultaneous and fast uptake, where mass deployment could start as soon as 2018. The continuation of the C-ITS platform alongside the corridor approach could play an important role in this alignment.

5. Though many uncertainties related to using existing cellular networks for C-ITS services remain (including coping with latency-critical services, lack of understanding of future business models or roaming issues, effect on individual service impacts, etc.), analysis[4] shows the benefits associated with the much increased coverage easily outweigh the extra data cost despite these costs being estimated higher than the investment cost for roadside units (the latter of course on selected roads only). In line with work carried out by WG6 (on frequencies and hybrid communications) the recommendation is to solve the open questions related to hybrid communications and reap the benefits associated with the coverage provided by existing cellular communication infrastructure.

6. Though many standards have been developed already, and further work is ongoing, practical implementations still encounter interoperability issues. However C-ITS largely depends on network effects to achieve long-term societal benefits at EU level, it is thus recommended that the interoperability issue is closely monitored, coordinated and addressed to achieve the critical mass required[5]. This includes geographical interoperability and backwards compatibility. Lessons learned from Field Operational Tests and from pilot deployment projects should function as feedback loops and evolve into implementation guidelines to complement standards. All new initiatives should contribute to and follow these implementation guidelines.

7. Main investment decisions lie with end-users and road authorities but benefits are both largely societal (as opposed to individual) and not achieved in the short-term. It is therefore recommended –in line with WG8 on Public Acceptance –that strong and clear messages, targeting amongst others politicians, investors, decision makers and the general public, should be prepared to secure these vital investments.

[4] Performed by Ricardo and supported by the members of the Working Group, see Organisation of Work

[5] This could take the form of strong EC support to facility deployment and guarantee coordination between MS initiatives

- Implement all necessary measures to explain the added value of C-ITS services to future C-ITS users (and the general public at large) as they will take up the bulk of investments in the form of in-vehicle or aftermarket C-ITS communication modules and/or devices.

- Compared with the equipment cost for connecting vehicles the infrastructure investment cost may appear relatively small, however this does not guarantee road authorities will easily find and free the budgets required for the support of C-ITS services. To support their investment decisions, more detailed work and CBA analysis at local/regional/sectorial level is required, providing them with the necessary arguments for justifying allocation of budgets.

3.5.2 Follow-up Actions

The collaboration of a relatively large group of experts resulted in strong recommendations to the EC and a study with well supported conclusions, but also identified several areas that require more detailing and routes for further improvement. Given the value of this Cost Benefit Analysis in supporting the deployment of C-ITS in Europe the working group recommends to continue the work, focusing amongst others on the following topics:

1. Recommendation 3 urges deploying as many services as soon as possible. This would also benefit the search for business cases, a topic that needs further exploration in the C-ITS platform (e.g. how will telecom operators be integrated in C-ITS services, in particular when roaming). The impact on the Human Machine Interface and driver distraction from bundling relatively large number of services then also becomes an area for further investigation. To further support recommendation 3 an assessment should be made on whether some actors or stakeholders could be targeted to reinforce the C-ITS platform in its second phase.

2. Recommendation 4 asks for a very strong, simultaneous and fast uptake through the alignment of all relevant actors (e.g. mass deployment in 2019 has already been proposed by some parties). Many questions however need answering to make this happen, such as identification of obstacles and enabling factors. Some of these will already have been answered by other Working Groups, some will remain open. Given the additional benefits related to faster uptake further work on the removal of obstacles should continue in the second phase of the C-ITS platform.

3. Recommendation 5 recommends solving the open issues concerning hybrid communication, i.e. the integration of cellular communication in C-ITS. This raises questions on data roaming and support for future ageing equipment as well as a need for decision strategies when conflicting information would arrive through different communication channels. This is a topic that should be subject of the continuation of the C-ITS platform.

4. Recommendation 6 asks for coordination of interoperability issues to ensure continuity of services, this is a topic that should be subject of the continuation of the C-ITS platform.

5. The current CBA estimates half of the benefits from C-ITS will be achieved in urban areas and several services are concentrated there, nevertheless only limited data is available on these services (e.g. how much traffic can be avoided through parking information services and how much can average speed be increased by intelligent traffic lights). Better insight into the benefits of C-ITS services could be obtained through the evaluation of R&I projects (with an increased focus on urban environments).

6. One could reasonably expect many, if not all, future new vehicles to be connected and it is also expected that a large market for aftermarket devices will be created in the existing fleet once C-ITS deployment takes off. It is however not very clear what form such devices will take, what their cost and/or business models will be, and what uptake rates should be assumed. Further work to evaluate the underlying assumptions is required.

7. Back-office systems for C-ITS services will link Road Side Units and integrate with traffic management systems. However little information exists on the cost of such systems, how many will be required and what their capabilities will be. Though this type of information has little impact on the CBA at EU level, it is potentially important at local/regional level and needs to be further detailed.

8. Most available impact and cost data today focusses on passenger cars. Obtaining reliable data for other vehicle types would further improve the CBA.

3.6. Annexes

1. WG1 - ANNEX 1 - C-ITS Service List.xlsx

2. WG1 - ANNEX 2 - Summary Report_FV. pdf

3. WG1 - ANNEX 3 - Summary of deployment assumptions 20151022_FV. xlsx

4. WG1 - ANNEX 4 - C-ITS impacts data overview_FV.xlsx

5. WG1 - ANNEX 5 - C-ITS impacts data assumptions by service_FV.pdf

6. WG1 - ANNEX 6 - C-ITS cost data assumptions_FV.xlsx

7. WG1 - ANNEX 7 - C-ITS cost data assumptions_FV.pdf

4. Working Group 2 - Business Cases

4.1. Executive Summary

The deployment of C-ITS requires the involvement of stakeholders from different industries and public sector actors, and cannot just rely on public funding. The decision to deploy Cooperative Systems has to be based on sound and convincing business cases for all the actors along the value chain, and hence which give sufficient confidence to the core stakeholders to invest.

The objective of WG2 on Business Cases & Models was to identify enablers and address barriers to the development business models and business cases for the deployment of C-ITS in the EU.

The very close inter-relations between WG2 and other WGs, in particular WG1 on Cost-Benefit Analysis and WG9 on Implementation Issues, were acknowledged from the early stages of the work. This situation added additional challenges to WG2 in terms of dependence on work to be undertaken in parallel in those WGs.

Having held a relatively small number of meetings, WG2 Chair realised that the dependence on outcomes to be coming out from other WGs, hence not available yet, made very extremely difficult to carry out the work. It was then decided to wait until these outcomes (especially from WG1 and WG9) would be available to continue the work within WG2. Finally, the Chair of the WG, decided to address the issues related to business models in the second phase of the C-ITS Platform, after January 2016.

4.2. Objectives of WG2 on Business Cases & Business Models

C-ITS deployment requires the involvement of stakeholders from different industries and public sector actors, and the benefits of one user group are often dependent on another user group's investment. However these user groups do not necessarily have a direct one-to-one business relation. C-ITS thus resembles an ecosystem where several groups have inter-dependant relationships.

Writing a single business case for C–ITS deployment would be very difficult. Not only can we expect an extensive overlap of actions of both the public and private sectors, but also these two sectors have very different objectives. This has hampered so far an agreement on a unified strategy for both across Europe. Define agreed operating business models around very specific services/applications might also be very difficult, since investment decisions by different actors in the value chain might be based on different parameters. However, an attempt could be made on defining shared outcomes in which all the actors in the value chain find their interests presented in a convincing way.

The objective of WG2 on Business Cases & Models was to identify enablers and address barriers to the development business models and business cases for the deployment of C-ITS in the EU.

4.3. Structure of the work

Working Group 2 held 3 meetings between December 2014 and February 2015. The work was based on face to face meetings

DG MOVE as chair of WG2 took care of organising WG meetings and teleconferences, maintaining relations with other C-ITS Platform WGs.

The very close inter-relations between WG2 and other WGs, in particular WG1 on Cost-Benefit Analysis and WG9 on Implementation Issues, were acknowledged from the early stages of the work. This situation added additional challenges to WG2 in terms of dependence on work to be undertaken in parallel in those WGs.

All results, outputs and expert recommendations of the C-ITS Platform WG2 have been produced, discussed and endorsed by nominated experts, representing the following organisations and Member States:

Organisation	Name
ADAC (Allgemeiner Deutscher Automobil-Club)	MAY Claudia
CLEPA (European Association of Automotive Suppliers)	WESSMAN Eleri
BOSCH	EISENMANN Susanne
DENSO	HENCHOZ Jean-Michel
ASFINAG	Jandritsis Marko
AustriaTech	Froetscher Alexander
BMW	Scholten Joachim
DENSO	Henchoz Jean Michel
ERTICO - ITS Europe	FLAMENT Maxime
FIA	Preuss Gerd
FIA	Krid Laurianne
GDV	Redlich Jürgen
GDV	Lubos Christian
IBM	Guillaume Philippe
IMTECH	Rozema Klaas
Independent Expert	Menéndez J. Manuel
Independent Expert	Sampson Eric
Independent Expert	Williams Bob
IRU	Jeftic Zeljko
IRU	Nielsen Michael
Municipality of Helmond	Blom Gert
OCA	Kaltwasser Josef

Organisation	Name
Siemens	Wunder Roland
SWARCO	Franco Gino
Transport for London	De Estevan-Ubeda Natalia
VTT	Rämä Pirkko
Xerox	Harris Richard
VOLVO GROUP	Wahlund Jörgen
MEMBER STATES	
FIN- Ministry of Transport	Forsblom Marko
NL - Rijkswaterstaat	Op de Beek Frans
UK - Department of Transport	Boucher Tony

The following European Commission Service has been involved in WG2:

EC-DG MOVE	Van Gaever Alain
EC- DG MOVE	Alfayate Maria
EC- DG MOVE	Depré Claire

4.4. Work items

The complexity of the C-ITS ecosystem, the large variety of actors involved, the non-direct relations between the investment made by one user's group and the benefits obtained by other user's group, and the difficulties to take into account the needs of the overall society as individual user's preferences are likely to ignore the bigger societal impacts, were brought to the table in the early stages of the discussions.

In addition, the difficulty of addressing business cases, for which information could be considered sensitive by players involved, made WG2 to decide focusing on "business models" instead of "business cases".

WG members decided to focus the discussions analysing existing C-ITS experiences in both urban and non-urban environments. In this respect, two issues were identified of high relevance when trying to address business models: "Infrastructure Investments" and "Access to data".

4.4.1 Infrastructure Investments

Consensus amongst WG2 members was that the Infrastructure side was an essential element in making C-ITS a success:

The complexity of investments in *city-environments* was pointed out. In cities there does not seem to be one killer application but rather a set of applications that would make C-ITS a success. Facilitating procurement and providing guidance to city authorities are some of the actions that need to be taken in order to facilitate C-ITS investments in cities.

For *motorway environments:* while confronted with similar hurdles than cities to initiate C-ITS investment, the purchasing process seems less complex.

The importance of having 'quick win' cases and ambassadors for C-ITS projects was also stressed.

The key question, which kept coming back, was on how to trigger initial C-ITS infrastructure investments. At some point it was suggested that initial deployments of C-ITS might well focus on using cellular communications and on specific V2V C-ITS application sets. Nevertheless, WG2 members pointed out that in this scenario there was a risk that certain benefits of Vehicle to Infrastructure communication (V2I and I2V) might never come to fruition.

4.4.2 Access to data

Highlighted during the discussions in WG2 were the need to have low barriers to entry in terms of access to data - and more specifically to in-vehicle data - in order to allow for the deployment of new C-ITS enabled services and applications. In this respect, WG2 expects to carry out further work in the future based on the outcomes of WG6 on "Access to in-vehicle data".

4.5. Conclusions

WG2 realised in the very early stages that the issues to be addressed in view of assessing possible business models, and analyse the barriers and enablers to them, were very much dependent on work on-going in parallel in other WGs, and hence not available yet. For instance, several issues that were raised during the discussions of WG2, are being –or have been - addressed in WG1 on Cost Benefit Analysis, and WG9 on Implementation:

- WG9 which deals with implementation issues – has addressed the issues related to implementation in both urban and non-urban (e.g. roads/highways) environments. WG9 noted that a lack of knowledge on what benefits C-ITS can bring; the difficulties to convince purchasing departments to invest in C-ITS equipment and/or to integrate them in their long-term planning are major road blocks.
- This is quite similar to the attention drawn in WG2 on the difficulties to develop business models in urban environments and how to trigger infrastructure investments. In terms of addressing this issue WG9 is recommending to stimulate knowledge sharing among stakeholders, and especially among public stakeholders, and promoting innovative public procurement processes.
- WG1 is studying the Cost/Benefit analysis for the introduction of C-ITS according to several different scenario's. This work, while certainly not straightforward due in some cases to the scarcity of available to data to populate the analysis model, has also great relevance for the analysis of business models.

- In addition, the list of Day1 services produced by WG1 will also be extremely helpful to focus the future discussions on business models, on those services more likely to be introduced in the first place.

In this respect, the Chair of the WG, took the decision to wait for the outcomes of the above-mentioned WGs, in order to consider how to best address the issues related to business models and cases in the second phase of the C-ITS Platform, after January 2016.

5. Working Group 3 - Legal Issues

5.1. Objectives of the Working Group

The deployment of Cooperative Intelligent Systems (C-ITS**)** includes a number of important potential legal questions. In this context two main issues were brought up to Working Group 3 (WG3):

First to establish whether or not there are any liability implications inherent to the deployment of C-ITS, identify whether with higher levels of automation liability becomes more of an issue, and in that context whether specific topics relate to road infrastructure. It should be noted that fully autonomous driving was excluded from the objective of this working group.

Second, the WG also analysed the implications of existing road traffic legislation applicable to road vehicles that should be taken into account.

5.2. Organisation of Work

The organisation of work was based on regular face to face meetings (WG3 conducted a total of 6 face to face meetings from November 2014 – December 2015 in the course of the first phase of the C-ITS Platform) and also on a number of phone conferences. The physical meetings were also used to approve the technical reports or section of the reports.

DG MOVE as Chair of WG3 took care of maintaining relationships with other Working Groups and informing the WG3 participants of work items which could be relevant for the Group to consider. A link was also established with the working group on legal issues within the "iMobility Forum".

All results, outputs and expert recommendations of the C-ITS Platform WG3 have been produced, discussed and endorsed by nominated experts, representing the following organisations and Member States:

Organisation	Name
ADAC (Allgemeiner Deutscher Automobil-Club)	MAY Claudia
CLEPA (European Association of Automotive Suppliers)	WESSMAN Eleri
BOSCH	EISENMANN Susanne
DENSO	HENCHOZ Jean-Michel
ERTICO - ITS Europe	FLAMENT Maxime
FEMA (Federation of European Motorcyclists' Associations)	ZEE Anna
IAV GmbH	FICKEL Frank

Organisation	Name
IDIADA	ARRUE Alvaro
Insurance Europe	FABRY Olivia
Insurance Europe	GELIN Thomas
Orgalime	GOMEZ Enrique
Transport for London	DE ESTEVAN-UBEDA Natalia
CH - FEDRO	RIEDERER Markus
MEMBER STATES	
BE - FOD Mobiliteit en Vervoer	WAYENBERGH Aurelie
BE - FOD Mobiliteit en Vervoer	HOFMAN Karel
DE - BMVI	GELAU Christhard
ES - Permanent Representation	GARCIA DE SANDOVAL Aurora
IE - Roads Division	MCCARTNEY John
IE - Department of Transport, Tourism and Sport	MALONE Margaret
NL - RDW; National vehicle and driving licence registration authority	VAN VLIET Arjan
NL - Rijkswaterstaat	OTTO MARCEL
UK - Department of Transport	HANSON Graham

The following European Commission Services have been involved in WG3:

EC - DG MOVE	VAN GAEVER Alain
EC - DG MOVE	ALFAYATE Maria
EC - DG MOVE	DEPRE Claire
EC - DG MOVE	LOPEZ BENITEZ Casto
EC - DG MOVE	LINDAHL Susanne
EC - DG MOVE	HAMET Philippe
EC - DG JUST	MOSER Claudia
EC - DG JUST	SANGUINETTI Angela
EC - DG GROW	LAGRANGE Anthony

5.3. Work items

5.3.1 Liability

5.3.1.1 Implications in relation to C-ITS

Due to the fact that day one C-ITS applications are for information purposes, the driver always remains in control of the vehicle. Therefore, the WG concluded that there are no changes concerning liability compared to the current situation. However, participants highlighted the potential of consumers “trusting technology” and becoming dependant of it. This could cause a series of implications.

It was also highlighted that this "trusting technology" effect could be stronger when the information was provided by public authorities.

Manufacturers can address the issue of consumers “trusting technology” beyond the use for which it is designed, by providing sufficient warning/information. It was recommended to study whether further action would be needed or warranted (e.g. via driver training / adapted human machine interface to raise awareness). Both issues have been subject of discussion within the context of WG9 on Implementation Issues.

The Working Group recommends public authorities use a general principle or disclaimer that the information provided inside the vehicle is for guidance purposes only.

The group also looked at the developments in terms of traffic signage which is expected to move from being provided on a physical infrastructure to being provided digitally (only) inside the vehicle. In that respect, the group concluded that accuracy of information becomes even more critical.

The same conclusion was identified in relation to C-ITS applications containing sensitive safety critical messages for the driver.

The working group recommends further analysing the role and responsibilities of road/traffic authorities. To that extend, it was recognised that additional expertise might be needed in the discussions: further legal, technical and commercial experts would be of added value. An active participation of the Conference of European Directors of Road (CEDR) would provide a better insight from road/traffic authorities’ perspective for example. Representatives of city authorities would also be required. In addition, technical experts able to identify any wrong doings (failures or misuse) in the data flow/value chain (from information providers, such as traffic management centres, to road side units and end users) would also help to get a better understanding of the issues at stake.

5.3.1.2 Liability in relation to higher levels of connectivity and automation

It was also recognised in the context of WG3 that legal and liability issues for higher levels[6] of in-vehicle automation will be studied within other fora (such as GEAR 2030) and hence

[6] SAE Level 4 and beyond

would not be analysed by the WG nor be addressed in this document. However, the group also noted that higher levels of automation entail changes/upgrades from the infrastructural point of view (not only the physical road infrastructure but also from a digital point of view). Hence questions regarding the roles and responsibilities of road/traffic authorities would need to be addressed. Road/traffic authorities have an important role within the connected but also automated road transport eco-system. Indeed, once higher levels of automation are reached, the importance of the information provided via C-ITS (but also via other means, like road markings for instance) increases significantly as it is expected to trigger a subsequent action from the vehicle. In such a scenario the information provided can no longer be regarded as for information only, meaning the question of liability needs to be re-evaluated.

Recommendation:

In the second phase of the C-ITS platform the WG will have a closer look on the implications of higher levels of automation on liability issues, in particular for road/traffic authorities.

5.3.2 Relevant existing road traffic legislation

The Group examined whether the existing Vienna Convention on road traffic would need any revision to allow C-ITS deployment. The conclusion from the WG is that as far as C-ITS applications are concerned, the current amendment to the Vienna Convention (Amendment Article 8, paragraph 5) will be sufficient.

The new amended Article 8, paragraph 5 (text in bold is new) as adopted by the UN on 23 September 2015 reads as follows:

5. Every driver shall at all times be able to control his vehicle or to guide his animals.

5.bis. Vehicle systems which influence the way vehicles are driven shall be deemed to be in conformity with paragraph 5 of this article and with paragraph 1 of Article 13, when they are in conformity with the conditions of construction, fitting and utilization according to international legal instruments concerning wheeled vehicles, equipment and parts which can be fitted and/or be used on wheeled vehicles.

Vehicle systems which influence the way vehicles are driven and are not in conformity with the aforementioned conditions of construction, fitting and utilization, shall be deemed to be in conformity with paragraph 5 of this article and with paragraph 1 of Article 13, when such systems can be overridden or switched off by the driver.

No specific recommendation was therefore issued by WG 3 for this specific topic.

6. Working Group 4 – Data protection and Privacy

6.1. Executive summary

The objective of the C-ITS Platform Working Group on Data Protection & Privacy (WG4) was to provide an analysis of the issues related to the Privacy and Data Protection landscape in the context of C-ITS and elaborate recommendations to efficiently address them.

Cooperative Intelligent Transport Systems (C-ITS) make use of information and communication technologies that enable different parts of the road transport network to share information. Using new forms of communications, vehicles are now capable of broadcasting or receiving data that allow them to communicate with each other and/or with the infrastructure. In addition to what drivers can immediately see around them, and what vehicle sensors can detect, all parts of the transport system will increasingly be able to share information to improve driver decision-making and optimise transport operations and safety.

The potential applications and end-user services covered by C-ITS are quite diverse and wide ranging. To test and develop solutions, WG4 identified a family of standardized messages relevant for the purpose of analysing the privacy and data protection challenges faced by C-ITS: the Cooperative Awareness Messages (CAM) and the Decentralized Environmental Notification Messages (DENM).

C-ITS equipped vehicles making use of these messages are **constantly broadcasting data**, including e.g. their speed and location.

This broadcasting is an inherent part of the system and hence raises potential concern as how to guarantee privacy and data protection. After an in-depth analysis, WG4 concluded that those messages are considered as “personal data” because of the potential of indirect identification of users. The European legislation on Data Protection 95/46/EC is therefore considered applicable and, consequently, WG4 examined the different legal basis to process legally these personal data.

The outcome of this work is a number of recommendations regarding measures to ensure a sound level of data protection and privacy when C-ITS is deployed. Particular attention is given to the issue of ensuring informed consent from the driver, for which WG4 elaborated solutions and recommendations. Eventually it is concluded that while the principle of the "informed consent" is of outmost importance, the secondary use of C-ITS data might also be taken into account. In most cases, an opt-out possibility should be offered to the drivers, authorizing the driver to shut down the broadcast (while fully informing him about possible adverse consequences).

Moreover, for C-ITS road safety and traffic management applications, where a "vital or public interest" is at stake and is demonstrated, WG4 concludes that a limited number of applications can process the data without drivers explicit consent, provided that the legal basis to process the data (according to the legal framework in place) and these applications are strictly defined and the data collected under these conditions are not further processed or re-purposed beyond these applications.

6.2. Organisation of Work

The work of WG4 was articulated over regular face to face meetings. A total of 11 meetings took place from November 2014 to December 2015. These meetings were used to elaborate in an iterative manner the different issues addressed, to foster participation amongst WG4 and to develop ownership and agreement on the technical results achieved and the associated recommendations.

DG MOVE and DG JRC chaired WG4 and took care of maintaining communication and collaboration with the other WGs of the Platform, informing WG4 participants of relevant work items in other WG's. This was particularly true with WG5 on security, as a number of techniques and provisions addressing security issues can be transposed to manage Data Protection challenges. This led to a special collaboration between the two WG's and to a number of joint meetings.

Substantial work was required to assess and classify the data exchanged with C-ITS CAM and DENM messages as personal data or not, and if so, to determine the adequate legal basis to process them legally.

Also, a specific effort was developed to analyse the threats and risks to privacy and data protection linked to the broadcast of CAM and DENM messages. In particular: unauthorized access to data, users low control, secondary uses and re-purposing of data, re-identification after anonymization, users profiling, instantiation of driver consent, negative public perception and loss of trust, frauds, malicious and criminal actions.

Similarly, much effort was spent to identify adequate mitigation measures, for instance, for enforcing valid informed consent or using specific security techniques for lowering the risks of tracking and tracing vehicles.

All results, outputs and expert recommendations of the C-ITS Platform WG4 have been produced, discussed and endorsed by the following nominated experts, representing the following organizations and countries:

Organisation	Name
Member State (DE) - German Federal Ministry of Transport and Digital Infrastructure	GELAU Christhard
HERE Deutschland GmbH	KUJALA Henri
Insurance Europe	GYFTOKOSTA Lamprini
ACEA	GREVEN Marc
Member State (SE)-Swedish Transport Agency	MARTON Marion
ERTICO-ITS Europe	FLAMENT Maxime
ASFINAG	JANDRITIS Marko
IBM	GREENWOOD Sarah
FIA	KRID Laurianne
Member State (HELLAS) - ICCS	AMDITIS Angelos

Member State (NL) Ministerie van Infrastructuur en Milieu	OTTO Marcel
Member State (NL) RDW, department of road transport	VAN VLIET Arjan STRIEKWOLD Peter
Member State (RO) Ministry of Information Society	MANESCU Corneliu
RENAULT	ROUSSEAU Christian
Tom Tom	HANIA Simon
FIGIEFA	GOTZEN Sylvia PATTEMORE Neil
Member State (IE)Department of Transport, Tourism and Sport	MALONE Margaret
CLEPA	WESSMAN Eleri
KAPSCH	LAX Richard
Member State (UK) Department of Transport	HANSON Graham
BMW AG	SCHOLTEN Joachim
EDPS	KLABUNDE Achim LAKSANDER Malgorzata CIESIELSKA Anna
IDIADA	ARRUE Alvaro
FEMA	DELHAYE Aline ZEE Anna
ORGALIME/SICE	GOMEZ Enrique
Member State (HELLAS) - ICCS	AMDITIS Angelos
BOSCH	EISENMANN Susanne
FIAT	BIANCONI Maria Paola
Individual Expert	SAMPSON Eric

The following European Commission Services have been involved in WG4:

Services	Name
EC CNECT	GAUDILLAT Eric
EC CNECT	ZAMBARA Nino

EC MOVE	LINDBERG Sara
EC MOVE	ALFAYATE Maria
EC MOVE	DEPRE Claire
EC MOVE	VAN GAEVER Alain
EC MOVE	MARTINEZ Bernardo
EC JRC	BALDINI Gianmarco
EC JRC	MAHIEU Vincent
EC JRC	BESLAY Laurent
EC JRC	NORDVIK Jean-Pierre
EC JUST	SCHEUER Ursula

6.3. Data Protection in C-ITS

6.3.1 General description of C-ITS

Every unit of a C-ITS network, being mobile or standing roadside, exploits the data received from other devices to generate strategic warnings, tactical advices and driver information. While vehicle units broadcast data about their position, speed and driving direction (via CAM) or event-driven information, such as an obstacle or changing environmental conditions (via DENM), roadside units deliver local data such as speed limits, signal phases and timing of traffic lights or information about traffic diversion.

The vehicle units integrate all data received to form a picture of the local traffic situation and generate information and warnings directly relevant for the drivers. For example, based on the exchanged data between vehicles and vehicles and vehicles and infrastructure a driver would receive information via an ergonomic Human Machine Interface (HMI) about works blocking the road ahead or would be warned regarding situations requiring attention.

Using the sensors of the vehicle' driver assistance systems and the communication capabilities of cooperative systems, hazardous locations like slippery roads or black ice and aquaplaning areas detected by one vehicle can be communicated to other approaching vehicles.

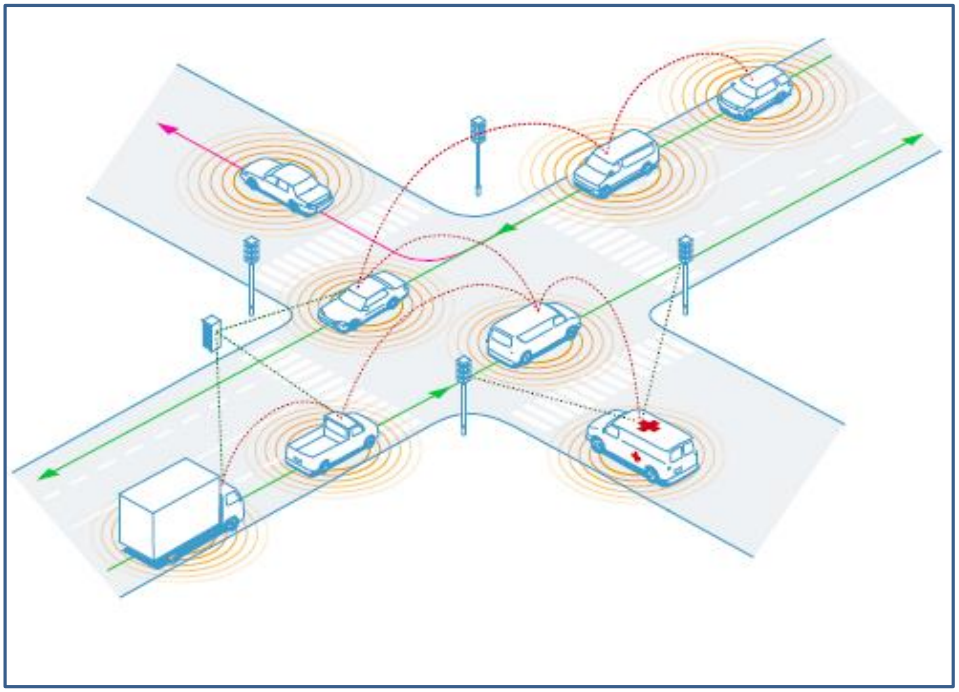


Illustration of typical interactions existing within a C-ITS network

6.3.2 C-ITS use cases and categories of applications

The need to focus the analysis in terms of data protection and privacy on a restricted number of use cases appeared quickly. The basic set of ITS applications defined in ETSI TR 102 638 was used as a reference.

ETSI TR 102 638 classifies the applications into the following clusters:

1. road safety,
2. traffic efficiency,
3. co-operative local services,
4. global internet services.

The selection of use cases in the clusters was made using the following criteria: amount of data involved, severity from misuse of such data, and frequency of occurrence of the application.

Eventually, WG4 selected the following three use cases:

- Intersection collision warning,
- Regulatory speed limits notification,
- Probe vehicle data collection.

The analysis of the above three cases revealed the majority of data privacy and protection issues related to the use of C-ITS. Indeed, a large majority of use cases present similar risks and issues (in terms of data privacy and protection).

6.3.3 Legal framework for Privacy and Data Protection

As indicated before, an important question debated by WG4 was to determine whether data exchanged via CAM and DEMN would be classified or not as personal data.

After various consultations (e.g. with EDPS and privacy experts), WG4 concluded that

"transmitted CAM and DENM messages are to be considered personal data",

mainly because these data give access to the vehicle identification and indirectly to the identity of the vehicle owner.

Therefore, the EU legislation on data privacy and data protection applies.

The legal framework concerning Privacy and Data Protection has evolved along the years. Starting from the 1980 OECD Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data, until the on-going discussions on the comprehensive reform of data protection rules in the EU, as proposed by the Commission in 2012, in particular the proposed General Data Protection Regulation (GDPR), COM(2012)11 of 25.01.2012.

At the time of writing the legal framework or reference is Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Article 7 of Directive 95/46/EC sets out the legal bases allowing the process of personal data, notably:

(a) Processing is based on **consent**,

Example: a driver gives his consent to receive targeted advertisement on local shops and services, using the vehicle location,

(b) Processing is necessary for performance of a **contract** to which the data subject is a party,

Example: a vehicle owner signs an insurance contract stipulating that the vehicle will be traced or that CAM/DENM messages will be recorded in an on-board platform. If the vehicle is rented or driven by other drivers, the owner should ideally inform the drivers about the 'contract' and the consequences,

(c) Processing is necessary for compliance with **legal obligations** imposed on the data controller,

Example: a law makes mandatory that tolling companies have to archive 1 year of CAM/DENM messages of the traffic flow,

(d) Processing is necessary to protect the **vital interests** of data subject(s),

Example: in case of imminent danger a C-ITS unit, being mobile or standing roadside, is authorized to make use and process data from the actors directly concerned by the

imminent danger (i.e. road interrupted by obstacle or works, tunnel traffic interrupted, wrong way driver, chain crash ahead, imminent collision, …),

(e) Processing is necessary for performance of a task carried out in **public interest**,

Example: a Ministry of Transport is performing mass roadside records for statistics on the impact of its road management policy, with the final goal of improving traffic flow,

(f) Processing is necessary for **legitimate interests** pursued by the data controller,

Example: an owner of a fleet of delivery vans is collecting and processing fleet location data without asking the consent to the drivers, to optimize his business.

6.3.4 Legal basis for processing data exchanged in C-ITS using CAM and DENM

In first analysis, as CAM and DENM messages are broadcasted constantly, it seems challenging to construe a contractual obligation around processing of CAM and DENM messages based on Article 7(b) of Directive 95/46/EC. Similarly, the WG4 was not aware of any upcoming specific legislation allowing the use of Article 7(c) or tasks justified by a public interest, which would legitimize processing of CAM and DENM messages based on Article 7(e). (Note though, that this situation may evolve, if new EU laws or obligations are enacted.). Also, Article 7(d) seems inappropriate, but for safety-critical applications, as vital interest can be justified only if substantial hazardous situations are present. It emerges that processing based on consent Article7(a) seems the most straightforward legal bases, at first sight, to justify processing of data exchanged over CAM and DENM.

Opinion 15/2011 of 13/07/2011 of the Art. 29 Data Protection Working Party provides a definition of consent. The legislative history of Directive 95/46/EC shows relative consensus on the conditions for a valid consent: consent has to be **freely given**, **specific** and **informed**. The proposed General Data Protection Regulation is adding additional requirements to the consent: it needs to be **explicit** and **verifiable**.

WG4 therefore examined how to implement consent in the case of C-ITS, taking into account the following elements:

- ID of the data subject,
- Information provided to the data subject,
- Whether consent given is really specific,
- Purpose limitation,
- Whether emergency and/or vital interests are at stake.

A paradox quickly emerged. How can a driver express a specific and informed consent for data being freely broadcasted? This would, indeed, be contrary to a requirement for a valid consent since a consent collected in these circumstances would not really be specific or informed, as purpose is unclear.

WG4 therefore considered first the solution to empower the driver with a way to enable/disable the broadcast. From a legal point of view, this gives the necessary power to

the data subject. However, disabling broadcast is a drastic opt-out of any C-ITS applications, including those improving road safety, thus reducing the overall expected benefit in terms of safety of C-ITS. This consideration led to a refinement of this solution with the identification of a concept of gradual and selective consent.

The following table provides the different legal basis that can justify the processing of data exchanged in the four categories of C-ITS applications identified in 6.3.2. It is worth noting that processing based on consent is limited to one category only.

C-ITS Applications	Possible legal Basis justifying the processing of data
Road safety	Processing is necessary to protect the **vital interests** of data subject(s)
Traffic efficiency	Processing is necessary for performance of a task carried out in **public interest**
Global internet services Infotainment Co-operative local services	Processing is based on **consent** and/or Processing is necessary for performance of a **contract**

The ad-hoc 'multi-conditional 'consent instantiation can be summarized as follows.

1. A distinction has to be made amongst the different categories of C-ITS applications, namely,

   - The "**vital interest**" type of applications,
   - The "**public interest**" type of applications,
   - Those applications not belonging to the categories above – and thus defined as the "**consent category**" requiring "consent".

2. In function of the category, the legal basis for processing would be different.

   (a) For processing data in applications within the **"consent category"**, a 'consent marker' has to be attached to the CAM/DENM messages to allow them to be legally processed. Consent needs to be instantiated at every journey. Alternative solutions, such as identifying data subjects, are more complex and costly. Consent has to be **informed**, **specific**, **unambiguous**. The challenge here is to maintain a list of clearly identified applications, accessible to the driver, to which the consent can be unambiguously linked. According to the number and variety of applications, more elaborated consent markers (with more dimensions) may be needed, so as to give data subjects a way to manage specific applications. Parties

processing personal data not marked for consent in applications requiring consent expose themselves to prosecution.

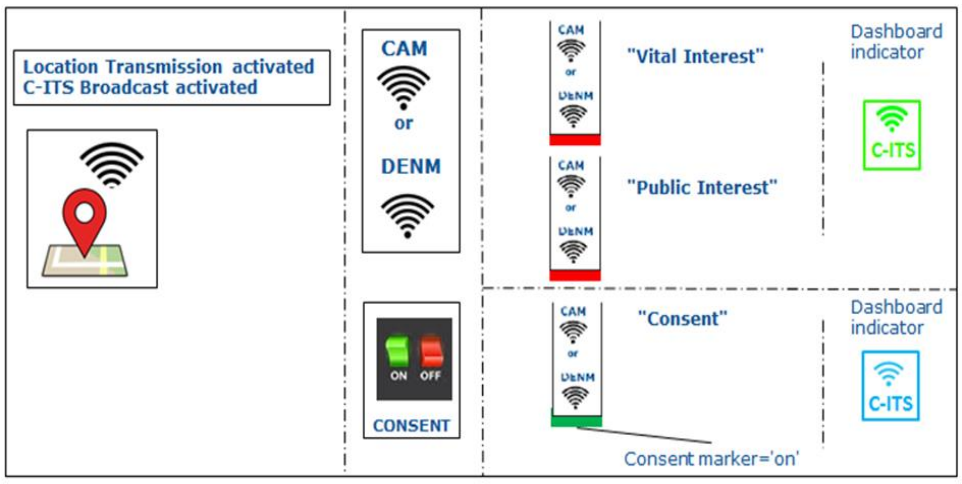
(b) For processing data in applications within the "**vital interest**" category, it needs to be demonstrated that these applications fall under the legal basis of "vital interest". The legal basis for Day 1 road safety applications may start with **consent**, and might be switched to **vital interest** in a second phase, if such vital interest is demonstrated.

(c) For processing data in applications within the "**public interest**" category, these applications need to be 'legally qualified' as fulfilling a public interest duty.

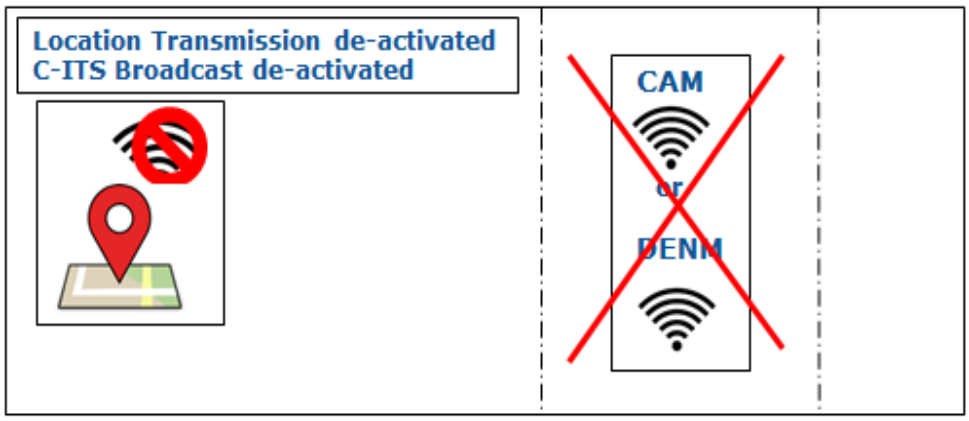
3. The driver should keep, at all times, the control over the CAN/DENM messages being broadcasted.

   This control also provides means to individuals (data subjects) to exercise their right to object, as required by article 14 of the Data Protection Directive.

   WG4 has designed a control functionality building on those planned for vehicles, where drivers are provided with means to deactivate the transmission of geolocation of their vehicles. Having in mind that without location information the broadcasting of CAN/DENM does not make sense, WG4 has envisaged to couple the possibility to "deactivate geolocation transmission" with the "deactivation of the CAN/DENM broadcasting", as illustrated in the following two figures.



Geo-location enabled (+ C-ITS)



Geo-location disabled (+ C-ITS)

The solution described above is based on the possibility to put a "consent marker" attached to the CAN/DENM messages to indicate, for those applications requiring a consent, that they can be legally processed.

Applications falling under the "vital interest" need to be qualified as such. The same consideration exists for applications falling under “public interests” or “legal obligations”.

CAN/DENM messages are not encrypted. Thus a 'rogue' actor could eavesdrop and illegally process the data exchanged via CAN/DENM. This issue is typical of applications using broadcast communications and not specific to C-ITS. A parallel can be drawn with Wi-Fi or mobile devices where personnel information can also be collected and processed. The proposed solution offers better protection, as the freely broadcasted data will have a marker specifying the ‘purpose’ and the applications for which they can be processed.

6.3.5 Further guidance to ensure compliance with privacy and data protection

Some additional pragmatic guidelines on how to ensure compliance with relevant data protection and privacy legislation has also been prepared in an attempt to define a basic framework of good practices for stakeholders, complementing the considerations already presented in the previous sections. Recommendations have been elaborated, taking into account the elements described below:

Actor-specific obligations

Obligations for all actors involved in the data chain (i.e. collector, processor, supplying, transmitting, storage, anonymizing) to follow a Privacy-by-Design approach:

- Perform privacy impact assessment prior to deploying a C-ITS application,
- Perform a risk and threat analysis and plan for mitigation solutions,
- Determine what is the legal basis of processing the data using the list provided above,
- Acquire consent where necessary,
- Apply the principles of data minimization and purpose limitation,
- Data sharing, only if mandated by law or after agreement with data subject.

Secondary use

It is important to identify the motivations and the various situations where secondary use or re-purposing of data may take place, together with a short identification of associated threats. The understanding of these threats is instrumental in the definition and design of mitigation measures.

Amongst the possibilities, the following ones were identified:

- Massive data records for statistics in one spot (e.g. for traffic management, "accidentology"),
- Massive records in different places for comparison and policies evaluations, social studies, etc.,
- Private initiative to aggregate data and derive business opportunities (e.g. as a data broker),
- Isolated CAN and DEMN captured by 'hacker', by challenge, or to investigate what value can be extracted - this would be illegal,
- Malicious activities leveraging on the information derived from gathering CAM and DENM messages - this would be illegal and probably criminal.

6.4. Conclusions

- A driver or owner of a vehicle is indirectly identifiable (and hence the CAM/DENM messages are to be considered personal data (as per art 2(a) of 95/46/EC)) when the data broadcasted are correlated with information from other sources that **directly identifies the owner or the driver of the vehicle**.

- Due to the potential of indirect identification, WG 4 concluded that CAM and DENM messages are to be regarded as "**personal data**" following the definition of 95/46/EC, as interpreted by Working Party Article 29 in its various opinions.

- The WG4 evaluated carefully the **various legal basis** to process this personal data and proposes a solution to implement efficiently C-ITS applications based on CAM and DENM messages, while **respecting the EU legislation on data protection**.

6.5. Recommendations

6.5.1 Legal basis

- Given that **CAM/DENM messages** are considered **personal data** and based on the analysis carried out on the legal basis to process such data, the **WG 4 strongly recommends** implementing the principle of "**informed consent**" (by providing the vehicles with ad-hoc technologies allowing to attach "consent markers" to personal data). This should ideally **require a standardization effort** to set out consent protocols rich enough to differentiate the applications.

- C-ITS applications based on "**vital or public interest"** can process data **without drivers explicit consent**, provided that:
    - **conformance** with "vital or public interest" with C-ITS road safety and traffic management applications objectives is assessed **on a case by case basis**;
    - the **legal framework** and the set of applications falling within the "vital or public interest" category are strictly defined;
    - data collected under these conditions are **not further processed** or **re-purposed** beyond that category of applications**.**

- A detailed **information awareness campaign** is needed to inform drivers on the **negative consequences** of disabling the broadcast, in terms of decreased road safety and possible absence of incoming messages, and on the **efficiency** of the **privacy protection** offered by **consent markers** and **security provisions**.

- WG4 calls on **Article 29** to define, together with the relevant actors and stakeholders, **criteria** that should be used to categorize applications that may fall univocally under public or vital interest.

- WG4 strongly recommends implementing **mitigation measures**, such as those in the field of security, that will contribute to lowering down the impact of C-ITS on privacy and data protection and consider measures that can **prevent abuse or misuse of personal data**.

6.5.2 Technical

- It is recommended to foster the principle of **'Privacy by Design'** and develop systems flexible enough to guarantee **full control of personal data** by the data subject. This may call for concepts as described in this document, with 'consent markers' attached to CAM and DENM messages, and with the use of Human Machine Interfaces (HMI) to **inform drivers**.

- CAM/DENM messages can be transformed into "**anonymized data**" at the moment of broadcasting, provided that additional technological, operational, organizational and legislative measures are taken. Implementation of **security measures supporting anonymization are strongly recommended**, notably measures guaranteeing short lifetime for temporary certificates (typical less than one 1 hour or even shorter), combined with a prohibition to keep any record correlating temporary certificates with vehicle certificates. The work carried out in the context of WG5 of the C-ITS platform on a common certificate policy in Europe is therefore of considerable importance.

- **Certificate Authorities** and **Vehicle Manufacturers** involved in any European C-ITS Public Key Infrastructure schemes, should be bound by technical, organizational and legal measures to ensure that:

    - only information required **to generate certificates** is exchanged;
    - the lifetime of the **temporary certificates,** taking into account overall cost and complexity, is minimized;
    - the **retention period** of transaction logs at Certificate Authorities, having regard to the purpose of retaining these logs, is minimized;
    - the **Certificate Revocation Lists (CRL's)** are kept for a minimum period of time, at all levels, for all authorities and all C-ITS units;
    - observed **CAM and DENM messages** and invalidated **Temporary Certificates** are not stored and retained in vehicles.

6.5.3 Organizational

- It is recommended to increase **awareness** of drivers (data subjects) on their ability to manage their personal data in this C-ITS context (see results of WG8 on public acceptance).

- It is recommended to develop a **code of conduct** for stakeholders offering Global Internet Services and Co-operative local services built on broadcasted CAM and DENM messages, for a fair use of these data.

6.6. Annex

Analysis of Data Protection & Privacy in the context of C-ITS:

WG4 - ANNEX1 - Analysis of Data Protection and Privacy in the context of C-ITS.docx

7. Working Group 5 - Security and Certification

7.1. Objectives of the Working Group

The objectives of the C-ITS Platform working group on Security & Certification were to investigate the main security aspects in Cooperative Intelligent Transport Systems (C-ITS), which must be addressed to support a secure and safe deployment of C-ITS in Europe. For this purpose, various experts in the C-ITS community and deployment initiatives from different categories of stakeholders (e.g., vehicle and equipment manufacturers, Member States, infrastructure operators, standardisation experts) participated to the C-ITS Platform meetings of the working group. A number of relevant working items were identified in the early phase of the activities of the working group. The working items were selected with the consensus of the WG5 participants on the basis of the need to support deployment of C-ITS in Europe.

One of the first selected work items was the definition of the trust model for C-ITS in Europe to support an European harmonized approach for the provision of trust among the main participating entities of C-ITS (e.g. C-ITS stations, C-ITS applications, etc.). The European C-ITS trust framework has been defined as E-SCMS (European C-ITS Security Credential Management System). Revocation of trust was another work item suggested by the WG5 participants to ensure that non-compliant C-ITS stations or misbehaviour are addressed. Another work item was to tackle the topic of crypto-agility and updateability, which was chosen to ensure that the security framework in C-ITS have adequate flexibility in the lifetime of C-ITS stations and applications. The last work item is the overall C-ITS compliance assessment process to ensure that only valid C-ITS stations can be deployed in the field.

Each work item had the objective to produce a technical report, where all the work group experts and involved organisations contributed with their point of view. All reports and outcomes of the working group are based on consensus and have been endorsed by all participating experts (during the work process the different views have been presented accordingly in the reports if no consensus was able to be reached on specific topics or recommendations). Note that the different work items are linked among each other and cannot be seen as individual items. The splitting into different work items was only necessary in order to have a workable process within the working group. For example, revocation of trust is clearly one of the functions to be defined in the certificate policy of the trust model. In another example there is a clear link between the compliance assessment and security results of the working group, as for instance the successful compliance assessment of a C-ITS station ensures that a C-ITS station can be trusted and that it will therefore receive the trust certificate from the Certification Authority (CA).

Some topics related to security of C-ITS (e.g., general cybersecurity threats) were not selected because they are indirectly addressed through the chosen work items described above or because they were considered manufacturers responsibility or because they were dealt in other working groups (e.g. WG6 on access-to-in-vehicle data discussions on in-vehicle security / gateways, etc.).

7.2. Organisation of Work

The organization of work was based on regular face to face meetings (WG5 conducted a total of 13 face to face meetings from November 2014 – December 2015 in the course of the first phase of the C-ITS platform) and also on numerous phone conferences to deal with specific sub-topics in the main work items. The physical meetings were also used to approve the technical reports of section of the reports.

DG MOVE chairing WG5 took care of maintaining relationships with other Working Groups and informing the WG5 participants of work items, which could be related. In the particular case of privacy and security in C-ITS, because privacy and security can be strongly related and security frameworks can also support privacy solutions in C-ITS, a special collaboration and a number of meetings were set up between WG4 and WG5. Further topics for WG 10 on international cooperation have been identified that require further discussion beyond Europe in the future.

All results, outputs and expert recommendations of the C-ITS Platform WG5 have been produced, discussed and endorsed by the following nominated experts, representing the following organizations and countries:

Organisation	Name
Applus IDIADA	ARRÚE Álvaro
Applus IDIADA	PILLADO Marcos
ASFINAG	JANDRISITS Marko
BMW	SCHOLTEN Joachim
BOSCH / CLEPA	KNIRSCH Matthias
Car 2 Car Communication Consortium	ANDERSEN Niels Peter Skov
CECRA	ARATHYMOS Neofitos
CEDRE	OP DE BEEK Frans
CLEPA	DEIX Stefan
Continental	ERDEM Bettina
Continental	KOCH Ingolf
CSI (UK) Ltd	WILLIAMS Bob
CTAG	PRIEGUE Francisco
DENSO Automotive Deutschland GmbH	LEINMUELLER Tim
ERTICO	FISCHER Francois
FIAT	BIANCONI Maria Paola
IBM	NEVEN Gregory
Kapsch TrafficCom	LAX Richard
Kapsch TrafficCom	TIJINK Jasja
Kapsch TrafficCom	WILDMANN Guenter

Member State (AT)	FRÖTSCHER Alexander
Member State (AT)	MOLIN Helge
Member State (BE)	POURTOIS Caroline
Member State (CZ)	PICHL Martin
Member State (DE)	BERNDT Sandro
Member State (DE) - BSI - Federal Office for Information Security	Schönherr Kerstin
Member State (DE) - BSI - Federal Office for Information Security	WIESCHEBRINK Christian
Member State (EL)	AMDITIS Angelos
Member State (FR)	OLLINGER Eric
Member State (FR)	PAGNY Roger
Member State (NL)	HAVINGA Hellen
Member State (NL)	LAMAITRE Gaston
Member State (NL)	OTTO Marcel
Member State (RO)	BANICA Sorin
Member State (UK)	BOUCHER Anthony
Member State (UK)	HANSON Graham
OpenTrust (SCOOP@F)	ABALEA Erwann
OpenTrust (SCOOP@F)	BLANCHER Remi
Pauls Consultancy BV	SPAANDERMAN Paul
PSA Peugeot Citroen	SERVEL Alain
Q-Free	EVENSEN Knut
RENAULT	LONC Brigitte
RENAULT	ROUSSEAU Christian
RENAULT	TISSOT Christine
Security Innovation	WHYTE William
SIEMENS	FUEREDER Herbert
SMMT / ACEA	DAVIS Peter
SWARCO / TISA	SCHMID Andreas
Telecom ParisTech / SCOOP@F FRANCE	LABIOD Houda
University of Murcia	SKARMETA Antonio
Volkswagen AG	BUBURUZAN Teodor
VOLVO Cars	BROBERG Henrik
VOLVO GROUP	WAHLUND Jörgen
VOLVO GROUP	ZAKIZADEH Hossein

The following European Commission Services have been involved in WG5:

Services	Name
EC CNECT	FREDERIX Florent
EC CNECT	HOEFS WOLFGANG
EC CNECT	ZAMBARA Nino
EC GROW	ESCOBAR GUERRERO Luis
EC GROW	LAGRANGE Antony
EC INEA	PALESTINI Claudio
EC JRC	BALDINI Gianmarco
EC JRC	MAHIEU Vincent
EC MOVE	ALFAYATE Maria
EC MOVE	CARABIN Gilles
EC MOVE	DEPRE Claire
EC MOVE	MENZEL Gerhard
EC MOVE	TZAMALIS Georgios
EC MOVE	VAN DER LINDEN Geert
EC MOVE	VAN GAEVER Alain

7.3. Work items of WG5

7.3.1 Trust Models for C-ITS

The main item that has been discussed in WG5 was the design of the Trust Model for C-ITS, because it is the essential pillar to ensure security and trust among the main entities of C-ITS.

The objective of this work item and the related technical report was to identify and analyse the main Trust Models for Cooperative-C-ITS based on a Public Key Infrastructure (PKI). While other cryptographic techniques could also be used (e.g., symmetric cryptography), the report focuses specifically on PKI. The report identifies the potential PKI-based trust models from literature and other case studies and assess them on the basis of the specific features of C-ITS and metrics of evaluation based on high level requirements.

The report describes similar case studies, which could provide input to the analysis for the C-ITS trust model both from existing running systems and from standardization activities. Case studies outside ITS were also considered.

The report identifies the main trust models based on PKI and the main requirements areas, which are used to evaluate the trust models. An analysis for each requirement area has been provided. The set of analysis has been used to provide final recommendations for the most appropriate trust model in C-ITS for Europe for a day one phase and a mature deployment phase.

The final report on this work item is WG5 – ANNEX 1.

7.3.2 Revocation of Trust in C-ITS

The work item of revocation of trust was chosen to ensure that misbehaviours of C-ITS station or applications (either intentional or unintentional) were dealt in the proper way. The work item and the related technical report presents an analysis of the expert members of the C-ITS Platform security working group 5 on the topic of revocation of trust in C-ITS in order to identify the requirements for revocation of trust in C-ITS and the related countermeasures. The report captures the relevant work from the state of the art both from research and standardization activities. The main threats and related incident scenarios are defined to illustrate the different needs (requirements) for revocation of trust, although this report does not claim to be a complete analysis. This report does not provide a full Threat, Vulnerability and Risk Analysis (TVRA) for the trust revocation function in C-ITS.

Technical solutions and design options for revocation are discussed to understand what a Trust Model can and should provide for deployment of Day 1 and beyond C-ITS services from different stakeholder viewpoints and what mechanisms can be used to control and mitigate risks. The WG5 experts agreed to a medium term solution with a strong involvement of stakeholders from private and public institutions. Some currently open aspects in the discussion of the revocation of trust topic still remain, which will need to be defined as topics and analysed further with the support of the respective stakeholders in order to facilitate the introduction of C-ITS in Europe.

The final report on this work item is WG5 – ANNEX 2.

7.3.3 Crypto Agility / Updateability in C-ITS

Crypto-agility is the ability of a protocol to adapt to evolving cryptography and security requirements. There are various reasons why the cryptographic algorithms already deployed in C-ITS must be updated. The reasons can be both intentional and unintentional. Intentional reasons can be a migration from a previous cryptographic algorithm to a new one. Unintentional reasons are related to a broken algorithm, which could make the system unusable.

Another aspect investigated in the report is software updateability. The use of software has increased considerably in recent years in the automotive market. Software can be updated and installed in the automotive components of cars but this opens new risk and threats, which are similar to the one affecting the computer industry (e.g., virus, worms). The report investigates the approaches and techniques, which can be used to support secure software update and activations.

This report aims to map the current positions of C-ITS Platform WG5 experts on how crypto agility and software updateability can be handled when deploying C-ITS systems.

The final report on this work item is WG5 – ANNEX 3.

7.3.4 Compliance Assessment in C-ITS

This work item was chosen because it is important that C-ITS station are fully functional before they can be trusted to be deployed in the field. The objective of the work item and

the related report 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” has been used to describe the process by which a C-ITS station is validated through a set of tests to be deployed in the market. For the achievement of key public policy goals, C-ITS stations require compliance assessment before being placed on the EU’s internal market. The report looked 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, the report discusses, in which cases compliance assessment procedures are necessary. The 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 final report on this work item is WG5 – ANNEX 4.

7.4. Recommendations/Follow Up Actions

7.4.1 Main high level WG5 Recommendations

The experts of WG5 have identified specific recommendations for all work items described in the previous chapters of this report. The following high level recommendations aim to summarise the main high level recommendations that can be derived from the more specific recommendations on the single work items in WG5 - ANNEX 1-4:

- One common C-ITS trust model all over Europe shall be deployed that shall support full secure interoperability at the European level.
- To that end, a common certificate policy of the trust model for C-ITS day 1 deployment in Europe needs to be defined urgently.
- The appropriate legislative framework for C-ITS (e.g. new delegated acts or the identification of the amendments to the existing regulatory framework) needs to be set in place quickly to support a C-ITS deployment starting from 2019.
- The roles of the entities at European level to support the deployment and operations of C-ITS in Europe need to be identified and defined (e.g. roles within a European C-ITS security credential management system or within the compliance assessment process).
- The financing scheme needs to be discussed to identify which parties will support or contribute to the financing scheme.
- Standardization activities for the gaps identified in the reports (e.g., revocation of trust) should be addressed urgently.
- A time plan for the design and deployment of the security elements (e.g., CA) of an EU wide C-ITS with the most significant milestones should be drafted.

7.4.2 Specific recommendations of the single work items

An abstract of the complete set of specific recommendations on the single work items is included in the following sub-sections. For further details please check each respective ANNEX for the full context of the analysis, details and conclusions that lead to the specific WG5 expert recommendations.

7.4.2.1 Trust Models for C-ITS

The analysis conducted in the trust model report (WG5 - ANNEX 1) has identified the following recommendations:

(1) The agreed objective is to **deploy one common C-ITS trust model all over Europe** that shall support full secure interoperability at the European level. Since the experts of WG5 recognise that this cannot sufficiently be provided by either a single EU Member State, nor by individual stakeholders (e.g. automobile manufacturers) a joint effort to develop EU-wide policy with clearly identified roles and methods is required. As described in WG5 - ANNEX 1, the EU-wide C-ITS trust model is the implementation of the trust model based on a Public Key Infrastructure (PKI) system with the associated policies, organizational structures and processes including the links to the C-ITS compliance assessment process for certain types of applications.

a) This trust model **shall be implemented in a single trust domain version** (e.g., one single cryptographic algorithm and certificate format) **for the start-up day one phase** of C-ITS.
b) **Beyond the Day 1 phase, C-ITS may be extended with multiple interoperable trust domains** if deemed necessary to take the variety of stakeholders (including the global dimension) and the responsibilities for private and public entities involved into account.

In order to deploy a common C-ITS trust model specific elements and steps are needed. According to the WG5 experts the following recommendations are therefore further defined:

(2) **Need for Legal Certainty**: The appropriate legislative framework (e.g. new EU delegated acts or the identification of the amendments to the existing EU regulatory framework) needs to be set in place **quickly**.

(3) In order to achieve legal certainty a careful **analysis and discussion with the relevant stakeholders** is needed. The list of relevant stakeholders identified by the WG5 experts includes (but it is not necessarily limited) to:
- Member States
  - Responsible National Security Agencies
  - Responsible National authorities, ministries or bodies
- Vehicle manufacturers

- Infrastructure operators
- Telematics manufacturers for vehicle, roadside infrastructure and nomadic devices.

(4) The **responsible policy bodies for the definition of the security policy, certificate policy and related implementation measures (e.g. certificate practice statement) have to be identified** – this should be done in parallel with setting up the appropriate legislative framework. An independent governance structure will be needed to coordinate the definition and subsequent implementation of the commonly agreed elements (e.g. certificate policy) for *Day One* C-ITS applications deployment. This includes the definition of the entities responsible for the setting up and implementation of the components of the trust model.

(5) The **financing scheme** needs to be discussed to identify which parties will support or contribute to the financing scheme.

(6) Compliance with the identified legislative framework in (2) **will need to be reflected in the compliance assessment process** for vehicle and roadside C-ITS equipment.

(7) A **time plan for the design and deployment of the EU wide C-ITS trust model** with the most significant milestones (e.g. identification of the CAs or definition of the certificate policies) should be drafted. The experience from the EU C-ITS corridor deployment initiatives, standardisation activities and pilot projects should be taken in consideration in the drafting of the time plan. The time plan should include at least the following milestones:

- Definition of the Certificate Policy, Certification Practice Statement and Security Policy
- Identification and design of the PKI
- Definition of the distribution channels for the certificates
- Definition of the compliance assessment process
- Definition of the financing scheme

7.4.2.2 Revocation of Trust in C-ITS

The analysis conducted in the revocation of trust report (WG5 - ANNEX 2) identified the following recommendations:

(1) Revocation of trust is to be considered as an important aspect to be covered by the **common certificate policy** that needs to be defined for C-ITS day one deployment in Europe (in accordance to the trust model recommendations of WG5).

(2) As a part of the definition of the common certificate policy the E-SCMS (European C-ITS Security Credential Management System) support for revocation shall be defined

based on the selection of countermeasures presented in this report, reflecting the stakeholder's positions appropriately.

(3) A time-plan on when the setup of the revocation countermeasures have to be finalised by all stakeholders for interoperable C-ITS Day 1 deployment should be defined at least 6 months prior to the start of operation of the E-SCMS (an envisaged goal for the start of operation of the E-SCMS would be in 2018).

(4) Further work needs to be done in the following area:
A common set of selected countermeasures related to the stakeholder's positions in this report needs to be defined for the E-SCMS operation.

- Definition of the formats, size and delivery mechanisms of the CRL (Certificate Revocation List) are urgently needed, e.g. through standardization of the design of CRL.
- Organization framework for the misbehaviour detection and subsequent revocation of trust is needed. In addition research into advanced misbehaviour detection is needed.
- Legal implications of revocation of trust need to be further analysed for operation.
- Analysis of responsibilities in the multi-application/domain setting on C-ITS stations.

7.4.2.3 Crypto Agility / Updateability in C-ITS

The analysis conducted in the Crypto Agility/Updateability (WG5 - ANNEX 3) identified the following recommendations:

(1) The responsible policy body for the definition of the security policy shall be in charge of defining updates of the security policy due to expiry/deprecation of crypto algorithms, and a migration plan that shall be observed by the C-ITS Station system manager.

(2) It is recommended to investigate and potentially amend the existing protocol defined in ETSI to allow, in a backwards compatible manner, a second signature, which uses a new algorithm and which can co-exist with the old signature during a certain period. The design of the protocol should take in consideration the analysis provided in section 6 of WG5 - ANNEX 3.

(3) C-ITS Station system managers shall estimate the risks related to certificate policy (e.g., new cryptographic algorithms) and software updates and have an appropriate risk treatment plan.

(4) Security recommendations on cryptographic algorithms for C-ITS can only be valid for a limited time and have to be reassessed on a regular basis.

(5) It is important to define a framework to reach quickly a consensus on the choice of new algorithms in case of a security breach. In other words, an organization and process should be put in place to reach quick solutions to security breaches in the cryptographic algorithms.

7.4.2.4 Compliance Assessment in C-ITS

The analysis conducted in the compliance assessment (WG5 - ANNEX 4) identified the following recommendations:

(1) to pursue a compliance assessment process for C-ITS as proposed and described in WG5 - ANNEX 4 for Day 1 deployment of C-ITS. During implementation of this process, at least the identified risks and challenges of the report 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 described in WG5 - ANNEX 4 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.

7.5. Annexes

WG5 - ANNEX 1 - Trust_Models_for_C-ITS_v1_1.pdf

WG5 - ANNEX 2 - Revocation_of_Trust_in_C-ITS_v1_1.pdf

WG5 - ANNEX 3 - Crypto_Agility_Updateability_in_C-ITS_v_1_1.pdf

WG5 - ANNEX 4 - Compliance_Assessment_in_C-ITS_v1_0.pdf

8. Working Group 6 - Technical Issues - Access to in-vehicle data and resources

8.1. Objective of the working group

8.1.1 Context

The increasing connectivity and digitisation of vehicles is currently changing the automotive industry landscape. Specific data that were previously accessed via a physical connection in the vehicle are now more and more accessible remotely. Independently of the model/solution retained to give access to in-vehicle data and resources, the main objective should be to allow customers the freedom to choose which service they desire, meeting their specific needs, in order to ensure open choice for customers. This goes through an open and undistorted competition for the provision of these services.

Recent changes in the legislation

This has been recognised in April 2015 by the legislators in Regulation (EU) 758/2015[7] of the European Parliament and of the Council concerning type-approval requirements for the deployment of the eCall in-vehicle system and amending Directive 2007/46/EC. This Regulation includes provisions regarding an interoperable, standardised, secure and open-access platform:

Recital (16): "In order to ensure open choice for customers and fair competition, as well as encourage innovation and boost the competitiveness of the Union's information technology industry on the global market, the eCall in-vehicle systems should be based on an interoperable, standardised, secure and open-access platform for possible future in-vehicle applications or services. As this requires technical and legal back-up, the Commission should assess without delay, on the basis of consultations with all stakeholders involved, including vehicle manufacturers and independent operators, all options for promoting and ensuring such an open-access platform and, if appropriate, put forward a legislative initiative to that effect."

Article 12(2): "Following a broad consultation with all relevant stakeholders and a study assessing the costs and benefits, the Commission shall assess the need of requirements for an interoperable, standardised, secure and open-access platform. If appropriate, and no later than 9 June 2017, the Commission shall adopt a legislative initiative based on those requirements."

The open in-vehicle platform is also part of priority area IV of the ITS Directive (2010/40/EU)[8], which calls on the Commission to adopt specifications and standards for linking vehicles with the transport infrastructure.

The relevance of the topic had already been highlighted by the European Commission back in 2008 in the framework of the ITS Action plan[9]. Action 4.1 aimed at the "Adoption of an

[7] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2015.123.01.0077.01.ENG

[8] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32010L0040

open in-vehicle platform architecture for the provision of ITS services and applications, including standard interfaces. The outcome of this activity would then be submitted to the relevant standardisation bodies".

Additionally, the Digital Single Market Strategy[10] provides a wider strategic framework for the digital economy including the connected car, and focusses on providing better access for consumers and businesses to online goods and services across Europe; creating the right conditions and a level playing field for digital networks and innovative services to flourish; and maximising the growth potential of the digital economy to boost industrial competiveness in particular through interoperability and standardisation.

Other relevant existing legislations

Several existing legislations, without mandating the concept of open platform, mandate nevertheless access to some in-vehicle data and resources:

eCall type-approval Regulation: in case of a serious accident, limited information (the Minimum Set of Data – aka MSD) has to be sent by the vehicle via the European Universal Emergency Number 112 to the emergency call centres.

Euro 5 Regulation and Diagnostic, and Repair & Maintenance Information: several EU Regulations[11] address the information to be provided for the complete vehicle to the independent aftermarket in a non-discriminatory and standardised way. Moreover, the 16 pin standardised connector is enshrined in this Regulation, although covering only emissions in a formal sense, it is used in practice to support diagnostics and to access to some in-vehicle data/information, other than emission data, for franchised and independent operators (current analogue "live data" port).

Current practices and initiatives for the access to in-vehicle data and resources

FMS standard (trucks and buses): optional and voluntary firewalled interface to the CAN (Controller Area Network) bus of major European truck and bus manufacturers. The Fleet Management Systems Interface (FMS) is an open standard for accessing electronic data from the internal CAN network of the vehicle. It is the sole existing interface for a safe data connection of 3rd party devices to the CAN-bus of a commercial vehicle. A remote FMS (rFMS) specification exists, it is part of the *extended vehicle* concept developed by vehicle manufacturers (see infra). It is currently restricted to a limited data set with a 15 minutes updating frequency.

OBD connector: On-board Diagnostic (OBD) data exchange since 1970s. 40 years established Open real-time In-Vehicle Data availability for the automotive aftermarket community. Now OBD II standard (1990s). The OBD II standard includes parameter, protocol and hardware interface descriptions. The 16 PIN On-board diagnostics connector is the current “live data” port, providing access to in-vehicle data and enables professional repairers to check the

---

[9] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52008DC0886

[10] COM(2015)0192

[11] Regulations (EC) No 715/2007, 692/2008, 595/2009

'health status' for diagnostic purposes. Safety and liability issues are related to the use of this interface: although this connector was originally mandated for the control of emissions and allowed monitoring of emissions data whilst driving, currently retro-fit devices for wireless transmission of in-vehicle data (plugged into the OBD port) are commercialised to access the vehicle data, which causes potential severe security issues which will certainly need to be solved in the future.

Some vehicles now being brought to the market, have limited OBD connector functionality (limited solely to emissions), providing no access to other in-vehicle data and resources; instead, access is via the internet (proprietary OEM server).

Extended vehicle concept - new standardisation project ISO 20077-20078-20080: new standardisation project, started in 2014, to be finalised in 2017 or 2018, including interfaces and a data server platform provided by vehicle manufacturers, to ensure privacy and data protection, cybersecurity, road safety and regulatory compliance, starting with diagnostic data. According to the description of the proposal, vehicle manufacturers would provide a "non-discriminating access" to independent operators against "fair cost compensation". The extended vehicle concept is meant to provide access to existing vehicle manufacturers' servers (see infra).

Vehicle manufacturers servers: most OEMs have currently developed their own data server platforms (in some cases managed by their IT partners), for internal quality and periodic maintenance or other services purposes, without generalised access for other service providers. Some OEM specific interfaces exist on the OEM servers.

C-ITS: the standardised messages (CAM, DENM) used in V2V and V2I communication include vehicle data for Cooperative ITS use cases based on broadcast between authenticated devices. The CAR 2 CAR Communication Consortium announced on 2 November 2015 that initial deployment of cooperative vehicles with ITS-G5 could begin as soon as 2019.

eCall (as from 1st April 2018 for new models of personal cars and light duty vehicles)**:** in case of a serious accident, a minimum set of data (MSD) is sent by the vehicle via the European Universal Emergency Number 112 to the public safety answering points (PSAPs). The content of the MSD is defined in the standard EN 15722. The eCall unit is not registered in the mobile networks (to avoid tracking) until the eCall is activated, automatically or manually. It remains registered for some time to enable call back from the emergency call centre and then goes back to "dormant mode" and cannot be reached from the network side. In addition to the mandatory feature, the car owner can have the option to purchase an active subscription from a mobile network operator and establish a contract with some service providers. eCall introduces an in-vehicle system that provides an advanced vehicle telematics function which may share the same basic hardware and software components that can also be used for other telematics system functions.

ICT platforms (e.g. Google/Apple/Baidu/TomTom/Here etc.): Data transfer to ICT platform and special App-Providers (including vehicle manufacturers). ICT platforms are in the in-vehicle infotainment system of vehicle and usually not related to safety functions of the vehicle. Data transfer to backend server will be via a connected smartphone. Availability is the sole responsibility of the user. Smartphone is connected with cable or wirelessly to the car. In vehicle interface is providing OEM specific data to ICT platforms for OEM specific Apps

on the ICT platforms/smartphones. Another new feature of some ICT platforms is intended for the vehicle manufacturer. These can be programmed with their own applications for the system in order to control, for example, various functions of the car. This implies a significantly deeper integration of the ICT platforms with the vehicle systems.

8.1.2 General objective of the working group

In order to engage with stakeholders on this topic, it has been decided to dedicate a working group within the C-ITS platform, to discuss the possible ways to access to in-vehicle data and resources. This working group has been identified as part of the working groups on "technical issues".

This working group involved the main stakeholders interested in the topic: automotive industry, Tier 1 suppliers, different sectors of service providers (repair and maintenance, insurance, associations of users etc.), road infrastructure managers etc. Several DGs of the Commission (MOVE, GROW and CNECT) participated in the discussions and DG COMP was regularly informed about the discussions.

The general objective is to identify the issues at stake and reach when possible a shared vision and common solutions on fair access to in-vehicle data and resources.

8.2. Organisation of the work and definition of a general framework

From November 2014 to December 2015, eleven meetings of the working group took place, with more than twenty participants in each meeting. Additional meeting with volunteers of the working group took place within task forces (see below) and a specific meeting on standardisation needs took place in June 2015.

After two first meetings in November and December 2014 which allowed first discussions on the objectives of the working group, a scoping paper (WG6 - A2D - ANNEX 1) was presented by the Chair to the working group.

This scoping paper allowed in particular for:

- the **approval** by the working group **of five guiding principles**,

- the identification of three possible solutions to be further investigated,

- the setting up of four Task Forces to provide, in a limited timeframe, input material for the working group's discussions.

The five guiding principles that should apply when granting access to in-vehicle data and resources are the following:

> **(a) Data provision conditions: Consent**
>
> The data subject (owner of the vehicle and/or through the use of the vehicle or nomadic devices) decides if data can be provided and to whom, including the concrete purpose for the use of the data (and hence for the identified service). There is always an opt-out option for end customers and data subjects. This is without prejudice to requirements of regulatory applications.

(b) Fair and undistorted competition

Subject to prior consent of the data subject, all service providers should be in an equal, fair, reasonable and non-discriminatory position to offer services to the data subject.

(c) Data privacy and data protection

There is a need for the data subject to have its vehicle and movement data protected for privacy reasons, and in the case of companies, for competition and/or security reasons.

(d) Tamper-proof access and liability

Services making use of in-vehicle data and resources should not endanger the proper safe and secure functioning of the vehicles. In addition, the access to vehicle data and resources shall not impact the liability of vehicle manufacturers regarding the use of the vehicle.

(e) Data economy

With the caveat that data protection provisions or specific technologic prescriptions are respected, standardised access favours interoperability between different applications, notably regulatory key applications, and facilitates the common use of same vehicle data and resources.

The three technical solutions that have been identified for this access to in-vehicle data and resources are the following:

- Two inside the vehicle:

  - **the On-board application platform** (allowing the unified deployment of certified applications and their subsequent execution directly in the vehicle, including access to the in-vehicle resources to host applications and to display these applications on the vehicle's HMI to allow the customer to select and implement them)
  - the **In-vehicle interface** (allowing the connection to the vehicle of external devices)

  Both solutions support real-time applications.

- One outside the vehicle:

  - the **Data server platform,** an external data server where relevant vehicle data are transferred to and made available to service providers. Contrary to the two inside the vehicle solution, it does not allow for all real-time applications.

A description of these three technical solutions can be found in §4 of WG6 - A2D - ANNEX 1.

The working group recognised that these three solutions would most probably have different time scales, but agreed to work in parallel on the analysis of the three possible technical solutions, and also on the possible definition of a reference dataset, which could

correspond to most of the expectable data needs foreseen by interested stakeholders. The objective being that all service providers, including vehicle manufacturers for their own service activities, would access on an equal footing to the same reference dataset.

The four Tasks forces set up to develop the following items are:

- On-board application platform (TF1)

- In-vehicle interface (TF2)

- Data server platform (TF3)

- Definition of a reference dataset (TF4)

These task forces were set up to provide, in a limited timeframe, input material for the Working Group's discussions.

The roadmap for Task Forces 1 to 3, always to be in line with the general principles, can be summarised as follows:

- Building blocks of the solution (e.g. security, physical mounting and powering if applicable, organisational issues etc.)

- Impact of the type of access (only access to data, access to data + other resources e.g. HMI or communication channels) on these building blocks

- Elements of the solution already available

- Gaps to be fulfilled (e.g. standardisation)

- Timeline to make the solution feasible

No decisions/conclusions were made within those task forces and once the input material was provided, the work resumed at working group level.

The work of the working group has then been structured accordingly, focussing on the following elements:

- Define the principles for the management of access to a data server platform (TF3)

- Further elaborate the specifications for the in-vehicle interface (TF2)

- Define a roadmap for the on-board application platform (TF1)

- Define a reference dataset that would serve all solutions (TF4)

8.3. Outcome, Conclusions and recommendations

The purpose of this part of the report is to describe the outcome, conclusions and recommendations of the working group regarding the four above-mentioned elements, as well as regarding horizontal elements such as: standardisation needs, positions of stakeholders regarding the concrete organisation of the access to data, positions of the stakeholders regarding concrete implementation.

As approved at an early stage by the working group, the following recommendation underpins all other subsequent recommendations:

Recommendation

- **Guiding principles:** the access to in-vehicle data and resources shall comply with the above-listed five guiding principles.

8.3.1 Data server platform

This solution was initially considered by the working group as the solution which technically "would come first", i.e. would be the easiest to implement in short term, as it does not imply substantial modification of the current vehicle networks/security layers. However, the way this solution would be implemented in order to support the five guiding principles was understood differently by the participants in the working group.

Likewise, there was a general agreement on the fact that, due to the current security status of most vehicles, for liability reasons and protection of data, the transmission of data between the vehicles and the data server platform should remain under the control of vehicle manufacturers at least for as long as these security issues persist. This security status was identified by the working group as a current issue which would need to be enhanced and future requirements to be defined in a reasonable timescale, also in relation to the in-vehicle interface and on-board application platform.

There was a general agreement on a possible technical architecture for the Data server platform but an open discussion on how to ensure fair, reasonable and non-discriminatory access, one of the main issues being the governance of the external server on which vehicle data would be stored and made available to service providers.

While the vehicle manufacturers advocated in favour of the Extended Vehicle solution (see infra), other participants understood the data server platform, managed and controlled by a neutral third-party, as only an intermediate step, the final (and best) solution being the on-board application platform. The fact that this kind of solution based on mobile communication would not support all real-time needs and therefore would not support all applications was also highlighted by several members of the working group.

The vehicle manufacturers represented in the working group supported the Extended Vehicle concept, currently being standardised at ISO level (ISO 20077-20078 – to be finalised in 2017-2018) with a first focus on information for remote diagnostic support (ISO 20080) and proposed the following description of the Extended Vehicle:

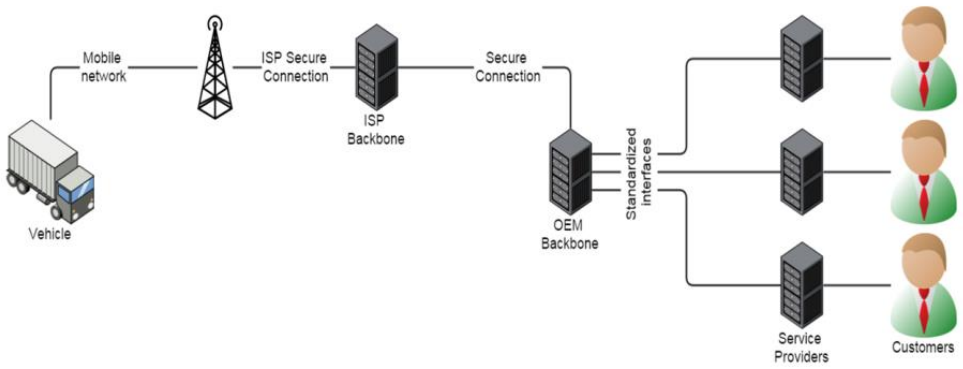
An extended vehicle is understood as a physical road vehicle with external software and hardware extensions for some of its features. These extensions are developed, implemented and managed by the vehicle manufacturer. The vehicle manufacturer is fully responsible for the communication among the various parts of the extended vehicle, especially between the internal and external software and hardware components.

The extended vehicle offers open access interfaces for the provision of services by vehicle manufacturers or third parties. The interfaces need to be designed and implemented in such a way that access to the extended vehicle does not jeopardize security, safety, product

integrity, data privacy or any other rights or legal obligations. Depending on the purpose for which access is sought, the extended vehicle can be accessed through various interfaces, one of which is a web interface (see ACEA concept paper on Extended vehicle in WG6 - A2D - ANNEX 14).

To simplify, this report will use the words "Extended vehicle" for the vehicle manufacturers' proposed service platform architecture described hereafter.

The Extended Vehicle is compatible and coherent with the service platform architecture described in WG6 - A2D - ANNEX 2:



With the data server of the Extended Vehicle, the data are transferred via the mobile telecom networks from the vehicle to the vehicle manufacturer's server (OEM backbone), and then made accessible to service providers via a standardised interface. Data types are linked to use cases, each use case can be a specific standardisation item. Independent operators and service providers pointed out that this does not sufficiently address the access conditions (time criticality, B2B contracts etc.).

An extensive discussion took place on the Extended Vehicle concept, the central issue being the control of the access conditions and extent of the in-vehicle data by the vehicle manufacturers via their external servers. A specific document illustrates this discussion with detailed answers from ACEA to the independent aftermarket sector's questions (WG6 - A2D - ANNEX 3). It has to be noted that representatives from other sectors than aftermarket (e.g. insurance sector, associations of users) expressed similar concerns relating to what they deemed as a non-compliance of the Extended Vehicle with some of the guiding principles, in particular principle (b) on competition.

The discussion allowed identification of the following main issues linked to the Extended Vehicle for the independent operators and service providers (others than vehicle manufacturers):

(for detailed Q&A please consult WG6 - A2D - ANNEX 3)

- monitoring of their activities by the vehicle manufacturers, who are their competitors, independent operators' customers will have to be registered with the vehicle manufacturer.

- risk of unfair competition (better/more data available or sooner available to their competitors, independent stakeholders' business become dependent on the business

model of their competitors in the secondary market). As the vehicle manufacturers are competitors with other service providers, in areas such as diagnostics, repair and maintenance, part sales, road side service, insurance and leasing, this creates a direct conflict of interest when vehicle manufacturers control in-vehicle data via their proprietary servers.

- limited data available (the ISO standardisation of each use case would be very slow and the Extended Vehicle concept is designed to release only a restricted set of data which is considered insufficient for many digital services), which restricts innovation, alternative competitive services and new business models.

- data available are linked to use cases, which limits innovation.

- the vehicle manufacturers' proposal to allow an independent audit (see infra) to ensure fair competition is challenged by the independent stakeholders on the grounds of technical feasibility.

The vehicle manufacturers addressed these main issues with the following answers:

- vehicle manufacturers assured that no monitoring of the service providers requesting access to the data would take place,

- they proposed to establish internal procedures to this effect and to consider subjecting it to an independent audit, in particular to ensure fair competition conditions,

- they proposed to apply the same conditions as described in their answers to the aftermarket sector to additional use cases and service providers from other sectors.

To conclude on the Extended Vehicle, the extensive discussions allowed a clear understanding of the solution, and the identification of the main issues which could not be solved by the working group. These issues are clearly not only technical issues stemming from the architecture of the Extended Vehicle, but also concerns linked to the lack of trust between competitors proposing similar services and alternative business models.

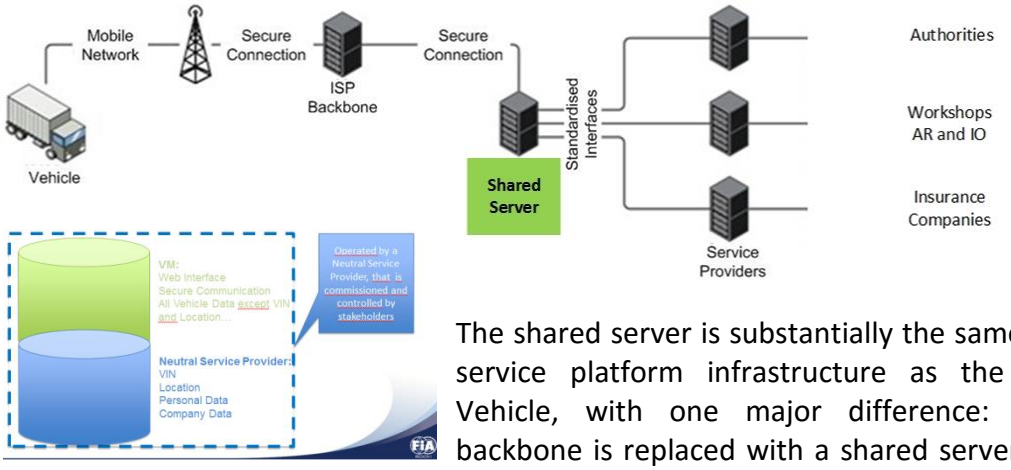
In order to try to resolve this impasse, two other data server platform solutions were proposed by some members of the working group in order to (try to) solve the above-mentioned issues:

- a shared server proposed by FIA, supported by FIGIEFA, CLEPA, Insurance Europe

- a B2B marketplace proposed by IBM

The shared server (see detailed presentation in WG6 - A2D - ANNEX 4)

Independent operators and service providers proposed another implementation of the data server platform, managed and controlled by a neutral third-party. They present it as only an intermediate step, the final (and best) solution being the on-board application platform.



The shared server is substantially the same technical service platform infrastructure as the Extended Vehicle, with one major difference: the OEM backbone is replaced with a shared server operated by a neutral service provider commissioned and controlled by a consortium representing interested stakeholders. This shared server would control at least personal and business data, other data remaining under the control of vehicle manufacturers.

Vehicle manufacturers questioned the workability of such a solution. They underlined the organisational difficulties to set up such a consortium of stakeholders, to reach agreement on all details regarding the establishment, maintenance, operation and management of the shared server, the selection of the server operator and any modifications that would need to be made over time. FIA distributed a document describing the shared server and providing answers to vehicle manufacturers' questions (see WG6 - A2D - ANNEX 17).

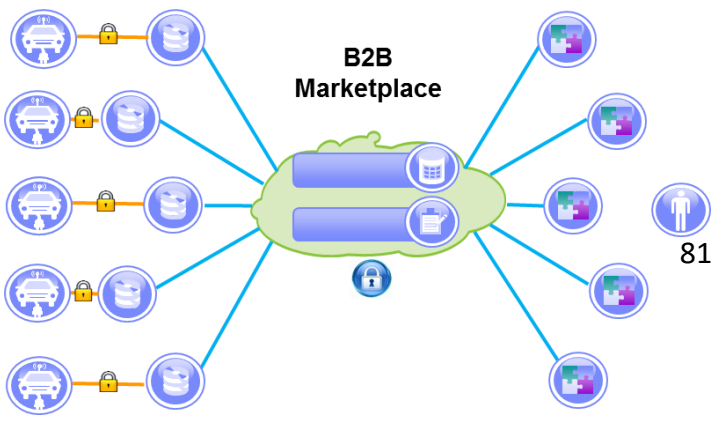
In addition, vehicle manufacturers claimed that due to liability reasons IDs linking the two databases could not be completely anonymised and complete encryption (without possibility for vehicle manufacturers to decrypt) would not be possible because it would lead to liability and type-approval issues. Therefore the shared server would not solve the service providers' issues (i.a. the non-monitoring).

Security issues were also mentioned by the vehicle manufacturers, to which FIA replied that same security measures than in the Extended Vehicle solution could be applied to a shared server.

From the discussion to date, it appears that consensus will probably not be reached among the working group on this solution.

The B2B marketplace (see detailed presentation in WG6 - A2D - ANNEX 5)

The B2B Marketplace is the central platform for all C-ITS stakeholders. The Core Services include Partner-, Contract- and Service-Management functionalities.



The B2B marketplace features a kind of additional layer between the vehicle and the service providers, which would be fed by vehicle manufacturers' back end servers. An association consisting of all C-ITS stakeholders is also required to control the marketplace, and one of the objectives is notably to solve the monitoring issue thanks to end-to-end encryption.

Vehicle manufacturers underlined that the proposed solution was a commercial platform, based on an open market ("not only IBM") to provide this kind of platform, and that it should still be possible to access data directly through the Extended Vehicle solution. In addition, they reminded that decryption between the vehicle and the vehicle manufacturer backend server should be open to vehicle manufacturers for liability reasons.

Same need for access to decrypted data was deemed necessary for liability reasons for all actors along the service delivery.

Independent operators and service providers explained that this proposal could be interesting only if end-to-end encryption would be ensured.

Talks within the working group are not yet completely exhausted, but first discussions seem to show that the added value of the B2B marketplace, in terms of solving the issues linked to the Extended Vehicle, seem to be rather limited.

Recommendations for the data server platform

- **Improve cooperation:** as demonstrated by the above-mentioned main issues, it seems that although this working group is placed among the "technical issues", most of the sticking points are not only technical issues, but also concerns linked to the lack of trust between direct competitors. Ways to improve cooperation should be explored to make some progress, in line with the overall objectives of the Digital Single Market Strategy.

- **Need for an analysis on legal, liability, technical and cost-benefits aspects:** in order to further progress and also to help in fulfilling the legislators request (cf Article 12(2) of the eCall type-approval Regulation), and on the basis of the five guiding principles, the different proposals for the data server platform put forward by the members of the working group should be included in a scenario-based analysis on legal, liability, technical and cost-benefits aspects of the different possible approaches.

8.3.2 In-vehicle interface

An initial and challenging dialogue took first place within Task Force 2, with very different views emerging on the necessary work to get the interface and on the timeline needed, followed by a similar dialogue within the working group. There was strong disagreement as to whether a complete renewal of the in-vehicle system would be a prerequisite to the availability of an in-vehicle interface.

In order to progress and to provide for coherence with other elements of the work of the working group, in particular the general timeline developed by Task Force 1, the Chair asked to develop a more progressive approach (in WG6 - A2D - ANNEX 6, accompanied by a security strategy in WG6 - A2D - ANNEX 7) which was rather quickly approved by the working group in July 2015 as a technical contribution, without commitment in terms of deployment.

A progressive approach

The main elements of this approach were the following:

- A constant vehicle data stream should be made available from the in-vehicle network with the consent of the data subject on an in-vehicle physical interface (plug). On this plug an external connectivity control unit (CCU) can be plugged in with a standardised connector and collect and process the data stream. The CCU can connect to external receivers (Road Side Unit, backend-server, ...) by different ways of communication (4G, 5G, Wi-Fi, ...).

- An upgraded OBD interface including gatekeeper and central gateway to the in-vehicle network. The market implementation is estimated to 5 years after the availability of the necessary standards.

- For these elements to happen concretely, a Commission mandate for the standardisation of connector, protocols and formats and a proposed legislation with a time line for implementation is deemed necessary.

Compliance of this approach with the guiding principles is checked in WG6 - A2D - ANNEX 6.

Vehicle manufacturers expressed nevertheless strong reservations regarding the above described in-vehicle interface as well as regarding the on-board application platform (infra), mainly for security reasons.

They argued that it is not sufficient to apply general security design rules to the CCU to guarantee the security of the whole system. The CCU, when connected, becomes part of the vehicle EE architecture. Therefore, vehicle manufacturers consider that the CCU protection must be compatible with and complementary to the security features of other embedded systems. In their view, the potential security weakness depends on each single architecture design and needs to be addressed at the level of the whole system. Similarly, they argued that cyber-attack countermeasures may affect the performance of the whole system. For vehicle manufacturers, all this implies that security issues cannot be addressed in one additional ECU but must involve the whole embedded system.

Recommendations for the in-vehicle interface

• **Standardisation needs**: Identify more precisely the standardisation needs (see infra paragraph on standardisation needs) and start standardisation work at appropriate level(s), including also possible retrofit solutions.
• **Need for an analysis on legal, liability, technical and cost-benefits aspects**: in order to further progress and also to help in fulfilling the legislators request (cf Article 12(2) of the eCall type-approval Regulation), and on the basis of the five guiding principles, the solution proposed for the in-vehicle interface should be included in a scenario-based analysis on legal, liability, technical and cost-benefits aspects of the different possible approaches.

8.3.3 On-board application platform

Two approaches, sequential and parallel, were supported by different members of the working group.

The sequential approach

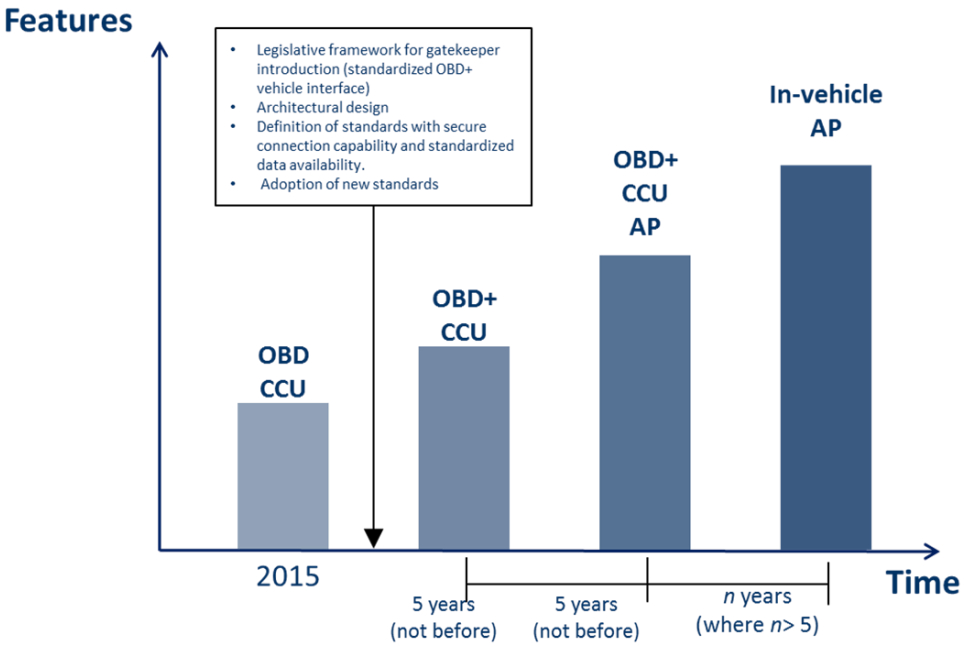
Task Force 1, including ACEA, FCA and CLEPA (with reservations from CLEPA on the announced timeline), prepared a roadmap (WG6 - A2D - ANNEX 8) which was presented as a four-steps evolution, starting from a server based solution, towards the end goal, the embedded on-board application platform:

1. A cloud- or server-based solution for access/sharing of data and OBD connected communication units (OBD CCU) – 201x;

2. An upgraded OBD interface including gatekeeper and central gateway to in-vehicle network (OBD+ CCU) – 5 years after gatekeeper and central gateway standard availability;

3. An OBD+ connected CCU featuring an open application layer (OBD+ CCU OP) - 5 years after OBD+ CCU availability;

4. An embedded on-board application platform (in-vehicle AP) – not yet determinable.



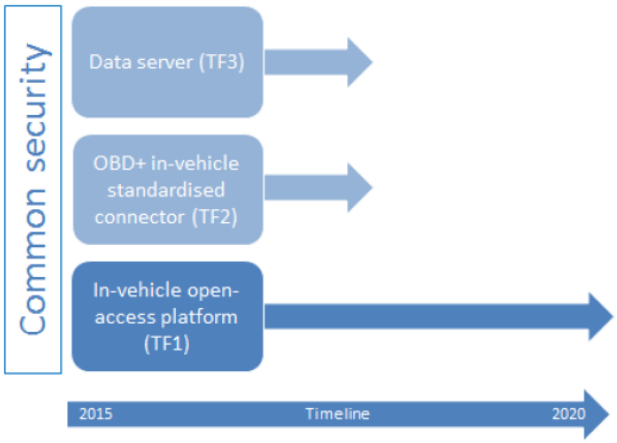
The figure above summarises this evolutionary approach, which underlines (see the box in the figure) the necessity to have a legislative framework for gatekeeper introduction (OBD+ vehicle interface), and the definition of necessary standards for the OBD+ interface, secure connection capability and standardised data availability, to see this evolution happen concretely.

This means that the members of the task force stressed that legislation and standardisation would be needed to see this evolution take place. This does not mean that all of them requested legislation, the nuance is of importance. Independent operators and service providers were in favour of legislation mandating gatekeeper introduction while vehicle manufacturers were not.

Each step of this evolutionary approach is presented as dependent from the previous step, because a deep evaluation activity on the field is deemed indispensable by the members of Task Force 1 to guarantee the safety of the vehicle whenever a global application platform is installed and to understand if the adopted technology will not interfere for its functionality with vehicle resources.

The parallel approach

Primarily because of its very long timeline, this sequential approach was challenged by several members of the working group. Independent operators and service providers argued that the sequential approach did not reflect what was currently technically feasible (in particular what is already being used by some vehicle manufacturers for their proprietary in-vehicle telematics platform and their cooperation with their chosen service providers) and advocated in favour of parallel development of the different solutions. They recognised that there are currently security requirements that should be considered to implement the solutions inside the vehicle (in-vehicle interface and on-board application platform), but claimed that standardisation work and legislation should start as soon as possible and that the work on all three solutions should take place simultaneously.



This parallel approach was detailed in an alternative proposal submitted by AFCAR (WG6 - A2D - ANNEX 9) in June 2015. The architecture of the in-vehicle open-access platform proposed in this parallel approach is described in WG6 - A2D - ANNEX 16 submitted in December 2015 and should be further discussed.

Independent operators and service providers pointed out that the technical feasibility of the proposal has in their opinion already been demonstrated when the OEMs incorporated Apple CarPlay and Google Android Auto into existing vehicles.

Divergences between these two approaches could not be overcome, ACEA explaining in particular that this parallel approach was against its members' position.

Some members of the group underlined that proprietary solutions could be developed quicker, could provide the necessary quality and that competition between proprietary systems could help in developing the market.

Recommendation for the on-board application platform

• **Standardisation needs**: Identify more precisely the standardisation needs (see infra paragraph on standardisation needs) and start standardisation work at appropriate level(s).
• **Need for an analysis on legal, liability, technical and cost-benefits aspects**: in order to further progress and also to help in fulfilling the legislators request (cf Article 12(2) of the eCall type-approval Regulation), and on the basis of the five guiding principles, the different approaches towards the on-board application platform put forward by the members of the working group should be included in a scenario-based analysis on legal, liability, technical, cost-benefits and future proofing aspects of the different possible approaches.
• **Follow-up:** make use of previous research projects (e.g. CONVERGE, OVERSEE etc.)

8.3.4 Reference dataset

A general document on data needs and requirements was approved by the working group in July 2015 (see WG6 - A2D - ANNEX 10), with the following comments:

- data quality requirements may vary depending on the type of access.

- existing standards shall be taken into account.

- necessity to find a balance between what can be done inside the vehicle and what can be done outside the vehicle.

This document highlighted the need to define a short reference set of data which would be common to all vehicles and brands, that could support a large number of applications, and which would be necessary and useful to standardise.

In order to be able to progress in that direction, and on the basis of a comprehensive list of use cases established through contributions of many members of the working group, volunteers within the working group representing in particular the independent operators and service providers, with very limited participation of vehicle manufacturers, identified whether the related data would exist (and possibly already be/ing standardised), partially exist, or would not yet exist in the vehicles, independently from brand or model. They also classified these use cases in three categories:

- existing or short term (2-3 years), i.e. the use cases which could/should come first (regulated use cases, C-ITS list of Day 1 applications (as identified by the C-ITS platform), use cases already on the market or near to the market etc.),

- mid-term (4-7 years)

- longer term

The outcome of this work, i.e. a comprehensive list of use cases and related data, is listed in a table in WG6 - A2D - ANNEX 11. This result would need to be further fine-tuned, in particular for quality requirements, in possible standardisation work.

The final objective of this work was understood differently by the participants.

Independent operators and service providers seeing it as a necessary step allowing the identification of a short reference set of data.

A strong disagreement remained on the conditions for service providers to access to data (see paragraph below on "Positions of stakeholders regarding the organisation of the access to data" and WG6 - A2D - ANNEX 15 for ACEA position).

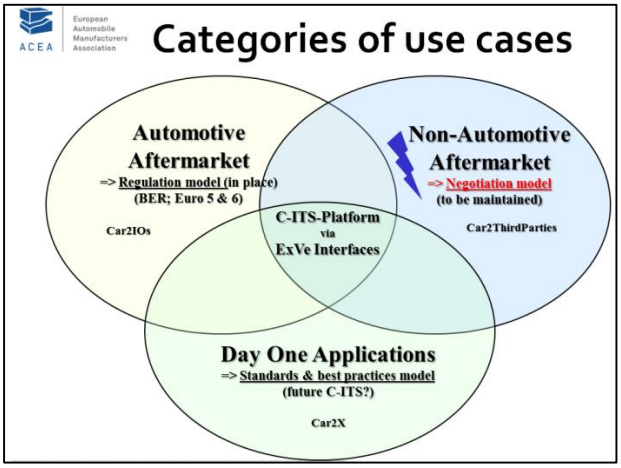
Vehicle manufacturers requested to define the data needs of third parties only on the basis of specific use cases, i.e. when it is clear which data is requested for which purpose by which party. When it comes to these use cases that are (being) harmonised (C-ITS day one applications, eCall, RMI, remote diagnostic support, fleet management systems for heavy duty vehicles), they suggested to use the data, processes and/or transmission channels as they are standardised in each case. Where a harmonisation or standardisation process is ongoing, they suggested letting that process run its course and use its results. With respect to other use cases, they argued that harmonisation was not really necessary to ensure that third parties are able to access and use the data they require in a specific use case since, as part of the ongoing standardisation of the “extended vehicle” within ISO, work is being done to develop a standardised language that would enable third parties to request and receive vehicle data for specific use cases regardless of their implementation in a human- and machine-readable format (see WG6 - A2D - ANNEX 15).

In addition, ACEA transmitted to the working group on 5 November 2015 a presentation (WG6 - A2D - ANNEX 12) summarising its position as to the definition of the list of data on the basis of different categories of use cases. In this position, use cases are to be classified in three categories:

- Day 1 applications

- Automotive aftermarket, including in particular regulated use cases.

- Non-automotive aftermarket, to which a negotiation model for the access to data is to be applied.



This recent position of ACEA **has not yet been discussed by the working group**.

8.3.5 Standardisation needs

New standardisation needs were notably identified during the work on the in-vehicle interface and on the on-board application platform, as an essential building block for these solutions to develop.

Therefore, the working group agreed in July 2015 on the following input for the 2015 Rolling Plan for ICT Standardisation:

"To develop the missing standards for an advanced physical/electrical/logical interface (e.g., evolution of OBD2) –which includes the necessary minimum level of security (i.e., integrity, authentication and availability) -, including minimum data sets and standardised data protocols enabling ITS services"

8.3.6 Positions of stakeholders regarding the organisation of the access to data

A parallel discussion to the discussions on technical solutions and data needs took place regarding the data access conditions, with the following **strong disagreement**:

- vehicle manufacturers expressed their preference for an access depending on use cases, with a pre-defined list of data linked to each use case. Legal reasons were notably presented, in particular the fact that the access to personal data should be proportionate to the accurately defined needs.

- independent operators and service providers explained that purely a use case based release of data would seriously restrict services and innovation. The data subject would give consent to applications, which would be based on a list of data described in the terms and conditions of each application. At least within the short reference set of data, each data type could then be combined with other data types, and not be part of a pre-fixed list linked to a specific use case. This would moreover allow for the flexibility needed as regards innovation of new use cases.

Recommendation for the organisation of the access to data

- **Need for a legal analysis of the data access conditions**: on the basis of the five guiding principles, the different approaches put forward by the members of the working group should be analysed further, in particular their impact on competition, privacy, data protection (privacy and consent) and liability of the different actors involved.

8.3.7 Positions of stakeholders regarding concrete implementation

The independent operators and service providers were in favour of additional legislation mandating the introduction of both the standardised in-vehicle interface and the on-board application platform.

Regarding the data server platform, several members of the working group (in particular FIA, FIGIEFA, CLEPA, Insurance Europe) called in particular for an additional article in the RMI legislation on a technically independent and secure access to in-vehicle data that would ensure a level playing field also in the telematics market.

8.4. Conclusion

Discussions within the working group have been rich and lively, with strong involvement of main stakeholders, investigating the technical requirements for the access to in-vehicle data and resources, in order also to address the eCall Regulation requirements regarding the interoperable, standardised, secure and open-access platform for possible future in-vehicle applications or services.

They allowed progress in terms of identification of standardisation needs, an agreement on a technical solution for the in-vehicle interface, progress in the identification of possible use cases, and the identification of the remaining sticking points.

As stated several times during the working group meetings, all issues could not be solved because these issues were not only technical, but were related to different and sometimes competing concepts or opposite strategies: different views on how data can be accessed, different strategies towards on-board application platform and data server platform, different views regarding concrete implementation and possible legislation.

In order to further progress and also to help answering legislators request (cf Article 12(2) of the eCall type-approval Regulation), and on the basis of the five guiding principles, all elements approved or identified within the working group should contribute to and benefit from a scenario-based analysis on legal, liability, technical and cost-benefits aspects.

This report of Working Group 6 Access to in-vehicle resources and data of the C-ITS platform has been endorsed by nominated experts, representing the organisations and countries listed in WG6 - A2D - ANNEX 13.

8.5. Annexes

Annexes to this working group report, unless specified in the report, reflect the views of specific working group members.

WG6 - A2D - ANNEX 1 - Scoping paper.docx

WG6 - A2D - ANNEX 2 - Extended Vehicle.docx

WG6 - A2D - ANNEX 3 - Q&A VM controlled backend server.docx

WG6 - A2D - ANNEX 4 - Shared server.pptx

WG6 - A2D - ANNEX 5 - B2B Marketplace.pptx

WG6 - A2D - ANNEX 6 - In-vehicle interface.docx

WG6 - A2D - ANNEX 7 - In-vehicle interface_Security_Requirements_CCU.pdf

WG6 - A2D - ANNEX 8 - Proposal TF1 on-board application platform.docx

WG6 - A2D - ANNEX 9 - Alternative proposal AFCAR on-board application platform.pdf

WG6 - A2D - ANNEX 10 - Data needs.docx

WG6 - A2D - ANNEX 11 - Use Cases - Data to be harmonised 23Nov 2015.xlsx

WG6 - A2D - ANNEX 12 - ACEA position on data needs.pptx

WG6 - A2D - ANNEX 13 - List of participants.docx

WG6 - A2D - ANNEX 14 - ACEA concept paper on Extended vehicle.pdf

WG6 - A2D - ANNEX 15 - ACEA - C-ITS short list of data.docx

WG6 - A2D - ANNEX 16 - AFCAR OTP architecture.pptx

WG6 - A2D - ANNEX 17 - FIA explanation of the Shared Server Concept V1.0.pdf

9. Working Group 6 - Technical Issues – Decentralised Congestion Control

9.1. Executive Summary

Cooperative intelligent transport systems (C-ITS) operating at 5.9 GHz for short range communication use an ad hoc network topology. This implies that there is no central coordinator, such as a base station or an access point, granting access to the wireless channel. All network participants are peers and share the wireless channel whenever they have something to transmit. However, when many network participants simultaneously want to access the channel, the performance of applications can be severely degraded due to saturation. To overcome this, a decentralized congestion control (DCC) scheme must be implemented[12]. DCC specifications for day one applications on a single channel are already in place and it will function satisfactorily for low to moderate densities of ITS stations (ITS-Ss), but might not be sufficient for multi-channel and day two applications asking higher data throughput and enhanced spectrum efficiency.

9.2. Objectives of the Working Group

The Working Group on DCC has discussed the currently available solutions and formulated recommendations on how to address congestion of C-ITS data traffic in the 5.9 GHz spectrum.

9.3. Organisation of Work

The work was based on one face to face meeting in January 2015 followed by additional phone conversations and email exchanges.

DG MOVE as chair of WG6 took care of organising the WG meeting and teleconferences, maintaining relations with other WGs and consolidating the working group report based on the input of the members.

All results, outputs and expert recommendations of the C-ITS Platform WG6 (Decentralised Congestion Control) have been produced, discussed and endorsed by the following nominated experts, representing the following organisations and Member States:

Organisation	Name
Car2Car	ANDERSEN Niels
Continental	ERDEM Bettina
FEDRO (CH)	RIEDERER Markus
FIAT	BIANCONI Maria Paola
FIGIEFA	PATTEMORE Neil
Imtech	ROZEMA Klaas

[12] See http://www.etsi.org/deliver/etsi_ts/102600_102699/102687/01.01.01_60/ts_102687v010101p.pdf

Indiv Expert	MENENDEZ Jose Manuel
Indiv Expert	SPAANDERMAN Paul
Kapsch	SMELY Dieter
Kapsch	LAX Richard
PSA Peugeot Citroen	SERVEL Alain
Public Roads Administration (NO)	OLSEN Eric
SCANIA	DEGERMAN Pär
Transport and Telecom (Greece)	AMDITI Angelo
Tom Tom	TZANIDAKI Johanna Despoina
Volvo	SJÖBERG Katrin
Yamaha	FISCHER Hennes

The following European Commission Services have been involved in WG6:

Services	Name
EC MOVE	TZAMALIS Georgios
EC MOVE	VAN GAEVER Alain
EC MOVE	VAN DER LINDEN Geert

9.4. Background to Decentralized Congestion Control

The preferred wireless technology for short-range communication is based on the ubiquitous standard IEEE802.11. In 2003, ASTM in the US released the first standard addressing connected vehicle technologies which was based on IEEE802.11a. In 2004, the Institute of Electrical and Electronics Engineers (IEEE) took over the work on developing a standard for vehicular communications, which is today known as IEEE802.11p. Europe decided to base its effort, known as ETSI ITS-G5, on the same technology.

9.4.1 Why Decentralized Congestion Control?

Early on it was identified that under high ITS-S density the ETSI ITS-G5 radio channel risks being overloaded due to:

- A medium access control method designed for low to moderate network loads
- An ad hoc network topology, meaning:
    - No access point or base station to grant resources on the wireless channel
    - Everyone needs to meet on the same frequency channel

DCC tries to tackle this issue by adapting the transmission parameters based on channel load measurements. In the following subsections this is further detailed.

9.4.2 Medium access control

The Medium Access Control (MAC) procedure determines when a node in the network is allowed to transmit and its goal is to schedule transmissions as to minimize interference between transmitters (avoid packet collisions in the air). With careful scheduling of transmissions reliability of successful packet reception is increased. MAC in IEEE802.11p is based on a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism (also used in legacy IEEE802.11). When a node employing CSMA/CA wants to transmit a packet, it first listens to the wireless channel for a predetermined listening period to detect activity (carrier sensing, in the order of 50-100µs). When no activity is detected the node transmits the packet immediately. If activity is detected the node needs to do a back-off procedure and randomizes a deferral time for its next transmission attempt (this can vary between 0 and slightly above 1ms in IEEE802.11p).

However, the node is only allowed to decrement its back-off timer when the channel is idle and must pause during on-going transmissions from other nodes. Once a node has reached a back-off value of zero it can transmit directly. The throughput of the channel will decrease in the presence of many simultaneous transmissions. This can be caused by (i) several nodes within radio range of each other reaching a back-off value of zero at the same time, and (ii) multiple nodes having sensed an idle channel but causing collisions at receivers in between them (a.k.a. the hidden terminal problem).

CSMA/CA is simple and it works fine for our home and office environments when there is an access point present but for ad hoc network it is less suitable, in particular during high network utilization periods. Further, it was designed for event-triggered or burst data traffic where the network regularly has time to recover. Many safety related C-ITS services however rely on continuous broadcasting of position messages.

The wireless channel for C-ITS is said to be full at 2000 packets/sec given a packet size of 400 bytes transmitted at a rate of 6 Mbps. The highest throughput however is achieved at 1200 packets/sec, which is where DCC tries to keep the channel load. It should be noted that regardless of the selected MAC method some form of DCC will be needed due to the ad hoc network topology.

9.4.3 Ad hoc networks

IEEE802.11p/ETSI ITS G5 has been developed as a standalone system (which is it strength). It uses an ad hoc network topology, which means direct communication can take place between all equipped traffic participants: vehicles, motorcycles, bicycles, pedestrians, urban rail and infrastructure as peers in the network. Since no access points or base stations are part of the network, there is no entity governing a possible channel switch if the communication channel is overloaded (e.g. handover between different base stations in mobile telephone systems). Hence frequency channels need to be fixed, otherwise interoperability throughout Europe would not be possible (e.g. a German vehicle can communicate with French infrastructure). Furthermore, as activity on the network cannot be predicted, all ITS-Ss need to implement DCC to ensure they have the same probability of success in accessing the channel.

The communication range for IEEE802.11p/ETSI ITS-G5 is up to 1000 meters in benign conditions but typically the coverage will be around 500 meters depending on the

environment. When many ITS-Ss in the vicinity are sending Cooperative Awareness Messages (CAM) and Decentralized Environmental Notification Messages (DENM) studies have shown that the 1200 packets/sec limit is easily reached resulting in poor communication performance.

CAMs are typically triggered 1-10 times per second depending on vehicle dynamics (high speed meaning more CAMs), whereas DENMs are only triggered when an event is about to happen but can then be sent up to 20 times per second and the period for sending can last several seconds. Further introduction of other, possibly larger, messages such as In-Vehicle Information (IVI), Signal, Phase and Timing (SPaT) and road topology (MAP) will further challenge capacity.

9.5. How does DCC work in practice?

DCC is a collective name for several techniques for counteracting high network channel loads, and is outlined in TS 102 687 V1.1.1. Since ETSI ITS-G5 is a broadcast system (one sender, multiple receivers) notification of successful reception is not included. In traditional home and office systems the majority of transmissions are unicast (one sender, one receiver) and they are usually followed by an acknowledgment. In ad hoc networks however, the number of ITS-Ss in the vicinity is constantly changing and the sender never knows how many stations are in radio range. To this end, each ITS-S estimates his number of neighbours based on received messages. This ad hoc network is therefore not seen as a communication but rather a sensor network in which each station (sensor) provides information to others without knowing whether someone needs the specific information. The metric used for estimating the number of neighbours is the Channel Busy Ratio (CBR).

The strategies to counteract a busy channel are:

Table 1: Different DCC strategies

DCC technique	Description
Transmit Rate Control (TRC)	TRC restricts the number of generated packets in each and every vehicle as the CBR increases (output power and transfer rate are kept constant).
Transmit Power Control (TPC)	TPC reduces the output power as the CBR increases. This shortens the effective communication range and thus fewer vehicles will receive the message.
Transmit Data rate Control (TDC)	TDC uses a higher transfer rate for increasing CBR, keeping the channel less busy because the packets will be in the air shorter. IEEE802.11p provides 8 different transfer rates between 3-27 Mbps.

For day one applications transmit rate control has been selected. Transmit power control will additionally be used when approaching a toll plaza in order to be co-existent with existing tolling services.

Depending on the current level of CBR, the vehicle will be allowed to transmit a certain number of packets. In Table 2, a possible mapping of CBR values and transmit rates is shown.

Table 2: CBR values vs allowed transmission rates.

State	Channel load or CBR	Packet or transmit rate
Relaxed	< 30%	10 Hz
Active 1	30-39%	5 Hz
Active 2	40-49%	3.33 Hz
Active 3	50-60%	2.5 Hz
Restrictive	> 60%	2 Hz

As can be seen in Table 2, there is no control above 60%. All ITS-Ss, regardless of the number of ITS-Ss within radio range, use a 2 Hz transmit rate.

9.6. DCC for day one applications

In the beginning of C-ITS deployment, the penetration of ITS-S will be low so the chance of coming in a congested situation will be limited. Thus DCC will only occasionally be active. CAM generation is speed dependent (e.g. driving on the highway at a speed of 120 km/h could give a CAM generation rate of approximately 8 Hz while standing still will reduce this to 1 Hz). CAM generation - and transmission - can also be restricted by DCC in Europe. The definition of the CAM rate is such that it allows each ITS-S to broadcast a reasonable minimum amount of CAMs for Day one applications, more or less equal to other ITS-Ss in the same area, and this also in congested situations.

DCC for day one applications will not restrict the transmit data rate of DENMs. Safety applications based on DENMs will, when required, get a higher priority in the DCC mechanism. Day two or three use cases for safety applications are based on CAMs too (e.g. intersection collision avoidance) and will produce additional DENMs. The growth of use cases, and differences in message behavioural requirements, will require differentiation in priority levels, multi-channel operation and may require DCC adoption.

9.7. DCC outlook and discussion

OEMs in the US are also working on DCC solutions, and they generally call it congestion control. DCC in the US will be included in their position message generation (called basic safety message, BSM). This implies at a low channel busy ratio more BSMs will be generated and when the channel busy ratio increases, less BSMs will be transmitted. Power control is also considered to be part of their day one deployment. Further, BSM will be sent on one specific channel in the US (safety channel 172) and it is only the BSMs that are subject to DCC. The other allocated frequency channels in the US have not yet been discussed to be used with DCC. In Europe, on the other hand, all frequency channels are subject to DCC.

DCC needs to be revisited for day two applications such as automated driving use-cases (e.g. C-ACC and platooning) but also for Infrastructural and Vulnerable Road User use-cases. The increase in data volumes exchanged and the increased message behavioural requirements demand further development of the predictability of the DCC as developed for day one applications (recall Table 2, where there is no control above a channel busy ratio of 60%

regardless of the number of vehicles within radio range). Work is thus needed on improving DCC for really challenging applications that use infrastructural messages sets such as SPaT, MAP and IVI and any other application critical for the safe operation of the vehicles.

The introduction of C-ITS for vulnerable road users will increase the number of C-ITS devices dramatically and will lead to much higher CBRs in urban environments. Better protection of VRUs is however an important safety goal, for which the following hurdles have to be overcome:

- Reliable and more accurate positioning technology for pedestrian detection (e.g. to distinguish if the pedestrian is walking on the sidewalk, wants to cross the street or is already crossing the street). This is especially true for urban environments, where current GNSS solutions often have poor performance.
- Designation of additional frequency spectrum for (future) C-ITS services.
- Development of DCC for high CBR and multi-channel strategies.

DCC does not affect interoperability as it does not affect the message sets or protocols needed for communication. The implication is that moving towards more sophisticated DCC solutions for more demanding applications in the future can be realized in parallel with other C-ITS developments. To accommodate new applications more channels could be used and different DCC strategies could be used on different channels (e.g. platooning may require a more predictable DCC).

9.8. Recommendations

- DCC has been standardized for day one applications in the approved standard ETSI TS 102 687 V1.1.1. This current specification is sufficient for early deployment of day one applications with a small penetration of ITS-S. The Working Group on DCC therefore recommends no further actions to start day one deployment.
- The introduction of future C-ITS services (e.g. inclusion of VRUs, infrastructure and automated use cases) will lead to a dramatic increase of ITS-Ss and channel loads, in particular in urban environments. The Working Group recommends that the 5855-5875 MHz, the 5905-5925 MHz and the 63-64 GHz band are designated to C-ITS services to cope with future capacity demand.
- Within the context of this increase of information exchange and increase of channel usage, an approach on the use of multiple channels for safety information exchange, including message priority needs to be developed. This needs to include development of multichannel DCC technologies.
- In order to accommodate safety critical applications (for example platooning and automated driving), predictability of upcoming DCC implementations is imperative and must be considered.

10. Working Group 6 - Technical Issues – Hybrid Communications and Spectrum allocation

10.1. Introduction

The availability of an increasing amount of ITS data enables the realisation of connected, cooperative and automated ITS services and applications, with highly varying functional and technical communication requirements. These services and applications require an open Hybrid Communication approach supporting future new technology adoption, today including a number of access and communication technologies[13]. For ITS safety and efficiency services and applications an increasing demand for data exchange is expected. Furthermore comfort and entertainment related services and applications will require even higher data exchange volumes. This overall high demand for data exchange requires a fast increasing amount of spectrum.

IEEE802.11p/ETSI ITS-G5 systems have been developed and their applicability for traffic safety and management related C-ITS has been demonstrated in various projects in Europe and USA. The evolution of cellular networks and cellular services already offer many ITS connected services and are expected to offer new opportunities in terms of coverage and technical performance in future. The Working Group concluded that currently neither ETSI ITS-G5 nor cellular systems can provide the full range of necessary services for C-ITS. Consequently a hybrid communication concept is needed in order to take advantage of complementary technologies.

The Radio Frequency Spectrum is a limited resource, and data exchange predictions show an increasingly high demand. Resource sharing among all users is required. This should be based on fair policies, ensuring current services stay enabled and safety is ensured. EU spectrum regulation provides spectrum in the 5.9 GHz band for traffic safety and management related services. Support for IEEE802.11p/ETSI ITS-G5 in this band needs to stay in place to ensure robust and safe operation. For Transport and Traffic Telematics (TTT) frequencies in the 5.8 GHz band are used.

10.2. Objectives of the Working Group

The present Working Group 6.3 of the C-ITS deployment platform has followed, discussed and elaborated recommendations to the latest issues in the radio frequency and hybrid communication domain in order to smoothen the process of balancing the needs of different industries and stakeholders.

[13] such as 3G/4G, LTE, LTE-D, 5G, WAS / RLAN versions of IEEE802.11, IEEE802.11p/ETSI ITS-G5, Bluetooth, ZigBee, UWB, CEN DSRC, DAB

10.3. Organisation of Work

The organization of work was based on regular Working Group meetings (WG6.3 conducted a total of 5 meetings in Brussels from December 2014 – December 2015 in the course of the first phase of the C-ITS platform). DG MOVE as Chair of WG6.3 took care of maintaining relationships with other Working Groups and informing the WG6.3 participants of work items, which could be relevant for the Group to consider.

All results, outputs and expert recommendations of the C-ITS Platform WG6.3 have been produced, discussed and endorsed by the following nominated experts, representing the following organizations and countries:

Table 8: WG6.3 members and organizations

Organisation	Name
ACEA	Aldo Celasco
ASFINAG	Marko Jandrisits
AustriaTech	Alexander Froetscher
BMVIT AT	Helge MOLIN
Car2Car Communication Consortium	Niels Peter Skov Andersen
CLEPA	Stefan Deix
Continental	Bettina Erdem
	Osvaldo GONSA
Ericsson	Anders Fagerholt
FIAT	Maria Paola Bianconi
FIGIEFA	Neil PATTEMORE
	Pete Houlden
GDV	Jurgen Redlich
Member State (HELLAS) - ICCS	Angelos AMDITIS
IBM	Volker Fricke
IDIADA	Alvaro Arrue
Kapsch	Dieter Smely
	Richard Lax
Norwegian Public Roads Administration	Erik Olsen
NXP Semiconductors	Marc KLAASSEN
OCA	Josef Kaltwasser
PaulsConsultancy BV	Paul Spaanderman
PSA Peugeot Citroen	Alain Servel
Q-Free	Knut Evensen
RENAULT	Christian ROUSSEAU
Rijkswaterstaat	Frans op de Beek
	Marcel Otto

Organisation	Name
SCANIA	Johannes Slettengren
	Pär Degerman
Swiss Federal Roads Office	Markus Riederer
Universidad Politécnica de Madrid	José Manuel Menéndez
Volkswagen AG	Corinna Deubel
Yamaha Motor Europe N.V.	Hennes Fischer

The following European Commission Staff have been involved in WG6.3:

Table 9: WG6.3 Commission staff

Services	Name
EC CNECT	RIZZO Giuseppe
EC CNECT	DAVILA GONZALEZ Emilio
EC CNECT	LINARTAS Ramunas
EC GROW	KUUKKA Sanna
GSA	DIANI Fiammetta
GSA	FERNANDEZ Alberto
EC MOVE	ALFAYATE Maria
EC MOVE	CARABIN Gilles
EC MOVE	DEPRE Claire
EC MOVE	MENZEL Gerhard
EC MOVE	TZAMALIS Georgios
EC MOVE	VAN DER LINDEN Geert
EC MOVE	VAN GAEVER Alain

10.4. Spectrum

10.4.1 Co-existence between and band usage of 5.8 GHz and 5.9 GHz

The band 5 795 MHz to 5 805 MHz has been harmonized for the use by Transport and Traffic Telematics (TTT), also called CEN DSRC, by the EC Decision 2013/752/EU (amending EC Decision 2006/771/EC on Short Range Devices) and the band 5 795 MHz to 5815 MHz has been designated for the use by TTT by ERC Recommendation 70-03 (Annex 5), which is primarily used for road charging systems in Europe and elsewhere. By issuing the Directive 2004/52/EC of the European Parliament and of the Council and Commission Decision 2009/750/EC the European Union has pointed to TTT to be used for road charging systems in Europe.

At CEPT (European Conference of Postal and Telecommunications Administrations) level the ITS Spectrum allocations are covered by ECC/DEC/(08)01 amended 3 July 2015 (5875 – 5925 MHz) and ECC/REC/(08)01 amended 3 July 2015 (5855 – 5875 MHz). It recommends the frequency sub-band 5855 – 5875 MHz for ITS non-safety applications, designates the frequency sub-band 5875-5905 MHz on a non-exclusive basis for ITS traffic safety applications and considers the designation of the frequency sub-band 5905-5925 MHz for an

extension of ITS spectrum noting that protection of ITS cannot be ensured in this sub-band. Additionally ECC Decision ECC/DEC/(09)01 allocates the 63-64GHz band for direct X2X traffic safety and management related communication systems. The Working Group agrees that the 5855-5875 MHz, the 5905-5925 MHz and the 63-64 GHz band need to be designated to cope with future capacity demand for C-ITS services.

A major item of this working group has been to discuss the co-existence of the above-mentioned applications in their respective frequency bands. An agreement has been reached on mitigation techniques to ensure co-existence between 5.8 GHz tolling DSRC and 5.9 GHz ITS applications. The approach that was developed to ensure the co-existence between 5.8 GHz tolling CEN DSRC and 5.9 GHz ITS is reflected in the update of the corresponding ECC DEC (08)01 and ECC REC (08)01 regulations and ETSI Technical Specifications TS 102 792.

Spectrum regulations on Smart Tachograph (Regulation (EU) 165/2014) and Weights & Dimensions (Regulation (EU) 2013/0105 (COD)) types of applications in the 5.8 GHz frequency band need to be approved by the Electronic Communications Committee (ECC) of the European Conference of Postal and Telecommunications Administrations (CEPT) or, respectively, current regulations need to be amended.

The harmonized standard[14] ETSI EN 302 571 referring to the last approved version of the technical specification TS 102 792 is now in final draft version. It will likely be ready by mid-2016 – and will then be published in the EU official journal.

10.4.2 WAS/RLAN expansion in the 5 GHz band

The extension of Wireless Access Systems / Radio Local Area Networks (WAS/RLAN) bands for wireless broadband poses a certain risk if no appropriate mitigation measures can be assured with incumbent services and applications. This is especially true for EU priority services and applications, in particular Copernicus (earth observation satellite) services operating in the band 5350-5450 MHz, the use of C-ITS services, including safety-related IEEE802.11p/ETSI ITS-G5 applications in the frequency band 5855-5925 MHz and the usage of TTT (Transport and Traffic Telematics) applications like electronic tolling in the 5795-5815 MHz and other current civil and/or military radio systems to which the bands 5350-5470 MHz and 5725-5925 MHz and adjacent bands have already been assigned or designated.

To enable an efficient use of the spectrum the European Commission has issued a Mandate to CEPT (RSCOM13-32rev3) to study and identify harmonised use and sharing conditions for spectrum use by Wireless Access Systems including Radio Local Area Networks in the bands 5350-5470 MHz and 5725-5925 MHz ('WAS/RLAN extension bands') for the provisioning of

[14] A harmonized standard is a European standard developed by a recognized European Standards Organisation: CEN, CENELEC, or ETSI (in this case ETSI).

wireless broadband services while ensuring uninterrupted robust operation of Copernicus, IEEE802p/ETSI ITS-G5 and TTT services and applications. It was decided at the RSC#54 meeting on 9 December 2015 that the response on the Mandate should be delivered by CEPT until the end of 2016.

ITS is included in the agenda of the World Radio Conference in 2019 to consider possible global or regional harmonized frequency bands, to the maximum extent possible, for the implementation of evolving Intelligent Transport Systems (ITS) under existing mobile-service allocations, in accordance with Resolution COM6/13 (WRC-15).

RLAN is also included in the agenda of the World Radio Conference in 2019 to consider issues related to wireless access systems, including radio local area networks (WAS/RLAN), in the frequency bands between 5 150 MHz and 5 925 MHz, and take the appropriate regulatory actions, including additional spectrum allocations to the mobile service, in accordance with Resolution COM6/22 (WRC-15).

10.5. Hybrid Communication

Connected, cooperative and automated ITS services and applications have highly varying functional and technical communication requirements. Depending on the business cases and requirements it should be possible to select the most effective access and communication technologies for each purpose. A Hybrid Communication approach including multiple technologies (including future new developments) and radios is the only way to support continued deployment of ITS services and applications today and in the future.

It is desirable to allow efficient and access-layer agnostic data exchange. The specific nature of some services and applications play a role in the technology of choice. The Working Group recognised the importance of this topic and discussed at length the various options.

The possible simultaneous provision of similar information through different information providers (including on-board sensors) could lead to validation problems at the receiving side, which might find it difficult to judge which information is better (more accurate, more timely, …) to use. The use of different communication channels when sending/receiving C-ITS messages – and the corresponding question on how to validate which message is most recent/relevant/accurate is being studied in various projects[15].

Proposed Multi Radio study: Regulatory requirements have led to the integration of multiple equipment on-board both passenger and commercial vehicles. These tend to use different radios/frequencies. It is recommended to study how these different regulatory requirements could be more effectively met. This could reduce the number of radios used, hence reduce

[15] ECO-AT (http://eco-at.info/), CONVERGE (http://www.converge-online.de/), A58 shockwave project (http://www.spookfiles.nl/).

the amount of hardware needing to be integrated and reduce the risk of interference between the different in-vehicle radios.

10.5.1 Access-layer agnostic

The WG6 experts conclude that it is important to ensure that C-ITS messages can be transmitted independently from the underlying communications technology (access-layer agnostic) wherever possible. Depending of the type and circumstance of C-ITS service or application it is possible to use short-range (e.g. IEEE802.11p/ETSI ITS-G5) and/or long range communication such as cellular (3G, 4G, 5G…) and/or broadcasting (e.g. DAB+) technologies. Note: certain use cases will not be possible over all communications technologies, due to latency, reliability, functional safety (ISO 26262) etc. requirements of these use cases.

10.5.2 Cellular Communication

10.5.2.1 Ensuring coverage across the road network

To ensure the possibility to disseminate C-ITS related information to all transportation users, and because road authorities will not always equip all roads with short-range communications, it is envisioned to stimulate the coverage of cellular communications to support connected & automated driving. It is therefore advised to consider geographical coverage obligations to complement existing population coverage requirements.

10.5.2.2 Open questions regarding the use of cellular type of communications

Given the difference between the automotive and telecom sector in terms of the lifecycle of equipment used, questions are raised on how to ensure communication capabilities of on-board vehicles over the whole lifetime of the vehicle.

Further work needs to address congestion on the cellular network to guarantee correct functioning of safety related C-ITS services.

Data roaming is still seen as presenting some issues for connected vehicles that cross country borders. Not only in terms of costs of data roaming – but also in technical, commercial and legal terms (e.g. hair pinning the data connection back to the country of origin).

10.5.3 Short Range Communication

Given that the 5.9 GHz frequency band supports short range communications between vehicles, between vehicles & roadside equipment and other transportation users it is important to ensure that the same communication system is used by all users within that frequency band. Agreement has been reached within the Working Group that for short-range communications in the 5.9 GHz band the communication system to be used initially is IEEE802.11p/ETSI ITS-G5. This access technology is the most mature and closest to deployment, based on experience in various demonstration projects.

With evolving technology other communication technologies will become available (e.g. LTE direct) – and when these meet the safety-related C-ITS applications requirements (e.g.

latency, reliability and functional safety…) these should be considered. This will likely require the use of another frequency range to avoid conflicts with IEEE802.11p/ETSI ITS-G5 communications.

Since the facility layer protocols are communication agnostic, Decentralized Environmental Notification Messages (DENMs) can in addition to IEEE802.11p/ETSI ITS-G5 be provided through other communication means such as cellular.

10.6. Recommendations and Follow-Up Actions

This chapter is split into two parts; the first concerns the recommendations from the experts of WG6.3 to the European Commission; the second lists possible follow-up actions, ways to further detail the actions towards resolving issues related to Frequencies and Hybrid Communication and suggestions on the continuation of WG6.3 in the second phase of the C-ITS platform.

10.6.1 Recommendations

1. The Working Group recommends that the 5855-5875 MHz, the 5905-5925 MHz and the 63-64 GHz band are designated to C-ITS services to cope with future capacity demand.

2. The Working Group recommends following up on all currently on-going and future co-existence issues to make sure C-ITS services, which offer amongst others safety related services, are not exposed to harmful interference. The agenda of the World Radio Conference in 2019 includes expanding WAS / RLAN into the 5725-5925 MHz band and sharing the spectrum with other services. This could lead to one example of such harmful interference.

3. The Working Group recommends exploiting the advantages of all communication technologies proposed for C-ITS services, meaning said services needing to be communication-layer agnostic. Such an approach would allow benefiting from the complementarity of current and future competing technologies, the working group therefore recommends including adequate migration strategies.

4. The Working Group, in line with WG1 on Cost Benefit Analysis, recommends solving the various outstanding issues with the use of cellular communications for C-ITS services in order to gain access to the wide coverage offered by existing infrastructure, leading to faster uptake of C-ITS services.

5. The Working Group recommends that for short-range communications in the 5.9 GHz band initially the communication system to be used is IEEE802.11p/ETSI ITS-G5.

6. Regulatory requirements have led to the integration of multiple different equipment on-board both passenger and commercial vehicles. These tend to use different radios/frequencies. The Working Group recommends studying how these different

regulatory requirements could be more effectively met. This could reduce the amount of radios used, hence reduce the amount of hardware needing to be integrated and reduce the risk of interference between the different radios.

10.6.2 Follow-up Actions

The collaboration of a relatively large group of experts resulted in recommendations to the EC, but also identified several areas that require more detailing and routes for further improvement. Given the importance of Frequencies and Hybrid Communication in supporting the deployment of C-ITS in Europe the working group recommends to continue the work, focusing amongst others on the following topics:

1. Recommendation 1 following up on all currently on-going and future co-existence issues, a first candidate for this could be Communications-Based Train Control (CBTC), which concerns safety applications in Urban Rail and also operates in the 5.9 GHz band. Sharing and mitigation measures with C-ITS systems should be studied.

2. Recommendation 4 recommends increasing coverage of C-ITS services through existing cellular communications infrastructure, the Working Group therefore estimates it sensible to study whether geographical coverage obligations can be introduced.

3. Strengthened cooperation between transport and telecommunications stakeholders to further progress the hybrid mode and associated communication technologies (e.g. 3GPP, since they are developing standards that could serve the business case of C-ITS).

4. It is advised to stimulate the realisation of Multi-Channel Operation (MCO) in IEEE802.11/ETSI ITS-G5 development and standardisation in order to support C-ITS in urban environments.

11. Working Group 7 - Standardisation

The work plan of the C-ITS platform has foreseen a working group on the topic of C-ITS Standardisation. All C-ITS platform members that originally wanted to participate in the Standardisation Working Group 7 have been invited to a first preliminary conference call, which was followed by one physical meeting of the Working Group in late 2014. In 2015 several follow-up phone calls took place, mainly on identifying the currently used C-ITS standards for deployment in Europe. Following the C-ITS platform first meetings in November it has been identified by the European Commission together with the stakeholders that the topic of standardisation is rather a horizontal issue than one specific topic that can be dealt with in a single working group of its own. Since standardisation is a topic that is crucial and almost always directly linked to specific topics and issues it was evident that the single C-ITS Platform working groups need to discuss these standardisation related topics within the single dedicated working groups.

It is important to note that a lot of work has already been done in other fora prior to the C-ITS platform regarding standardisation and gap analysis, therefore there was no need to start from scratch. It was therefore agreed that the work regarding standardisation within the C-ITS platform shall be based on existing work wherever possible. There are several already existing fora working on the topic of standardisation, for instance the ITS Coordination Group where the European Standardisation Organisations (ESOs) and the European Commission are directly involved in. In order to work most effectively the way forward was to make use of the existing groups as much as possible.

Within the C-ITS Platform the topic of standardisation has therefore been dealt within the individual working groups. When the C-ITS platform working groups have produced concrete results and recommendations requiring effort on the topic of standardisation these have been recorded in the individual working group reports and recommendations (e.g. Working Group 5, Working Group 6, Working Group 9 and Working Group 10).

C-ITS Standards used in European deployment initiatives

Within the C-ITS Platform a horizontal overall discussion took place on the general needs regarding the topic C-ITS standardisation from a deployment perspective. The following key items have been identified:

- The need for elaboration of test standards
- The need for profiling of standards to ensure interoperability in implementation
- The need for proper maintenance of standards due to implementation needs

In order to meet the above mentioned needs a first step was taken in the C-ITS platform to collect an overview of the standards being used within C-ITS deployments initiatives in Europe. This exercise has only focused on C-ITS deployments that are currently being implemented or are going to be deployed in the next 2-3 years. Therefore the Day 1 List of C-ITS services identified and agreed within the C-ITS Platform (Working Group 1) has been inserted in this overview file.

The main aim has been to elaborate a excel list of standards that are currently being used and which therefore are relevant for interoperability in Europe. The results of the exercise

aim to give a picture of what is currently (i.e. now and in the coming 2-3 years) used for implementation in Europe, not in 5 years or even longer periods of times. The target has been to provide a snapshot of the current activities at the end of 2015 as result of the input of the C-ITS Platform experts.

The topic of actual profiling of standards and elaboration of test standards has not been the main target of this exercise yet – the result is the first important starting point which will help to lay the necessary foundation to further discuss how profiles can and have to be defined for EU-wide interoperable C-ITS deployment in the future. However, the current profiles that are in-use or being elaborated have been listed in a specific section at the end of the excel standards list to map which profiles are currently being USED and/or SUPPORTED within the single deployment initiatives.

C-ITS platform members as well as additional stakeholders have been requested to return the filled-in file – this exercise has been promoted to e.g. the C-ITS Corridor projects NL-DE-AT, Amsterdam Group, Car2Car, CODECS, CEF deployments projects like NordicWay, SCOOP@F, C-ITS deployment initiatives in the UK, CZ, etc. in order to facilitate the delivery of the results as input for the EC C-ITS Platform. All delivered results have been merged into one single file that constitutes WG7 - ANNEX 1.

It is planned to update the list with additional contributions from deployment initiatives that have not been able to send-in their contributions for the first version in December 2015.

12. Working Group 8 - Public Acceptance

12.1. Executive Summary

To support widespread deployment of C-ITS in Europe Public Acceptance is vital. A strategy for public acceptance takes public concerns seriously and finds answers that reassure users, consumers and the general public that benefits of a new technology or major infrastructure outweigh the disbenefits. It is necessary to gain acceptance even from those groups that will not benefit from the technology directly. To contribute to this confidence gaining the Working Group decided it first needed to identify who the public is and what the key questions are that need addressing. The members of the WG8 on Public Acceptance worked on both these issues and established a very detailed matrix of all stakeholders and their respective acceptance factors.

In a second phase an analysis of the commonalities in the exhaustive list of acceptance factors allowed the working group to identify and agree on 11 key acceptance factors that cover all stakeholders. The aim of this reduction exercise was to zoom in on the core message that needs to be transmitted to stakeholders. It should be noted that the core message does not equal a unique or single message, in fact the message should be tailored to each user category targeted.

Another important conclusion from this focusing exercise is that there are essentially two different types of messages to be constructed. The first focusses on the benefits and spelling out to the different stakeholders the reasons why investing in C-ITS is the way forward in creating a transport environment that is safer, more comfortable and environmentally sustainable. The second message addresses all concerns related to the introduction of this new technology, ensuring these are thoroughly evaluated and given clear, robust and factual answers.

The working group formulated several recommendations and urges in particular that progress be made on addressing the concerns related to this technology. If not properly handled these concerns risk jeopardising the chances for widespread Public Acceptance.

12.2. Objectives of the Working Group

The objective of the C-ITS Platform working group on Public Acceptance is to produce policy recommendations for the development of effective educational and communication programs for improving the acceptance of Cooperative Systems by the general public and the different communities of beneficiaries. A broad representation of all players is imperative and the entire value chain should contribute to the topic of acceptance as it is an essential prerequisite for the deployment of C-ITS in Europe.

This process started with the working group agreeing quickly on the need for a draft mapping of all the relevant stakeholders and a list of potential questions concerning public acceptance to be addressed to other C-ITS platform groups (e.g. for freight transport or

logistics quantified benefits such as cost-savings from reduced fuel consumption should be highlighted whereas for personal transport qualitative benefits such as comfort seem more appropriate).

In order to produce policy recommendations the working group then embarked on an analysis distilling the core messages and established – and agreed on – a list of eleven Key Acceptance Factors. Further discussions during the working group meetings also led to the appearance of two distinct families of messages, one focusing on the benefits and perceived usefulness of C-ITS services, the other addressing all threats to Public Acceptance of technologies that rely on connecting of vehicles and sharing of data.

Finally some initial reflections and guidelines on the delivery methodology were formulated to complement the recommendations focusing on the content of the Public Acceptance messages.

12.3. Organisation of Work

The organization of work was based on regular Working Group meetings (WG8 conducted a total of 7 meetings in Brussels from May 2015 – December 2015 in the course of the first phase of the C-ITS platform). DG MOVE as Chair of WG8 took care of maintaining relationships with other Working Groups and informing the WG8 participants of work items which could be relevant for the Group to consider.

All results, outputs and expert recommendations of the C-ITS Platform WG8 have been produced, discussed and endorsed by the following nominated experts, representing the following organizations and countries:

Table 10: WG8 members and organizations

Organisation	Name
ACEM	Veneta Vassileva
ADAC E.V.	Christoph Hecht
BLERVAQUE Sprl	Vincent Blervaque
CEDR	Torsten Geissler
City of Helmond	Gert Blom
ERTICO	Angeliki (Lina) Konstantinopoulou
European Cyclists' Federation	Ceri Woolsgrove
FEMA	Anna Zee
FIA	Laurianne Krid
IAV GmbH	Frank Fickel
Independent	Eric Sampson
Member state (NL)	Henk Schuurman
Scania CV AB	Tomas Östlund
Swiss Federal Roads Office (FEDRO)	Markus Riederer

Organisation	Name
TNO	Kerry Malone
Transport for London	Natalia de Estevan-Ubeda
VDA	Michael Niedenthal
Member State (BE-FL)	Eric Kenis
Yamaha Motor Europe N.V.	Hennes Fischer

The following European Commission Staff have been involved in WG8:

Table 11: WG8 Commission staff

Service	Name
EC MOVE	ALFAYATE Maria
EC MOVE	CARABIN Gilles
EC MOVE	DEPRE Claire
EC MOVE	MENZEL Gerhard
EC MOVE	TZAMALIS Georgios
EC MOVE	VAN DER LINDEN Geert
EC MOVE	VAN GAEVER Alain

12.4. Public Acceptance

Generally speaking obtaining Public Acceptance can roughly be split into four steps, the first is creating awareness, the second is removing all negative perceptions and concerns regarding the technology, the third step involves highlighting the benefits of C-ITS and creating willingness to use the system and a final (optional) step is creating willingness from the user to pay to gain access and/or use the system.

12.4.1 Stakeholders

C-ITS is not limited to drivers alone and various demographics were taken into account when listing all relevant stakeholders. The working group decided to proceed by grouping the very exhaustive list of stakeholders in three main categories:

1. Deployment Partners: OEMs, Cities, Road authorities, Public transport operators, Technology developers, Service Providers, Telecoms, Navigation and maps providers, Infrastructure engineers and planners

2. Users: Drivers, Cyclists, Pedestrians, Disabled road users, Users in non-automated vehicles, Transport companies, Fleet/Bus/Freight/Taxi operators, Emergency/Fire/Police services, Road-side recovery services, Utilities and Sharing/leasing/renting services

3. Other stakeholders: Trade bodies, Automobile clubs, Insurance companies, Legal services, Vehicle maintenance services, Legislators, Media services and Port authorities

All details can be found in **WG8 - ANNEX 1 - Stakeholder groups with acceptance factors_final_.doc**

12.4.2 Acceptance Factors

Understanding the audience is essential when addressing Public Acceptance, e.g. connected, automated and – in a later stage – autonomous vehicles have a large potential for increasing the mobility of an ageing population, but at the same time research shows that older generations are the least likely to embrace new technology.

To increase this understanding, a list of both positive and negative acceptance factors was drafted for each individual stakeholder defined in 12.4.1. Examples on the positive side include better incident management, more effective use of the infrastructure, reductions in operating costs, reduced fuel consumption, improved social inclusion, increased safety, and congestion mitigation leading to increased reliability of delivery services.

On the negative side issues identified include lack of trust in the use of personal data, driver distraction, uncertainty on standards and regulation, digital security, complacency about road safety, lack of benefits until sufficiently high uptake rates are achieved and – paradoxically – increased congestion due to increased popularity of road transport.

All details can be found in **WG8 - ANNEX 1 - Stakeholder groups with acceptance factors_final_.doc**

12.4.3 Reduced list of Key Acceptance Factors

When evaluating the list of all positive and negative acceptance factors established in 12.4.2 it is observed that many acceptance factors are common to many stakeholder groups, albeit sometimes in a slightly different form. The Working Group therefore found it useful to reduce this very long list to a much shorter list of common Key Acceptance Factors that combined cover all stakeholders. The group agreed on the Key Acceptance Factors that can be found in Table 12.

Table 12: List of key Acceptance Factors

#	Key Acceptance Factors	Benefit	Concern
1	Improved Road Safety	Yes	*(Yes)*[16]
2	Traffic network performance	Yes	
3	Enhanced Information	Yes	
4	Comfort	Yes	
5	Environmental impacts	Yes	
6	Innovation and economic growth	Yes	

[16] Though road safety is clearly expected to improve by the introduction of C-ITS services - and in line with the work done in WG9 - a risk of additional driver or road user distraction exists.

#	Key Acceptance Factors	Benefit	Concern
7	Privacy and Data Protection		Yes
8	Digital Security		Yes
9	Cost	*(Yes)*[17]	Yes
10	Perceived usefulness	Yes	
11	Accessibility and social inclusion	Yes	

All details can be found in **WG8 - ANNEX 2 - acceptance factors per user group.xlsx**

12.4.4 Two different types of messages

Further discussions and analysis of the eleven Key Acceptance Factors defined in 12.4.3 resulted in the Working Group agreeing on two distinct families of messages – of equal importance – to improve Public Acceptance. The first concentrates on the so-called positives, the benefits, the advantages this new technology can bring in terms of road safety, reduced fuel consumption and emissions and increased comfort and reduced stress levels whilst on the road. The second addresses the negatives, the legitimate concerns related to data protection and digital security that risk hindering the widespread acceptance of C-ITS services.

12.4.4.1 Benefits

One of the main challenges with C-ITS services is that the benefits are both largely societal (as opposed to individual) and not achievable in the short-term. This relative lack of immediate and personal benefit makes it considerably more difficult to build Public Acceptance, despite the fact that 8 out of the 11 Key Acceptance Factors can be categorised as benefits. Elements such as road safety for example have a dual character; clearly all stakeholders understand and value the importance of increased road safety, but nobody relates to the possibility that they are the subject of the service, i.e. that their behaviour or actions need assistance from C-ITS to achieve an increase in road safety.

The working group therefore suggested focusing first on those services that do provide an immediate and personal benefit (e.g. Green Light Optimal Speed Advisory is a good candidate as nobody likes to brake for or wait at traffic lights and the benefits in terms of brake wear and fuel consumption are obvious). In a second phase promote services which have an immediate but less personal benefit (e.g. drivers don't want to be identified as a threat to Vulnerable Road Users, but they too are at times pedestrians or cyclists or powered two-wheeler riders). Only in a later stage can network effects be added to generate additional long-term benefits (such as reduced congestion due to improved traffic

[17] Cost in this table, and later in the text, is primarily seen as a concern given the relatively low willingness to pay for C-ITS services. Several of the listed benefits (e.g. traffic network performance) could however reduce operating costs, making it a benefit, one which is particularly important for fleet owners.

management). Though these are absolutely essential in generating the overall benefits of C-ITS the pre-requisite of sufficient uptake rates might discourage first-movers.

Infrastructure owners and operators on the other hand are likely more susceptible to systemic benefits, such as much improved real-time information on traffic flows, more precise traffic management and reduction in incidents linked to congestion or accidents. When convinced of the benefits their long-term nature would be less of an issue, though it should be stressed that securing the investments when budgets are scarce is absolutely vital.

Finally, and in accordance with WG1 on Cost Benefit Analysis, to increase the individual benefits associated with C-ITS services should always be bundled.

12.4.4.2 Concerns

As stated earlier addressing the concerns of a new technology is at least as important and can generally be considered a prerequisite for highlighting the benefits. Testimony to this each major concern identified by the Working Group can be associated with at least one other Working Group in the C-ITS platform. Establishing links with these groups in itself is however not sufficient, the important work done there and the solutions proposed need to be translated into clear messages designed to improve Public Acceptance.

Privacy and Data Protection, most drivers would agree to provide their data in anonymous form for traffic related issues (e.g. road safety or congestion management). However many would raise concerns regarding commercial use of driver data and few would provide information in order to have access to commercial services. Having robust mechanisms to guarantee that data is secure and that existing Data Protection legislation can efficiently be enforced is therefore vital. The work performed in WG4 on Data Protection is thus of key importance in finding workable solutions and building Public acceptance.

Digital Security is a major concern, the possibility (real or not) of the vehicle being hacked and controlled by a person outside the vehicle is detrimental for Public Acceptance. The recommendations of WG5 on how to address these concerns and mitigate the risks are absolutely vital to obtaining widespread adoption of C-ITS services.

Cost is always a factor but in this particular case the willingness to pay is currently relatively low due to the fact that the direct benefits of these services are not always for the user; the benefits may even be perceived as negative (e.g. the negative association of being a threat to VRU) and the benefits often depend on sufficient uptake rate, creating a first mover disadvantage. The work of WG2 on business cases and WG9 on implementation issues plays an important role in this aspect of Public Acceptance. Additionally, road safety-related information should, where possible, be provided to the end-users free of charge (Directive 2003/98/EC, known as the 'PSI Directive', on the re-use of public sector information entered into force on 31 December 2003. It was revised by Directive 2013/37/EU which entered into force on 17 July 2013). This means that no hidden costs should be added later on and the

user benefits from all future initiatives to provide higher-quality, more timely information to C-ITS users.

12.4.5 Shaping messages for building Public Acceptance

The two families of messages described in the previous paragraph were somewhat colloquially categorised as "positive" and "negative". The Working Group however also defined another fundamental difference between them, which is that the "negative" messages can be considered horizontal, e.g. the issue of digital security, the solutions prepared by WG5 to ensure it, and the message addressing it from Public Acceptance point of view is common to all stakeholders. The messages related to the benefits of C-ITS on the other hand need to be tailored to specific stakeholders and their interests.

For example – and focusing on the prime target categories identified in WG1 on Cost Benefit Analysis – all infrastructure owners or operators need to be shown how the benefits from C-ITS justify their investing in physical and digital infrastructure, such as road-side units, telecommunication and back office upgrades. A key argument here is surely the gradual shift from expensive physical infrastructure (e.g. overhead gantries with Variable Message Systems) towards the far cheaper option of transmitting messages straight to in-vehicle displays.

Potential end-users on the other hand, both professional and private, need to be provided with clear information on how their benefits (e.g. safety, comfort, decision support, enhanced information, reduced fuel consumption) justify paying for in-vehicle installations of C-ITS equipment. A potentially important argument for them might be that under certain circumstances they might be offered trade-offs, e.g. sharing data on the vehicles location in return for cheaper or better information, and how to judge when it might be beneficial to engage.

The horizontal messages on the concerns should be factual and though they address matters that are likely not to occur to the vast majority of purchasers, the Working Group agrees this does not diminish in any way their role in Public Acceptance. For example on cost, interoperability should be stressed; designing and delivering services that work any time anywhere is slower and more expensive than selling non-upgradeable proprietary products. On the other hand an investment in C-ITS services also brings potential savings such as a positive impact on insurance premiums.

We also need to issue factual educational material on data ownership and the associated topics of privacy, data protection and anonymity that describes the different scenarios and sets out what is being done to protect the consumer and (as noted above) where there are discretionary decisions for the consumer. This material should also discuss hacking and try to give some real world estimates of risk and how consumer behaviour can reduce it or increase it.

Additionally, research shows limited awareness exists regarding C-ITS, whilst at the same time studies show a marked improvement in acceptance rating after a hands-on experience, even a simulated one. It is also known that the vast majority of potential users have little interest in how the technology works but are interested in its benefits and cost. The Working Group thus suggests that awareness campaigns would heavily benefit from promotion via Field Operational Tests and deployment pilots, demonstrating the benefits first-hand. This is a role that could at some point be taken over by early adopters.

12.5. Recommendations and Follow-Up Actions

This chapter is split into two parts; the first concerns the recommendations from the experts of WG8 to the European Commission; the second lists possible follow-up actions, ways to further detail the actions towards obtaining Public Acceptance and suggestions on the continuation of WG8 in the second phase of the C-ITS platform.

12.5.1 Recommendations

1. The working group identified several dozen stakeholders related to C-ITS, all of which need to receive a tailored version of the same core message on the benefits of C-ITS services. Incremental changes in automated safety systems will likely be deployed anyway, but it is recommended that the EC keeps up the pressure in terms of legislation. To build Public Acceptance where it matters most the Working Group recommends to start by focussing on five target audiences – these do not aim to be exhaustive or cover all defined stakeholders but include all groups that should be addressed first:

    - **Infrastructure owners** – the assumption is that this is largely public sector focussed (albeit some bridges, toll roads and tunnels are privately operated, and probably ahead of the game on ITS already). Key messaging needs to be on education about benefits, but also reassurance that they will not invest in technologies that are outdated and obsolete within a few years, but which are capable of future technology updates.

    - **Fleet Owners** – economic benefits and reductions in operating costs are essential, whilst air quality and environment are less likely to be the driving principles here. Better reliability of delivery services due to reduced accidents and congestion are very important secondary effects.

    - **Professional Drivers** – probably use telematics, dynamic satellite navigation systems, etc. already so acceptance should be high. However a concern would be the perception of total surveillance by the employer and a big challenge will come with full automation of buses and taxis, whereby professional drivers become redundant.

- **Private Drivers** – are price sensitive, but the majority probably welcome systems that make driving tasks less stressful. The key issue will be to reduce distracted driving in the short to medium term, and address the fact that private drivers are reluctant to pay for certain systems, i.e. most drivers don't think they will crash, so won't pay extra for the latest safety systems as optional extras. Fears also exist that C-ITS could be used to prosecute driving violations or that their vehicles may be traced by the police.

- **General Public** – Citizens in general should be concerned about the societal cost of road accidents and fatalities and the justifiable investments in technologies that aim to reduce it. Vulnerable Road Users could gain as connected vehicles bring in a real leap in road safety, reduced air pollution and less congestion through better traffic management.

2. The Working Group warns that public acceptance is different from product marketing. A strategy for public acceptance takes public concerns seriously and finds answers that reassure users, consumers and the general public that the benefits of a new technology or major infrastructure outweigh the disbenefits. It is necessary to gain acceptance even from those groups that will not benefit from the technology directly. Arguably, it is even more important to convince the public that potential risks are handled properly than to convince them of potential gains. The Working Group therefore recommends building clear educational and factual messages on Privacy and Data Protection, Digital Security and Cost. These messages should build on the work from WG4 on data protection, WG5 on security and certification, WG1 on Cost Benefit Analysis and WG2 on Business cases. In the same manner the solutions developed in these working groups must take into account Public Acceptance concerns.

3. The Working Group recommends further investigating the impact difference between making C-ITS services optional or compulsory. From a Public Acceptance point of view this makes a big difference, e.g. EC regulation foresees mandatory fitting of Electronic Stability Control Systems but for Public Acceptance reasons it is beneficial that these systems can be deactivated, even when users tend to never use this option. This should be aligned with the work of WG4 on data protection, which also foresees the possibility of opting out, with the possible exception of safety related services, e.g. there is no opt-out for eCall.

12.5.2 Follow-up Actions

The collaboration of a relatively large group of experts resulted in recommendations to the EC, but also identified several areas that require more detail and routes for further improvement. Given the importance of Public Acceptance in supporting the deployment of C-ITS in Europe the working group recommends that work is continued, to include focussing on the following topics:

1. Recommendation 1 focusses on the benefits of different stakeholder groups, in particular for the infrastructure and fleet owners; further work on establishing reliable and evidence based Cost Benefit Data is needed to strengthen the message.

2. Recommendation 2 stresses the need for factual messages addressing legitimate concerns related to C-ITS services. Further work needs to be done in defining clear non-technical messages on demonstrated solutions based on reliable evidence. Focusing on concrete use cases could help construct such clear messages.

3. Recommendation 3 addresses the impact difference between the optional or compulsory character of certain C-ITS services. Further work should look into the various mechanisms (e.g. incentives) to obtain a workable and acceptable solution finding the balance between societal and individual needs.

4. In view of the evolution towards an increasingly connected (and automated) transport system, further work needs to be done on public acceptance issues of non-connected road users – in particular those that are likely to remain non-connected.

12.6. Annexes

WG8 - ANNEX 1 - Stakeholder groups with acceptance factors_final_.doc

WG8 - ANNEX 2 - acceptance factors per user group.xlsx

13. Working Group 9 - Implementation Issues

13.1. Executive Summary

The C-ITS Platform Working Group on Implementation Issues dealt with a variety of practical issues of very diverse nature, faced at the moment of deploying cooperative systems in the EU through a series of meetings held between November 2014 and December 2015.

Work issues discussed during these meetings were structured around a package of "road safety-related issues", and a second package of "non-road-safety related issues" grouping a collection of very diverse topics.

The "road-safety related package" identified three work items in relation to the impact of C-ITS deployment on road safety: human machine interaction, non-equipped user, and training & awareness. WG9 developed recommendations in relation to the three of them. In particular, in relation to human machine interaction, WG9 produced a recommendation for the revision of the European Statement of Principle on Human Machine Interaction.

Most pressing topics covered in the "non-safety related package" of this report were identified on the basis of the presentations of challenges encountered by some of the first deployment initiatives and pilots in Europe. Despite the initial intent to distinguish between experiences in urban and non-urban areas, it became clear that a large number of issues are not specific to a particular geographical environment. Based on the discussions, WG9 developed recommendations regarding future work to be carried out in many different areas.

13.2. Objectives of the Working Group

The objectives of the C-ITS Platform Working Group on Implementation Issues were to investigate practical issues of very diverse nature, faced at the moment of deploying cooperative systems in the EU.

The draft work programme prepared by the European Commission prior to the launch of the C-ITS Platform, already identified a non-exhaustive list of issues such as "human machine interaction", "how to foster deployment", "the role of incentives" or "the role of legislation", as possible topics for discussion to be agreed with WG members.

A package of "road safety-related issues" was discussed during the first six sessions until May 2015. Three work items were identified in relation to the consequences for road safety derived from the deployment of C-ITS: human machine interaction, non-equipped user, and training & awareness.

After concluding the "road safety related chapter", and following a first discussion of the topics included the draft work programme, the group decided holding two sessions focused on (1) implementations issues linked to C-ITS deployment in urban areas and, (2) implementation issues linked to C-ITS deployment and infrastructure and corridors. Presentations and discussions held within the WG meetings showed that many of these

issues were not specific to one or the other geographical environment; hence recommendations regarding these topics were addressed independently from the geographical criteria.

Following this approach, this report presents two different chapters: the first one is dedicated to "road safety related issues", the second covers a collection of very diverse non-road-safety related topics. For each of them conclusions and recommendations agreed by WG 9 are highlighted.

Considering the remit of its work, WG9 covered issues which were, for some aspects at least, addressed in other WGs as well. In those cases, the link with other WGs' discussions was ensured through the WGs' Chairs. Where appropriate, topics were discussed in the different relevant WGs. For some issues the discussion was referred to the appropriate technical WG.

13.3. Organisation of Work

The organisation of work was based on regular face to face meetings (WG9 conducted a total of 11 face to face meetings from November 2014 – December 2015, in the course of the first phase of the C-ITS Platform), as well as several phone conferences to deal with specific sub-topics of the main work items. The physical meetings were also used to approve the WG Final Report or sections of the report.

DG MOVE representatives chairing WG9 meetings took care of ensuring close relationships with other Working Groups, keeping WG9 participants informed on issues being dealt by them and of interest for WG9 work items.

All results, outputs and expert recommendations of the C-ITS Platform WG9 have been produced, discussed and endorsed by the following nominated experts, representing the following organizations and countries:

Organisation	Name
ACEM	Vassileva Veneta
ADAC	Hecht Christoph
ASECAP	Kallistratos Dionelis
ASFINAG	Jandritsis Marko
Austriatech	Froetscher Alexander
BMW	Scholten Joachim
CH - FEDRO	Riederer Markus
Continental	Erdem Bettina
CTAG	Fernández José
	Martínez José Manuel
Car to Car Communication Consortium (C2C)	Andersen Niels
European Transport Safety Council (ETSC)	Carsten Oliver
	Townsend Ellen
European Cyclist Federation (ECF)	Woolsgrove Ceri
European Road Federation (ERF)	Diamandouros Konstantin

Organisation	Name
FEMA	Zee Anna
FIA	Brangeon Victor
BLERVAQUE Sprl	Blervaque Vincent
	Spaanderman Paul
IRU	Jeftic Zeljko
Member State (AT)	Molin Helge
Member State (BE)	Kenis Eric
	Pourtois Caroline
	Wayenbergh Aurelie
Member State (F)	Ollinger Eric
Member State (DE)	Gelau Christard
Member State (IRL)	Mc Carthy John
Member State (ROM)	Banica Sorin
Member State (SE)	Biding Torbjörn
	Marton Maria
Member State (UK)	Ferguson Anthony
	Hanson Graham
Municipality of Helmond	Blom Gert
POLIS	Hoadley Suzanne
PSA Peugeot Citroen	Servel Alain
TISA-SWARCO	Schmidt Andreas
TOM-TOM	Kamalski Theo
TNO	Malone Kerry
Transport for London	De Estevan Ubeda Natalia
VDA	Niedenthal Michael
VOLVO Group	Wahlund Jörgen
YAMAHA	Fisher Hennes

The following European Commission Services have been involved in WG9:

Services	Name
EC GROW	LAGRANGE Antony
EC MOVE	ALFAYATE Maria
EC MOVE	CARABIN Gilles
EC MOVE	DEPRE Claire
EC MOVE	LOPEZ BENITEZ Casto

13.4. Work items of WG9

The major obstacle for C-ITS deployment is that significant upfront investments are required both on the vehicle and the infrastructure level and that enhanced co-operation needs to be

established before any benefits will occur. Hence, synchronisation of actions is key, considering existing inter-dependencies.

C-ITS, indeed, is different from traditional ITS implementation because there is a need to put a substantial deployment of the systems in place, before return on investments becomes visible. Therefore, there is no 'bottom up' growth path with steadily increasing benefits of scale. Benefits are supposed to take off swiftly after a few years of continuous efforts but there will be little intermediate 'ribbon cutting' or intermediate successes to be celebrated.

Therefore, a long-term engagement from key stakeholders is absolutely critical, and an overarching shared vision and a roadmap for deployment need to be established. In this respect, WG9 members acknowledge the unique opportunity provided by the C-ITS Platform to play a role in developing, with all relevant public and private stakeholders, a shared vision on the deployment of C-ITS and paving the way for the development of an implementation roadmap.

Due to the horizontal nature of this WG, members faced the not easy task of prioritising among a vast amount of "implementation-related topics" to be dealt with during the first phase of the C-ITS Platform.

13.4.1 Road Safety Issues

This section presents a summary of the package of "road safety-related issues" discussed during the first six sessions until May 2015. Three working items were identified in relation to the consequences for road safety derived from the deployment of C-ITS: human machine interaction, non-equipped users, and training & awareness.

13.4.1.1 Human Machine Interaction

Driving safely requires that the driver is at all times able to perform the primary tasks required for driving. The deployment of C-ITS is likely to result in a more complex interaction between the driver and the machine with potentially negative consequences for road safety. In this context WG9 decided to discuss on the effects of C-ITS deployment on the human-machine interaction focusing the discussion on the European Statement of Principles on Human Machine Interface which was published as a European Commission Recommendation in 2008[18]. The group discussed whether, in light of the deployment of C-ITS a revision of the ESoP on HMI was required addressing the following questions in the discussion:

- How does the development of C-ITS influence/affect safety?
- What are the additional sources of distraction?
- Is the ESoP on HMI an effective instrument to achieve improved road safety?
- Is the ESoP on HMI still relevant in view of the technological developments?

[18] COMMISSION RECOMMENDATION of 26 May 2008 on safe and efficient in-vehicle information and communication systems: update of the European Statement of Principles on human-machine interface, OJ L 216, 12.8.2008, p 1.

- Are some relevant elements/topics missing?
- Is an update of the ESoP on HMI necessary?

The final report on this work item is included as WG9 ANNEX 1.

13.4.1.2 Non-equipped users

The working group discussed the potential consequences for road safety resulting from the co-existence of users equipped with C-ITS and other users not equipped with these technologies. The aim of the work was to identify specific safety problems or challenges and discuss if and how they could be addressed.

New cars are gradually being equipped with driver assistance technologies which may assist the driver in some tasks or even take control of the vehicle in an emergency situation. The deployment of C-ITS will result in more advance assistance systems made possible on the basis of communication between vehicles (V2V) or between vehicles and infrastructure (V2I).

The deployment of such systems will be gradual, which means that cars with very different levels of equipment will inevitably circulate at the same time. This situation is likely to be prolonged for a very long time. The fact that vehicles equipped with these technologies and other vehicles or users not equipped will share the road may give rise to some new risks, mainly related to user behaviour. The group addressed this topic on the basis of the following questions:

- What are the main safety challenges/risks that could result from the gradual deployment of C-ITS?
- Are these safety challenges and risks distinct from those raised by non-cooperative technologies?
- In order to speed the deployment of some of the C-ITS, should it be to some extent mandatory?
- Should the administration legislate to shorten the deployment period?
- Would this be justified on the basis of road safety?
- Is retrofitting possible? Could it be partly based on nomadic devices?

Safety challenges may appear in the initial phase of deployment, when few vehicles are equipped. This could happen if a vehicle fitted with a C-ITS performs in a way which is unpredictable or unexpected in relation to non-equipped vehicles.

Some C-ITS systems, e.g. congestion warning, can be beneficial for all road users already at low deployment rates, like for example 5%. The benefit results from the changes in the behaviour of non-equipped users induced by the changes in the behaviour of equipped users.

Safety problems may also appear when the deployment rates are very high, i.e. 80 to 90 %, since this could result in compensation strategies leading some drivers to take more risks on the assumption that all vehicles are equipped with safety systems.

The 'motorcycle approach indication' and possible systems for other vulnerable road users, were cited as an example of system which could result in a risky behaviour on the part of the motorcyclist, should he or she assume that all cars are equipped to receive and process the signal emitted by the motorcycle/vulnerable road user.

Finally, traffic rules may also need to be adapted in order to allow for the deployment of some technologies, for example to redefine the minimum distance to the preceding vehicle in case of truck platooning

13.4.1.3 Training and Awareness

Cars are being equipped with new technologies to assist with the driving task (ADAS) and to provide the driver with information related to the driving environment and to his trip. C-ITS will enhance the functionalities of driver assistance technologies and the quality and quantity of the information that can be made available to the driver.

Most drivers are not aware of the on-going deployment of the new technologies. Or they may have little or no knowledge about their functionalities, even when driving a car equipped with some of them. Members of WP9 discussed whether such a lack of awareness or knowledge may be problematic in relation to road safety.

The group identified some potential safety risks linked to the driver's lack of knowledge or awareness about the deployment and functionalities of C-ITS, false perception and over-reliance on the system, and ignorance on the non-continuity of the service whether this is due to the vehicle or to the infrastructure.

Most of the safety systems being deployed (e.g. emergency breaking) are conceived to assist and/or warn the driver in case of an emergency. Safety systems of this kind do not require specific training, although awareness of their functionalities is desirable.

In addition to emergency safety systems, driver assistance technologies are also being deployed. In the future partial automation will appear allowing the driver to rely on the vehicle for certain tasks. Most drivers are not aware of the on-going deployment of the new technologies, and may not fully understand the functionalities offered by driver assistance systems, their capabilities and, most important, their limitations. Moreover, even if these functionalities are well understood by the driver, he/she may have not been trained in how to use them, neither been exposed to their functioning in practice.

Members of WG9 discussed whether such a lack of awareness or knowledge may be problematic in relation to road safety. The group discussed also whether some measures could be taken to make users aware of the possibilities, limitations and challenges, brought by these new technologies, and if training concerning their use could be appropriate. The discussion was organised around the following questions:

- Could lack of knowledge or inexperience concerning driver assistance or information systems be a road safety problem?
- If so, is training on the functioning of driver assistance or information systems needed or desirable for drivers?
- Would training be needed for all systems or only for some of them?

- Which systems should be subject of training?
- How should training be implemented?
- Should training on driver assistance or information systems be part of the curriculum for the driving licence?
- Could simulation be used as a tool to expose drivers to dangerous situations and to the functioning of driver assistance systems?
- How could currently licensed drivers be reached?
- Could public awareness campaigns be useful?
- If training on driver assistance or information systems is required, what should be its content?

13.4.2 Recommendations /Follow Up Actions on Road Safety Issues

13.4.2.1 Human-Machine Interaction

As a result of the discussions, the group concluded that it is appropriate to revise the European Statement of Principles on Human Machine Interface (ESoP on HMI) because its content needs to be adapted to the current scientific knowledge, and the developments in the technology fitted to new vehicles. The group also agreed that the ESoP on HMI should keep its status as a Commission recommendation.

The aspects of the ESoP on HMI that the group recommended to update concern its scope, driver workload definition and possible limitation, the information provided to the driver, or the various forms of feedback.

Therefore, WG9 believes that the Commission should consider leading the review of the ESoP on HMI on the basis of expert advice and building on the work already carried out in the framework of the iMobility Forum.

Standards regarding functionality that require human machine interaction need to be developed in conformance with the principles of the ESoP. Relevant existing standards need to be evaluated before they are implemented. Many standards were developed prior to C-ITS, and may not fulfil all the requirements needed for a successful and sustainable implementation, especially in hybrid systems.

Detailed recommendations are included in Annex I.

13.4.2.2 Non-equipped users

The Working group agreed that the simultaneous presence on the road of vehicles equipped with the new C-ITS, and also non-cooperative ITS may create some safety challenges. However the working group did not identify major safety risks resulting from this situation.

The working group also concluded that the possibilities for action to accelerate the deployment of C-ITS technologies are limited, and recommended exploring possible measures aimed at compensating the safety challenges resulting from the co-existence of road users with various levels of C-ITS equipment.

The following recommendations were agreed upon:

- Promote research on the interaction between equipped and non-equipped users.
- Consider to adapt driver education to stress the importance of understanding that safety systems are not meant to take additional risks, but instead as a backup in case of human error or distraction.
- Consider the need to adapt traffic rules to the deployment of an increasing number of driver assistance systems (including C-ITS), which include more and more automated functions.
- Consider a retrofitting strategy, possibly based on nomadic devices, as a possible way of accelerating the deployment of critical safety systems, thus reducing the challenge of non-equipped users.
- Promote the sharing of safety-relevant information between, on the one hand infrastructure-based or equipped users and, on the other hand, non-equipped users, on the basis of nomadic devices or infrastructure based systems
- Make use of infrastructure-based C-ITS to compensate for non-equipped users, e.g. by providing them with safety-relevant information coming either from other vehicles that communicate with the infrastructure, or from infrastructure-based systems.

13.4.2.3 Training and awareness

The group agreed that many road users, including drivers, will not be familiar or aware of the functionalities, safety benefits and limitations of the new technologies, in particular C-ITS. The group agrees it is appropriate to make current and future drivers aware of these technological developments by reaching them through the most appropriate means, be it awareness campaigns or driver training, be it pre- or post- licensing.

The group agreed on the following recommendations aimed at avoiding road safety risks resulting from the lack of awareness of some road users concerning C-ITS and other driver assistance technologies:

- Make use of public awareness raising campaigns to inform road users about the existence, functionalities and limitations of the new technologies. E.g.: raise public awareness through actions taken by relevant stakeholders, like insurances companies and rating organisations (e.g. EuroNCAP).
- Adapt driving licence education to inform about the technologies that new drivers are likely to be confronted with, in particular safety-related ones, but also others, such as traffic management or eco-driving.
- Encourage post-license training, possibly linked to the acquisition of an equipped vehicle, to update drivers concerning the new safety-related technologies.
- Make use of periodic training for professional drivers to provide information and possibly training on the use of the new technologies.
- Encourage vehicle manufacturers to offer complete information on the new technologies fitted through sales agents, including for example a demonstration or training session as part of the sales package.

13.4.3 Other Implementation Issues: The Issues and Recommendations

WG9 discussed about the other implementation topics listed in the C-ITS Platform Draft Work Programme, though decided to map other relevant issues for discussion based on practical experiences from C-ITS pilot projects in urban and not urban areas. The issue of integrating C-ITS decisions for deployment within the long –term investment plans was also identified as an essential one to be addressed..

As explained in the chapter describing the objectives of the working group, WG9 members realised that the distinction between implementation issues linked to the introduction of C-ITS in urban, and non-urban areas was somehow artificial, and not fitting the purpose, since a large number of issues are not specific for a concrete geographical environment. Hence, recommendations presented below are in most cases, common to both geographical environments.

C-ITS Deployment issues

C-ITS are to be considered as an enabling technology, and not as an objective in itself. The way to go is still long, and there are still important challenges to the deployment of C-ITS, among them:

- The lack of hard evidence of benefits: How can C-ITS help to deliver policies?
  Why a C-ITS solution could be better than the already ITS existing ones?
  There is a need of a good business case: showing benefits in terms of policy, cost-effectiveness and performance over existing systems
- No clear understanding of the costs and lack of business models
- Legacy and integration: How can C-ITS build on existing investments?
- Legal and liability issues: Who is liable if a technology failure leads to an accident?
- Which are the missing standards, and how to address standard profiling

  Ensuring interoperability, and the role that cross-site tests could play on this, Coordination and knowledge sharing, Ensuring the coexistence of hybrid communication,

In urban areas, there is a shift in priority for ITS deployment from traffic control, to a tool for promoting travel behaviour change, hence a policy responsive instrument, once it is considered that no major scope for further efficiencies in traffic control are easily applicable.

Generally speaking, there is a poor understanding among the C-ITS community of the urban policy framework and factors driving procurement decisions: cities are comparatively more complex environments than corridors, strongly policy driven and risk-averse when it comes to new technologies. Furthermore, there is often inappropriate communication of C-ITS: excessively focussed on car driver benefits, while cities are not especially interested in this issue but on solutions for their transport problems, addressing sustainability, modal shift, in brief the potential of a standardised communication platform offering two way communication, as required for C-ITS.

In relation to corridors, despite the specificities linked to each of the individual corridors and other types of roads in which C-ITS services are being deployed/tested in the EU, there are

many more commonalities, barriers and enablers that stakeholders faced while implementing them.

Recommendations

In view of accelerating the deployment of C-ITS in the EU, financial support both from national and European levels will be essential. In this respect, WG9 strongly recommends the Commission to continue the on-going financial support of C-ITS deployment projects in the context of the Connecting Europe Facility. Furthermore, it is considered that all the existing, and upcoming projects, should engaged in the exchange of results and experiences through stable mechanisms.

The C-ITS Platform is providing, a unique tool for the engagement of key stakeholders. As deployment gets closer through the development of the shared vision by the C-ITS Platform, and the Masterplan and Roadmap by the European Commission, a reflection upon how the most appropriate instruments to ensure future stakeholders involvement should probably be considered. WG9 recommends to bring forward this exercise in the second phase of the C-ITS Platform.

13.4.3.1 C-ITS and infrastructure: Bridging the gap between long-term planning and C-ITS investment

Nowadays, information and communication technologies are a prerequisite for a well-functioning transport system. Intelligent transport systems contribute significantly to making it possible to meet today's mobility requirements of people and goods. The introduction of ITS solutions is partly steered via the EU ITS Directive and its Delegated Acts, and partly through the plans, choices of measures and investments made in EU Member States.

At the moment of phasing the deployment of ITS, EU national and regional road operators have to stimulate the transfer of knowledge, looking at the substantial impact this could have in central processes for infrastructure planning and investment. Research and innovation are also important areas, but must be clearly linked and aligned to the needs and requests of national/regional road operators and municipalities, as well as to those of the transport and automotive industries, and society in general.

There is currently a big gap within Member State's transport administrations, particularly between deployment (processes linked to the introduction and use of C-ITS by road operators), and research & innovation (processes and networks linked to research and innovation of C-ITS). This is valid, both in terms of knowledge, and insight into the contribution C-ITS-related applications/services can make towards solving known problems within the transport system.

ITS and more recently C-ITS, have benefitted from the European Research Framework Programmes since the late 1980s. However, the number of people from the planning departments of European Road Operators involved in this research is certainly very low. The mismatch between the long time planning period requested for the construction of road and railways (12-30 years), and that of C-ITS applications (much shorter, with a time span of about 2-5 years) represents an additional challenge.

Bridging the gap between long term planning and C-ITS investment requires actions, in order to develop methods and tools for raising the knowledge level within the C-ITS environment, and specifically to train employees in the planning departments of EU road operators and municipalities.

Recommendations:

WG9 recommends the Commission:

1. To take an active role in this area, teaming up with relevant partners, such as the Conference of European Directors of Roads (CEDR), to develop practical tools to be used in this direction.

2. To support public investment, by means of harmonised C-ITS pre-commercial procurement schemes, which could be as well an effective tool to help bridging this gap.

13.4.3.2 Building upon the stakeholder experience

Understanding the benefits: What's in it for me?

For some stakeholders, both public and private, it is not really clear, what role they can or shall adopt in a C-ITS environment*. They might lack to understand easily, how they can act in order to get "C-ITS benefits"*.

In fact there are many options, and all over Europe manifold choices are made. For instance, there are cities which are leading implementation and deployment, investing on their own infrastructure and fleets, and cities which promote the deployment through new business models for service and technology providers.

Somehow, an easy entry guidance would be helpful, and key examples would certainly help. For instance: showing for one bundle of applications different role scenarios, and why C-ITS still works seamless for travellers across different environments. Although, in any case, it has to be taken into account that, the final decision and allocation of roles lies with the stakeholders in different European regions.

To be successful in C-ITS deployment, decision makers must be presented a "tangible value" of what is achieved by the C-ITS applications in their specific context. Though not exclusive, this issue is of particular relevance for urban actors.

The right applications, their naming and the quantification of their benefits, e.g.: figures showing financial or resource savings, are key to take deployment decisions. Hence, there is a big potential on knowledge sharing among stakeholders, and especially among public stakeholders.

Recommendations:

1. The first clear recommendation from the analysis of the stakeholder's experience, is the need to use harmonised standards that ensure interoperability, and continuity of services through national borders. WG9 members stress the importance to keep in mind this guiding principle when developing the roadmap for the deployment of C-ITS in the EU.

2. Furthermore, the Commission should contribute together with other actors, to develop practical tools to support C-ITS deployment. For instance, tools like pre-commercial procurement could stimulate the roll-out of C-ITS at local, regional and national levels.

3. Experience from very diverse stakeholders underlines that two key issues to be considered when facing C-ITS deployment are “security” and “privacy”, both being dealt within the C-ITS Platform. WG9 members recommend the Commission to continue working in both areas in the upcoming phase of the C-ITS Platform.

13.4.3.3 Coordination and knowledge sharing

This issue is intimately linked to bridging the gap between long and short term planning, and it is essential for the deployment of C-ITS. When taking the first steps in the deployment of C-ITS in the EU it is vital reducing the risk of fragmentation and lack of interoperability by developing an EU-wide harmonised and synchronised implementation plan for C-ITS deployment.

WG9 members have found in this WG meetings in particular, as well as in many others of the C-ITS Platform, a very useful tool to share experiences obtained when implementing their projects and initiatives.

Sharing knowledge is a key element to ensure convergence of European/national/local C-ITS deployment activities. This could have a strong influence in order to build EU-wide C-ITS market and to create trust between policy makers, decision makers and investors, enabling a faster deployment of C-ITS.

Recommendations:

WG9 recommends the Commission:

1. To stimulate and support through the use of the appropriate tools, the development of guidance material, specially addressing public stakeholders.

2. In order to strengthen coordination among existing activities, to reflect upon the possibility of establishing cooperation mechanisms among existing activities, irrespective of their source of funding. In particular, it is considered of interest, to stimulate cooperation between at least two groups of Member States or cities, frontrunners and followers, to keep momentum, encouraging replication and ensuring scalability.

3. To work towards developing common methodologies for impact assessment of large scale tests and pre-deployment projects, as well as agreeing on a set of common key performance indicators. This "toolbox" could enable comparison and consolidation of results, and the development of an EU-wide common understanding on C-ITS performance & impact assessment and cost benefits.

13.4.3.4 Using the right language

C-ITS deployment relies on a large variety of stakeholders, from vehicle manufacturers to road operators, traffic planners, service providers, various other businesses and of course the users. All these stakeholders have different backgrounds, focus and different level of technical and strategic understanding of C-ITS. Dealing with such a heterogeneous 'audience' it is crucial to use the 'right language' for each of the parties involved.

Generally speaking, C-ITS developers tend to use a technical language with many acronyms and unknown expressions for the non-initiated ones, which make topics look very complicated. This situation happens as well between 'specialists' of different technical fields. A common and more 'simplified' language pointing out the key benefits, and/ or challenges only might help to understand the issues of the other parties.

Recommendations:

In order to bring some clarity (and increase accessibility) to C-ITS, WG9 formulates the following recommendations to the Commission, that could eventually be considered to undertake further work in the context of existing or new WGs in the upcoming phase of the C-ITS Platform:

1. To compile a list of "higher transport policy goal" statements and map them with the "Applications" as they have been defined by WG1
2. In the medium term target to write "C-ITS Application-specific White Papers". These papers would be a sort of "stakeholder specific implementation guidelines", for instance:
   - For cities and urban areas (maybe according to city sizes and typologies, e.g.: small medium and strongly connected urban area)
   - For freight transport
   - For vulnerable road users
   - For other groups which may be not in our focus now in Day-1, but could be in the future
3. Develop and maintain a 'language manual', listing the different stakeholders and describing their involvement in technical or strategic issues, intentions, expectations, concerns, etc, that could really become a first step to help paving the way from 'specialist-language' to a 'target focused single language' communication.

13.4.3.5 Which standards are available and what is missing?

Out of the discussions held in the context of WG9, it appears that there is a need for further standardisation beyond the "air interface". Both, the linkage of the C-ITS station to the backend infrastructure or to the vehicle were pointed out in several presentations held during the meetings. This includes architecture to define how information can find its way to the "internet" and even "broadcast" scenarios. In this respect, discussions shown that there are several approaches to standards implementation (e.g. in the C-ITS Corridor involving Germany, Austria and The Netherlands), and harmonisation will be required.

Recommendations:

1. It is essential that a test mode is foreseen from Day1 one onwards. This is needed to enable testing of new functionality in an operational environment without disturbing existing services.

2. "Profiling of standards" is a field on which there seems to be a substantial work to be undertaken. Unfortunately, time did not allow making sufficient progress into mapping the issue and future actions to be undertaken. WG9 recommends the Commission to continue exploring this area, in order to have a good understanding, and when appropriate transfer the issues identified to the appropriate technical WGs.

13.4.3.6 The "Hybrid" Issue: How to make with 802.11 p / mobile internet / 5G choices and still creating a workable system?

The working group took note of the concerns from road infrastructure operators with hybrid communication. They have uncertainties about the technology in which they should invest for C-ITS. For instance, technology progress in the medium-long term (10, 20 or 30 years) is uncertain. It is not fully clear where to focus the investments: regions, locations, hot spots with a high level of accidents or traffic jams, end customer visibility; where is the break-even for these services?; who is the driver of a technology?

So far, discussions have been focused on technical aspects, while organisational aspects have not been addressed, e.g.: Who issues contracts to the telecom network operators for an area or a region? Is there any experience known anywhere? These are topics that deserved being addressed in the follow-up phase of the C-ITS Platform.

Recommendations:

In view of the upcoming phase of the C-ITS Platform, WG9 recommends:

To elaborate on potential needs / lacks emerging from the "hybrid issue", including the organisational side of C-ITS. More concretely, consider organising some specific meetings where both technical experts and people involved in implementation issues could share their views, and help progressing in view to develop practical tools such as investment guidelines for cities in relation to which communication types are the best suited depending on the needs to be fulfilled through C-ITS applications.

13.5. Annexes

WG9 - ANNEX 1 - Road safety - Human-Machine Interaction.doc

14. Working Group 10 - International Cooperation

14.1. Executive Summary

International cooperation is fundamental for Cooperative Systems and worldwide markets have global players which therefore require global strategies.

The objective of the C-ITS Platform working group on international cooperation was to investigate and identify the areas in which international cooperation would benefit European stakeholders in view of the deployment of C-ITS in the EU.

An implementing arrangement for the cooperation in ICT applications to road transport between the European Commission and the US Department of Transport, and the Japanese Ministry of Land, Transport and Tourism is on-going since respectively 2009 and 2011. A lot of good work had been produced throughout the years in the context of this trilateral cooperation. In particular, the areas of security policy and harmonisation of standards are to be highlighted due to their relevance.

Nevertheless, at the moment of embarking into the development of a European strategy for the deployment of C-ITS, the WG10 on international cooperation was asked to reflect upon the international cooperation carried out so far, assessing whether the work should continue in the same areas or open new ones, whether new approaches should be established in existing areas, whether cooperation should be open with new countries/regions, etc.

A significant amount of progress has already been achieved and C-ITS is now moving, from research and pilot projects to the stages of early deployment. Such new activities have been recognised as an important driver to take into account when revisiting aspects and priorities for future international cooperation and new challenges that need to be addressed.

Issues including the role of governments, knowledge sharing, mapping existing cooperation bodies are regarded as priorities by representatives of governments of the different regions.

Technical areas identified by the Working Group as critical to continue cooperation are those in which the well-established dialogue has already brought substantial progress, such as communication and spectrum issues, and security and data protection. Furthermore, learning from collaboration: pilots, implementation and associated policies, as well as sharing information about regulatory frameworks, has also been identified as a priority area for international cooperation. WG10 has developed recommendations on all these areas.

14.2. Objectives of the Working Group

International Cooperation is fundamental for Cooperative Systems. Transport involves worldwide markets with global players and their associated global strategies. Global markets also generate savings for end users as they benefit from the resulting from scale effects and the availability of harmonised products and platforms. Both private and public players are conscious of the importance of cooperation, and have been actively pursuing it for many years.

The objective of the C-ITS Platform working group on international cooperation was to investigate and identify the areas in which international cooperation would benefit

European stakeholders in view of the deployment of C-ITS in the EU. Stakeholders can be addressed in two senses by looking into the benefits for end users and system owners/operators on the one hand, and European suppliers of components, complete systems and system services such as testing and compliance on the other.

Despite the fact that Europe is a leading worldwide players in the field of C-ITS, it should be recognised that other regions, such as the US and Japan, advanced their strategies for the deployment of C-ITS much faster than Europe. Hence, there are certainly lessons Europe could learn from such international experiences. This was the reason why in 2009 an implementing arrangement for the cooperation in ICT applications to road transport was applications signed between the European Commission and the US Department of Transport, which included C-ITS among its contents, and in 2011 the "Memorandum of Cooperation on Cooperative Transport Systems" between the European Commission and the Japanese Ministry of Land, Transport and Tourism (MLIT). Furthermore, a third similar agreement was also signed in 2010 between the US and Japan. In practice, these three cooperation agreements function as a trilateral cooperation between the three regions. Other countries, such as Australia, Canada or South Korea are associated to some of the task forces on C-ITS Security Policy included in this cooperation framework.

A lot of good work had been produced throughout the years in the context of this trilateral cooperation. The areas of security policy and harmonisation of standards can be specifically highlighted due to their relevance and implications in further work carried out in the different regions, as it has for instance be seen in the work of the C-ITS Platform WG5 on Security and Certification.

Nevertheless, at the moment of embarking into the development of a European strategy for the deployment of C-ITS, the WG10 on International Cooperation was asked to reflect upon the international cooperation carried out so far, assessing whether the work should continue in the same areas or open new ones, whether new approaches should be established in existing areas, whether cooperation should be open with new countries and regions, etc.

In carrying this task, WG10 has liaised and built upon the outcomes coming out from the other C-ITS Platform working groups.

14.3. Organisation of Work

The organisation of the work was based on regular face to face meetings (WG10 conducted a total of 4 face to face meetings from September – December 2015 in the course of the first phase of the C-ITS platform). In addition to the "regular" WG meetings, a special session with international guests took place back to back to the ITS World Congress in Bordeaux. This session with the participation of government representatives from the US, Japan, Australia and Canada, besides WG10 members, facilitated an open and informal exchange of views among the leading worldwide regions in the field of C-ITS, on the work done so far, and where the accent should be put in the future.

DG MOVE took care of maintaining relationships with other working groups and informing the WG10 participants of the feedback received regarding possible areas to begin/continue international cooperation. In particular, WG5 on Security & Certification provided very

valuable elements to progress international cooperation that are presented in the following section.

All results, outputs and expert recommendations of the C-ITS Platform WG10 have been produced, discussed and endorsed by the following experts representing organisations and countries:

Organisation	Name
C2C	ANDERSEN Niels
IAV	FICKEL Frank
Independent expert	SAMPSON Eric
BLERVAQUE Sprl	BLERVAQUE Vincent
Member State (DK)	SORENSEN Anders Bak
Member State (POR)	BARRADAS Pedro
Member State (SE)	MARTON Maria
Member State (UK)	FERGUSON Anthony
Q-Free	EVENSEN Knut
Swiss Transport Ministry	RIEDERER Markus
TISA/WDR	KUSCHE Thomas
VOLVO GROUP	ZAKIZADEH Hossein

The following European Commission Services have been involved in WG10:

Services	Name
EC CNECT	HOEFS WOLFGANG
EC MOVE	ALFAYATE Maria
EC MOVE	CARABIN Gilles
EC MOVE	DEPRE Claire
EC MOVE	MENZEL Gerhard
EC MOVE	TZAMALIS Georgios
EC MOVE	VAN DER LINDEN Geert
EC MOVE	VAN GAEVER Alain

14.4. Work items of Working Group 10

WG10 started the work by tacking stock of the past and ongoing activities with international players. An overview of the work carried out in the framework of the implementing arrangements signed by the European Commission respectively with US and Japan was provided. Group members, representing very different backgrounds, and interests,

acknowledged the importance and usefulness of the work carried out so far, in particular in relation to areas such as C-ITS security policy and harmonisation of standards.

An important aspect was underlined by WG 10 members, and later confirmed during the informal meeting with international guests held in parallel to the ITS World Congress in Bordeaux: the huge progress done so far on C-ITS requires a change in activities, moving from research and pilot projects to the stages of early deployment. This was recognised as an important driver to take into account when revisiting aspects and priorities for future international cooperation. This brings new challenges that definitively need to be addressed.

Issues like the role of governments, knowledge sharing, mapping existing cooperation bodies are seeing as a priority by representatives of governments of the different regions. Working on them could be a very good enabler accompanying cooperation in technical areas.

On the basis of the information shared on previous cooperation carried out so far, and bearing in mind that the overall objective of international cooperation is supporting European stakeholders in the early and future stages of C-ITS deployment, an open discussion followed on the following key topics:

- which were the areas and through which form of cooperation should be continued,
- which new areas should be looked at,
- which new regions should be looked at to start new cooperation,
- what type of new paths could be explored beyond "formal" cooperation frameworks

WG10 members developed a matrix to collect information from other WGs in relation to their requests for future international cooperation. In the process of internal and external discussions with members of other C-ITS Platform WGs, and multiple stakeholders, the original list of issues was reduced to the topics referred below, on which WG10, building on top of the input received, has developed conclusions and recommendations.

There is no surprise from the fact that on technical issues, areas identified as critical to continue cooperation are those in which the well-established dialogue has already brought substantial progress, such as communication and spectrum issues, and security and data protection.

14.4.1 Communication, spectrum and protocols

Communication can be seen as the basis of C-ITS: to allow effective data exchange through wireless technologies between vehicles or between vehicles and infrastructure, or vehicles and vulnerable road users. However, C-ITS are not the only services deployed on roads that require bandwidth in the radio spectrum.

For instance, in Europe, electronic charging and the enforcement of the digital tachygraphy operate in the 5,8GHz band, meaning that this frequency is used for the implementation of the Interoperability of Electronic Fee Collection Systems Directive (2004/52/EC), and the Decision on the Definitions of the European Electronic Toll Service and its technical elements (2009/750/EC). While on the other hand, the 5,9GHz frequency band is reserved for safety related applications (ITS-G5), through a Commission Decision (2008/671/EC). Hence, the latter is critical for the deployment of C-ITS.

Similarly, in the US, the Federal Communication Commission (FCC) allocated a 75 MHz band at 5.850-5.925 GHz especially intended for ITS: “to improve traveller safety, decrease traffic congestion, facilitate the reduction of air pollution, and help to conserve vital fossil fuels”.

Currently, existing road traffic safety critical applications in the EU have modest bandwidth requirements, but they have high concurrent requirements on short delay and high reliability. Co-existence between C-ITS and other wireless technologies, e.g., RLAN, in the 5.9 GHz band needs to be studied thoroughly and taken seriously. Interference from other wireless technologies in the 5.9 GHz band where road traffic safety applications are operating, can put lives at risk and raises serious liability questions.

It is important to notice that for safety critical V2V applications, dedicated short-range communications does not require the intervention of the infrastructure for the applications to work and ensure a consistent performance. It is also important to consider that the spectrum required can be used free of charge.

Although vehicles cross borders, they usually do not cross oceans. Nevertheless, for safety reasons and commercial benefit, the underpinning message protocols need to be harmonised. For OEMs, harmonisation on frequency bands and wireless technology on different continents are a request to facilitate road traffic safety and road traffic efficiency applications. The wireless technology, which is contained in silicon, is together with the antenna dictating the performance of the whole system. OEMs have been working with ITS-G5/IEEE 802.11p for many years now and they know both the weaknesses and strengths of the technology.

By having a harmonized wireless technology, the same performance of road traffic safety applications can be expected on different continents. Higher-layer protocols are not as crucial to be harmonised as the wireless technology. Those are in software and several protocols can be supported in a communication system. Message sets for traffic efficiency applications have been harmonized to a great extent between Europe and US already through collaboration between SAE, ETSI and CEN/ISO. For new upcoming applications such as cooperative adaptive cruise control, harmonisation is already in place and liaisons between SAE, ETSI, and CEN/ISO have been established, both formally as well as informally.

14.4.2 Security and Compliance Assessment

The agreed objective within the C-ITS Platform WG5 is to deploy one common C-ITS trust model all over Europe that shall support full secure interoperability at the European level. This trust model shall be implemented in a single trust domain version for the start-up Day 1 phase of C-ITS. Beyond the Day 1 phase, C-ITS may be extended with multiple interoperable trust domains if deemed necessary to take the variety of stakeholders and the responsibilities for private and public entities involved into account.

While this single trust domain in Europe is envisaged to be based on one common agreed certificate policy, it is currently not envisaged to implement the PKI (Public Key Infrastructure) with one single root certificate authority. This results in a definite need for international cooperation beyond Europe to discuss how interoperability of other domains (outside Europe) with the single European trust domain can be realized. This topic is even more relevant for the future (Day 2 and beyond) where the emergence of multiple trust

domains (moving away from a common certificate policy) in Europe may occur, making the topic and the stakeholder relations of the needed cross-certification even more complex.

Another important topic for discussion would be the harmonisation of the procedures or technical approaches of elements of the certificate policy or security policy of the trust model. Even if it is acknowledged that the design of these procedures is often related to the specific regulatory context, the harmonisation of procedures can enhance the international cooperation for C-ITS. This work could enhance the full life cycle of security, and in particular interoperability, between different root systems.

The EU-US Task Force has already achieved a significant amount of progress in HTG6 (Harmonisation Task Group 6) that has also been considered in the C-ITS Platform. Alongside the recommendations of the C-ITS Platform, the reports of HTG6 give recommendations on how interoperability between different regions could be achieved.

Compliance assessment is needed for assuring interoperability and minimum performance of equipment. The international dimension is needed to avoid suppliers having to conform to different test regimes in different parts of the world, something that would increase costs and greatly hamper the deployment of C-ITS.

14.4.3 Learning from Collaborations

Learning from collaborations with partners within the same geographical region or at international level also represents a key asset for future progress.

In this respect, at least two distinctive areas could be distinguished: learning from pilots, and learning from implementation and associated policies. A third potential area of growing importance as we progress towards higher levels of vehicle automation, would be the regulatory framework.

14.4.3.1 Learning from Pilots

C-ITS pilots are considered as a key step in the preparation of large scale deployment of C-ITS services by all countries committed to implement C-ITS solutions as part of their transport and mobility policy. By bringing together stakeholders representing public authorities at different levels, industry, research and users to experiment innovative C-ITS solutions in real-life conditions, pilots create a unique opportunity to set up long term partnerships within the C-ITS ecosystem, with the objective to assess multiple impacts (safety, traffic efficiency, environment, socio-economic…), and to deliver clear evidences about associated benefits.

Pilot results are of great importance to develop common understanding on deployment scenarios and potential issues to be addressed before moving towards large scale deployment. In this respect, WG10 members agreed that pilots are a great source of information to feed knowledge sharing ambitions, and European stakeholders can highly benefit from pilot experiences gained from abroad.

To date, several countries in Europe and in other regions are running C-ITS pilots. For instance in Europe: France, Germany, Austria, The Netherlands, Finland, Sweden, Denmark, Norway, the Czech Republic, the UK, Spain, etc. in some cases co-financed with EU funding, but in others just relying on national funding. And overseas: the US, Japan, South Korea.

Other countries are on their way to launch C-ITS pilots such as Canada, China, Singapore and Australia.

Learnings from pilots open opportunities in many different fields and directions, such as:

- Technical
    - Testing in real life conditions to assess real performances of C-ITS services
    - Evaluation methodology (adoption of harmonised methodology facilitates consolidation and comparison of results from different pilots)
    - Data collection and management (how to deal with scalability from small scale to large scale)
    - Improvements of standards ("learning by doing")
- Organisational
    - Long-term partnership between public and private stakeholders
    - Governance for successful C-ITS service operations
    - Legal aspects for C-ITS pilots on public roads
- Political
    - Facts on impact assessment and evidence on benefits to shape C-ITS transport policy and to take fully informed decision on large scale deployment
    - Awareness raising of policy makers
- Commercial
    - Awareness raising of decision makers, investors and end-users
    - Pre-commercial procurement of C-ITS equipment
    - Business models with all stakeholders along C-ITS service chain
    - Business opportunities when demand meets with supply

14.4.3.2 Learning from Implementation and Associated Policies

Large scale implementation of new C-ITS systems on roads, which in many cases are administrated and financed by the public sector, requires substantial public funding, and hence acceptance from a policy making perspective. However, policy makers can sometimes have a sound scepticism and reluctance towards allocating money to new and not fully proven technologies.

Furthermore, the big challenge about C-ITS systems is their need to be interoperable across borders, allowing a continuity of service levels to gain full benefits from the investments. Hence, there can be a tendency to wait for other partners to be first movers and settle the technology and standards to be used in order to be sure that you "bet on the right horse" when you invest in C-ITS systems.

In reality, C-ITS technology and standards are maturing, and the risk of ending up with a fragmented and non-interoperable system a few years after investment is probably decreasing. However, there is still a long way to go, and learning from experiences beyond pilot projects and early deployment initiatives around the world, touching upon how policy makers in the different regions are approaching deployment can be most beneficial, and have a positive effect in the willingness and readiness to invest in C-ITS deployment in the near future.

The EU and the US are fully conscious of the importance of cooperation among administrations in relation to C-ITS deployment, set up two years ago an exchange on evaluation findings and successful deployment practices between the European Commission and the US DoT, first on an informal basis, later formalised as a Working Group within the existing EU-US Framework for Cooperation on C-ITS. Following the informal discussions held with representatives of other regions, there seems to be room and real interest, to consider the enlargement of this exchange beyond the US and Japan.

14.4.3.3 Sharing information about Regulatory Frameworks

This third possible area of learning from collaboration could be seen more as a clear follow up to the two earlier ones, in the format of "fact-finding" exercise, as we move from connected mobility towards connected and highly automated vehicles.

14.5. Recommendations/Follow Up Actions

14.5.1 Main high level WG10 Recommendations

The working group strongly recommend focusing future international cooperation on those aspects closer to deployment, which might not fully coincide with those included to date into the existing inter-regional cooperation.

14.5.2 Specific recommendations of the single work items presented above

14.5.2.1 Communication, Spectrum and Protocols

On the basis of the reasoning presented in the presentation of this issue in section 3, WG10 recommends that:

1. For the existing frequency allocation in 5.9 GHz:
    - Seek international cooperation for protecting the spectrum
        - Joint studies of potential sharing with other systems,
        - Forming joint positions on sharing
    - Working with new market for adoption of 5.9 GHz as the band for C-ITS
2. Seek international cooperation towards a common global allocation for additional spectrum for future C-ITS application.
    - Joint studies on spectrum needs
    - Joint research and result sharing on feasibility of using frequencies, e.g., the 63 GHz range

14.5.2.2 Security and Compliance Assessment

Security:

Recommendations regarding Security have been presented in the previous section.

Compliance Assessment:

Building upon the conclusions and recommendations of WG5 on Security, WG10 emphasises that the recommended C-ITS compliance assessment process of the C-ITS Platform WG5 should be discussed at international level, in order to identify areas where harmonisation is

needed. This topic is very tightly linked to the overall process of enrolment, operation with upgrade and decommissioning of C-ITS stations in the network to ensure that the envisaged levels of interoperability, safety and security are met.

Closely linked to the C-ITS compliance assessment process, the overall topic of defining the different elements and services comprising C-ITS has been discussed within the C-ITS Platform. It is of crucial importance, to bring this broad topic to an international level, for example in order to ensure a common understanding of *WHAT* and *HOW* C-ITS services are expected to function.

At the same time the mutual recognition of C-ITS station setup and start procedures between Europe and international partners, can be an agreed topic included in the compliance assessment, and used to support market access in non EU countries.

14.5.2.3 Learning from Collaborations

Pilots

In addition to the role of the C-ITS Deployment Platform to actively support ongoing cooperation on European C-ITS pilots, WG10 members consider of major importance to expand this cooperation outside Europe, where knowledge sharing could bring many benefits to European stakeholders.

WG10 recommends the Commission to encourage the exchange on technical, organisational and political learnings coming out of pilots in different regions, while other aspects more closely linked to commercial issues could be addressed by the private sector in parallel.

Implementation and associated policies

In line with the discussions held with international partners, WG10 members recommend the Commission to enlarge cooperation on deployment practices at government level with other regions, such as Canada, Australia, and beyond with South Korea and other countries. As it came out from the discussions held with representatives from these regions, cooperation could be stimulated and carried out on informal basis.

It is suggested that a first basic, though very useful tool, could be mapping all the existing frameworks/ bodies/organisations currently involved in international cooperation, as well as the areas covered by them.

Regulatory Frameworks

In line with the description presented above and considering that this an area that is in a "taking off stage", WG10 merely indicates the convenience to closely follow international developments in this field, in coordination with other initiatives, on-going or to come, in the field of automation.

15. Conclusion

Based on the commitment and dedication of all its public and private members, the outcome of this first phase of the C-ITS Platform contributes effectively to a common vision on the coordinated and interoperable deployment of C-ITS in the EU.

Many conclusions of the C-ITS Platform working groups bring concrete answers to initial questions on why, how, where, when, by whom and which C-ITS services should be deployed in the EU and also propose follow-up measures to further work on and accompany this deployment.

A first general conclusion that can be drawn from the activities of the C-ITS Platform is that a coordinated action in the EU is paramount: a unique legal and technical framework is essential and coordinated efforts to ensure quick uptake of C-ITS are requested.

A second general conclusion is urgency: the technology is ready, the industry is already deploying C-ITS equipped vehicles in other parts of the world and announced to be ready to deploy in the EU by 2019, provided that the above-mentioned framework is in place sufficiently in time.

Regarding access to in-vehicle data and resources, a scenario-based analysis on legal, liability, technical and cost-benefits aspects is required to further progress and also to help answering legislators' request regarding an open-access platform.

The members of the C-ITS platform welcome the work achieved during this first phase that has benefitted from such an inclusiveness process and suggest following the same methodology when addressing further the remaining issues, implementing the agreed recommendations and start considering vehicle automation and related road infrastructure issues.

The C-ITS platform members are calling the European Commission to build on these conclusions and the outcome of the C-ITS Platform when envisaging further actions and measures in order to, without delay, actively guide the interoperable deployment of C-ITS in the EU with clear timeline, goals, objectives and actions.

This report of the C-ITS platform has been endorsed by nominated experts, representing the organisations and countries listed in the Register of Commission Expert Groups[19]. On an ad hoc basis, individual experts have been invited to participate in the work of specific working groups and are listed in the attendance list of each working group.

[19] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3188