Access to In-vehicle Data and Resources

Final Report

Written by Authors M McCarthy, M Seidl, S Mohan, J Hopkin, A Stevens, F Ognissanto
Project Manager N Kathuria
Technical Referee R Cuerden
[May – 2017]

TRL

EUROPEAN COMMISSION

Directorate-General for Mobility and Transport
B – 1049 Brussels

Offices:
Rue J.-A. Demot, 24-28
B – 1040 Brussels

Contact:
E-mail: move-infos@ec.europa.eu
Tel: **00 800 6 7 8 9 10 11** (toll-free)

Europe Direct is a service to help you find answers to your questions about the European Union.

Freephone number (*):

00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

LEGAL NOTICE

The information and views set out in this study are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

More information on the European Union is available on the Internet (http://www.europa.eu).

Luxembourg: Publications Office of the European Union, 2015

© European Union, 2017
Reproduction is authorised provided the source is acknowledged.

Printed in Belgium

IMAGE(S) © TRL, 2017 (UNLESS OTHERWISE SPECIFIED)

Contents amendment record

This report has been amended and issued as follows:

Version	Date	Description	Editor(s)	Technical Referee
1.0	18/05/2017	Final Report	Mike McCarthy	Richard Cuerden

Framework Contract No: MOVE/C3/SER/2015-344/S12.736158
Document number: CPR2419
Prepared By: TRL
Quality approved: N Kathuria (Project Manager), Richard Cuerden (Technical Reviewer)

Executive Summary

Automotive technology is advancing rapidly along a path to automation, with vehicles generating, storing and using greater quantities of data to monitor and activate system functionality in order to provide benefits for drivers, passengers and other road users. The data generated have the potential to support a large market of services and the way in which this market develops over the coming years will have potentially large effects on how and who can access and exploit the data. This will affect both existing services and stimulate new services and although the size of the future market(s) cannot be accurately estimated, these are expected to be significant.

For nearly a decade, there have been calls for the way in which in-vehicle data are made available to be defined and make it accessible. For example, Priority area IV of Directive 2010/40/EU[1] and the recent eCall type-approval Regulation (Regulation (EU) 2015/758[2]), both require definition of measures to achieve a secure and open platform on which services can be offered. In particular, the Platform for the Deployment of Cooperative Intelligent Transport Systems in the European Union (C-ITS Platform) established Working Group 6 (WG6) to examine the potential ways to give access to in-vehicle data and resources in order that service providers could propose services based on this data to their customers.

WG6 proposed three technical solutions for the access to in-vehicle data and resources. These comprised the following technical architectures:

- Data Server Platform
- In-vehicle Interface
- On-board Application Platform

Key features of the *Data Server Platform* concept are that the data from the vehicle is sent to a back-end server where it can be made available. Therefore, both the vehicle data and the application using the data are outside the vehicle system. Access to data using an *In-vehicle interface* is enabled via an upgraded OBD interface inside the vehicle; any application using data would run outside the vehicle system, either on an external device or on a layer on the interface itself. Finally, the *On-board Application Platform* would allow access to vehicle data and the execution of applications inside the vehicle environment.

WG6 also described three derivatives of the *Data Server Platform*: the *Extended Vehicle*, which proposed direct access via an ISO-standardised interface from the vehicle manufacturers' back end servers; the *Shared Server*, which proposed access from a server controlled by a consortium of stakeholders (rather than the vehicle manufacturer) with an equivalent link to the vehicle; and the *B2B Marketplace*, which proposed an additional layer between the vehicle and the service providers, which would be fed by vehicle manufacturers' back end servers, but be maintained by a service provider that would facilitate access by the market.

[1] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32010L0040

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

Furthermore, the WG6 report[3] presented:

- two methods of *defining the data made available* irrespective of the technical architecture, with this either being determined by the development of use-cases describing the purpose of the application and the specific data needs, or access depending on applications, which implies availability of a larger dataset with access based on a list of data parameters described in the terms and conditions of each application; and
- ACEA's proposed categorisation of use-cases which described access to data for applications (other than those regulated or C-ITS 'day one' applications[4]) using a *negotiation model* that allowed access to data on the basis of terms and conditions agreed between the car manufacturer and the third party.

In order to further progress and to assist the legislator's request, the aim of this study was to provide further guidance on appropriate actions and to:

- identify and quantify legal issues relating to: the two methods of defining which in–vehicle data are accessed (use-cases or application-dependent access), the negotiation model proposed by some stakeholders, and the three technical solutions and their different technical implementations put forward by Working Group 6 of the C-ITS Platform;
- assess the technical aspects of each solution (based on a review of literature and standards, through consultation with stakeholders and engineering expertise) to recommend the most suitable specifications and technical requirements;
- carry out a cost-benefit analysis (CBA) of direct and indirect economic, social and environmental impacts; and
- develop and analyse a set of scenarios, taking into account the market development, the current EU, national and international legislations and the work of the Working Group 6 of the C-ITS platform.

This study did not define the size of the future market for in-vehicle data, but assessed these as being very significant and considerably greater than the cost of implementing any solution. Costs and impacts for individual stakeholder groups were defined from limited objective data, and were also informed by qualitative analysis to scale the expected effects.

This study developed a series of options that could be implemented to address the issues identified with a range of possible technical solutions. Due to the large scope of these technical solutions, the level of objective data available and uncertainty regarding the size of future markets and their data needs, these options have been framed at a relatively high level.

This report assesses the legal, technical, and cost-benefit implications of the most likely scenarios for access to in-vehicle data and the associated resources in the near future (next two to five years), with the objective to address the risks related to the baseline scenario and to ensure the materialisation of an interoperable, standardised, secure, and open-access platform.

Concerning any possible policy measure, in a currently highly evolving market, the study recommends firstly monitoring how the eventual technical solutions selected by the

[3]http://ec.europa.eu/transport/sites/transport/files/facts-fundings/tenders/doc/specifications/2015/s248-450626-annex6-report.pdf

[4] A list of 'Day 1 services' agreed by the C-ITS Platform that, because of their expected societal benefits and the maturity of technology, are expected to and should be available in the short term

market comply with the five guiding principles agreed by WG6. If any action by the Commission is deemed necessary for a specific technical solution, such action should be subject to an exhaustive impact assessment. The assessment must include a thorough cost-benefit analysis of several policy options; one of them covering the inclusion of specific technical requirements and administrative provisions in relevant EU legislation(s).

Overall, the main findings of this study can be summarised as:

Legal

- Each of the WG6 solutions could in principle work within the existing legal framework. However, each option is likely to give rise to a range of legal obstacles that will need to be navigated by market participants and there is a risk that the current legal framework may allow the market to develop in a way that is inconsistent with the five guiding principles agreed by WG6 and with relevant European legislation in general (e.g. competition legislation).

- From a strictly legal perspective, there are no significant differences between providing access to data based on use-cases or providing access to data depending on the terms and conditions in the applications. However, the legal analysis is more supportive of access to data on the basis of use-cases, because the purpose of the data is well defined, meaning that it may be easier for data subjects to give consent that is more specific as to the purposes for which the data can be used.

- The primary legal challenge of the negotiation model is its interaction with competition law. Existing law should in theory be sufficient to ensure fair and undistorted competition. However, although legal protection against anti-competitive behaviour exists, the practical application of this law is very complex. The model of access to in-vehicle data should ideally mitigate the concentration of power with one group of market participants to prevent the situation where, before competition law can be effectively applied, the market has already been distorted to the detriment of consumers.

Technical

- This study found that all solutions proposed by WG6 are technically feasible, but no one solution satisfied all guiding principles agreed by WG6.
    - The data server platform derivatives cannot support real-time data, whereas in-vehicle interface and on-board application platform have access to real-time data. This could be an increasing issue in the future as more applications demand real-time data.
    - Data server platforms result in access to the Human Machine Interface (HMI) in the vehicle being more limited, although a level of access is possible if accesses to the HMI via mobile platforms are relied upon. However, the on-board application platform provides equal access to the vehicle HMI and is most compliant with the guiding principle on fair and undistorted competition.
    - The investment required for safety and security, while being a pre-requisite for all technical solutions, is greater for the on-board application platform and in-vehicle interface than it is for the data server solutions.

Key areas for safety and security are development of a security layer and the implementation of a hypervisor[5].
    - Largely due to the effort required to improve security, data server solutions are estimated to be able to be implemented sooner (1-2 years) than the in-vehicle solutions (approximately 5 years)
    - All technical solutions currently exist in the market with advantages to specific stakeholder groups; therefore although the technical solutions were assessed individually, the later scenario analysis also considered the effects of the existence and development of different systems in parallel.

- The main challenge is in balancing the demands of safety and security with fair and undistorted competition, whilst ensuring that any interventions are proportionate and do not inflict unreasonable burdens on market participants.
    - Key areas for safeguarding fair competition are ensuring equal access to resources (HMI) and data (both in terms of types of data available and timeliness) and avoiding the ability of any one participant to delay, dilute or deny access to data.
    - Safety and security is required for all solutions and was cited by some stakeholders as a reason to favour a data server technical solution. This is because the development of a suitably secure in-vehicle interface could have potentially large impacts on the automotive industry.

- Irrespective of the specific in-vehicle data access model implemented, several 'horizontal issues' can be identified:
    - Standardisation of data so that data from all manufacturers can be used by the wider market to encourage innovation.
    - Whether data is accessed by the market on the basis of a list of application-dependent data (i.e. the application provider has access to all available in-vehicle data and the user consents to access particular data elements depending on the application) or on the basis of use-cases (i.e. specific pre-defined data is available for applications with a particular purpose), both these approaches could be served by a minimum data set (i.e. a list of data parameters that allow the majority of services to be developed).
    - TRL note examples of the minimum dataset concept being successfully established in regulation elsewhere (e.g. CPR 49 Part 563 in the US[6]) and this approach would be favoured by certain stakeholder groups. However, even with such an approach, a mechanism to establish access on the basis of new use-cases or the addition of data elements to the agreed dataset would also be required in parallel so that innovation is not stifled by being limited to a specific dataset.
    - Ensuring actions on standardisation, the timely agreement of data and/or a minimum dataset is considered to require intervention at EU level to bring these about.

[5] A hypervisor manages the separate execution of software tasks; in this context allowing the management of messages to vehicle ECUs and the prevention of unauthorised access to safety-critical ECUs or to functions that are not authorised for the application.

[6] US minimum specification for data recorded by Event Data Recorders (EDRs)

Impact Assessment

- Overall socio-economic benefits of each of the technical architectures are dependent on the specific application(s) implemented that use the data and the effectiveness of these at bringing about improvements in safety and/or environmental performance. Access to in-vehicle data could support a large number of existing and new services; for example remote diagnostics and prognostics, pay as you drive insurance, incentives to the driver to access particular automotive services based on location, etc. These services have massive potential benefits, many times greater than costs required to implement access to data in the market. From this perspective, the action to implement access to in-vehicle data is proportionate because the estimated benefits far outweigh the costs of implementing any model of accessing the data.

- An assessment of the costs of the various components of systems for access to in-vehicle data were compiled from the literature review, known sources of data on the costs of ITS components and from stakeholders consulted during this project. A qualitative comparison of the costs involved in developing, setting up, operating and maintaining the various elements of the technical solutions resulted in similar, relatively low cost levels for each of the data server solutions. Higher cost levels were estimated for both the on-board application platform and the in-vehicle interface, largely because of the cost of technical development and the cost of equipping and maintaining 12 million new vehicles each year across Europe.

- Remote access to in-vehicle data and resources obtained using any of the architecture solutions provides some benefits that are applicable to all stakeholders. These include the ability to provide new and more efficient services, which benefit all of the stakeholders involved, as well as society in general. Examples are safety and environmental benefits of driver training tailored to the individual and customer relationship management. Set against these overall benefits, some stakeholders warned that there are potential risks to security and safety involved in any method of obtaining in-vehicle data and that the system established to access in-vehicle data could have large effects in terms of market fairness and equality.

- The stakeholder preferences, which were indicated by their responses to the consultation, showed that for several stakeholder groups there is a preference for the On-Board Application Platform. Whereas vehicle manufacturers would prefer a data server solution combining the 'extended vehicle' concept with a neutral server, and road authorities (according to their stakeholder responses) would prefer any of the other data server solutions.

- Directive 2010/40/EU[7] (the ITS Directive) sets out the principles for specifications and deployment of ITS in its Annex II. The extent to which the individual technical solutions comply with these principles is an indication of the extent of their compliance with the principles of the ITS Directive. These and a number of other important factors were rated based on the information available to provide

[7] Directive 2010/40/EU of the European Parliament and the Council on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport. Official Journal of the European Union, L207 6 August 2010.

the overall impacts. In these qualitative assessments, the rating scale ranged from --- (most negative) to +++ (most positive).

Impacts	On-Board Application Platform	In-vehicle Interface	Data Server - Extended Vehicle	Data Server - Shared Server	Data Server - B2B Marketplace	Extended Vehicle/ Neutral Server
Component costs	---	---	+++	+++	+++	+++
Consumer choice	+++	+	---	++	++	++
Competitiveness	+++	---	---	++	++	++
SMEs	--	--	--	++	+	++
Public authorities	---	---	0	-	0	-
Innovation and research	+++	+++	+	+	+	+

Compliance with the principles of the ITS Directive	On-Board Application Platform	In-vehicle Interface	Data Server - Extended Vehicle	Data Server - Shared Server	Data Server - B2B Marketplace	Extended vehicle/ Neutral Server (ACEA proposal)
Effective	+++	+++	+	+	+	+
Cost-efficient	---	--	+++	+++	+++	+++
Proportionate	+	+	+++	+++	+++	+++
Support continuity of services	+	+	+	+++	++	+++
Deliver interoperability	+++	+++	+++	+++	+++	+++
Support backward compatibility	0	+	++	++	++	++
Respect existing national infrastructure and network characteristics	0	0	0	+	0	+
Promote equality of access for VRUs	0	0	0	0	0	0
Support maturity	+	+	++	+++	+++	++
Deliver quality of timing and positioning	++	++	0	0	0	0
Facilitate inter-modality	++	++	0	0	0	0
Respect coherence	0	0	+++	0	0	+++

The technical solutions proposed by Working Group 6 were assessed against the guiding principles in order to identify the degree of compliance and to highlight areas that might warrant measures to mitigate the risks identified.

Technical solution	Data provision conditions – consent	Fair and undistorted competition	Data privacy and data protection	Tamper-proof access and liability	Data economy
On-board Application Platform					
In-vehicle Interface					
Data Server – Extended Vehicle					
Data Server – Shared Server					
Data Server – B2B Marketplace					

Assessment of compliance with WG6 guiding principles	**Rating**
Compatible with guiding principles	
Minor issues with compatibility or issues that could be addressed with low cost/impact	
Issues with compatibility or issues that could be addressed with medium cost/impact	
Significant issues with compatibility or could be addressed with high cost/impact	
Incompatible with guiding principles in current form	

Scenario-based Analysis

Four scenarios were assessed based on assumptions about the current market and possible measures to implement short- and long-term architectures to provide an interoperable, standardised, secure and open-access platform for access in-vehicle data and resources. These scenarios and their rationale are as follows:

Scenario	Rationale
Scenario 0 – No action (Extended vehicle/neutral server; the baseline scenario)	If there is no market intervention, the 'Extended Vehicle/Neutral Server' proposed by ACEA is expected to become established (alongside proprietary On-board Application Platforms) as the predominant technical solution.
Scenario 1 – Scenario 0 with measures at European level to accompany market development and address risks	Supporting measures to ensure that the Neutral Server aspect of the technical solution is implemented and a range of further measures designed to mitigate the risks of market distortion.
Scenario 2 – Short term: Shared server	The Shared Server solution could be encouraged in preference to the Extended Vehicle/Neutral Server concept. This maintains the short-term security of the vehicle and does not place large additional burdens on the automotive industry while on the other hand providing, with the addition of interventions at European level, features more aligned to delivering fair competition than the Extended Vehicle/Neutral Server.
Scenario 3 – Long term: On-board application platform	For this solution to be implemented and to result in an interoperable system, it is strongly recommended that legislation will be necessary. In the longer term (up to 5 years before it is accessible to the market), the On-board Application Platform could be encouraged because this provides all market participants with access to real-time data and the vehicle HMI and is therefore the solution with features most aligned to delivering fair and undistorted competition. We acknowledge the safety and security challenges of this solution (the burden of which lies with the vehicle manufacturers), but measures could focus on limiting access to non-safety critical data and using an "if fitted" approach. This could also be implemented in phases to provide adequate time for manufacturers to integrate the required technical development into their existing E/E versions/model cycles.

For each of the four scenarios considered, options for interventions at European level were described that could improve compliance with the five guiding principles and mitigate the risks identified. These measures can be summarised as follows:

Scenario	Measure	Rationale
1, 2 and 3	Monitoring of how consent is obtained and managed	To ensure that all market participants have the ability to gain consent and this can be given for a specific user, or for each journey, and that consent can be revoked by the user at any time
1, 2 and 3	Supporting the emergence of a standardised and customer-friendly approach for providing consent	To suggest legally acceptable standard procedures and making available suitable standard contract clauses

Scenario	Measure	Rationale
1, 2 and 3	Clarification of which data is made available to the market and the timescales in which it is made available in terms of: 1. Equal quality of data (update frequency, resolution, latency etc.) available to all market participants ; 2. A harmonised minimum dataset, covering at least the data needs of existing and short term use-cases could be standardised; and 3. A requirement that a reasonable request for data could not be rejected by any vehicle manufacturer. A system similar to the SERMI scheme could be used to ensure that requests originate from appropriate third parties.	To ensure that as far as is allowed by the characteristics of the specific technical solution that the relevant data is available at the same quality and timeliness to all market participants
1, 2 and 3	Mandating timescales for access to the OBD port while the vehicle is in motion for regulated parameters and remote diagnostics for all market participants	To allow market participants that would be affected by the closure of the OBD port while the vehicle is in motion or restriction on the data parameters available sufficient time to adapt their business models
1, 2 and 3	Measures to verify that the design of the vehicle electric/electronic (E/E) architecture delivers an appropriate level of functional safety and cyber security	To ensure that the security of the E/E system has been appropriately designed with functional safety and cybersecurity risks in mind
1, 2 and 3	Provision of specific safety performance guidelines for HMI design	To address risks resulting from driver distraction
1, 2 and 3	Measures to encourage the standardisation of data	To ensure that the data is interoperable
1	Formalisation of the 'Extended Vehicle/Neutral Server' solution in voluntary agreements or legislative requirements	To guard against a 'roll back' to the Extended Vehicle solution which does not include the neutral server that makes the party accessing data anonymous to the vehicle manufacturer
2	Legislation to achieve the implementation of the Shared Server solution	It is considered that legislation is required to fully implement this technical solution in the market over and above the baseline extended vehicle/neutral server model.
2	Encourage the formation of a consortium of relevant stakeholders	To put in place the necessary architecture to deliver the shared server
3	Legislation to achieve the implementation of the On-board Application Platform	This could be achieved by making the provision of an open on-board application platform mandatory for every connected car or mandated if an on-board application platform is implemented in a new vehicle model and used by the OEM to offer aftermarket services.

Scenario	Measure	Rationale
3	Ensure equal access to the vehicle HMI	To support fair competition and reduce the risk of the market being distorted, the access to the vehicle HMI should be ensured for all market participants
3	Support the provision of a documented API and an SDK for software developers	To ensure that the programming interface is clearly defined and that a software development kit is available to facilitate the offline development of applications in the same environment as that when installed on the on-board platform
3	Non-discriminatory compliance guidelines that clearly define the process, timelines and acceptance criteria (safety, security, technical performance, content, design, commercial and legal aspects) applied for the pre-deployment application check and approval by the OEM. This could be supported by defining a fair process for arbitration in case of disputes	To ensure that the certification process for applications is defined in a transparent way and that there is a mechanism to deal appropriately with disputes
3	Supporting the development and implementation of automotive cyber-security standards	Development of effective and standard approach to cybersecurity to mitigate against this risk and ensure that a common design requirement is met
3	Encourage the development of a single, interoperable platform	To standardise the platform such that developers could deploy applications across brands thereby avoiding fragmentation of the market and maximising exploitation potential

All technical solutions currently exist in parallel. Therefore, any implementation scenario should:

- take account of the characteristics of the market and the timescales within which these desired objectives should be achieved;
- consider actions across all technical solutions such that if measures are implemented for one solution, measures should also be applied to other technical solutions where this is appropriate; and
- be compared against other policy options through a detailed impact assessment, including a cost-benefit analysis.

The potentially achievable outcome of each scenario in regard to compliance with the five guiding principles, should interventions at European level achieve the desired effect are predicted to be as follows:

Technical solution	Data provision conditions – consent	Fair and undistorted competition	Data privacy and data protection	Tamper-proof access and liability	Data economy
Scenario 0					
Scenario 1					
Scenario 2					
Scenario 3					

Assessment of compliance with WG6 guiding principles	**Rating**
Compatible with guiding principles	
Minor issues with compatibility or issues that could be addressed with low cost/impact	
Issues with compatibility or issues that could be addressed with medium cost/impact	
Significant issues with compatibility or could be addressed with high cost/impact	
Incompatible with guiding principles in current form	

TABLE OF CONTENTS

1 Introduction

1.1 Background

Automotive technology is advancing rapidly with vehicles collecting greater quantities of data in order to operate and monitor systems and provide benefits to drivers, passengers and other road users; for example in route planning, system diagnostics etc. As well as providing benefits to the driver, this data is valuable to an increasing market that can use this data to target and offer related services to the customer.

The variety and demand of in-vehicle technical data is expected to increase with the further development of automotive technology and the method of accessing the data will transform from traditional wired access via the OBD-II connector towards remote, over-the-air access. Clearly, with the introduction and development of new ways to access data via a new interface, there will also be potential opportunities to not only collect but also use and post-process the data for other purposes.

For nearly a decade, there have been calls for the way in which in-vehicle data is made available to be defined. For example the ITS action plan (2008) included Action 4.1 aimed at "the adoption of an open in-vehicle platform architecture for the provision of ITS services and applications, including standard interfaces". Since this time, this objective has been reiterated in Priority Area IV of Directive 2010/40/EU, requesting the definition of the necessary measures to integrate different ITS applications on an open in-vehicle platform.

This has also been recognised in 2015 by the eCall type-approval Regulation (Regulation (EU) 2015/758) which includes provisions and empowerments 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."*

Additionally, the Commission's Digital Single Market Strategy for Europe[8] from 2015 provided a wider strategic framework for the digital economy including the connected car, and focussed 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

[8] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015DC0192

potential of the digital economy to boost industrial competiveness in particular through interoperability and standardisation.

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) with a clear goal to support the development and emergence of a common vision across all actors involved in the value chain. The C-ITS Platform gathers information from public and private stakeholders, and represents all of the key stakeholders along the value chain including public authorities, vehicle manufacturers, suppliers, service providers, telecomm companies etc., contributing towards a shared vision on the interoperable deployment of Cooperative Intelligent Transport Systems in the European Union. C-ITS Working Group 6 (WG6), given the specific task of addressing technical issues, successfully developed and agreed upon five guiding principles for access to in-vehicle data and resources in an attempt to harmonise the development of an interoperable, standardised, secure and open-access platform.

WG6 proposed three technical solutions for the access to in-vehicle data and resources. These comprised the following technical architectures:

- Data Server Platform
- In-vehicle Interface
- On-board Application Platform

Key features of the *Data Server Platform* concept are that the data from the vehicle is sent to a back-end server where it can be made available. Therefore, both the data itself and the application using the data are outside the vehicle. Access to data using an *In-vehicle interface* is enabled via an upgraded interface inside the vehicle; any application using data would run outside the vehicle system. Finally, the *On-board Application Platform* would allow access to data and the execution of applications inside the vehicle environment. WG6 also described three derivatives of the *Data Server Platform*: the *Extended Vehicle*, which proposed direct access to an ISO-standardised interface from the car manufacturers' servers, the *Shared Server*, which proposed access from a server controlled by a consortium of stakeholders rather than the car manufacturer, and the *B2B Marketplace*, which proposed an additional layer between the vehicle and the service providers, which would be fed by vehicle manufacturers' back end servers, for access by the market.

Furthermore, the WG6 report[9] presented:

- two methods of *defining the data made available* irrespective of the technical architecture, with this either being determined by the development of use-cases describing the purpose of the application and the specific data needs, or access depending on applications, which would be based on data described in the terms and conditions of each application; and
- ACEA's proposed categorisation of use-cases which described access to data for applications (other than those regulated or C-ITS 'day one' applications[10]) using a *negotiation model* that allowed access to data on the basis of terms and conditions agreed between the car manufacturer and the third party.

[9]http://ec.europa.eu/transport/sites/transport/files/facts-fundings/tenders/doc/specifications/2015/s248-450626-annex6-report.pdf

[10] A list of 'Day 1 services' agreed by the C-ITS Platform that, because of their expected societal benefits and the maturity of technology, are expected to and should be available in the short term

Further detail on the technical solutions can be found in Section 3.1.

1.2 Objectives

The aim of the study is to carry out legal, technical, cost-benefit, and subsequent scenario analyses based on proposals developed by WG6 on the access to in-vehicle data and resources to address the following:

- identify and quantify legal issues relating to the two methods of accessing in-vehicle data (use-cases or application-dependent access), the negotiation model proposed by some stakeholders, and the three technical solutions and their different technical implementations put forward by stakeholders;
- assess the technical aspects of each solution (based on a review of literature and standards, through consultation with stakeholders and engineering expertise) to recommend the most suitable specifications and technical requirements;
- carry out a cost-benefit analysis (CBA) of direct and indirect economic, social and environmental impacts; and
- develop and analyse a set of scenarios, taking into account the market development, the current EU, national and international legislations and the work of the Working Group 6 of the C-ITS platform.

2 Task A: Legal Analysis

2.1 Introduction

TRL have worked with our legal partners Mills & Reeve LLP to provide a legal analysis of the solutions considered by Working Group 6 for accessing in-vehicle data and their different proposed implementations under applicable EU laws. We have summarised the key findings of our analysis in the following sections. A more detailed analysis of the legal aspect is presented in Appendix A.

The legal analysis has focussed on the following aspects:

- the three different technical solutions proposed by WG6 and their derivatives;
- the two different methods of accessing data; and
- the 'negotiation model' proposed by ACEA.

Mills & Reeve have summarised the key legal issues that apply to accessing in-vehicle. Most of the issues addressed apply across all of the solutions and methods of accessing data.

The legal analysis takes into account the Commission's objective to ensure that customers (vehicle owner/drivers) will have the freedom to choose a service based on accessing in-vehicle data to meet their specific needs, which the Commission assumes will require an open and undistorted competition for the provision of these services. As well as considering the legal issues that could prevent such open and undistorted competition, the legal analysis has also sought to identify issues that might hamper the development of such services more generally in accordance with the Commission's wider objectives as described in the Communication "Building a European Data Economy" COM (2017) 9 final[11].

2.2 Technical solutions and their derivatives

Each of the solutions, methods and models considered as part of this legal analysis can in principle work within the existing legal framework. There are no insurmountable legal issues that would necessarily favour the development of one proposed solution, method or model over another. Therefore, legal considerations alone should not determine which option identified by Working Group 6, if any, should be supported by market intervention.

That being said, each option is likely to give rise to a range of legal obstacles that will need to be navigated by market participants. The Mills & Reeve analysis identifies how a number of these obstacles might be dealt with in practice and indicates where the current legal framework may allow the market to develop in a way that is inconsistent with the five guiding principles and the agreed objectives of Working Group 6.

The issues identified will not in principle prevent the development of any of the proposed technical solutions. However, there is a risk they may undermine the incentive for OEMs to allow access to in-vehicle data using particular solutions. Some of the key issues identified and their anticipated effects are summarised below.

- Each solution will need to allow any entities making use of personal data to comply with their data protection obligations. In the case of the on board application platform and the in-vehicle interface, the number of entities handling

[11] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41205

the data and their relationship to the data subjects will be broadly similar. However, in the case of the data server platform (particularly in its shared server and B2B implementations), the relationship between a data subject and the entities processing his or her personal data may be more remote and less clearly defined. This means informing and obtaining the consent of (if necessary) the data subject may be more challenging. However, it should be noted that there are potential solutions to this aspect, so these challenges should not prevent a modified version of this model from being able to meet the requirements in relation to consent.

- The complexity of the concept of data ownership (as discussed in "Legal study on Ownership and Access to Data (SMART 2016/0085)") is likely to mean that the entity controlling the source of the data (most likely the vehicle manufacturers) will seek to control access to the data and obtain a return on its investment through a chain of contracts leading to the ultimate service provider. This approach may be problematic from the perspective of the vehicle manufacturers in the case of the in-vehicle interface. The introduction of an interoperable standardised interface is likely to mean there will be no contract between the vehicle manufacturer and the provider of the interfaced device. The vehicle manufacturer will therefore have no means to exploit its effective control of the data to reward the investment required to make the data available in this way. This is not necessarily fatal to the development of a market around the in-vehicle interface, but it may remove the incentive for vehicle manufacturers to develop the necessary technical solution without external/regulatory influence.

- It is a consistent theme that existing competition law should in principle be sufficient to ensure the development of a fair and undistorted market. However, although market participants are likely to be aware of these broad principles of competition law, their application in practice is often complex and highly fact sensitive. This means that to the extent each technical solution potentially concentrates market power with particular entities, there will be an associated risk of anti-competitive behaviour. This is despite the fact that such behaviour would be unlawful. Close co-operation within the European Network of Competition Authorities may be necessary in order to ensure the consistent application of the competition rules to issues of this type as and when they arise.

- The implementation of any of the three technical solutions will have significant liability implications. The majority of these will apply equally to each of the three solutions. Allowing access to in-vehicle data, particularly write access, will introduce a range of additional risks that will need to be managed. To the extent these can be controlled by the party exposed to the associated liability, this is unlikely to deter the development of a technical solution. However, where there is a risk of strict liability falling on the vehicle manufacturers, they may be unwilling to allow access (in particular write access) to third parties. This may be less of a problem for the on-board application platform to the extent the OEM is able to control third party access. For the other two solutions, there is a risk that, from the vehicle manufacturer's perspective, the risks of allowing access will outweigh the benefits.

2.3 Two methods of accessing data

On the assumption that 'use-cases' can be clearly defined and differentiated, and on the assumption that terms and conditions can be clear and adequately accepted by each user of the vehicle, there are no significant differences from a legal perspective between providing access to data depending on use-cases and providing access to data depending on the terms and conditions in the applications.

However, there are significant practical differences between these two methods which mean a purely theoretical legal analysis is of limited benefit. The two assumptions made

in the first paragraph demonstrate some of these practical differences. Will it be possible to clearly define and differentiate between the use-cases? Even if all use-cases can be defined at the outset, what about new use-cases that evolve as the technology evolves? Will there be a constant need to define and regulate for additional use-cases? In relation to the acceptance of terms and conditions, will there be sufficient legal certainty given by a single acceptance of terms and conditions? Will acceptance need to be given every time the vehicle is used? Every time a new passenger gets into the vehicle? Will this acceptance need to be per application or could a more global form of acceptance be given depending on the application or group of applications in question?

Although such questions will need to be answered, we do not see any legal impediment to the adoption of either of these two different methods of accessing data. Each method will require different legal or contractual structures to be put in place, and such structures will impact differently on different stakeholders, but in our view there is no legal reason to favour one method over the other.

2.4 The negotiation model

The primary legal challenge of the negotiation model is its interaction with competition law. As noted above in relation to the three technical solutions, the foundations of European competition law align with Working Group 6's guiding principles. So the currently existing law should generally be sufficient to ensure fair and undistorted competition in any implementation of the negotiation model.

The main risk with the negotiation model is that it will have a tendency to concentrate market power in the hands of any party that controls access to the data. This is not necessarily incompatible with the development of a fair and undistorted market provided those parties ensure they act in accordance with competition law. However, the complexity of the application of competition law to a new market is likely to mean it will take some time before the finer details of exactly what activity actually has an anti-competitive effect are established. During this period, there would be an increased risk of anti-competitive practices developing. Close co-operation within the European Network of Competition Authorities may be necessary in order to ensure the consistent application of the competition rules to issues of this type as and when they arise.

For a more detailed analysis of these aspects, please refer to Appendix A for the detailed report supplied by Mills & Reeve on the following tasks:

- Task A1: Review two methods of accessing data and identify stake holder impacts
- Task A2: Analysis of the negotiation model proposed by WG6 and assessment of compliance with existing legislation
- Task A3: Analysis of three specific technical solutions proposed by WG6 and their implementation to access in-vehicle data

3 Task B: Technical Analysis

3.1 Review WG6 proposal

3.1.1 Background

Due to the accelerated growth of technology within the automotive industry, there has been an increasing demand by various stakeholder groups, such as insurance, road authorities, repair and maintenance, and others, for access to in-vehicle data and resources. This access could enable fair and undistorted competition and provide third parties the opportunity to offer at least a similar range of services as the vehicle manufacturers. In the following sub-sections we will describe in more detail the methods of accessing in-vehicle data and the technical solutions and highlight some key issues raised during the WG6 discussions. Note that TRL's main technical analysis is provided in Section 3.4.

The C-ITS platform, a forum consisting of public authorities and external stakeholders was initiated with the aim to ensure interoperable deployment of co-operative systems in Europe. WG6 agreed five guiding principles for access to in-vehicle data:

- 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.
- 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.
- 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.
- Tamper-proof access and liability
    - Services making use of in-vehicle data and resources should not endanger the 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.
- 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.

Working Group 6 identified three different technical solutions for access to in-vehicle data and resources and also started to define a reference dataset, which would satisfy the expected data needs foreseen by interested stakeholders. Hence, four tasks forces (TF) were set up to provide input material for the Working Group discussions by developing the following items, respectively:

- On-board application platform (TF1)

- In-vehicle interface (TF2)
- Data server platform (TF3)
- Definition of a reference dataset (TF4).

C-ITS WG6 identified two possible methods of accessing in-vehicle data and three possible technical solutions for implementation. The suggested methods are:

1) Access depending on pre-defined use-cases
2) Application-dependent list of data (based on terms and conditions of each application)

Any of these methods can be combined with any of the suggested technical solutions:

1) On-board application platform
2) In-vehicle interface
3) Data server platform.

3.1.2 Access to data based on use-cases

A car generates different macro-categories of data and this could enable a wide range of use-cases. Access to data based on use-case is a specific set of data made available for a certain need; for example, repair and maintenance or usage-based insurance.

On the one hand, access based on use-cases would enable third party services to get access to relevant data sets to develop their own applications, but each use-case has a standardisation timeline before it is made available which could, depending on the length of the timeline, be a significant barrier to innovation.

It is not clear which party holds the authority to define use-cases and, in the case that this is the vehicle manufacturer, under which circumstances they could prevent a use-case being added or amended. This raises two areas of risk: that the manufacturer could, under some circumstances, impede innovation or that the manufacturer could possibly obtain knowledge regarding new competitor services.

Another aspect is to understand the difference between defining a use-case and a software/algorithm that runs on the Electronic Control Unit ECU (ECU) to generate data to fulfil the use-case. The former is accepted as an obligation to vehicle manufacturers to grant equal and fair access to in-vehicle data, functionalities and resources but the latter is propriety to the vehicle manufacturer.

ACEA summarised their position on data made available by use-cases and classified them into three categories:

- **Day one applications**
    - Traffic management
    - Accident/incident notification / emergency call
    - Electric vehicle integration needs for transportation and smart grid
- **Automotive aftermarket**
    - Repair and maintenance information
    - Diagnostics data and information
    - Remote diagnostics (fault codes)
    - Predictive service, maintenance, breakdown or vehicle use data and information
    - Roadside breakdown and recovery data and information
    - Proactive breakdown service
    - Accident/incident notification / emergency call (?)
    - Tyre pressure monitoring (?)

- **Non-automotive aftermarket OR the negotiation model**
    - Usage based insurance data and information
    - Theft notification / recovery
    - Driver coaching
    - Risk assessment of drivers' behaviour
    - Real-time location-based services
    - Real driving consumption
    - Vehicle operational information for fleet vehicle operators
    - Traffic management (?)
    - Accident/incident notification / emergency call (?)

Currently, certain parts of this category (e.g. C-ITS day one applications, eCall, RMI, remote diagnostic support, fleet management systems for heavy duty vehicles) are in the process of being harmonised. Therefore, vehicle manufacturers suggested using the data, process and transmission channels defined for each of these use-cases. For the remaining categories and new use-cases, they argued the fact that the 'concept of extended vehicle is being standardised at ISO' which would enable third party to request and receive vehicle data for specific use-cases regardless of their implementation in a human and machine readable format. The repair and maintenance industry held the view that limiting access to use-cases would take too long to agree the data provided and would stifle innovation and because they would be out of date by the time they were agreed. They also flagged concerns regarding the manufacturers being in control of the data provided, rather than data being provided to the market for the development of services.

The analysis so far shows that the concept of a use-case has advantages in clearly defining the how the data will be used which is important for complying with data protection requirement since it provides a clear and defined purpose for the data. However, the time that it may take to authorise and make data from a use-case accessible is a concern as well as the lack of clear responsibilities for the acceptance and approval of use-cases as well as changes to existing ones.

3.1.3 Access to data based on terms and conditions of each application

Unlike the use-cases, the independent operators and service providers reasoned that a release of data purely based on use-cases would severely restrict services and innovation, and therefore suggested access to data based on terms and conditions of each application. In this arrangement, users/data subject who use the application would give consent to applications, which would be based on a list of data described in the terms conditions of each application. This way, the restrictions of a pre-defined list of data (as for use-cases) can be removed and data can be combined to create new applications which the aftermarket argued would foster innovation in services exploiting in-vehicle data.

In this situation, the data subject can provide consent for using specific data fields via the terms and conditions of the application but the way in which the consent is given means that the purpose of the data use is less prominent. Our legal analysis, although finding both approaches possible, found this approach to be marginally weaker in this respect, although it should be noted that smartphones and tablet applications use this method of consent.

3.1.4 A harmonised minimum dataset

Both the two possible methods of accessing in-vehicle data described in the preceding sections are compatible with a minimum dataset approach. For the 'use-cases' approach the minimum dataset could be defined by the cumulative data defined as new use-cases are agreed, or as a specific dataset. For access based on terms and conditions of the application, some views were that this would be less compatible with EU data protection

legislation, which requires that the purpose for which data will be used is specified to the vehicle user. However, as discussed in the Data Protection section of the legal report at Annex A, it is only the actual use of personal data by service providers that would require the consent and notification of the data subject. Provided an appropriate mechanism is put in place to allow the service provider to notify the data subject and obtain any necessary consent before it begins processing their personal data, making a full dataset available to third party service providers would not in itself breach EU data protection legislation.

3.1.5 Technical Solutions

3.1.5.1 The on-board application platform

An on-board application platform allows unified deployment of applications on the HMI of the vehicle whilst also allowing hosting of applications on the HMI using the vehicle internal resource. This platform creates a unique opportunity for all stakeholders to access data from the vehicle on fair and equitable basis to create a wide range of applications.

The advancement in automotive technology already makes it possible for intelligent vehicles to offer an on-board telematics platform that not only controls certain functional features such as remote features, but also provides a platform for applications to protect and assist drivers (e.g. electronic road tolling (etoll), emergency call (eCall), breakdown call) and a wide range of other infotainment applications (e.g. traffic information service etc).

Secondly, the existence of application platforms such as Apple CarPlay and Google Android Auto makes it possible for drivers to connect their smartphones to a compatible vehicle HMI and access mobile applications on the HMI. The concept of Apple CarPlay and Google Android Auto is a mechanism to primarily extend the smartphone screen to the vehicle HMI. It is not a platform which runs on the in-vehicle embedded systems and neither is an integrated part of the vehicle. It is a merely an extension of the smartphone screen to the vehicle HMI with the facility to integrate with some of the infotainment system functionality (i.e. controlling volume from the steering wheel controls). These Apple and Google platforms are not performing any 'hard writing' on the main Controller Area Network (CAN) of the vehicle.

The functional requirements of an on-board application platform would require the presence of a host management controller that controls the core and service runtime environments while on the other hand separates local and remote access control. The non-functional requirements such as safety, security are equally important to protect the platform from the intrusion of malware, spyware or other external threats. The host can send updated applications to the application platform to improve the functional performance, while on the other hand provide upgraded security patches/policies so that the platform is secure and safe.

The applications which will be hosted on the on-board application platform will need to be tested, verified and certified in way that illegal modification of the applications are not permitted once they are installed on the platform. The local access control monitors all application messages and applies access control on them, thus making sure that the correct resource is allocated to talk with the desired application. The remote access control is responsible for authentication and authorisation of incoming messages. Each message should be time stamped and signed to enable authenticity of that message. On the whole, local and remote access control maintains the integrity of the applications and data by blocking incoming data from unauthorized parties.

Taking functional, non-functional (security), development, testing and validation of such a platform into consideration, ACEA and CLEPA proposed a four step sequential approach towards the evolution of an embedded in-vehicle application platform as shown in Figure 1.

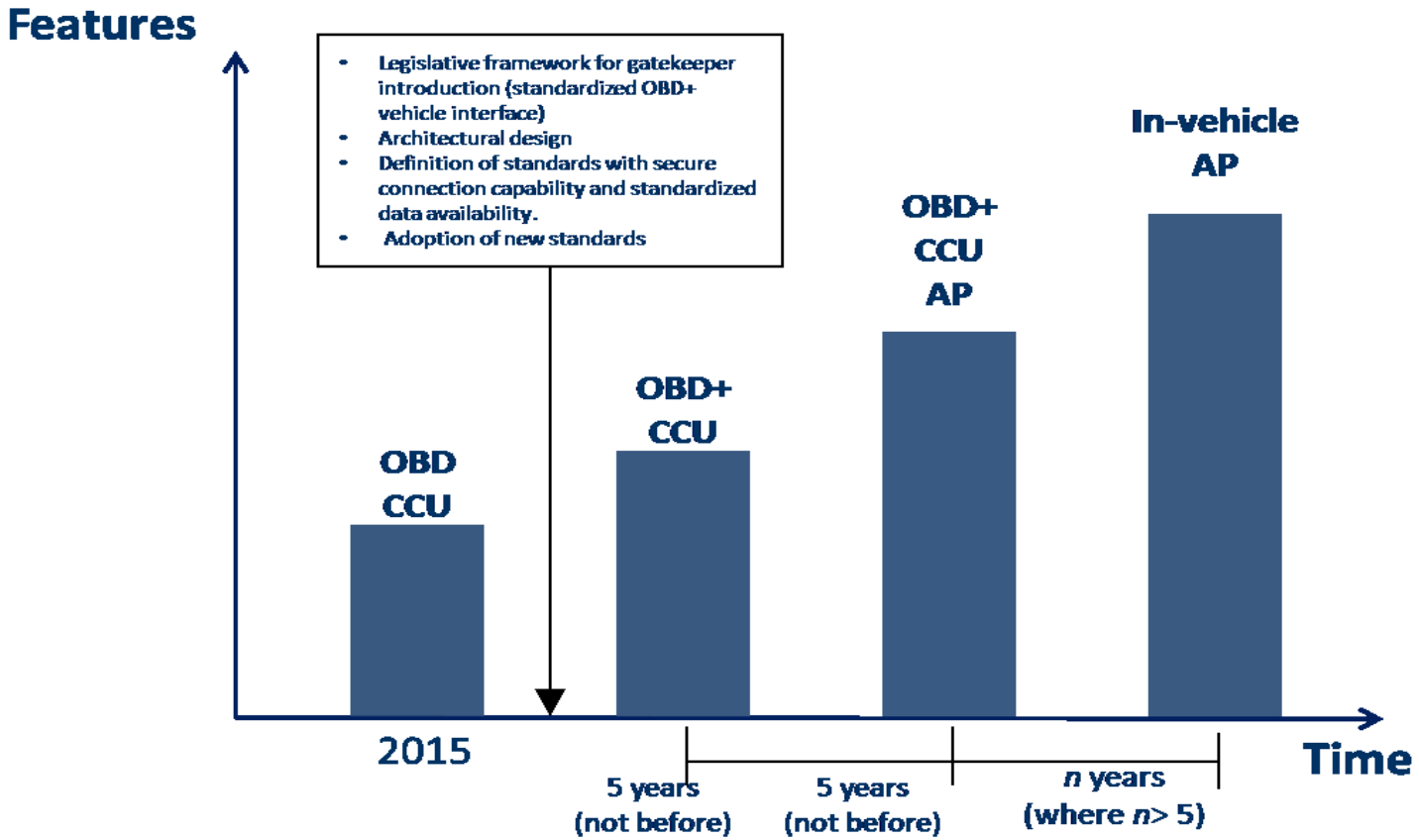


Figure 1 : Roadmap proposed by car manufacturers for in-vehicle on-board application platform (CCU: Connectivity Control Unit; AP: Application Platform)[12]

[12] WG6 - A2D - ANNEX 8 - Proposal TF1 on-board application platform

Step 1 – OBD CCU: A server based solution for access/sharing of data and OBD connected communication units

Communication of data from within the vehicle is a key element for many vehicle applications. The rapid development of technology now makes it possible for in-vehicle data to be transferred efficiently wirelessly to a cloud based server/system. The data in question, generated by the vehicle, is known as 'operating data'. It excludes data imported by vehicle users (such as mobile phone contact lists and selected destinations for navigation) and data received from external sources (like information transmitted by roadside units, other vehicles or vulnerable road users).

Based on the review of the WG6 report a short-term approach to collect data already exists in the market in the form of "OBD dongles" (a small device plugged into the OBD socket). These dongles connect the OBD interface wirelessly with a smartphone and other consumer devices. This scenario has an immense threat and risk to the vehicle OBD interface from the wireless connection between the smartphone and OBD dongle, as the wireless connection between the phone and the dongle is not secure. Some OBD dongles don't even have an internal firewall which may further impose additional security risks to the on board systems. Unwarranted and untimely access and hacks on smartphones that connect to the OBD dongles could also jeopardise the in vehicle systems.

The other approach to access data from inside the vehicle and be made available to third party participants is by connecting the existing on-board diagnostics (OBD) to a Central Connectivity Unit (CCU) as shown in Figure 2. This concept is very much similar to an extended vehicle proposed by vehicle manufacturers which provides a much secure way for access to data. A more detailed analysis will be provided in the technical analysis task B4.

As technology is evolving, the number of ECUs in a vehicle is rapidly increasing. These ECUs comprise both critical drive train components as well as less critical components such as windshield wipers, door locks and entertainment functions. The year 2015-16 saw the hacks and attacks to a vehicle CAN network on a Jeep and a Chrysler where the OBD-II port were the first place for intrusion into vehicle's CAN network . A specific set of messages and signals were injected on a vehicle's CAN bus (via OBD-II) to control key components (e.g. lights, locks, brakes, and engine etc.) as well as injecting code into key ECUs to create a bridge across multiple CAN buses. Hackers, instead of merely compromising one ECUs on a target car's CAN network and using it to spoof messages to the car's steering or brakes, also attack the ECU that sends legitimate commands to those components. This poses risks to the vehicle security, safety, and integrity of systems.

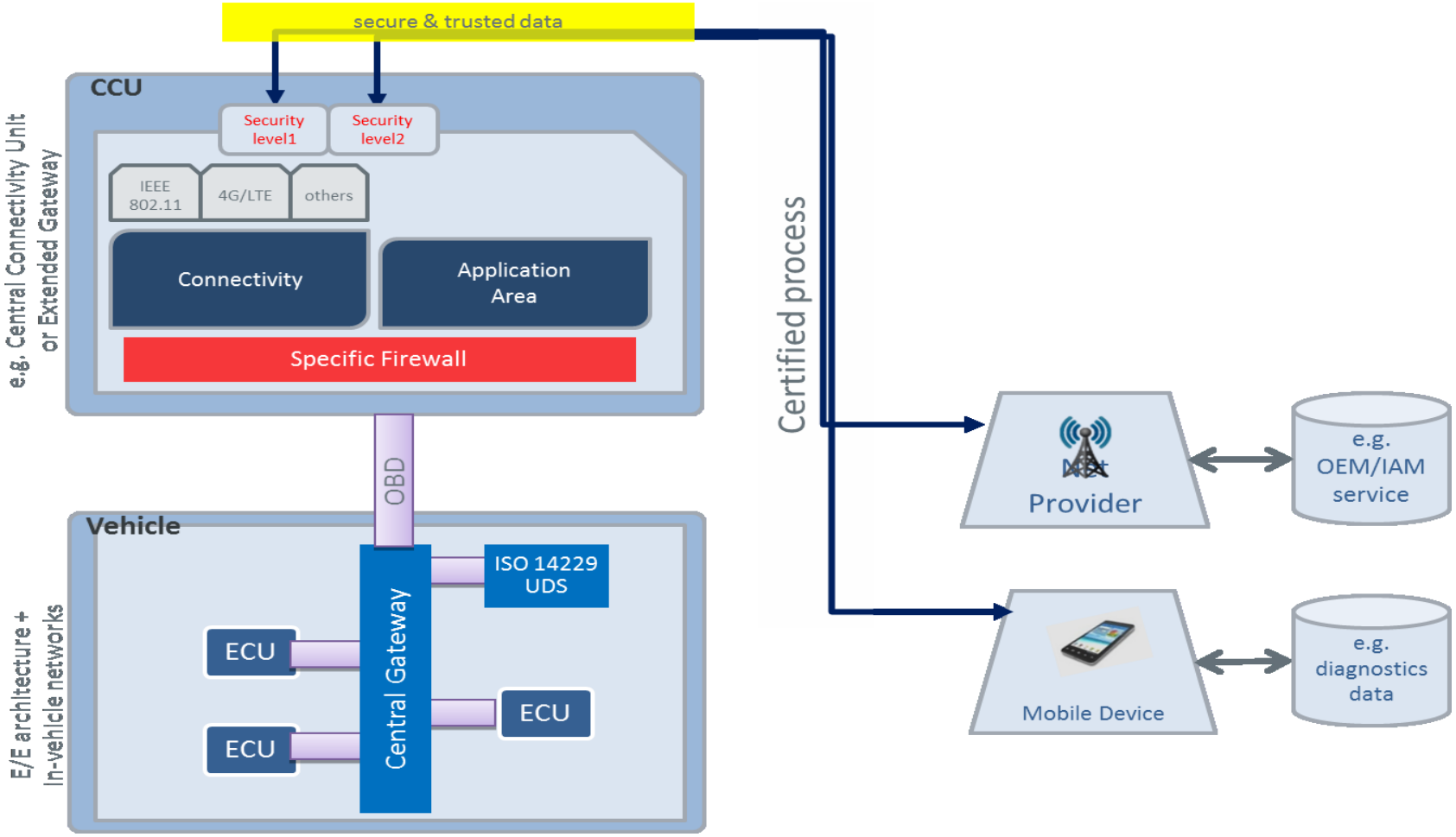


Figure 2 : Access of data through OBD connected communication units (OBD CCU)[13]

[13] WG6 - A2D - ANNEX 8 - Proposal TF1 on-board application platform

Due to these threats and the fact that the OBD-II port has been used to gain entry to a vehicle's CAN network, the present OBD-II interface requires improvements in security.

Vehicle manufacturers propose an alternate arrangement where vehicle data is made available in a secure manner using a cloud/server based system. The vehicle manufacturers would transmit relevant data from the current OBD-II port to a server-based solution using a communication control unit (CCU). The communication to the server happens over a secure and encrypted communications network. The CCU is guarded by an internal firewall and has additional security layers at each exit port to the market participant. Data from the server can then be accessed by different market participants.

The legal position on liability in this situation is discussed in the Legal Report at Annex A (in the main Liability section of the as well as the Liability subsection of the On-Board Application Platform section). The legal position on whether the vehicle manufacturer, any third party service provider, or the user is in a position to control what happens to the data is discussed in the Data Ownership, Contract and Data Protection sections of the Legal Report at Annex A.

Step 2 - OBD+ CCU: An upgraded OBD interface including gatekeeper and central gateway to in-vehicle network – 5 years after gatekeeper and central gateway standard availability

As shown in Figure 3 the next step proposed by ACEA and CLEPA towards an in-vehicle application platform with managed access requires an advanced interface standard (OBD+). A vehicle has many built-in mutually linked electronic control units (ECUs) that exchange signals, forming a number of communication networks. Several of these ECUs are linked to each other using different protocols such as CAN/FlexRay/LIN/MOST etc. The Central Gateway is a dedicated module that connects these ECU networks and their intermediates, acting as a communication station to coordinate signals being exchanged. Since, the in-vehicle networks handle a variety of communication protocols and data formats, converting them into an understandable format for the other network without causing any delay is the main function of the central gateway module. The Central Gateway unifies various local gateways/DCUs (Domain Controller Units), helps in synchronising the global and relative time and connects the individual function networks to a single module.

Domain controller units (DCU) are ECUs that integrate several functions/ECUs into one. It not only helps in reducing significant costs of the E/E architecture, but also increases the flexibility and scalability of the E/E architecture. It increases the possibility of adding functions on the electrical architecture of the vehicle. Domain Control Units provide the main software functionality for a vehicle domain, while delegating the very basic functions of actuator control to connected intelligent actuators/sensors.

The central gateway of the vehicle connects to the gatekeeper of the vehicle. The gatekeeper ensures relevant security mechanisms are in place to protect the in vehicle networks. These gatekeepers can be in the form a hardware security module which protects the in-vehicle networks from unauthorised access. Clearly, the timeline to implement these security strategies and put them in place requires additional developmental and testing time.

The OBD+ (with the central gateway and the gatekeeper) is connected to a CCU which features different security levels to manage access. The two important units for establishing communication and hosting applications are the CCU and the application unit (AU). The components implemented on the CCU essentially handle all communication from the physical up to the network layer. Applications that require low latency will also run on the CCU. In addition the CCU also provides the application unit with internal vehicle data sent via the CAN (Controller Area Network) bus. Besides the data coming from the external communication the application unit is responsible for hosting the majority of the C-ITS applications.

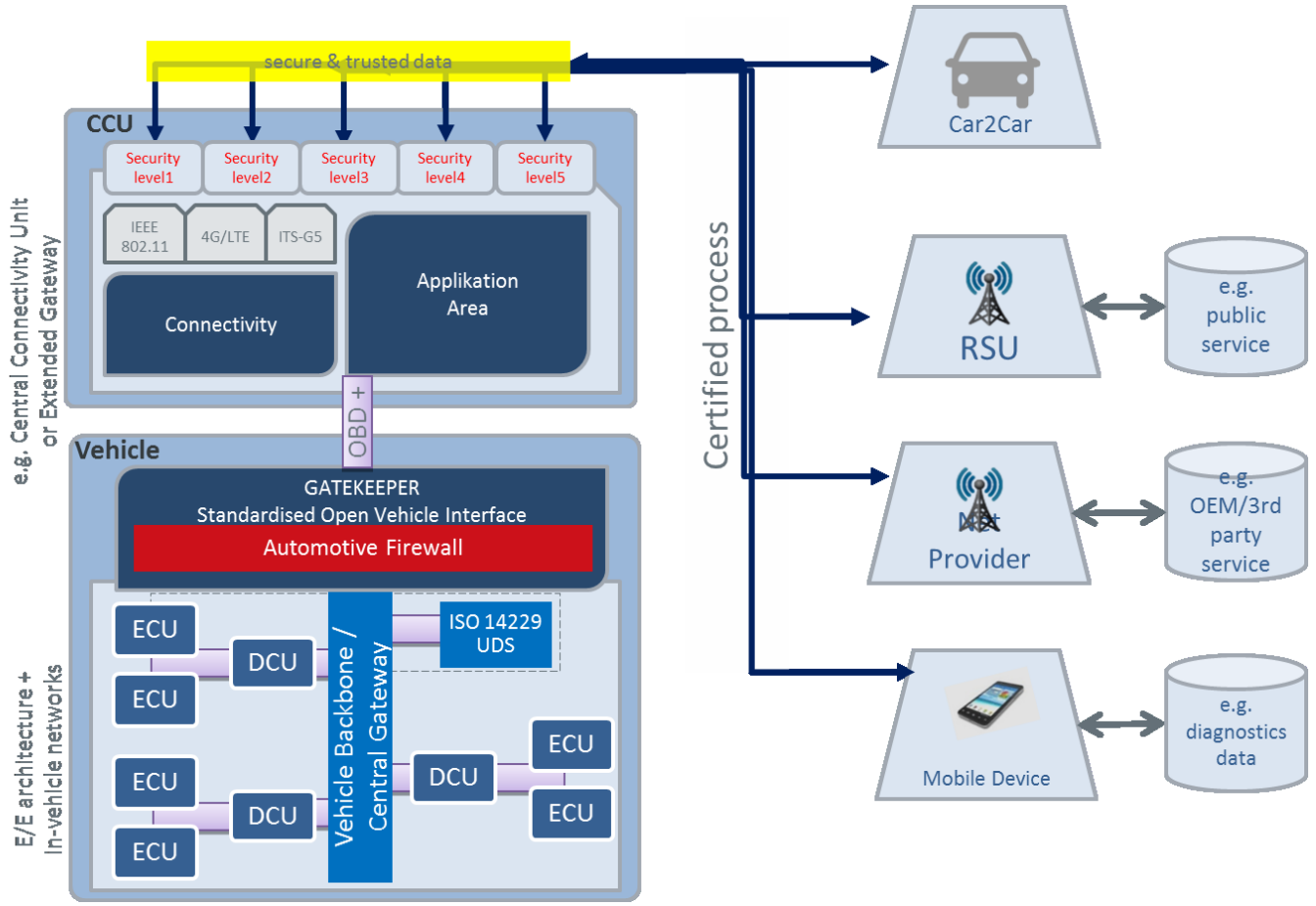


Figure 3 : Upgraded OBD interface including gatekeeper and central gateway to in-vehicle network (OBD+ CCU)[14]

[14] WG6 - A2D - ANNEX 8 - Proposal TF1 on-board application platform

Step 3 – OBD+ CCU OP: An OBD+ connected CCU featuring an open application layer

The next step introduces an on-board operating system featuring an API (application programming interface) in the CCU to the already developed application layer as shown in Figure 4. Security is managed within the vehicle by an automotive firewall and also at the CCU level.

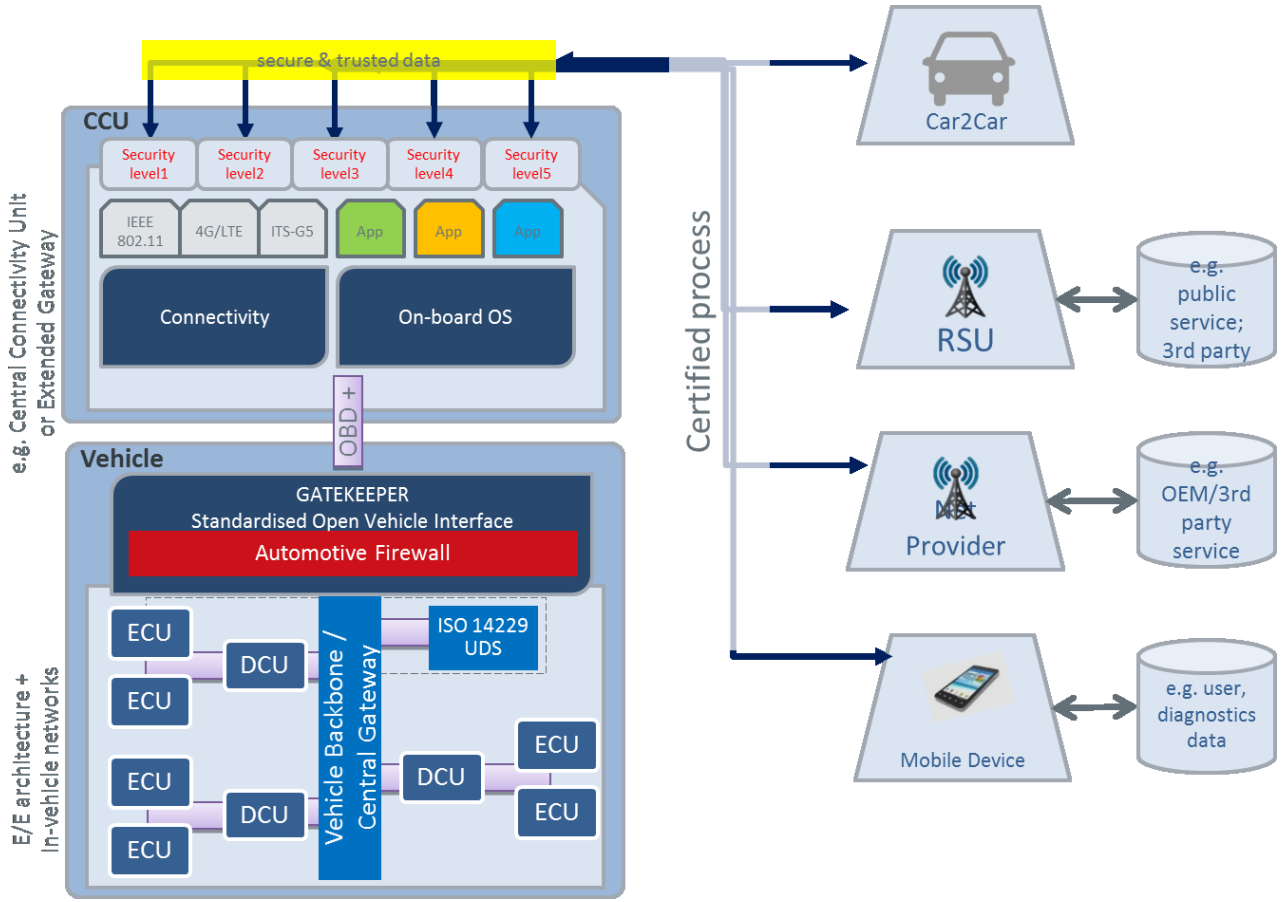


Figure 4 : OBD+ connected CCU featuring an open application layer (OBD+ CCU OP)[15]

[15] WG6 - A2D - ANNEX 8 - Proposal TF1 on-board application platform

A suitable SDK (software development kit) will provide means and tools for third parties to produce applications as well as data access according to the granted security level. Third-party applications should be certified by vehicle manufacturers to verify that there is no safety or security risk to the overall vehicle functionality. A framework for selecting applications and a mechanism to upload third-party applications will be necessary to enable the user to choose from a wide range of third-party applications with respect of privacy and security and the supervision of manufacturer. The need for vehicle manufacturers to be able to demonstrate that enabling the use of third-party applications within the vehicle system (and the associated risk of doing so) does not itself mean the vehicle system constitutes a defective product is discussed in the Liability section of the Legal Report presented in Appendix A.

Step 4 - In-vehicle AP: An embedded on-board Application Platform

The last and final step according to the timeline proposed by ACEA and CLEPA is a combination of the preceding three steps. This leads to a platform that is secure, can host various applications, has an internal operating system to support the applications and can give real time access to data. The steps involved to achieve the on-board application platform represent a sequential approach where OBD+ and the concept of data server exist in parallel, at least until the platform is uniformly deployed and potentially beyond.

According to the car manufacturers there is a sequential timeline for the development of a security layer, firewall, application controller, application unit, operating system, testing and validation before the services offered can be realised. In contrast, independent operators, although identifying the same technical steps necessary, propose a parallel approach to reduce the timeframe for the deployment of such a platform.

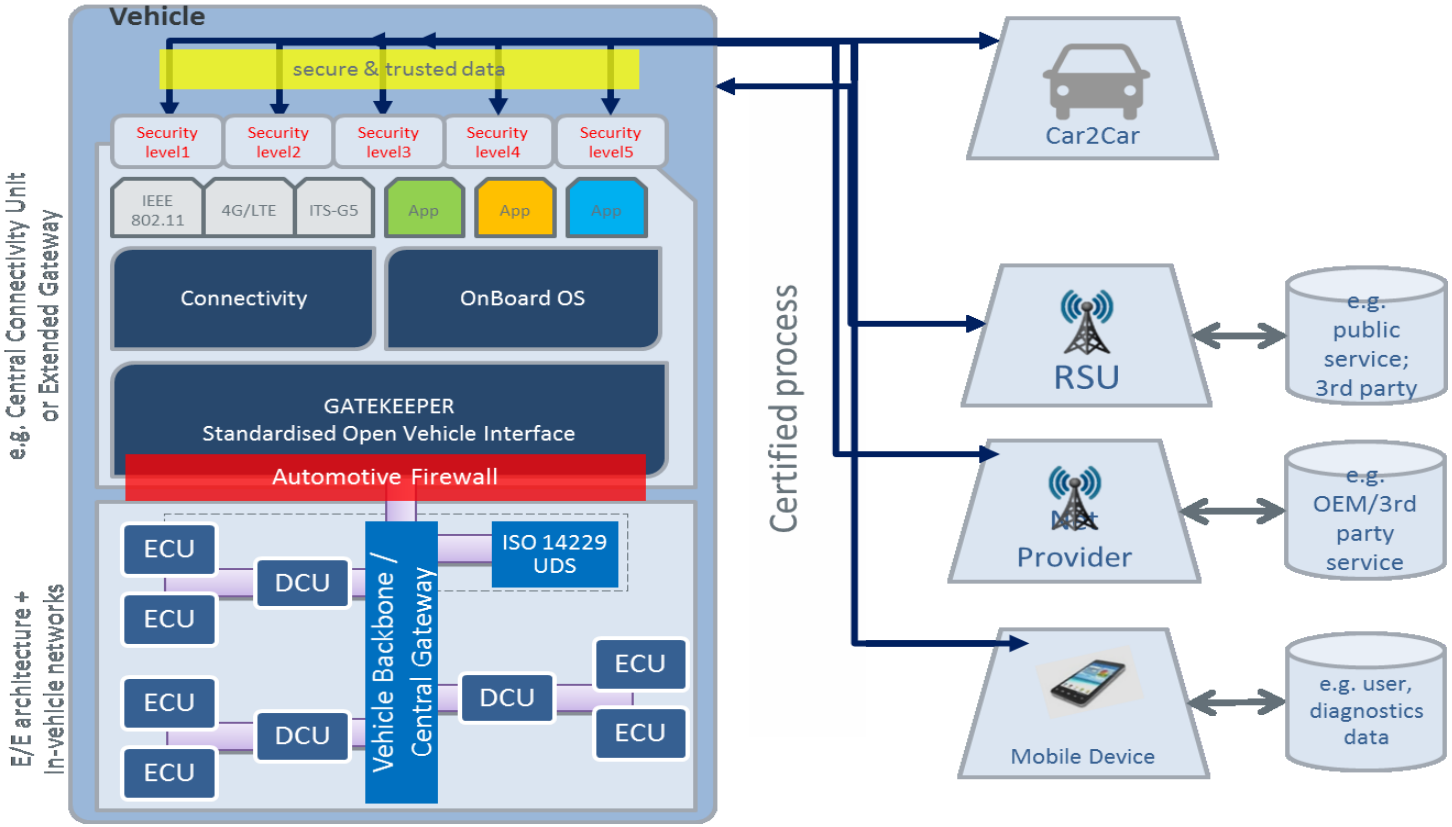


Figure 5 : An embedded on-board application platform (in-vehicle AP)[16]

[16] WG6 - A2D - ANNEX 8 - Proposal TF1 on-board application platform

Potential issues with the on-board application platform

Safety and security are the main issues for the on-board application platform. These aspects must be assured before this technical solution can be implemented. The legal concerns relevant to the risks associated with selling vehicles that have the potential to be dangerously overloaded by the number of installed apps are discussed in the Liability section of the Legal Report presented in Appendix A. The technical steps, feasibility and timelines required to achieve this will be addressed in the final report.

Car manufacturers cited concerns writing to ECUs – especially those with safety critical consequences, and the risk of causing buffer overflows that could affect the safe operation of the vehicle systems. Installation of multiple applications on this platform might degrade the overall functionality of the vehicle, with the safety critical systems being of particular concern. For example, a large volume of individual apps installed within normal usage might affect the performance of an individual safety critical function. These are examples of outcomes that would need to be fully addressed by improvements to the security layer to prevent writing to safety critical ECUs and responses to repeated messages that might create buffer overflows.

Manufacturers also expressed concerns about third parties changing software within the vehicle and cited the product liability risks of any consequences of the changed software. Legal input indicated that alterations to the software could be the responsibility of the third party unless the manufacturer was negligent in allowing unsafe changes. Therefore, applications would need to be developed and tested on an SDK and certified by the manufacturer before being installed on the vehicle. The key legal considerations regarding product liability are discussed in the Liability section of the Legal Report at Annex A.

Overall, this concept would require suitable and adequate security standards implemented for service providers to start development and deployment of applications on this platform.

3.1.5.2 In-vehicle interface

This solution already exists in the market: the OBD-II interface. As described above, in step 1 of the on-board application platform, this interface allows connection to devices outside the vehicle such as OBD dongles, central connectivity unit, etc. The OBD-II interface allows access to a standardised set of data such as emissions, fault codes etc as per current regulations. Independent and authorised repairers and workshops use the current interface to query a fault code or DTC, flash or upgrade existing software in a dedicated ECU on the vehicle using an OBD connector.

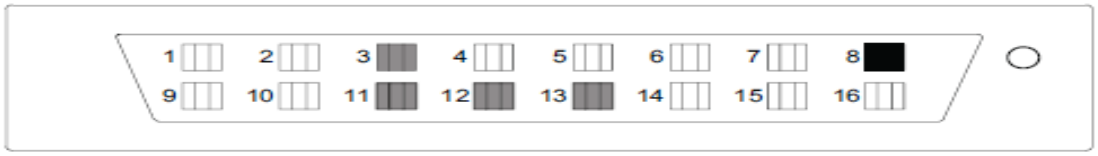
The OBD-II interface provides a method for easy access to in-vehicle data. The data observed is real time and of high quality. What the current OBD-II interfaces lack is sufficient protection/security measures to prevent any threats from the outside world to in-vehicle networks.

Current in-vehicle electrical architecture consists of Electronic Control Units (ECUs, sensors, radars etc. and the vehicle network bus e.g. CAN, Flex Ray, LIN etc.). Current in-vehicle networks provide real-time data, but on a much lower bandwidth compared to non-real-time data (such as infotainment systems). Future vehicles will use more real time information for applications on-board the vehicle from a variety of ECUs and sensors. The real time information can be in the form of CAMs DENMs or real time traffic information, breakdown alert and all the other Day 1 applications. Therefore, to develop this technical solution, the OBD-II port must not only fulfil the real-time access condition, but at the same time be able to deliver data on a much higher-bandwidth. This would require upgrading the current OBD-II to an advanced OBD+ which could house a much faster data bus in order to process data with high computational power.

The current state of technology allows for a standardised SAE J1962/ISO 15031 connector (the current OBD) as the repair and maintenance industry use legacy tools to

connect to the existing OBD connector. The current OBD interface is also used by some service providers for offering remote diagnostics support and fleet management services. Therefore, developing a completely new connector would be challenging. A plan to introduce a new connector at ISO level which supported DoIP received very little attention especially from CARB (California Air Resources Board) and was therefore cancelled. The only connector which prevailed was the current state of art SAE 1962 connector or the current OBD-II. To counter certain limitations of the existing OBD-II interface such as low speed data, the increasing interconnections of vehicle ECUs, increasing time to flash programming, some OEMs have already started using the existing OBD-II connector for Ethernet for DoIP with some restrictions. DoIP is the packaging of diagnostic messages in Ethernet frames for communication of a vehicle and a diagnostic tester. DoIP is a standardized diagnostic transport protocol i.e. ISO 13400.

WG6 members agreed on a physical interface as shown in Figure 6 as a possible solution. The proposed future layout will need only two pins on today's OBD connector to provide the mirrored data stream to a connected external CCU.



PIN	ISO 15031-3/SAE J1962 definition	Ethernet 100BaseTx usage
1	Defined in ISO 15031-3/SAE J1962	
2	Defined in ISO 15031-3/SAE J1962	
3	Discretionary	Ethernet Rx (+)
4	Chassis ground	
5	Signal ground	
6	Defined in ISO 15031-3/SAE J1962	
7	Defined in ISO 15031-3/SAE J1962	
8	Discretionary	Ethernet activation line pull-up
9	Defined in ISO 15031-3/SAE J1962	
10	Defined in ISO 15031-3/SAE J1962	
11	Discretionary	Ethernet Rx (–)
12	Discretionary	Ethernet Tx (+)
13	Discretionary	Ethernet Tx (–)
14	Defined in ISO 15031-3/SAE J1962	
15	Defined in ISO 15031-3/SAE J1962	
16	Permanent positive voltage	

Figure 6: Example of pin-out for Ethernet recommended for 100BaseTx on the ISO15031-3/SAE J1962 diagnostic connector; taken from ISO 13400-3[17]

The CCU allows transfer of data from the OBD+ to a dedicated server. A concept of a centralized, firewall protected Gateway was proposed, where a subset of vehicle data will be made available on a standardized data link connector. Different security layers/levels shall manage access to the in vehicle network. Therefore a two-step approach was proposed:

1) A cloud- or server-based solution for access/sharing of data and OBD connected communication units (OBD CCU) – where a constant vehicle data stream will be provided on an in-vehicle interface plug. As a first step, an external Connectivity Control Unit or

[17] WG6 - A2D - ANNEX 6 - In-vehicle interface

the CCU, can connect using a connector. The CCU can collect and transmit data to external receivers (RSU, backend-server) by different ways of communication (4G, 5G, WiFi etc.) for further processing.

2) A second step was to provide an upgraded OBD interface (OBD+) including gatekeeper and central gateway to in-vehicle network (OBD+ CCU OP) featuring an open application platform, in such a way that data collected is processed inside the CCU and provided to applications hosted by the CCU, as shown in Figure 7**.**

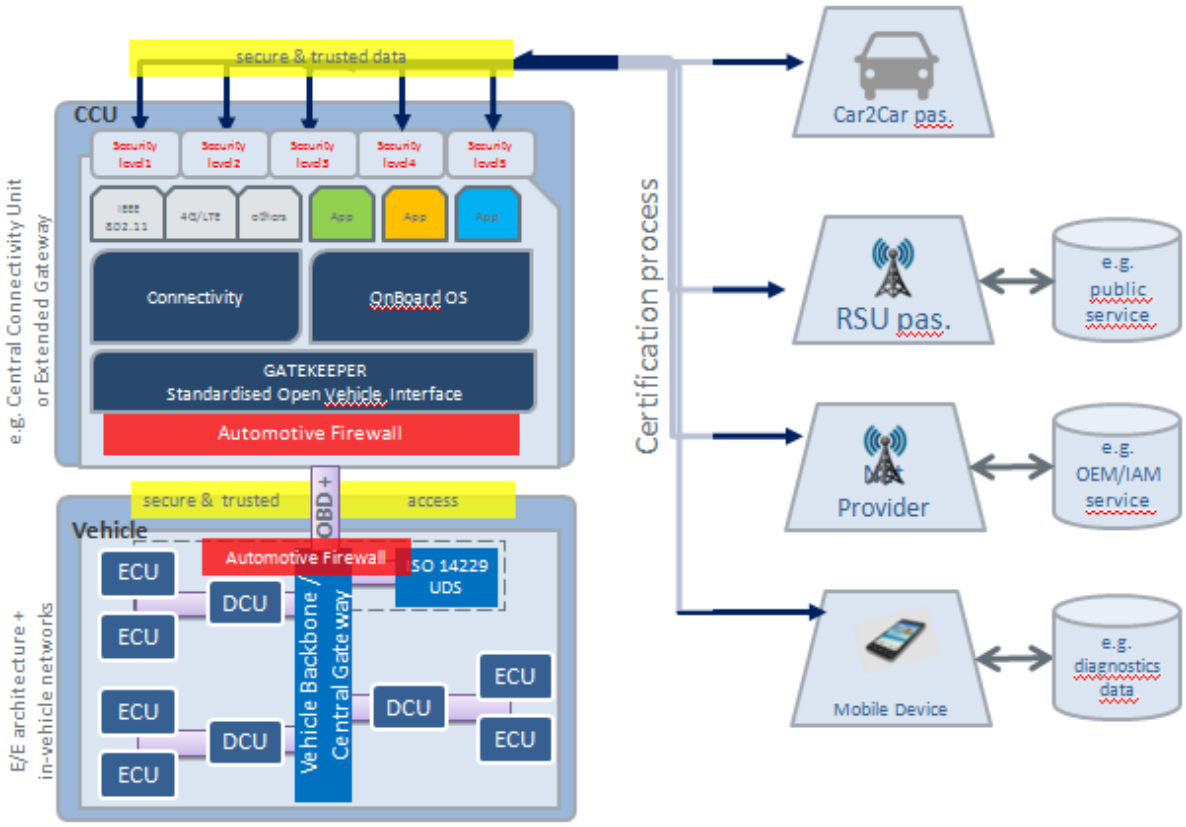


Figure 7: OBD+ connected CCU featuring an open application layer (OBD+ CCU OP)[18]

The CCU provides various levels of security and access to data, e.g. read, write, etc. In order for the communication and access to be secured, the following security guidelines have been approved by WG6 as a technical contribution and a list of relevant items have been compiled, including the three mentioned below. The full list can be found in the WG6 - A2D - ANNEX 7 - In-vehicle interface_Security_Requirements_CCU.

- Secure Communication between CCU and the Backend
- Ensure Authenticity and Integrity of Transmitted Data
- Ensure Confidentiality of Data

Potential issues with in-vehicle interface

The in-vehicle architecture consists of electronic control units (ECUs) connected by Controller Area Network (CAN), Local Interconnect Network (LIN) and Flex Ray buses.

[18] WG6 - A2D - ANNEX 6 - In-vehicle interface

Significant operational and security related issues have been flagged by stakeholders that could limit the computational power of the on-board ECUs. Traditional ECUs have limited computational power; primarily because of lower data requirements, but also because of the small number of ECUs connected on the vehicle CAN bus.

With the growing technology and the need for real-time applications some stakeholders warned that traditional ECUs were not capable of real-time operations and could not be used for this purpose. Additional infotainment functionalities also consume the data bandwidth limitations of traditional ECUs. Therefore, not only ECUs with high computational power, but also a high band width data bus will be required to solve issues surrounding collection and processing of real time data. At the same time, to be competitive and innovative, an upgraded physical interface should also be made available. This drives a change for a new in-vehicle interface that is capable of not only handling large amounts of real time data, but also provides a safe and secure access to in-vehicle data.

The in-vehicle network would need to be secured from unauthorized, untimely access by applications and services external to the IVN. The security strategy had to include several elements, including:

- secure and encrypted communication
- a definition of firewall strategy
- protection of the physical layer
- mandatory penetration tests
- protected back-end solutions that take over the provision of encryption keys and fulfill the part of a multiple-access.

Data being put on the interface would need to be in a standardized format for all third-party applications and services to access. The owner/user of the vehicle should have the ability to restrict access to the data. Therefore, a mechanism should also be implemented that allows the user to choose which data is transferred to which party and for which purpose. A cloud- or server-based solution for access/sharing of data and OBD connected communication units (OBD CCU) already exists in the market. To have an upgraded OBD interface including gatekeeper and central gateway to in-vehicle network (OBD+ CCU+OP) featuring an open application layer will, in the opinion of car manufacturers, add 5 years after the standard availability. A more detailed analysis on timeline has been provided in task B4 after the bilateral meeting responses and stakeholder inputs have been studied.

3.1.5.3 Data server platform

The third technical solution is the data server platform. The key difference to the previous solutions is that it is external to, rather inside the vehicle. It is an external data server where relevant vehicle data are transferred to and made available to service providers.

The data server is further classified into three derivatives of this technical solution, namely:

1) Extended vehicle
2) Shared server
3) B2B market place

Extended vehicle

An extended vehicle is a vehicle with external software and hardware extensions for some of its features. These extensions are developed, implemented and managed by the vehicle manufacturer. The concept entails a connected vehicle that communicates to backbone servers via mobile networks. Vehicle data from the server is then made

available to stakeholders via standardized interface. A high level overview of the concept is presented in Figure 8.

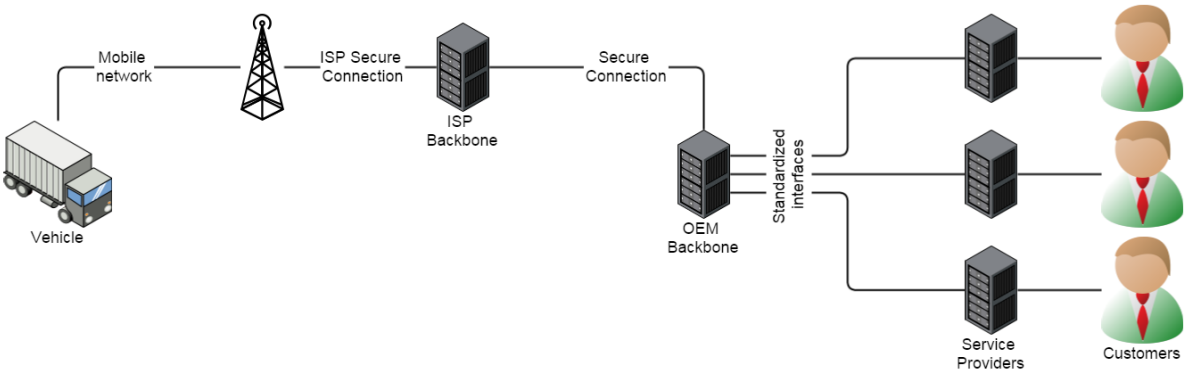


Figure 8 : Overall architecture of the Data Service Platform[19]

The extended vehicle is a concept developed by OEMs where data generated by vehicle is sent over a secure and encrypted communication channel to a dedicated OEM server. Data made available at the OEM backend server using a standardised interface will standardise sets of data that can be used by vehicle manufacturers or third-party participants for post processing and development of applications for vehicle users. Extended vehicle concept is being used by many vehicle manufacturers across Europe.

The relevant standard to have a standardised set of data available at the backend interface is being worked upon at ISO level as ISO 20077-1 and ISO 20078-1. ISO 20078-1 will provide for web service access to the 'extended vehicle' as defined in ISO standard 20077- 1.

ISO 20077-1 is the Road Vehicles — Extended vehicle (ExVe) methodology and ISO 20078 - Road vehicles -- Extended vehicle (ExVe) 'web services. A short literature survey on these standards is covered in Task B2.

The ISO standards will help in defining specific sets of data available to service providers in the form of use-cases.

Shared server

Conceptually, the shared server is the same technical service platform as the extended vehicle but the OEM backbone server is replaced by a shared server operated by neutral service providers. The neutral service provider will be commissioned and maintained by a consortium of interested stakeholders.

Data from the all vehicle manufacturers will be sent to a shared data server from where service providers can access data via a standardised interface as shown in Figure 9. The ISO standard 20078 is being developed specifically for this purpose. It provides for web service access to the 'extended vehicle' as defined in ISO standard 20077- 1.

[19] WG6 - A2D - ANNEX 2 - Extended Vehicle

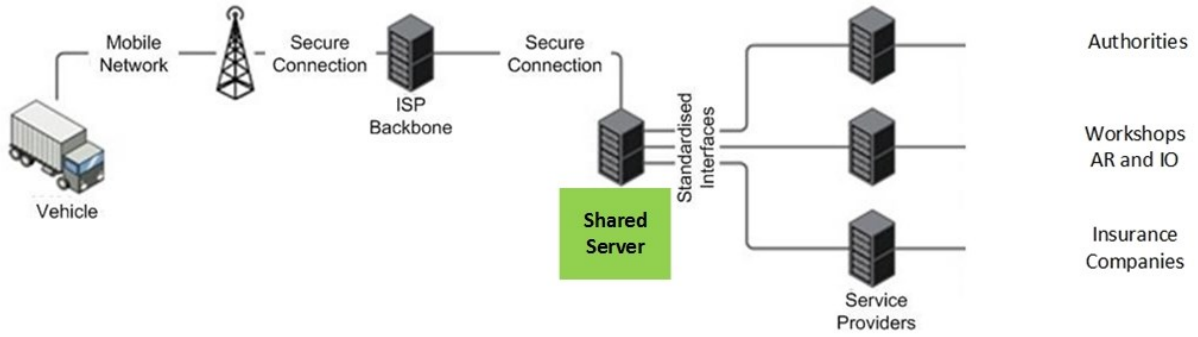


Figure 9 : Data Server Platform: Shared Server[20]

The shared server is neither financed nor operated by an OEM. The OEM plays a role of a system administrator for the transfer of data between the vehicle and the shared server. Data available at the standardised interfaces should be of the same quality as the data of OEM backend.

B2B marketplace

B2B marketplace technical solution is again similar to the other data server solutions but the 'marketplace' allows an independent third party to service and operate access to the vehicle manufacturer server. Data from the vehicle manufacturer's dedicated server (i.e. the extended vehicle) will be forwarded to the neutral server from where third parties obtain access as shown in Figure 10.

The commercial platform provider (or the neutral server provider) could be a big data/IT company which provides bulk storage of data, keeps track of incoming and outgoing data and ensures data access demand from independent operators and third parties are met within a stipulated timeframe. For example, neutral server providers could be companies like Google, IBM etc.

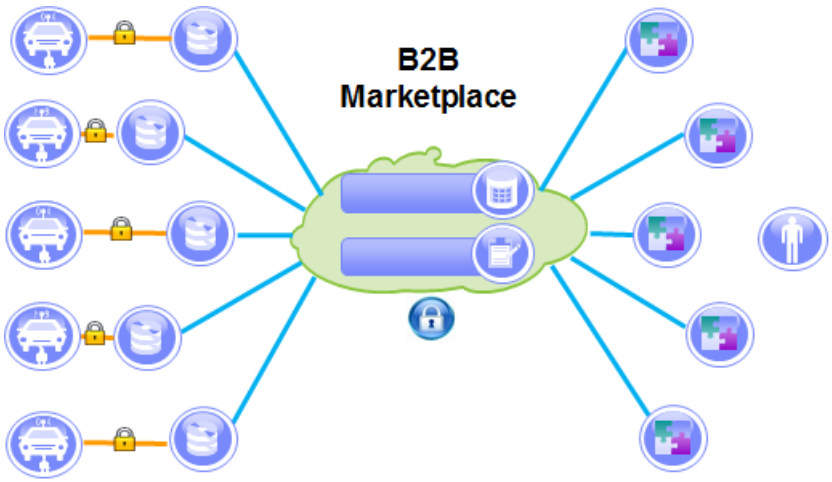


Figure 10 : B2B Marketplace [21]

[20] WG6 - A2D - ANNEX 4 - Shared server

It is the neutral server provider's responsibility to ensure that if there is an additional request for data which is not present on the neutral server, that they approach the manufacturers to obtain access to the data. A key feature of this technical solution is that the identity of the application developer requesting the new data is not disclosed to the vehicle manufacturer.

A more detailed technical analysis on the logistical implementation aspects of this solution, for example: who will select the neutral server provider; the timescale needed to set up the neutral server will be carried out in Task B4.

Potential issues with data server platform

Stakeholders have raised several issues with the data server platform. These are summarised below:

Lack of access to real-time data

All data server solutions involve data being passed to a server external to the vehicle. This fundamental architectural arrangement means that the data at the backend is not real-time because the data is inevitably subject to technical restrictions (e.g. varying transmission times). This prevents services that require true real-time data to operate. For the B2B marketplace solution the latency is greater because of the additional data transmission between the OEM backbone and the neutral B2B marketplace.

Contact with the customer

All derivatives of the data server platform described here mean that third-parties cannot access the vehicle HMI. Since this is the main interface with the driver, repair and maintenance stakeholders highlighted that this was not fair and equitable.

Control of the data

In the data server technical solutions, communication to and from the vehicle is routed through the OEM backbone, which allows a complete control of the data exchanged. Stakeholders expressed concern that the vehicle manufacturer would be able to control the content and quality of the data available to third parties and thus control competitor's ability to provide competing services. It was argued that this violates one of the guiding principles, requiring fair and undistorted competition. Whether this would mean competition law has been breached will largely depend on whether it has an overall negative impact on consumers (see the Competition section of the Legal Report at Annex A for more discussion).

Manufacturer oversight of access to data

In the extended vehicle solution, the OEM could have sight of the third party accessing the data and which data they were accessing. Since the car manufacturers are competing with the third parties accessing the data, this has the potential to distort the market. The shared server and B2B marketplace solutions have addressed this issue by making anonymous the party accessing the data from the point of view of the manufacturers.

Methods of accessing data

As mentioned in Section 2.3, there are two methods of accessing data: on basis of data elements defined by pre-defined use-cases or based on data elements selected in the application. The implementation and operation of the technical solution used to access

[21] WG6 - A2D - ANNEX 5 - B2B Marketplace

in-vehicle data could have implications for third parties accessing data. For example, the development of new applications and services may require data (or data at a particular quality) that does not exist on the server.

In this case the first option is to approach the neutral server provider (in the case of the shared server or B2B marketplace) to ask for additional data. The neutral server provider would then arrange access to the data in question with the vehicle manufacturers by amending their existing contract. This process could involve a significant lead time to negotiate the request with manufacturers and in this time, service providers may have already lost significant time to market. Furthermore, the negotiation could result in the outcome that the data is provided or manufacturers rejecting the data need. Alternatively, third parties could hold a contract directly with the manufacturers. On the one hand this process could reduce the negotiating time, but on the other exposes the business idea of the service providers to the vehicle manufacturers who may also be competitors in this area. In both of these instances, there is a risk that the market could be distorted or third parties discriminated against with respect to access to data.

3.2 Literature Survey

3.2.1 Literature survey method

The literature survey process is made up of three main elements: a desktop-based internet search; an in-depth search, by the TRL library team, of a selection of major databases; and obtaining relevant documents from stakeholders. Once completed, the sources were screened for relevance then reviewed.

The survey aimed and succeeded to identify information on the following aspects:

- What are the positions of all relevant stakeholder groups with regard to the different technical solutions.
- What are the relevant European strategies and wider legislative considerations regarding the European Data Economy and ITS.
- What do current vehicle standards and legislation prescribe regarding the Extended Vehicle, Remote Fleet Management System and schemes related to RMI
- What relevant technical implementations for access to in-vehicle data and resources exist today or are announced.

Other aspects were addressed in the search, but no tangible information that would go beyond the WG6 documents could be obtained from publicly available sources:

- Costs of individual technical solutions in terms of hardware, software, R&D, staff time, etc.
- Quantified benefits of the technical solutions for society, environment, etc.
- Evidenced estimates of timescales to implementation of the technical solutions.

The outcomes from an initial phase of this literature survey and the WG6 documents review (Task B1), and the remaining gaps identified in those reviews formed the basis of an online stakeholder questionnaire.

3.2.2 Position papers

The positions of relevant stakeholder groups with regard to the different technical solution were studied to understand the specific interests each group in access to in-vehicle data and resources. Short summaries of the relevant aspects contained in position papers published during and after the WG6 meetings are provided in the following.

3.2.2.1 FIA Region 1 (Europe, the Middle East and Africa)

The FIA believes adopting the Extended Vehicle concept could lead to suppliers having limited access to data if the data server is solely under the vehicle manufacturer's control. This solution could also limit the consumer's choice of any future service providers to a list of manufacturer-approved suppliers.

A Shared Data Server could solve some of the Extended Vehicle issues by having a mutually agreed neutral third party run the data server controlled by a consortium representing interested stakeholders. This is already being done in the SERMI[22] Association. The SERMI association was set up by a group of vehicle manufacturers and independent operators to allow a fair and secure access to sensitive vehicle data. It does this by defining an accreditation process to allow access to security related data. Any decision on the scheme needs unanimity of stakeholders. Inspired by this, the FIA suggests using similar ideas by ensuring the neutrality of a server solution by having a mixed consortium and for stakeholders to work out criteria to be fulfilled by applications in order to ensure driver safety and security.

To control the collection and processing of vehicle data, specific rules on data ownership and guidance on personal data use should be used. Vehicle drivers and owners should be given control over the data their vehicles produce by allowing the vehicle owner or driver to give consent to certain rules by opting in or out. (FIA, 2016)

3.2.2.2 European Association of Automotive Suppliers (CLEPA)

In their 'Open Telematics Platform' position paper from July 2015 (CLEPA, 2015), CLEPA supported an interoperable standardized and secure in-vehicle open telematics Platform (on-board application platform). They believed an intermediate solution should provide data access via a competition-neutral backend server (data server platform) together with a data access via an in-vehicle connector (in-vehicle interface).

CLEPA stated that:

- It is vital that there is fair competition between vehicle manufacturer's distribution network and the independent aftermarket and that the costumer has the choice to go to any supplier even if they are non-authorised.
- The Motor Vehicle Block Exemption Regulation states independent garages or repairers must have access to all spare parts and parts manufacturers must be able to sell directly to the aftermarket. In addition to this, authorized repairers must also have the ability to source spare parts from the supplier of their choice.
- The vehicle driver and/or owner must have the choice to decide whom he wants to give access to in-vehicle data.
- Euro 5/6 regulation ensures independent operators to have direct access to in-vehicle data, free of charge, in an unmonitored and non-discriminatory way using today's on board diagnostics (OBD). (CLEPA, 2015)

In December 2016 it was announced that ACEA and CLEPA will work together to find a balanced concept which addresses the concerns of their members (ACEA & CLEPA, 2016). The press release states that access to in-vehicle data must be safe and secure. Direct third-party access to vehicle functions could increase exposure to hacker attacks and additional safety risks in terms of driver distraction could arise if external parties are granted uncontrolled access to the vehicle's on-board systems, user interfaces and function displays. The proposed concept to achieve a safe and secure way of accessing

[22] http://www.vehiclesermi.eu/

data, based on neutral servers, is explained in more detail in the context of ACEA's position paper below.

It should be noted that this concept is a move away from the on-board application platform concept, which was supported by CLEPA initially, towards a data server platform solution. CLEPA's position on the potential discontinuation of access to data via the OBD port while driving, which was also announced in ACEA's recent position paper, is not known.

3.2.2.3 Alliance for the Freedom of Car Repair (AFCAR)

AFCAR do not believe the Extended Vehicle concept is a suitable solution because car dealers and repairers need equal access to vehicle data. A standardised platform is required to allow independent service providers to develop applications which would work across an entire vehicle range. Without it, third party service suppliers would have to create products or services for each individual vehicle model of each manufacturer. This would not be economically viable for them. If this were the case, it would leave consumers with a restricted choice offered by the vehicle manufacturers.

Standardisation does not refer to the overall in-vehicle system and therefore does not limit the choice of the vehicle manufacturer for a specific form of in-vehicle system. However, to maintain fair competition and to encourage innovation, the platform must have a standardised application programming interface (API). (AFCAR, 2016)

3.2.2.4 European Automobile Manufacturers' Association (ACEA)

In their 'Strategy Paper on Connectivity' from April 2016 (ACEA, 2016a), ACEA supported the Extended Vehicle solution as the best method to ensure that third parties have access to vehicle data they require to offer services to vehicle owners or drivers while allowing vehicle manufacturers to ensure vehicle safety, product monitoring, IT security and data protection compliance as there is no way for unwanted services, offers or advertising to reach the vehicle or the customer.

According to ACEA, the data that can be made available is 'vehicle generated data' or 'operating data'. It excludes any data imported by vehicle users (e.g. from a mobile phone contact list, selected destinations for navigation) and data received from external sources (e.g. information transmitted by roadside units, other vehicles or vulnerable road users). The access to in-vehicle data will be granted depending on the use-case, the nature of usage and type of data. (ACEA, 2016a)

In December 2016 it was announced that ACEA and CLEPA will work together to find a balanced concept which addresses the concerns of their members (ACEA & CLEPA, 2016). ACEA's position paper 'Access to vehicle data for third party services' (ACEA, 2016b) describes this concept in more detail: The idea focuses on neutral servers operated by independent third parties which collect equivalent quality data from the extended vehicle server and arranged via a B2B agreement between the server operator and the vehicle manufacturers (Figure 11).

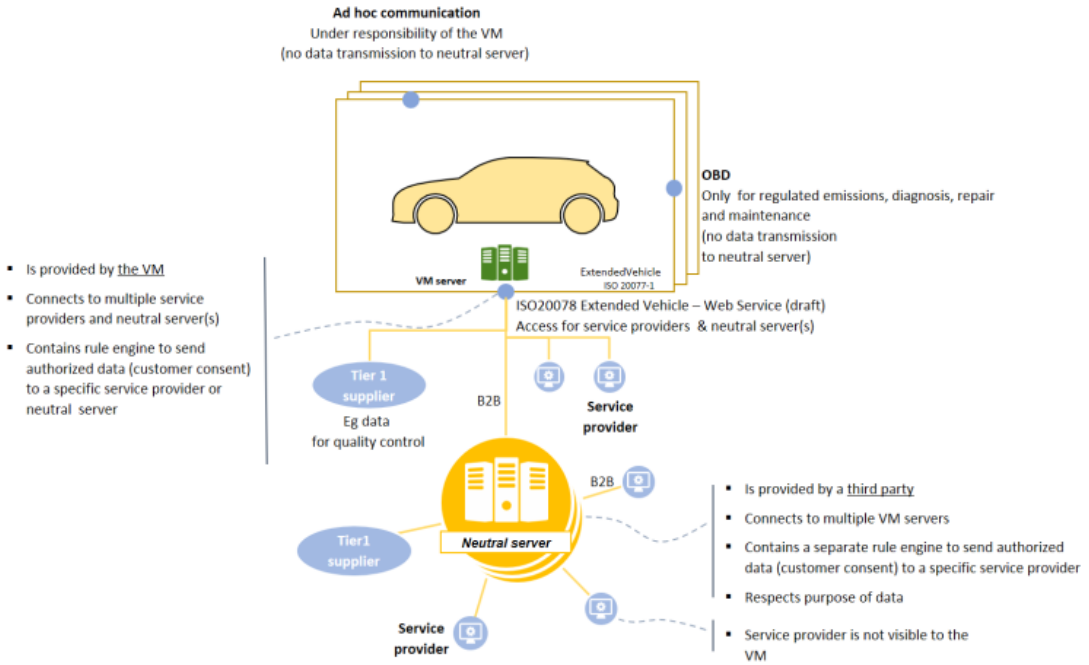


Figure 11: ACEA's proposed neutral server concept (ACEA, 2016b)

This concept is essentially an Extended Vehicle solution with the addition of a 'neutral server'. The neutral server operator can negotiate with the vehicle manufacturers for additional data fields to be included on their servers without revealing by whom and how this data will be used. This will help maintain a level of competition as service providers will get the choice between going through the vehicle manufacturer or the server. The neutral servers are not financed or run by the manufacturer which means, according to ACEA, they will not be able to monitor who is accessing what data except for security reasons and for overall system improvement.

For cyber security reasons caused by incidents relating to third party connected plugs (dongles) vehicle manufacturers reserve themselves the right to limit the data accessible via the OBD interface to those required for diagnosis, repair and maintenance and only when the vehicle is stationary. Access to vehicle data via an OBD interface when the vehicle is stationary, for system diagnosis will still be possible in accordance with EU law. (ACEA, 2016b).

3.2.2.5 German Association of the Automotive Industry (VDA)

The VDA believe access to vehicle data should be based on the business-to-business (B2B) model. Each OEM has the role of a system administrator and will be responsible for the safety and secure transfer of vehicle generated data from the vehicle to a standardized and maintained OEM B2B interface. Third parties will then be able to access vehicle data through the OEM B2B interface or via a neutral server that gathers data from the OEM servers. To avoid risks to customer and public safety third parties will not have direct access to the vehicle. (VDA, 2016)

3.2.2.6 Verband der TÜV e.V. (VdTÜV)

The Association of Technical Inspection Agencies (VdTÜV) strongly believes the automatization and interconnection of cars will increase in the future. It is crucial to provide both protection of the customers data and against cyberattacks as well as to establish equal conditions for all competitors with data-based business models. With this view, VdTÜV proposes a Security Architecture (Automotive platform) in connected vehicles that complies with all the requirements.

According to VdTÜV, a highly secured communication platform, installed in all vehicles as standard, could be implemented to connect all the electronic control devices in the different domains of the vehicle. Any information leaving the vehicle shall be processed in advance by this platform in accordance with specific user profiles. Following the allocation of the data, it shall send the data signed and encrypted to different service providers (OEMs, suppliers, insurance company, owner, fleet management, emergency service, smart city services, car parks, warning services, testing authorities, etc.). And the same applies for any information entering the vehicle. This would create a uniform and interoperable standard for safety and security in the vehicle with the following security features:

- Information flow control (firewall)
- Authentication/ Identification
- Access control to the vehicle interface
- Auditing
- Encryption (cryptographic signing method)
- Random number generator

VdTÜV recommends a European legislative initiative that shall enforce strict data protection provisions for the development of such a data exchange system which would be in the interest of consumers, and also would improve the compatibility of connected vehicles in the European Single Market through uniform standards across Europe. (VdTÜV, 2017)

3.2.2.7 Society of Motor Manufacturers and Traders (SMMT)

In their 'Connected and Autonomous Vehicles position paper' from February 2017, SMMT supported a view that various stakeholders are increasingly interested in accessing and using the growing amount of vehicle generated data. According to SMMT, the vehicle generated data can be divided into three distinct types:

- Type 1: Non-brand differentiated data
  Data that is not differentiated by vehicle manufacturers; not considered IP sensitive.
- Type 2: Brand differentiated data
  Data that is differentiated by vehicle manufacturers; considered IP sensitive.
- Type 3: Personal data
  Data that supports services requiring user or vehicle identification.

Another type of data relevant to autonomous driving, but falls outside the above framework, would be pre- and post-crash data. This type of data shall be stored in a Data Storage System for Automatically Commanded Steering Function (DSSA), which would act as an event data recorder for automated driving at SAE Level 3 and above.

In its view regarding the access to vehicle generated data, SMMT believes that access to vehicle generated data shall uphold the principles of security, safety and privacy without stifling innovation and fair competition. SMMT also supports the guiding principles on granting access to in-vehicle data and resources set out in the European Commission C-ITS Platform.

SMMT also supports the development of guidelines for ensuring vehicle cyber security currently being developed under the auspices of the WP.29 at the UNECE, specifically:

- Verifiable security measures based on existing security standards
- Integrity protection measures
- Appropriate measures to manage used cryptographic keys
- Protection of the integrity of internal communications between controllers
- Strong mutual authentication and secure communication for remote access for online services. (SMMT, 2017)

3.2.2.8 Input from the Independent Aftermarket to the Commission Communication on "Free Flow of Data"

FIGIEFA published this memorandum in 2016 as input during the preparation of the Commission Communication on Building a European data economy (FIGIEFA, 2016).

The authors describe today's situation where analogue access to technical vehicle data is possible through the physical OBD interface, which allows independent operators to apply different diagnostic methods and offer alternative repair methods, such as repair of single components rather than replacement of an entire unit. The data available on the CAN and provided via the OBD is, to a large extent, not standardised but various independent operators have specialised in reverse engineering the information and then offering documentation as well as soft- and hardware allowing independent operators to interpret the data. The authors stress that this access to real time data is a prerequisite for developing alternative repair methods and explain this on an example of a turbocharger, where fault diagnosis requires data with millisecond precision. For future predictive repair and maintenance services, direct access to this raw data was of paramount importance.

The extended vehicle concept, as proposed by the OEMs at the time the document was published, is perceived by FIGIEFA as being in conflict with the principle of free and undistorted competition for the following reasons:

- OEMs face a conflict of interest because they control the in-vehicle data and at the same time are competitors in the aftermarket diagnostics, repair and maintenance, part sales, road side service, insurance and leasing.
- OEMs could exclude market players because a telematics contract between the manufacturer and the customer is a precondition for any data being transmitted and these telematics contracts often already include a range of mandatory services.
- OEMs could exclude market players by making exclusive agreements with single providers.
- Because all data is channelled through OEM servers, they could analyse competitors' behaviour and pricing model.

The authors also comment on potential liability issues when allowing third-party software on a vehicle. These could be overcome by means such as remote verification of the vehicle's software at start-up, pass-through programming, and/or a fingerprint system to register any changes that have been carried out on the vehicle.

FIGIEFA assert that independent market participants need to be able to communicate wirelessly and in real-time with the vehicle in order to ensure fair and undistorted competition. Specific emphasis is placed on the following points:

- Direct access for independent operators to in-vehicle generated real-time (live) data, unmonitored by the vehicle manufacturer as data controller and direct competitor.
- Possibility to apply own applications/functionalities/know-how.
- Same access conditions as the vehicle manufacturers in terms of data and latency and same access conditions for in-vehicle generated data with the possibility to implement embedded applications to evaluate and aggregate that data in the vehicle telematics system.
- Availability of the data via a standardised interface, „interoperability by design".
- Same possibility as the vehicle manufacturer to present services directly via the in-vehicle display to the automobile consumer ("Who owns the dashboard/HMI").
- No disclosure of customer data to the vehicle manufacturer.

FIGIEFA therefore support an interoperable telematics platform, which is an integrated vehicle network interface allowing access to in-vehicle resources and real-time data via a standardised API.

3.2.2.9 Input from Insurer Representatives

Thatcham Research, the Association of British Insurers, the German Insurance Research Association (GDV) and Allianz Center for Technology (AZT) have collaborated in support of a paper regarding the identification of automated driving systems and the provision of data recording and storage suitable for the insurance industry (Thatcham Research, AZT, ADIG, 2016). Whilst this does not directly address the different technical solutions, it does express some intentions regarding data access that are of relevance. The insurers have augmented the proposals of the Data Storage System for Automated driving (DSSA) in Regulation 79 on steering. They emphasise that insurers should be allowed neutral, unbiased access to decoded data either by direct access or via over the air telematics links through a neutral 3rd party data handler. The insurers also require that the system should resist attempts to manipulate or delete data. Standardised non-discriminating access to the data for all parties with a legitimate interest in an individual insurance case (owner of the vehicle, driver, insurer, vehicle manufacturer, supplier, authorities) should be guaranteed. The insurers also suggest that an independent trustee for the DSSA could possibly guarantee impartial access, while providing for data security and data protection.

3.2.3 European frameworks

3.2.3.1 Building a European data economy

The European Commission has recently published a Communication *Building a European data economy*, COM(2017)9 (European Commission, 2017a) and an accompanying Commission Staff Working Document SWD(2017)2 (European Commission, 2017b). These documents, which have a wider focus than just the automotive sector, announce that the Commission intends to explore a possible future EU framework for data access. Such framework could be highly influential for the future developments discussed in the present study (and vice versa). Note, in this context, also the *European Data Market Study* (IDC, 2017), commissioned by DG CNECT, which defines and forecasts relevant indicators to measure the European data economy.

In addition, the earlier Communications *Towards a thriving data-driven economy*, COM(2014)442 (European Commission, 2014) and *A Digital Single Market Strategy for Europe*, COM(2015)192 (European Commission, 2015) set out the features of a data-driven economy and set out conclusions to support an economy that realises the benefits of data, including enabling the infrastructure and systems that allow access to data in a standardised way.

The authors of the recent Commission Communication on data economy stress that, in general, exchange of data between companies remains limited to date and most analysis is done in-house by the same company that created it (or subcontracted out under restrictive terms). The mobility sector is mentioned as an example where companies are opening up some of the data they hold through APIs for access by third party applications. This appears to be done because the data can be used for such a wide range of applications and services that it would not be realistic for the data holding company (in this case the OEM) to develop them all in-house or through commerical partnerships. The new services based on in-house data analytics are often closely related to the traditional non-data product of the company.

The document acknowledges that enterprises and actors in the data economy are dealing with both personal and non-personal data, and data flows and datasets regularly contain both types. This is a common theme linking the free flow of data with the emerging issues of access and transmission of data and is also true for the automotive sector when considering for instance location data which can be related to persons.

In some cases, such as the automotive industry, manufacturers become, according to the authors, the *de facto* 'owners' of the data that their machines or processes generate, even if those machines are owned by the user. A *de facto* control of this data can be a

source of differentiation and competitive advantage for manufacturers. This could result for instance in users and businesses becoming locked into exclusive data exploitation arrangements. Voluntary data sharing might emerge, but negotiating such contracts could entail substantial transaction costs for the weaker parties, when there is an unequal negotiation position or because of the significant costs of hiring legal expertise.

The Commission therefore considers the generation of an EU framework for data access that facilitates the development of a European data economy. A set of five objectives is defined in the Communication:

- Improve access to anonymous machine-generated data
- Facilitate and incentivise the sharing of such data
- Protect investments and assets
- Avoid disclosure of confidential data
- Minimise lock-in effects

The Commission intends to discuss with stakeholders the following possibilities:

  - **Guidance on incentivising businesses to share data**: Provide guidance on how non-personal data control rights should be addressed in contracts with a view to lowering transaction costs.
  - **Fostering the development of technical solutions for reliable identification and exchange of data**: Watermarking of data, technical guidance or standardisation of metadata and APIs.
  - **Model contract terms**: Make available model provisions for data usage licences to lower transaction costs.
  - **Default contract rules**: Lay down default rules for B2B data usage licences in case parties have not foreseen contractual clauses on a specific point.
  - **Access for public interest and scientific purposes**: Grant more authorities and scientific researchers a right to access commercially-held data.
  - **Data producer's right (for non-personal or anonymised data)**: Create a new data producer right, which could assign the exclusive right to utilise and licence data or allow to sue in case of illicit misappropriation of data. Who is the data *producer* would take into account the investments done and resources put into the creation of data. For personal data a data producer right is not possible, as the protection of this data is a fundamental right.
  - **Access against remuneration (to non-personal or anonymised data):** Identify certain types of data to which access can be given to third parties with welfare-enhancing effects without impinging on the economic interests of the player that has invested in the data collecting capabilities and grant non-discriminatory access.

The Communication also covers the topic of portability of non-personal data. For personal data, the GDPR contains a right for data subjects of transmitting data which they have provided to a controller from one controller to another, where technically feasible, and for the data subject to receive the data from the controller. One of the intentions behind this is to prevent lock-in situations for the consumer. Regarding non-personal data, the documents state that introducing a general right to data portability for this data as well could be seen as a possible means to enhance competition, stimulate data sharing and avoid vendor lock-in. Other potential interventions could include recommended contract terms for switching providers or sector-specific data standards encoding access and portability rules.

The cooperative, connected and automated mobility sector is mentioned specifically as being considered for a dedicated real-world trial for assessing the suitability of possible solutions for data access. The first step, however, will be a public consultation.

3.2.3.2 Intelligent Transport Systems (ITS) Directive 2010/40/EU

A new legal framework (Directive 2010/40/EU) was adopted on 7 July 2010 to accelerate the deployment of innovative transport technologies across Europe. This directive is an important instrument for the coordinated implementation of Intelligent Transport Systems (ITS) in Europe. It aims to establish interoperable and seamless ITS services while leaving Member States the freedom to decide which systems to invest in. This directive also aims to adopt specifications (functional, technical, organisational or services provisions) to address the compatibility, interoperability and continuity of ITS solutions across EU within the next seven years in the following areas.

- Optimal use of road, traffic and travel data
- ITS road safety and security application
- Linking the vehicle with the transport infrastructure
- Continuity of traffic and freight management ITS services.

Following are the delegated acts under this directive;

- An interoperable EU-wide eCall – Regulation (EU) No 305/2013
- Safety related minimum universal traffic information – Regulation (EU) No 886/2013[23]
- Information services for safe and secure parking places for trucks and commercial vehicles – Regulation (EU) No 885/2013
- EU-wide real-time traffic information services – Regulation (EU) No 962/2015

The following rules on privacy, security and re-use of information were framed under Article 10 of this directive.

- The Member States shall ensure that the processing of personal data in the context of the operation of ITS applications and services is carried out in accordance with union rules protecting fundamental rights and freedoms of individuals, in particular Directive 95/46/EC and Directive 2002/58/EC.
- The Member States shall ensure that personal data are protected against misuse, including unlawful access, alteration or loss.
- In order to ensure privacy, the use of anonymous data shall be encouraged, where appropriate for the performance of the ITS applications and services.
- Without prejudice to Directive 95/46/EC personal data shall only be processed insofar as such processing is necessary for the performance of ITS applications and services.
- The Member States shall also ensure that the provisions on consent to the processing of special categories of personal data are respected (Directive, 2010).

The adoption of specifications and deployment of ITS applications and services shall comply with a set of 12 principles, which are set out in Annex II of the directive.

3.2.3.3 European Strategy on Cooperative Intelligent Transport Systems (C-ITS)

The European Commission has adopted a European Strategy on Cooperative Intelligent Transport Systems (C-ITS), with a view to regulate cooperative, connected and automated mobility. The strategy aims to deploy vehicles that can communicate to each other and to the infrastructure, by 2019.

[23] Note that service providers are required, under this Regulation, to share road safety-related traffic data collected for the information service. This means that private as well as public service operators (and road operators) have to make the data available through an access point and have to ensure their timely renewal and quality.

The Commission expects the new strategy to significantly improve road safety, traffic efficiency and comfort of driving, while enhancing the market of cooperative, connected and automated driving. Following the recommendations of the C-ITS platform, the Commission has identified issues which should be tackled to ensure coordinated deployment of C-ITS services. The main elements of the strategy are as follows;

1. Avoid a fragmented internal market
   Since many C-ITS deployment activities are currently taking place in the EU; the first objective of the strategy is to avoid fragmented internal market and to create synergies between different initiatives throughout Europe.
2. Define and support common priorities
   The availability of C-ITS services across the EU for end-user must be ensured. Hence, the strategy considers a list of technically mature C-ITS services with clear benefits for transport and society at large, which should be deployed quickly throughout the EU by Member States and local authorities, vehicle manufacturers, road operators and the ITS industry.
3. Use a mix of communication technologies
   The strategy presents a hybrid communication approach combining complementary and available communication technologies. Currently, the most promising hybrid communication mix is a combination of Wi-Fi based short range communication and existing cellular networks.
4. Address security and data protection issues
   The strategy includes the development of a common EU security policy for C-ITS, as well as specific actions to safeguard the right of citizens to control their personal data.
5. Develop the right legal framework
   The strategy includes the development of legal framework to ensure that the necessary technical rules are widely applied in close cooperation with, and learning from experience of C-ITS deployment projects such as the initiatives gathered under the C-ROADS platform.
6. Cooperate at international level
   The Strategy includes the continuation of cooperation with international partners and initiatives in order to learn from each other, in particular the twinning of research and innovation projects (EC, 2016).

3.2.4 Technical standards and vehicle legislation

3.2.4.1 Extended Vehicle ISO standards

The ISO standards related to the Extended Vehicle (ExVe) may be grouped into three categories as shown in Figure 12.

These categories are: the design methodology for generic ExVe standards (ISO 20077-2), the ExVe interface (ISO 20078) and Remote Diagnostics Support (ISO 20080).

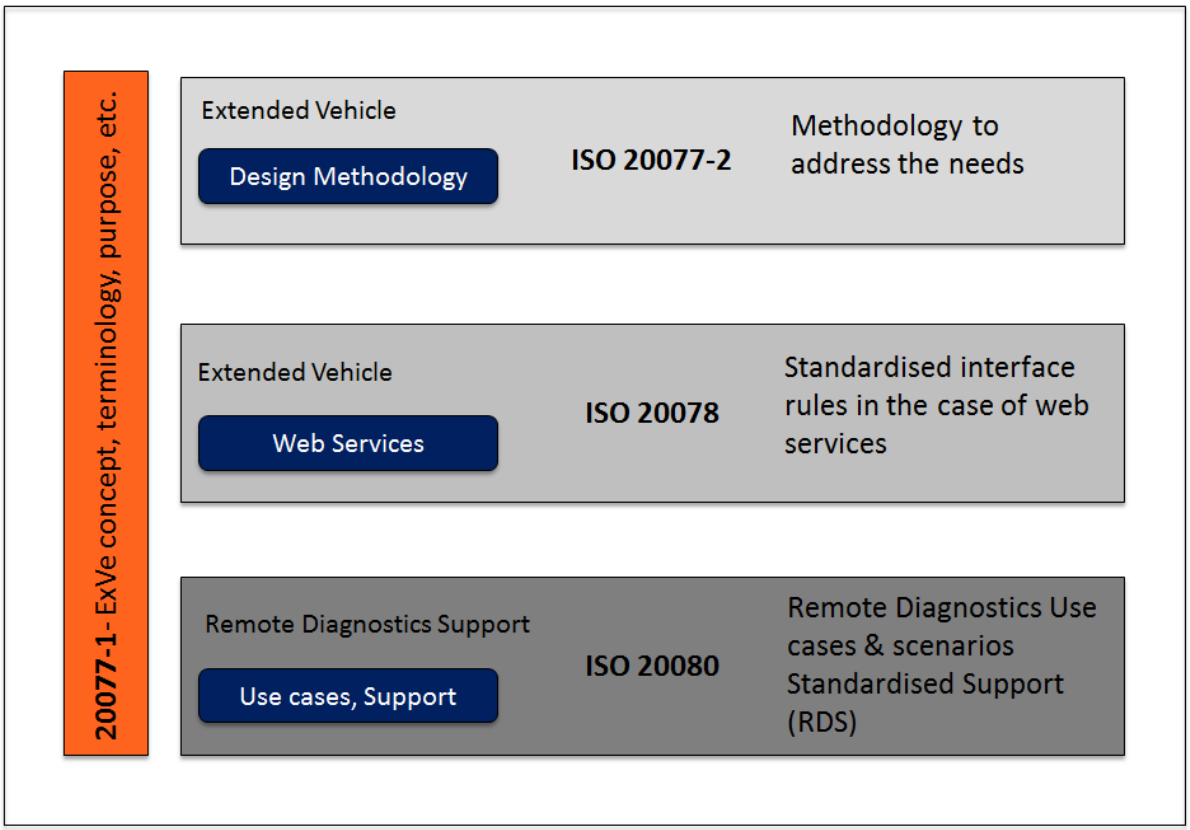


Figure 12: ISO 20077, 20078, 20080 Standards and Projects

ISO 20077 – Series of Standards

The ISO 20077 – series of standards contain diverse generic specifications proper to the extended vehicles and are broadly classified into two parts.

- ISO 20077-1 (part 1) contains essential definitions, concepts and examples concerning extended vehicles and related standards.
- ISO 20077-2 (part 2) contains methodology to design an extended vehicle.

However, these series of standards does not contain any technical specifications.

ISO 20077-2 specifies a set of broad principles and rules from which each vehicle manufacturer shall derive its own methods or procedures to design an extended vehicle that address a specific set of use-cases and scenarios. In general, ISO 20077-2 addresses the below:

- A guidance or template to be used by the requesting party, that fully describes the usage the extended vehicles is requested to address (the use-cases proper, the use-case scenarios, and the use-case functional needs)
- A guidance to be used by the vehicle manufacturers for not omitting any design step in the design process.
- A guidance to be used by the vehicle manufacturer for expressing to the requesting party the technical result of the design.

According to ISO 20077-2, the Extended Vehicle Manufacturer shall take the appropriate measures in its own design methods and procedures. The following principles are to be taken into consideration during the design or a design change of an Extended Vehicle.

1. The Extended Vehicle Manufacturer is responsible for the design of the Extended Vehicle.

2. The Extended Vehicle Manufacturer is responsible for the designing of all the interfaces of the Extended Vehicles that will permit communication with that Extended Vehicle.
3. The Extended Vehicle Manufacturer is responsible for deciding on the implementation of any Extended Vehicle functionality.
4. The Extended Vehicle Manufacturer is responsible for assessing the impacts of a new ExVe functionality during the life-cycle phases of the ExVe.
5. The Extended Vehicle Manufacturer is responsible for managing the additional risks attributed to an existing functionality when it becomes extended and remotely available.
6. The Extended Vehicle Manufacturer is responsible for managing the impacts of an additional remote functionality taking into account the existing design.
7. The Extended Vehicle Manufacturer is responsible for defining the priorities between all functionalities of the Extended Vehicle.
8. The extended Vehicle Manufacturer is responsible for securing that the additional functionality doesn't affect already designed and implemented functionalities of the Extended Vehicle, in particular by taking into consideration the available resources of that Extended Vehicle.
9. The Extended Vehicle design methodology is applicable regardless of the type(s) of communication (wired or wireless).
10. For a given use-case and use-case scenario, the Vehicle Manufacturer is responsible for defining the appropriate Extended Vehicle's interfaces for the considered functionality, and for designing them so that they can be supported to any requester in a non-discriminatory manner.
11. The Extended Vehicle Manufacturer is responsible for validating the design of the complete Extended Vehicle as a complete system, including the case of an additional or modified ExVe functionality.
12. The Vehicle Manufacturer is responsible for ensuring that the designed ExVe functionality respects that the correlation between the vehicle owner and the performed functions is not monitored for competition purposes or in a way which would breach data protection.
13. The Vehicle Manufacturer is responsible for ensuring that the designed ExVe functionality respects that the correlation between the after-sales service provider and the performed functions is not monitored for competition purposes or in a way which would breach data protection.

ISO 20078 and ISO 20080

The ISO 20078 includes typical ISO specifications related to ExVe web services. And the ISO 20080 includes specifications for the remote diagnostics support. The contents of these standards could not be accessed by TRL since they are currently in the draft stage. These standards are expected to be published in Q1 of 2018.

3.2.4.2 Repair and Maintenance Information (RMI) Legislation

Independent operators are needed to increase consumer choice and provide competition for vehicle manufacturer network in the aftermarket. Thus in order to compete in the vehicle repair market, independent operators must be able to access vehicle Repair and Maintenance Information (RMI). This technical information is increasingly important due to the greater complexity of vehicles, growing number of parts and more use of on-board electronics. The European legislation regulated in Regulation 715/2007 (the "Euro 5" Regulation) to ensure that independent operators have easy, restriction-free and standardised access to vehicle.

In the first quarter of 2014, the European Commission consequently conducted a study to review the operation of the system of access to vehicle RMI. The study report (EC RMI, 2016) from the Commission to the European parliament and the Council on access to vehicle Repair and Maintenance Information (RMI) provides a comprehensive and detailed analysis, followed by recommendations, covering six areas essential for understanding the operation of the system.

Following are the implications from the study;

- The RMI study considers there may be a need for further clarification and guidance on access to security-related RMI. However, the introduction of the SERMI (SEcurity related Repair and Maintenance Information) scheme could improve the situation.
  - *The SERMI scheme, provided for in Article 13(9) of Regulation (EC) No 692/2008, aims to create a European-wide process for accreditation, approval and authorisation to access security-related RMI, which would streamline the current patchwork of OEM systems*.
- The study strongly supports that increasing connectivity of vehicles is currently changing the automotive industry landscape. The data that were previously accessed via a physical connection in the vehicle are now increasingly accessible remotely. This would open up the possibility of providing access to real-time information, allowing for remote diagnosis support and prognosis, as well as many other services (e.g. usage based insurance, assistance services, location-based services, smart charging of electric vehicles, car sharing, traffic management, etc.).

The RMI study concludes that in general the scope of vehicle RMI is likely to include at least some information transferred wirelessly. But the precise definitions and means for data exchange would need to be further clarified and included in the RMI Regulations to ensure fair access to information.

3.2.4.3 Remote Fleet management System (rFMS)

The rFMS is the technical standard for accessing fleet management information of trucks remotely through the backend system. The European truck OEMs Daimler, MAN, Scania, Volvo, Renault, DAF and IVECO together developed the FMS-Standard in 2002 to make manufacturer-independent applications for telematics possible by mutually agreeing to give access to vehicle data. The rFMS standard is an evolution of the conventional FMS with capability to connect and transmit information remotely.

Figure 13 shows OEM specific contract and subscription details.

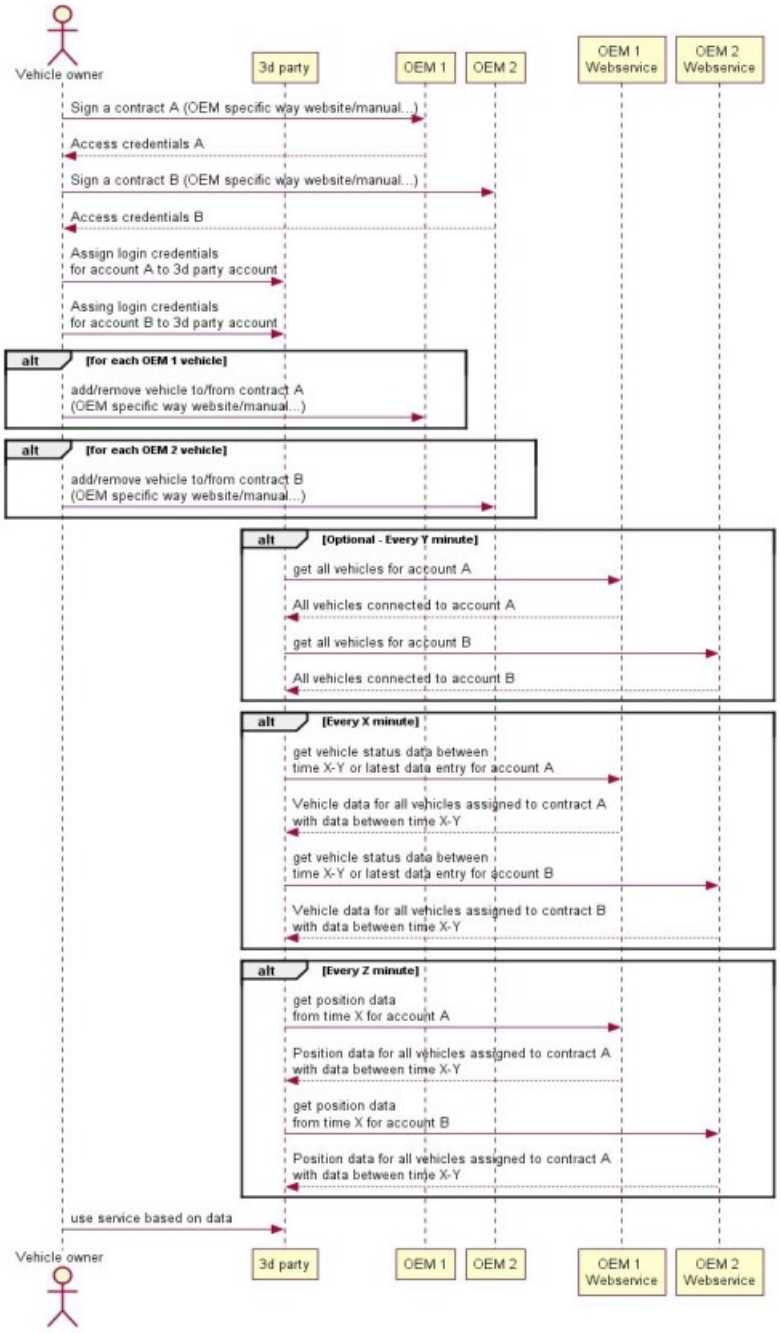


Figure 13 Contract and Subscription (FMS Standard, 2016)

The communication in rFMS is implemented as RESTful (Representational State Transfer) API over https. The RESTful API breaks down a transaction to create a series of small modules. Each module addresses a particular underlying part of the transaction, leveraging lesser bandwidth and making it more suitable for internet usage. The request interval in rFMS is limited to maximum of one minute (i.e., the same request using the same user credentials from the IP address is only allowed every minute).

The following data are broadcasted at the interface;

- Vehicle list – Information about the vehicles user credentials
  - Vehicle Identification Number (ASCII)
  - Customer vehicle name
  - Plate number
  - Services supported

- Vehicle position (current and historical) – Delivers information about the vehicle position with minimum update rate of 15 minutes and storage period of minimum 2 weeks.
  - Vehicle Identification Number
  - Position
  - Speed
- Vehicle status (current and historical) – Delivers information about the vehicle status with minimum update rate of 60 minutes and storage period of minimum 2 weeks.
  - Vehicle Identification Number
  - Position
  - Vehicle Weight
  - Fuel information
  - Mileage
  - Speed

3.2.4.4 SEcurity related Repair and Maintenance Information (SERMI)

The 'EU Forum on Access to Vehicle Information' was established according to Article 13(9) of Regulation (EC) No 692/2008, with an aim to elaborate a pan-European harmonised accreditation scheme and process architecture to help independent operators to service and repair vehicles in a secure manner even if this involves the security features of the vehicle.

Based on the report issued by the EU Forum which describes complete process and architecture on access to security-related RMI, SERMI developed a new scheme version following the suggestions from the European co-operation for Accreditation (EA) in the course of the requested scheme validation.

As per the scheme, the independent operator employees would need a hardware key and pin protected electronic certificate and an authorisation when accessing vehicle manufacturer's website. An employee would only be authorised for security-related RMI access if their employer company has also been approved. The company approval and authorisation are valid only for a period of 36 months, unless revoked due to misuse.

The Security Forum process is as follows.

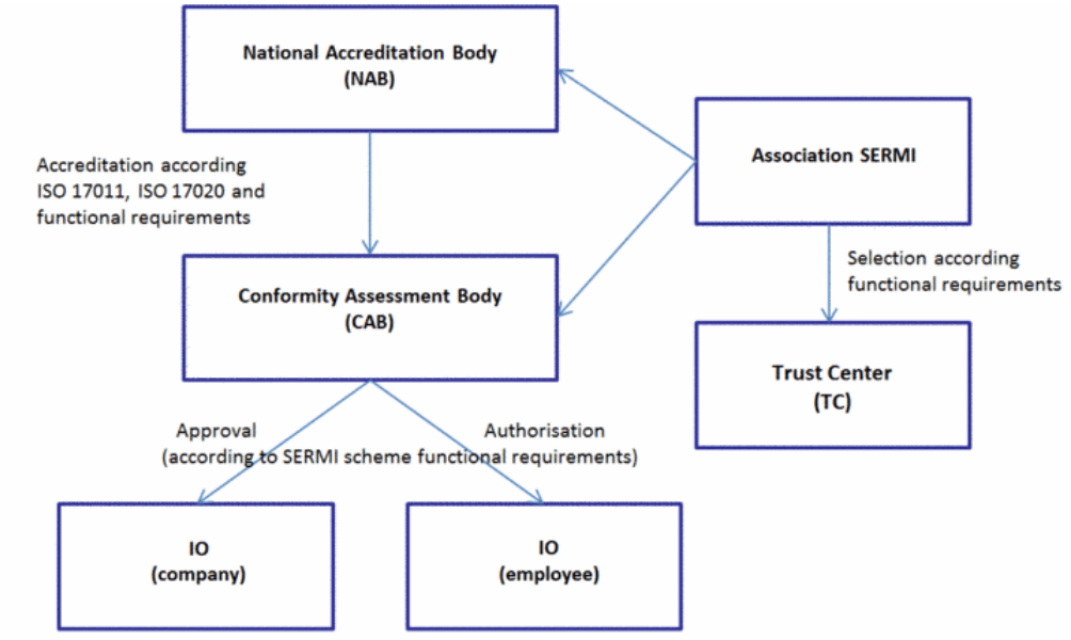


Figure 14 SERMI Security Forum Process (SERMI, 2017)

1. *The Independent Operator (IO) who wishes to conduct security related work will approach a Conformity Assessment Body (CAB).*
2. *The CAB will then carry out the necessary approval (for the commercial enterprise/company) and authorisations (for the individual employees).*
3. *After notification, the Trust Centre (TC) will issue hardware and certificates to be distributed by the CAB to the Independent Operator as appropriate.*
4. *The CAB will be accredited and assessed by the National Accreditation Body (NAB).* (SERMI, 2017)

On 26th April 2016, the Independent Garages Association (IGA) announced that the body for European Accreditation (EA) had officially signed-off SERMI. The SERMI scheme would now go forward into European Type Approval, which would fully approve the scheme once complete.

3.2.4.5 Pass-Thru Vehicle Programming

Pass-Thru vehicle programming demonstrates that it is technically possible to deliver an API that can enable interoperable access to data stored on ECUs and enable third parties to write to ECUs.

Pass-Thru is a concept that was originally developed to enable flash programming of an emission related ECU by independent repairers. Today it is used for many other diagnostic tasks, particularly for OBD tasks. J2534 is an interface standard designed by SAE and mandated by the US EPA (Environmental Protection Agency) for vehicle ECU reprogramming. Its purpose is to create an API (Application Program Interface) which would be adopted by all vehicle manufacturers, allowing the independent aftermarket the ability to reprogram ECUs without the need for a special dealer-only tool.

The use of reprogrammable memory technology in vehicle Electronic Units (ECUs) has increased the flexibility of being able to use a single ECU hardware in many different vehicle configurations. Reprogramming of ECUs in the service environment also allows for ease of field modification of system operation and calibration. The *SAE J2534* allows a single set of programming hardware and vehicle interface to be used to program modules for all vehicle manufacturers. This programming application software supplied by the vehicle manufacturer would run on a commonly available generic PC. The following two interfaces were discussed in the SAE J2534 document.

1. Application Program Interface (API) between the programming application running on a PC and a software device driver for the pass-thru device.
2. Hardware interface between the pass-thru device and the vehicle.

The following recommendations were framed by SAE J2534 for Pass-Thru vehicle programming practice;

- The API should contain a set of routines that may be used by the programming application to control the pass-thru device and to control the communication between the pass-thru device and the vehicle.
- The manufacturer of an SAE J2534 pass-thru device must supply both the device driver software and the hardware that communicates directly with the vehicle.
- The interface between the PC and the pass-thru device can be any technology chosen by the tool manufacturer, including RS-232, RS-485, USB, Ethernet or any other future technology, including wireless technologies.
- The interface between the pass-thru device and the vehicle shall be an SAE J1962 connector for serial data communications. The vehicle manufacturer would need to provide information about connections to any connector other than the SAE J1962 connector.
- Additionally, the pass thru device must support simultaneous communication of an ISO 9141 or ISO 14230-4 protocol, an SAE J1850 protocol and a CAN or SCI based protocol during a single programming event.

- The OEM programming application does not need to know the hardware connected to the PC, which would give the tool manufacturers the flexibility to use any commonly available interface to the PC.
- Similarly, the pass-thru device does not need any knowledge of the vehicle or the control module being programmed. This would allow all the programming applications to work with all pass-thru devices and enable programming of all control modules for all vehicle manufacturers (SAE, 2002).

3.2.4.6 UN Regulation No. 49

The UN Regulation 49 details the provisions concerning the measures to be taken against the emission of gaseous and particulate pollutants from Compression-Ignition engines and positive ignition engines for use in heavy vehicles (*categories M1, M2, N1 and N2 with a reference mass exceeding 2,610 kg and to all motor vehicles of categories M3 and N3*). The Annex 9 and 14 under this regulation specifies information related to the access to vehicle OBD (On-Board Diagnostic) system.

Based on the world-wide harmonized OBD global technical regulation (GTR) No. 5, the Annex 9B of Regulation 49 states that Access to the OBD information shall not be dependent on any access code or other device or method obtainable only from the manufacturer or its suppliers. Interpretation of the OBD information shall not require any unique decoding information, unless that information is publicly available. It also states that a single access method to OBD information shall be supported to retrieve all OBD information possibly by means of a wired connection. And this method shall permit access to specific smaller information packages using at least one of the following series of standards;

a) ISO 27145 with ISO 15765-4 (CAN-based)
b) ISO 27145 with ISO 13400 (TCP/IP-based)
c) SAE J1939-73

As per the current regulation, the following information recorded by the OBD system would be available upon off-board request;

- ***Information about the engine state*** (read only access)
  According to the standards specified, the OBD system shall provide the following information:
  - Discriminatory/non-discriminatory display strategy;
  - The VIN (vehicle identification number);
  - Presence of a continuous-MI;
  - The readiness of the OBD system;
  - The number of engine operating hours during which a continuous-MI was last activated (continuous-MI counter).
- ***Information about active emission-related malfunctions*** (read only access)
  The OBD system shall provide the following information according to the standards specified.
  - The GTR (and revision) number, to be integrated into Regulation No. 49 type-approval marking;
  - Discriminatory/ non-discriminatory display strategy;
  - The VIN (vehicle identification number);
  - The Malfunction Indicator status;
  - The Readiness of the OBD system;
  - Number of warm-up cycles and number of engine operating hours since recorded OBD information was last cleared;
  - The number of engine operating hours during which a continuous-MI was last activated (continuous-MI counter);
  - The cumulated operating hours with a continuous-MI (cumulative continuous-MI counter);
  - The value of the B1 counter with the highest number of engine operating hours;

- The confirmed and active DTCs for Class A malfunctions;
- The confirmed and active DTCs for Classes B (B1 and B2) malfunctions;
- The confirmed and active DTCs for Class B1 malfunctions;
- The software calibration identification(s);
- The calibration verification number(s).

- ***Information for repairs*** *(read and delete access)*
  The OBD system shall provide the following malfunctions of engine system and related information according to the specified standards.
  - GTR (and revision) number, to be integrated into Regulation No.49 type-approval marking;
  - VIN (vehicle identification number);
  - Malfunction indicator status;
  - Readiness of the OBD system;
  - Number of warm-up cycles and number of engine operating hours since recorded OBD information was last cleared;
  - Monitor status (i.e. disabled for the rest of this drive cycle complete this drive cycle, or not complete this drive cycle) since last engine shut-off for each monitor used for readiness status;
  - Number of engine operating hours since the malfunction indicator has been activated (continuous MI counter);
  - Confirmed and active DTCs for Class A malfunctions;
  - Confirmed and active DTCs for Classes B (B1 and B2) malfunctions;
  - Cumulated operating hours with a continuous-MI (cumulative continuous-MI counter);
  - Value of the B1 counter with the highest number of engine operating hours;
  - Confirmed and active DTCs for Class B1 malfunctions and the number of engine operating hours from the B1-counter(s);
  - Confirmed and active DTCs for Class C malfunctions;
  - Pending DTCs and their associated class;
  - Previously active DTCs and their associated class;
  - Real-time information on OEM selected and supported sensor signals, internal and output signals;
  - Freeze frame data required by this annex ;
  - Software calibration identification(s);
  - Calibration verification number(s).

The regulation also emphasis to include features to deter modification of OBD information, except authorized by the manufacturer in case modifications are necessary for the diagnosis, servicing, inspection, retrofitting or repair of the vehicle. And any reprogrammable computer codes or operating parameters shall be resistant to tampering and afford a level of protection at least as good as ISO 15031-7 (SAE J2186) or J1939-73.

3.2.4.7 UN Regulation No. 83

The UN Regulation 83 details the provisions concerning the approval of light vehicles with regard to the emission of pollutants according to engine fuel requirements (*vehicles of categories M1, M2, N1 and N2 with a reference mass not exceeding 2,610 kg*). The Annex 11 under this regulation applies to the aspects of On-Board Diagnostic (OBD) system for the emission control of motor vehicles. The regulation specifies the following requirements;

- All vehicles shall be equipped with an OBD system to enable it to identify types of deterioration or malfunction over the entire life cycle of the vehicle.
- Access to the OBD information required for the inspection, diagnosis, servicing or repair of the vehicle shall be unrestricted and standardised.

- Manufacturer may temporarily disable the OBD monitoring under certain circumstances where malfunction detection might not be reliable (e.g. at low engine starting temperatures or low fuel levels).
- Upon request, the Approval Authorities shall make relevant information on the OBD system available to any interested components, diagnostic tools or test equipment on a non-discriminatory basis.

However, the regulation does not provide any information on the data access methods and security procedures.

3.2.5 Technical implementations

The following section provides an overview of the most relevant technical implementations related to the access to in-vehicle data and resources, which exist on the market today or were announced recently.

3.2.5.1 Toyota T-Connect

Toyota Motor Corporation announced (June 18, 2014) a new telematics service 'T-Connect', with an advance navigation system and a wide range of services including optimal route guidance and information regarding the chosen destination. This service would only be available in Japan and some selected countries in the Middle East.

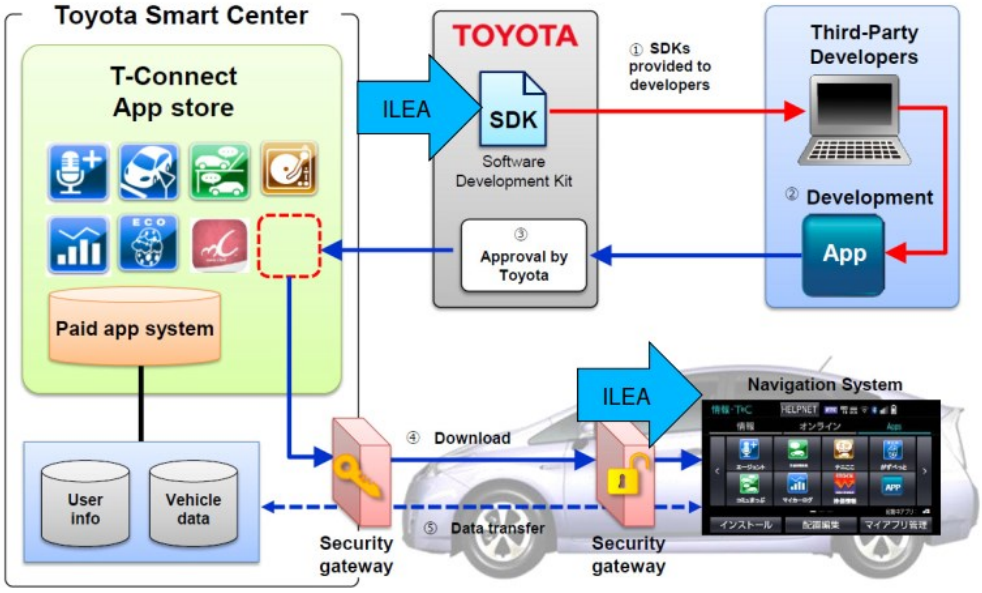


Figure 15 Toyota Open Vehicle Architecture (IBM, 2015)

T-Connect allows third-party applications to be downloaded to the car's navigation system and also an online help service that integrates and improves on the functions provided by the current G-BOOK (Toyota's current Telematics subscription service). T-Connect also features a dedicated smartphone app in conjunction with the in-car navigation screen, which features to record mileage, travel distance and route history (Toyota, 2017).

As part of T-Connect, Toyota created an open development environment called Toyota Open Vehicle Architecture (TOVA), and provides software development kits to prospective developers. Following approval by Toyota, apps would be hosted in the T-Connect app store with a payment framework allowing developers to charge for their apps. To make T-Connect easily accessible, the system comes with Wi-Fi connectivity as standard. Customers could use their smartphone or participating Wi-Fi spots to connect to various services available through the Toyota Smart Center (IBM, 2015).

3.2.5.2 GM's OnStar Go and Next Generation Infotainment Software Development Kit (NGI SDK)

General Motors and IBM announced (26th October 2016) a partnership to bring the existing OnStar and IBM Watson together to create 'OnStar Go', a cognitive mobility platform. The new platform is expected to deliver personalised content directly onto the car's dashboard display based on the current location. It could include avoiding traffic when on low fuel, activating a pump at the fuel station and paying from the car via dashboard interface, receiving news and weather updates and in-vehicle entertainment based on real-time location. Further, brands such as ExxonMobil, iHeartRadio, MasterCard and Parkopedia have announced applications for this platform (IBM, 2017).

Following the launch of OnStar Go, General Motors announced (26th January 2017) a next generation infotainment software development kit (NGI SDK) that allows developers to develop and test in-vehicle applications for their infotainment systems. With the NGI SDK, applications could be built to run directly on the vehicle using HTML5 and JavaScript. General Motors allows two distinct and separate ways for developers to build applications. The first method involves interacting remotely with the vehicle using a simulated environment through a smartphone, tablet or computer, while the second method makes use of simulated in-vehicle information such as location data or vehicle diagnostics, to create apps that could be incorporated into the vehicles infotainment systems upon approval by GM and made available through the AppShop.

The development kit includes the native Application Program Interfaces (APIs), that allows developers access to nearly 400 vehicle data points including;

- Instrument panel measurements - trip odometer and vehicle speed
- Driver information - presence of passengers or if the windows are open or closed
- Vehicle features - radio or backup camera
- Performance and maintenance - oil life and tire pressure
- Lights and indicators – lightbulb status or low washer fluid.

3.2.5.3 PSA Continental Infotainment Platform

PSA group and Continental presented (28th November 2016) a new infotainment system 'Connect', which combines online services and broad smartphone integration solutions. The system is based on the Linux open-source operating system and complies with GENIVI Alliance (open development community collaboratively producing automotive software components, standard APIs, and a development platform for in-vehicle infotainment and connected vehicle solutions) software standard.

The 'Connect' head unit incorporates an embedded navigation system from the supplier TomTom, which integrates a variety of current online services including live traffic information, weather forecasts, parking information, and fuel prices. The real-time traffic information also enables the system to predict the exact arrival time. Alongside the online connected services, the system also features smartphone connectivity via USB based on the mirroring principle, with Apple CarPlay and MirrorLink. Further, the system is expected to be integrated deeply into the vehicle structure through links with the interior/ dashboard cameras and location-based services (Continental, 2017).

3.2.5.4 Ford Smart Device Link

SmartDeviceLink (SDL) is an open-source technology developed by Ford for connecting mobile apps with in-car interfaces. It is a standard set of protocols and messages that connect applications on a smartphone to a vehicle head unit. This messaging enables a consumer to interact with their application using common in-vehicle interfaces such as a touch screen display, embedded voice recognition, steering wheel controls and various vehicle knobs and buttons. There are three main components that make up the SDL ecosystem.

- The Core component is the software which Vehicle Manufacturers (OEMs) implement in their vehicle head units. Integrating this component into their head unit and HMI based on a set of guidelines and templates enables access to various smartphone applications.
- The optional SDL Server used by Vehicle OEMs to update application policies and gather usage information for connected applications.
- The iOS and Android libraries are implemented by app developers into their applications to enable command and control via the connected head unit.

SDL Core: The core's primary function is to pass messages between connected smartphone applications and the vehicle HMI, and pass notifications from the vehicle to those applications. It connects a smartphone to vehicle's head unit via a variety of transport protocols such as Bluetooth, USB, Android AOA, and TCP. Once a connection is established, Core discovers compatible applications and displays them to the driver for interaction via voice or display. The core component is implemented into the vehicle HMI based on a set of integration guidelines. The core component is configured to follow a set of policies defined in a policy database and updated by a policy server. The messaging between a connected application and core is defined by the Mobile API (Application Program Interface) and the messaging between sdl core and the vehicle is defined by the HMI API.

SDL Server: The SDL server handles authentication, data collection and basic configurations for SDL connected vehicles. In general these tasks are accomplished using JSON (Java Script Object Notation) documents called Policy Tables that are configured by the server and then downloaded by other SDL components. The server's backend API handles these types of requests and could be easily extended to handle more. Configuration of Policy Tables, or any other data, could be done using the server's front-end GUI (GENIVI , 2016).

3.2.5.5 Android Auto

Android Auto is a smartphone projection technology developed by Google to extend the Android platform running on the smartphone into the vehicle head unit. The user's Android device connects to the vehicle via USB cable. Rather than running on its own operating system, the head unit will serve as an external display for the Android device, by presenting a car-specific user interface. User may interact with compatible apps and services through voice actions and the vehicle's input controls (like a touchscreen or dashboard buttons).

As part of the Open Automotive Alliance (an alliance of automotive manufacturers and technology companies aimed at using Android in automobiles), Android Auto was announced on January 6, 2014, with 28 automotive manufacturers and mobile tech supplier NVidia. Android Auto is now available in a majority of OEM models and several aftermarket car audio systems including Pioneer, Kenwood and Panasonic.

With Android Auto, the connected mobile device would have access to vehicles sensors and input units as below;

- GPS Antennas
- Steering-wheel mounted controls/buttons
- Speakers/ Microphones
- Wheel speed
- Compass
- Car data (under development)

3.2.5.6 Apple CarPlay

CarPlay is Apple's standard to enable a car radio or head unit to be a display and controller for an iPhone, first announced during the Apple WWDC (World Wide Developer Conference) in 2010. It requires OEMs to implement hardware and software components in the car, so that the car controls (touch screen, knob, steering-mounted buttons) can

be used to send commands to the application on the iPhone and results from the application can be displayed on in the car displays. By design, the CarPlay architecture allows deeper integration with in-car functionalities such as monitoring fuel level; the extent of integration is only limited by the respective OEMs willingness and ability. The majority of OEMs and some aftermarket car audio systems like Alpine, Kenwood, Pioneer and JVC have already adopted Apple's CarPlay.

The phone could be connected to the car by two methods.

- Wired connection – USB (Lightning cable)
- Wireless connection (Wi-Fi and Bluetooth)

For wired CarPlay, the data is wrapped in IP (Internet Protocol) and transmitted via USB, except for the iAP2 communication protocol. The information from vehicle sensors is sent over iAP2 as is audio, telephony and turn-by-turn metadata. The iAP2 protocol (iPod Accessory Protocol) is used in Bluetooth communications between iOS device and wireless accessories such as dock station or car adapters. This profile enables to exploit Apple-specific features such as play control of iOS device, transferring metadata/ contact information, receiving media/ call information, sending RAW data, etc. The communication plug-in is the source code provided by Apple that receives the incoming video and audio streams as well as an additional communication stream. The audio and video is sent to the head unit's infrastructure, connected to the speakers, microphone, and display.

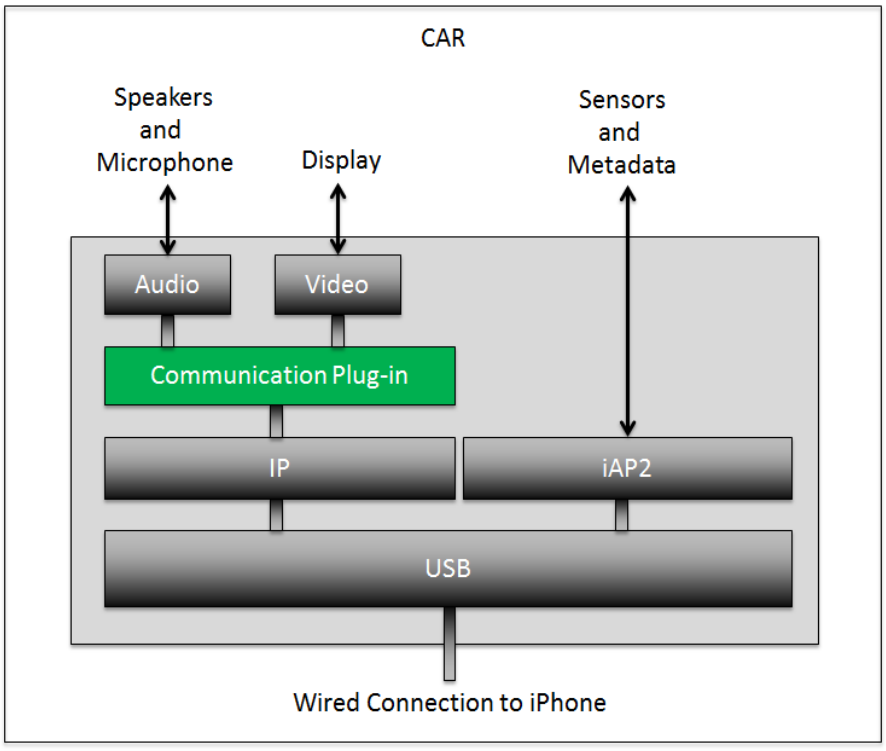


Figure 16 Wired Architecture overview; figure created by TRL based on (Apple Inc, 2017)

In case of wireless CarPlay, the overall architecture is similar, but all data (including iAP2) is wrapped in IP and the connection is established via Bluetooth and Wi-Fi. Bluetooth is only used for discovery and initial connection. Once the Wi-Fi credentials are sent to the phone over Bluetooth, all subsequent CarPlay communications are over Wi-Fi, and Bluetooth is disconnected.

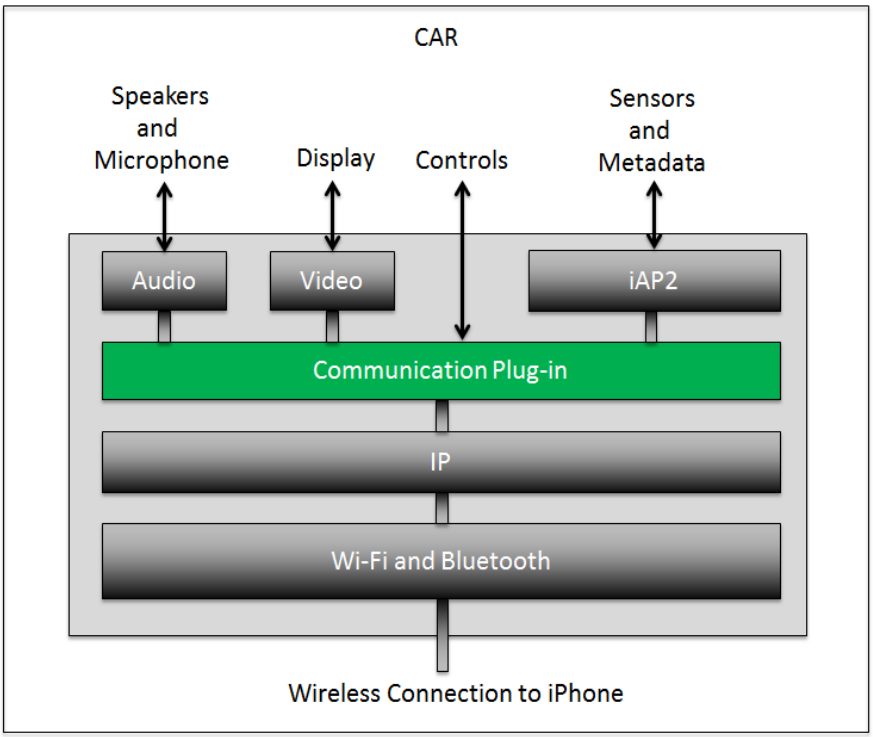


Figure 17 New Wireless Architecture overview; figure created by TRL based on (Apple Inc, 2017)

The Apple CarPlay architecture also allows parallel operating systems inside the car (i.e. both OEM and Apple OS). An application communicates with the vehicle to perform functions such as changing radio stations, climate controls, etc., after receiving commands from the CarPlay interface.

CarPlay apps are available through Apple's App Store (after approval by Apple). The majority of approved apps are Apple's own software with a limited number of third-party infotainment apps. Car manufacturers have started recently to offer their own CarPlay apps: In 2016 SEAT was first to introduce its DriveApp, which allows vehicle data and servicing information to be checked while still within Apple's interface on the vehicle's HMI. The DriveApp was developed to work with Mirrorlink technology, but is also compatible with Apple CarPlay and Android Auto. It allows the car's 'health status' information such as oil level, battery, wheels, lights, wiper fluid or engine faults to be checked. It also gives warnings when the car detects a need for maintenance in any of these areas and allows the nearest SEAT dealerships to be located. SEAT also uses the app to provide the driver via Apple's interface on the vehicle's HMI with offers and special deals for services of SEAT repair garages. The data flow between the car's bus system, the HMI and the phone running the DriveApp are not publicly documented, but it should be noted that the functionality offered could be realised by transmitting in-vehicle data via an OEM server (from the car's connectivity control unit via an OEM server and the phone to the vehicle HMI), i.e. it does not indicate that SEAT accesses in-vehicle maintenance data directly via CarPlay.

3.2.5.7 Jaguar In-Car Payment System

Jaguar and Shell introduced (on 15th February 2017) a new in-car payment platform to pay for fuel at shell service stations using PayPal or Apple Pay via the car's touchscreen infotainment system. Android Pay to be added later in 2017. An electronic receipt will be displayed on the touchscreen, so customers can leave the forecourt confident of having paid. It also features to send the electronic receipt directly from the pump to the driver's email address. Further, Jaguar plans to extend this cashless technology to parking and drive-through restaurants payments (Jaguar, 2017).

3.2.5.8 Open Telematics Platform

The Open Telematics Platform (OTP) is a system that is available on the market currently and is an open and non-discriminatory platform for modern telematics services. This is an instance of an in-vehicle interface solution as considered by WG6. It allows the use of modern telematics applications via smartphone or other connected devices, even on older vehicles (from 2001) with OBD-II interface.

The Open Telematics Platform consists of the OTP backend, the OTP adapter and the OTP API. The OTP backend manages the OTP adapters, vehicles, devices and users and regulates the authorized and secure access to the vehicle operating data. The OTP adapter connected to the OBD-II interface reads vehicle operating data and transmits this data to authorized devices via Wi-Fi or to cloud applications via UMTS (Universal Mobile Telecommunications Service). Devices could be any Wi-Fi enabled devices, e.g. Smartphones, PCs or other OTP adapters. The applications of the telematics providers use the OTP API to read the vehicle operating data from the OTP adapter. For this, the application needs to be installed and authorised on the device for particular OTP adapter. With its own platform, OTP regulates the trustworthy communication of vehicle data by signing and encrypting all data only to devices and cloud applications that are authored by the user.

Generally, the exchanges of data are controlled by a Telematics Control Unit (TCU), which serves as an information gateway in the vehicle. It is connected to both the wireless link via a GSM module and internally to the vehicle's communication busses and to the physical OBD connector. By providing an additional external communication to the vehicle data busses, there is an increased security threat (otp, 2014).

A set of fundamental security requirements for a modern connectivity control unit was developed by CLEPA for WG6 (WG6-A2D - Annex 7 - In-vehicle Interface Security Requirements CCU), which were also re-iterated by FIGIEFA as security concept for an Open Telematics Platform (FIGIEFA, 2017). These include:

1. Secure communication between TCU and the backend servers
    - Ensure authenticity and integrity of transmitted data
    - Ensure confidentiality of data
    - Mutual authentication of entities
    - Ensure validity of fresh data messages
    - Ensure perfect forward secrecy
    - Usage of a suitable protocol for the secure communication
2. Security guidelines for the TCU
    - Unique Cryptographic Identities
    - Hardware-based Security
        - Key storage
        - Hardware Support/Acceleration for Cryptographic Algorithms
        - Usage of Hardware Security Modules
    - Use Strong Cryptography with Sufficient Key Lengths
    - A robust TCU Operating System
    - Employ a Security Engineering Process during ECU/TCU Development
    - Perform Penetration Tests of the TCU
    - Control communication to the Vehicle Bus
    - Secure boost
    - Secure programming
    - Secure confidential and private data on the CCU
    - Secure physical access to the CCU
        - Secure debug
        - Authentication of external interfaces
        - Securing the money
3. Security guidelines for the backend servers
    - Employ mechanisms in the backend servers to isolate malicious TCUs
    - Establish a private communication network.

3.2.6 Conclusions

The literature survey could not identify tangible information on costs, quantified benefits or evidenced estimates of timescales to implementation of the technical solutions. Regarding the other aspects researched, relevant findings were made and these helped inform the other topics of the project, in particular the technical analysis, the stakeholder questionnaire and the scenario analysis:

The latest stakeholder positions were summarised and some aspects were found to have developed considerably since the WG6 final report. Notably, ACEA and CLEPA have shown willingness to work together on a common solution and ACEA promotes an 'Extended vehicle'/neutral server solution, which is in many aspects akin to the 'Data Server - B2B marketplace' discussed in WG6. Aftermarket stakeholders appear to largely oppose to this concept and do not consider it to be a viable solution to their concerns expressed during WG6 around data control by the car manufacturers. FIGIEFA instead support an interoperable telematics platform (analogous to the On-board Application Platform), which is an integrated vehicle network interface allowing access to in-vehicle resources and real-time data via a standardised API. VdTÜV promotes a highly secured communication platform installed in all vehicles as standard and recommends a European legislative initiative that shall enforce strict data protection provisions for the development of such a data exchange system.

The European strategies and Commission Communications, such as the Communication on 'Building a European data economy', demonstrate that legislative actions (including hard and soft measures) are being considered in the wider area of ownership, exchange and access to machine- or process-generated data. Portability of non-personal data is another subject covered in these considerations. The cooperative, connected and automated mobility sector is mentioned specifically as being considered for a dedicated real-world trial for assessing the suitability of possible solutions for data access.

The review of the Extended Vehicle standards was hampered by the fact that TRL could not obtain access to the draft versions of ISO 20078 and ISO 20080, because these cannot be shared outside the ISO working group. Parts 1 and 2 of ISO 20077, containing definitions, concepts and methodologies, were summarised; however, their technical content is limited. With regard to recent developments in the RMI sector, SERMI is described to show an example of how an accreditation scheme can ensure access for independent operators to service and repair vehicles in a secure manner even if this involves the security features of the vehicle. This involves hardware keys and pin protected electronic certificates for workshops to access critical information vie the OEM's website. Pass-Thru is an example of an interface standard (API) implemented by some OEMs that allows the independent aftermarket the ability to reprogram ECU's without the need for a special dealer-only tool. Further, OEMs have announced that they reserve the right to restrict access via the OBD-II port to the legally required minimum conditions. The summary of OBD prescriptions in UN Regulations No. 49 and 83 gives an overview of the extent of data that would remain available via the OBD-II port if this was the case.

The review of existing and announced technical implementations for access to in-vehicle data and resources identified a perceived high level of activity in this area and describes the most relevant recent examples, including the smartphone projection standards Android Auto and Apple CarPlay. It was found that OEMs have started providing their own apps, such as SEAT's DriveApp, which uses CarPlay to indicate the repair and maintenance status of the vehicle and offer special deals at SEAT repair garages on the in-vehicle HMI. This survey also identified examples of recently introduced open on-board application platforms, e.g. Toyota's T-Connect and GM's Next Generation Infotainment SDK. These platforms allow third parties to develop apps that can be executed on the vehicle HMI after approval by the OEM.

In TRL's view, this demonstrates two important points: That OEMs do have an interest of making data accessible to third parties in order to allow their

customers access to new apps and services; and that it is indeed technically feasible today to provide an open app platform for third parties in a safe and secure way that allows access to in-vehicle data and can display information on the vehicle HMI.

3.3 Stakeholder Consultation

TRL hosted an online questionnaire on smartsurvey.co.uk with an aim to assist the Commission in further progressing on this topic and in fulfilling the legislators request regarding an interoperable, standardized, secure and open-access platform. The questions were designed to solicit initial stakeholder information on the legal, technical and cost-benefit aspects as part of the work to understand the issues associated with each of the models to access in-vehicle data.

The respondents in general produced similar or identical responses to the online questionnaire indicating strong agreement of opinion. In particular the 'repair & maintenance' respondents had a similar view and put together an agreed response.

The responses on timelines indicate that the data server solution was most commonly expected within one year of selection, although a few thought it might take a few years longer. The extended vehicle version was more strongly expected within one year. The shared server version was a more even mix through the timescales, perhaps indicating a less clear forecast, although the largest response was still for within one year. For the on-board application platform the most common response was 5-10 years, although 2-5 years was a close second; this is seen as a mid-term solution by most respondents although the car manufacturers considered it would take 10 or more years, citing sequential technical steps necessary to achieve appropriate security. The in-vehicle interface was also viewed as a 2-5 year implementation, although the OEMs indicated that they thought it would take 10+ years to implement the in-vehicle interface solution.

Generally, respondents favoured the data-server platform in the short-term and the on-board application platform the in the medium and long term. This reflects the general outcome of the C-ITS WG6 report. However, many of the responses were from 'repair & maintenance stakeholders, meaning that co-ordinated responses for the on-board platform skewed the results toward the responses for this stakeholder group. Some respondents indicated a road-map approach whereby the short-term solutions of data server platform and in-vehicle interface would ultimately result in the on-board application platform.

Generally, respondents indicated that the Data server platform was the preferred short term solution because the technology and system is already in place, so benefits can be attained immediately using a secure system. While the Extended Vehicle provides vehicle manufacturers with all access controls of the in-vehicle data and become the only controllers of data, most of the repair and maintenance and third-party participants found this solution not a level playing field because the OEMs would control the data and monitor their activities. Many respondents here felt that the OEMs might control or restrict access to the data. Secondly it restricts access to real time data and functions needed for time critical services. Thirdly, it restricts innovation and may add extra costs for third parties to access data, for example by the OEMs charging for access to the data.

Generally, respondents favoured the data-server platform in the short-term and the on-board application platform the in long term. This reflects the general outcome of the C-ITS WG6 report. The on-board application platform allows direct access to data in real time for all stakeholders. However, the implementation of a security layer with a connectivity control unit (CCU) is necessary and this should be developed before the next generation of cars pave the path for automated driving. Most respondents suggest this solution provides fair competition, a non-discriminatory access to data and a level playing field.

The "second best" solution for the long term according to responses was equally split between the in-vehicle interface and the data server platform. Some respondents

indicated a road-map approach whereby the short-term solutions of data server platform and in-vehicle interface would ultimately result in the on-board application platform.

The second aspect of questionnaire asking for cost estimates were not well answered with many respondents not providing cost estimates. General feedback was that it was not possible to quantity costs without significant work. TRL contacted individual stakeholders to get supplementary information and to ask if they had to provide any other information, but the majority of them were happy with what they initially provided to the online questionnaire and preferred not to add any extras.

For detailed questionnaire analysis please refer to Appendix B.

3.4 Analysis of key technical aspects

This task collates information gathered in Sections 3.1 to 3.3 to provide a detailed assessment of the key technical aspects with respect to implementation of the WG6 solutions. These were defined from the various points of contacts with stakeholders in the project that highlighted areas of disagreement between stakeholder groups. TRL identified eight key technical aspects:

1) Safety and security
2) Choice of communication provider
3) Data availability in the car
4) Access to vehicle HMI
5) Futureproofing
6) Contractual control
7) Read/write access
8) Methods of access

3.4.1 Safety and security

Safety and security are critical for all technical solutions that access in-vehicle data and resources. The primary concern expressed by vehicle manufacturers was that providing access to vehicle data directly in the vehicle (i.e. via an in-vehicle interface or the on-board application platform) poses a threat to the electrical architecture of the vehicle which could expose the vehicle and its occupants to unacceptable safety and security risks. Other market participants acknowledged that developments in safety and security were required but were of the view that these could be implemented to ensure acceptable levels of safety and security.

Vehicle manufacturers cite concerns relating to CAN bus overload for example if multiple application providers request access to data from the vehicle at the same time. This event could result in an application crashing on the HMI or a possible memory dump. A scenario such as this could become life threatening to the occupants in the case of an emergency where safety critical messages (for example: AEB activation, restraints/seat belt/fuel supply etc.) could not obtain broadcast priority because of a CAN bus overload.

Third parties cited Apple and Google as platforms which can host multiple applications; vehicle manufacturers pointed out the fact that there are many applications which crash on an Apple iPhone even though it has a good architecture. However, crashing of applications on a mobile device presents a different set of outcomes compared to applications crashing on the HMI of the vehicle, where other safety critical functions could be adversely affected.

Another scenario which presents a similar risk of CAN bus overload is if a command requesting data from a dedicated ECU (to which the ECU responds) is sent repeatedly at a very high frequency. During this event, safety critical messages could also be delayed or prevented from entering the CAN bus because of the volume of traffic. Hence, malicious intent or even a programming error while designing the application could fill

the bus with unnecessary messages and compromise the safe functioning of the vehicle system.

For both these examples, certification of applications by the manufacturer prior to deployment is essential.

Safety and security must be ensured throughout the lifetime of the vehicle. The development process of a vehicle before it is launched into the market includes certain key phases, for example: concept creation, clay design, building prototypes, testing and validation. This process could take six to seven years before the customer takes delivery of the vehicle. Once a vehicle is produced, it is extremely difficult to re-engineer and add additional components or ECUs for extra functionality. This could not only complicate the existing systems, but also lead to potential failures of the on-board systems.

In addition, before a vehicle is launched in the market the vehicle goes through a series of certifications and tests for example crash tests, EU type-approval, EMC tests, etc. Adding extra components would require the vehicle manufacturers to recertify the engineered product, re-conduct a series of checks, tests and certifications before vehicles can be placed on the market. This process therefore adds complexity and cost for the vehicle manufacturer.

Manufacturers also asserted that security and cybersecurity are never a constant. Security needs to be ensured end-to end on all systems and a component and has to last until the vehicle is taken off the market; this timeframe can be in the range of 20 years. Following the product development life cycle and the security challenges, in the opinion of car manufacturers, would be extremely difficult to manufacture or integrate an on-board application platform or an in-vehicle interface which would meet the safety and security requirements over the life of the vehicle. While updating of software would be feasible, updating hardware becomes problematic.

Since vehicle manufacturers currently take liability for any vehicle parts that malfunction on the vehicle, providing direct access to in-vehicle data to third party application service providers could, in their view, increase the manufacturer liability.

Some other stakeholders groups presented an opposing view asserting that there were already sufficient safety and security measures available and that these could be implemented in a shorter timeframe than that proposed by the car manufacturers. Current security technologies such as firewalls, public key infrastructure (PKI) and hardware security modules (HSM) could be used to ensure safety and security of the vehicles and therefore no principal new technical developments are required to enable the on-board application platform, only implementation of available technology.

Some third party service providers also indicated that standardisation is in their view the incorrect approach to address security because it is too slow compared with the evolving security threats. Instead they proposed a group of stakeholders comprising vehicle manufacturers and third parties are formed to define a process with a protection profile (PP). A PP is a document used as part of the certification process according to ISO/IEC 15408 and should reflect the minimum trust assurance levels. This profile would consist of latest security implementations and objectives for the environment for the target of evaluation (TOE) in the Security Target (ST) while also establishing a security evaluation criteria. A process to include a PP could easily be applied to the existing solution (i.e. using SIM cards) and can be updated regularly by a consortium of stakeholders and checked during PTI inspections. An example of PP is the Remote Provisioning Architecture for Embedded SIMs (eSIMs) which consists of a provisioning and an operational profile.

Third party service providers indicated that in Geneva, vehicle manufacturers are developing safe and secure measures for automated driving for speeds up to 130 km/h and for safe over-the-air (OTA) updates. In their view, this indicates that vehicle manufacturers are already introducing security into their vehicles. Some members

pointed out towards the WG6 security document (WG6-A2D Annex 7; In-vehicle interface security requirements_CCU) which describes how security can be ensured.

The repair and maintenance stakeholders were of the view that security must be standardised, otherwise it is always subject to business decisions that tend to lead to the minimum level of security being implemented. If there were a specified key length and the amount of processing power required for the encryption systems, this would ensure a common maximum security standard.

The same stakeholders cited Android Auto and Apple CarPlay as examples of platforms that interact with vehicle data (using the vehicle HMI and also related functionality, for example, the volume control) and still remain safe. Since Apple and Google aim to have a unified user experience across various different car manufacturers, they have very detailed requirements with respect to hardware (control design, display requirements) as well as in-car software-interfaces. Both system architectures (Android Auto and Apple CarPlay) allow the integration of deep in-car functionality by design.

3.4.1.1 TRL's analysis

As vehicles evolve from being mechanical to more software-based systems, the in-car software and electronics are exposed to different risks and must to be increasingly safe and secure. Modern cars have multiple ECUs, cables, software - and most importantly - several in-vehicle networks. Whether one of the technical solutions delivers greater safety and security over the others for these vehicles emerged as one of the key questions.

There are examples of on-board platforms that exist currently (for example, Toyota T-Connect and GM NGI) that demonstrate that access – at least to the HMI – can be provided and that third parties can 'write' to obtain the status of some vehicle systems. While this is limited – it does not for example, extend to true safety critical systems, it shows that the safety and security of some car manufacturer's systems will allow this type of access and shows that it is technically feasible. The evidence therefore suggests that the on-board application platform is feasible and could arguably be implemented in a shorter time frame than estimated by some car manufacturers. Even for those manufacturers whose electrical architectures require updating in order to implement an on-board platform, the timescales are considered to be shorter than that proposed.

Following the various developmental stages of ISO 26262[24] – a standard on functional safety - some of which are: Hazard analysis and risk assessment (HARA), functional safety concept, functional safety requirements and concept phase review, a similar cybersecurity concept can be developed in parallel to make sure that both the issues of cybersecurity and functional safety are addressed while a product is being developed. Although security is never a constant, the risk of adding security as an extra layer can be mitigated by ensuring that ECUs or systems are developed with functional safety and cybersecurity. This approach could lead to a safe, secure and a functional ECU, rather than applying security once a system has already been developed.

As part of the system design, one way to make a system safe and secure is segregation of safety critical functions from non-safety critical functions. This functionality of segregating safety critical functions from others can be achieved by using the concept of a 'hypervisor'. The hypervisor turns a microchip into several virtual machines capable of simultaneously executing separate software tasks, allowing the isolating of safety-critical functions and consolidation of applications into fewer ECUs, therefore managing costs and system complexity. Technical developments indicate the feasibility of using

[24] ISO 26262: Road vehicles – Functional safety

hypervisor systems and support this as technology that is available to be implemented. For example, OpenSynergy ARM Cortex -52 real time processor, Visteon's Phoenix SDK and SmartCore domain controller and Renesas R-Car connected car platform multivisor (essentially the same functionality as a hypervisor) have developed hypervisor systems which incorporate multiple OS to run simultaneously and multiple applications to operate in parallel. The security package in these systems allows secure booting and secures updates to meet changing security requirements.

A hypervisor on a SoC[25] on the on-board application platform comprises of the following components:

- a hardware layer,
- a virtualisation layer,
- a secure operating system,
- an application layer (partition) which ensures integrity of applications,
- Secure I/O partition, system partition, security partition and HMI partition.

Overall, the introduction of hypervisor technology will prevent vehicle manufacturers from re-designing a product from its basics, allow safe access to safety critical ECUs and help in combining several functions on one SoC.

There are existing security-related standards in other industries, which can be used in combination with the automotive standards, and there has also been research projects in this area which show that applications can be run on the vehicle in a secure and safe way. Some of the security related standards and research projects are listed below:

- ISO/IEC 9797-1: Security techniques – Message Authentication Codes.
- ISO/IEC 11889: Trusted Platform Module.
- ISO 27002: Code of Practice – Security.
- ISO 27018: Code of Practice – Handling PII / SPI (Privacy).
- J2945: Dedicated Short Range Communication (DSRC) Minimum Performance Requirements.
- J3101: Requirements for Hardware-Protected Security for Ground Vehicle Applications.
- EVITA - E-safety Vehicle Intrusion Protected Applications Co-funded by the EC.
- TPM - Trusted Platform Module
- SHE - Secure Hardware Extensions (SHE): From the German OEM consortium Hersteller Initiative Software (HIS).
- OVERSEE – An open-vehicular secure platform providing a standardized generic communication and application platform for vehicles, ensuring security, reliability and trust of external communication and simultaneous running applications.

To prevent any unwanted access on the CAN bus (either read/write), designers of ECUs should be aware of the techniques of CAN message manipulation and design systems that are resilient to it. To prevent CAN manipulations, the read-only diagnostic protocol

[25] SoC – System on Chip; an integrated circuit that integrates all components of a computer

must provide the same level of protection as in the case of write i.e. data transmission for input/output control and remote activation of a command routine.

Therefore, in TRL's view, it is possible to achieve safety and security for all technical solutions; there are existing standards and technologies that need to be combined and implemented to achieve this outcome.

3.4.2 Choice of communications provider

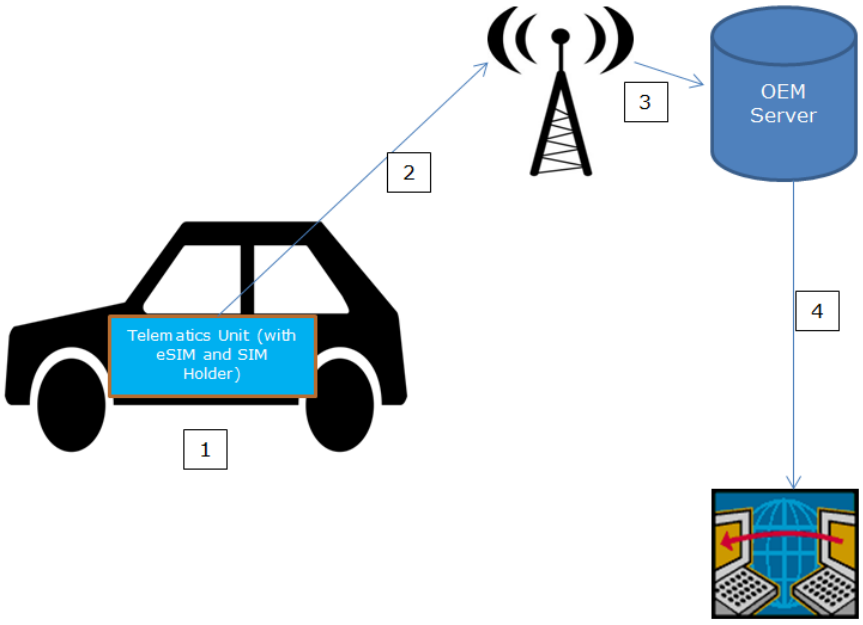


Figure 18: eSIM and SIM holder

Connected cars require a SIM card for sending data from the vehicle to a server for further processing. Figure 18 represents an eSIM and SIM holder connected to the internal CAN network of the vehicle, where:

- 1-Represents a Telematics unit (with an eSIM OR a SIM holder) connected internally to the CAN controller in the vehicle.
- 2-Represents the data transmission between the vehicle and the cellular network provider (communication).
- 3-Represents the connection from the cellular network provider to the OEM backend server.
- 4-Represents the internet connectivity from the OEM backend to the user interfaces.

The telematics control unit (TCU) is connected internally to the CAN network through a CAN controller. The TCUs are either pre-installed with embedded Subscriber Identity Modules (eSIMs) soldered on the motherboard, or require additional connection to an external SIM holder. Due to the increasing number of ECU's in a vehicle which introduces wiring complexity, some vehicle manufacturers prefer using eSIMs because of the following advantages

- It involves no additional connectivity to an external SIM holder
- Offers flexibility to the vehicle manufacturer's to perform profile settings and remote provisioning of SIM cards.

On the other hand, some manufacturers also offer the TCU with an additional SIM holder offering more flexibility to the customer to use either their personal SIM cards or the vehicle manufacturer's SIM card.

Using eSIMS or SIM cards offered by the manufacturer at the point of sale enables the manufacturer to offer specific services. They also provide advantages for the consumer that all data charges (including roaming charges) are accounted for. This process ties a customer into a telematics contract with the manufacturer as soon as the vehicle is

purchased. An opposing argument was presented that the data subject should be free to establish a contract with the manufacturer or another third party to provide services.

3.4.2.1 TRL's analysis

In TRL's view, there is no legal obligation of the vehicle manufacturer to hold a telematics contract with the owner of a vehicle before data can be transferred from a vehicle and thus a communication contract could also be established with a third party (which then becomes data controller) without violating the General Data Protection Regulation.

TRL acknowledges that there are distinct advantages to the vehicle manufacturers of using eSIMs:

- Automatically establishes the vehicle manufacturer as a data controller.
- Facilitates a relationship with the customer.
- Allows the manufacturer to offer additional telematics services when a consumer purchases a vehicle and allows the manufacturer to bundle services in this 'first contract' with the customer.
- Helps in collecting limited personal data sets from services like bCall (breakdown call) and stolen vehicle tracking which could be used to offer extra services.

Nevertheless, the use of eSIMs means that other market participants are dependent on the data server connectivity provided by the vehicle manufacturer. If an external SIM card holder was provided this would enable other SIM cards to be used allowing equal opportunity to other market participants. This would place additional burden in designing a new SIM holder (for vehicle manufacturers who do not currently use an external SIM holder), but would allow the customer to decide who will provide the communications contract and would place all market participants on a more level playing field with respect to the 'first contract' with the customer.

3.4.3 Data availability in the car

During discussions with stakeholders it became clear that defining which data is available in the car was not well understood by all parties. This is important in the context of defining which data is made available to market participants

Figure 19 represents a general vehicle electrical architecture where each ECU is connected to the CAN bus of the vehicle. Some of these ECUs are further connected to their respective sensors (i.e. Sensor 1 and Sensor 2 as seen in Figure 19.) which carry out dedicated function. Data collected by these sensors are real-time in nature (for example: data from the lambda sensor, radar sensor and a powertrain sensor) which are used by their corresponding ECUs to make internal calculations. The output of these calculations are then broadcast on the CAN bus. Therefore, the vehicle manufacturers point out that because only selected data is broadcast on the CAN bus not all of the data is available.

Stakeholders also suggest that some vehicle manufacturers allow Tier 1 suppliers direct access to data. This is to be expected as the components (ECUs and sensors) are designed, tested and manufactured by the tier 1 suppliers. Providing direct access to Tier 1 suppliers helps vehicle manufacturers to fix issues in lesser time ultimately helping end users in reducing vehicle downtime.

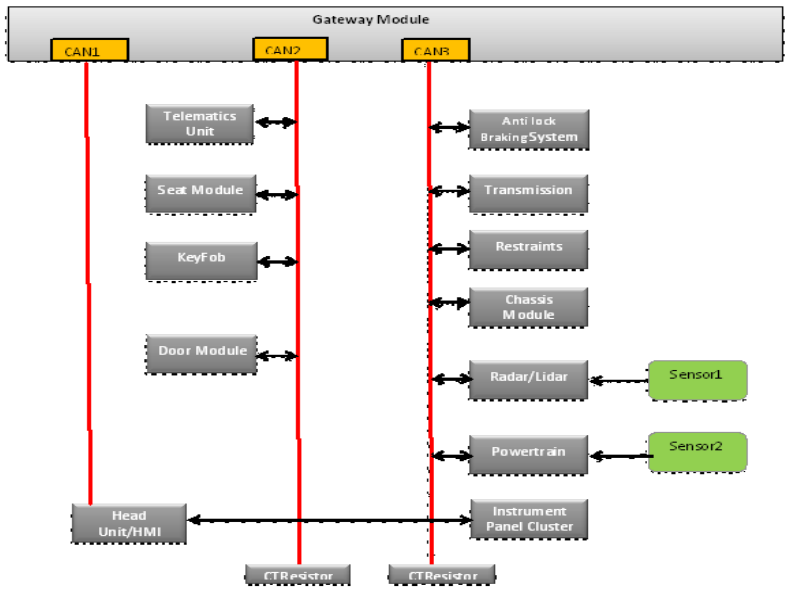


Figure 19 : Vehicle architecture

Third party service providers request access to the same data that is available to car manufacturers to enable a level playing field with respect to competition. Therefore, in effect, this means the same level of access to data on the CAN bus and data produced by sensors not broadcasting on the CAN. Third parties put forward the view that not allowing access to these data breaches the five guiding principles in terms of fair and undistorted competition which they equate to having access to the same data.

3.4.3.1 TRL's analysis

The guiding principle relating to fair and undistorted competition can only be fully met if all market participants have access to the same data, since otherwise there is a degree of inequality that could lead to the distortion of the market. The important point here is that the risks to inequality are minimised as far as practicable.

Providing access to Tier 1 suppliers to sensor data is part of a contractual arrangement between the manufacturer and that supplier. This is required for monitoring of issues by the supplier and manufacturer and in order to affect timely fixes to any issues that might arise. While this means that certain market participants have access to data that others do not, we judge that in this instance this is proportionate. The sensors that generate data are proprietary and linked to the design of the vehicle; providing direct access to all data – i.e. including the proprietary data generated by these sensors - would affect innovation and competition between manufacturers.

It is also clear that demands for data not currently broadcast could lead to issues relating to capacity of the existing vehicle network and could also involve technical challenges for manufacturers to actually make the data available. However, where there was a genuine and acceptable request for data not currently available, this could be made actioned subject to the safety and other considerations. The decision as to what was an acceptable request would need to be determined by a neutral party.

Overall, to ensure fair and undistorted competition, all market participants should have as close as possible access to the same data from the vehicle. Initially, this should be data that can currently be broadcast on the vehicle network, provided that the request for such data does not create capacity or other safety issues for the vehicle bus. Requests for data not currently accessible should be assessed by an appropriate neutral party to decide if they are proportionate bearing in mind the burden on manufacturers to facilitate access to such data.

3.4.4 Access to vehicle HMI

Equal opportunity with respect to contact with the driver (or customer) is an important aspect of ensuring that the guiding principle of fair and undistorted competition is met. The screen console within the vehicle is the main interface with the driver in current vehicles. In the future, this is also likely to extend to voice activation and perhaps more advanced forms of interaction.

As discussed earlier in Task B4 under safety and security, providing direct access to the HMI, could lead to severe conditions such as: an application crash, CAN bus overload, CAN bus congestion, priority messages being discarded and, last but not least, driver distraction. Some vehicle manufacturers filter certain content of applications based on priorities. For example YouTube videos are not allowed to be displayed on the HMI when priority actions like rear view camera while reversing is taking place. Priority actions will supersede any secondary actions like navigation maps and minimise the YouTube window.

Vehicle manufacturers propose indirect access to the HMI by using Apple CarPlay and Google Android Auto. According to the manufacturers, this gives third parties an opportunity to develop applications and present them to the customer on the HMI. These applications mirror certain applications supported by Apple and Google on the vehicle HMI using a USB or Bluetooth connection. Applications are installed and run on the phone, but can also be controlled using the vehicle HMI and steering wheel buttons because of the existence of compatible software and hardware inside the vehicle. According to vehicle manufacturers, these applications use mobile data either to update or get the latest information to be displayed on the HMI.

Standardisation of the on-board application platform for accessing HMI is something which the vehicle manufacturers do not support. Currently, manufacturers offer their proprietary in- vehicle platforms. This helps them to build software compatible with their platforms and also allows the necessary B2B arrangements with service providers for additional services. In their view, standardisation would hamper new innovations in the infotainment/HMI technologies area and would be not be competitive; standardisation of the platform would take away the essence of their brand and limit them from offering competitive services to their customers.

Repair and maintenance stakeholders view equal access to vehicle resources (i.e. the HMI) as essential to ensure fair competition so that all market participants have the same interaction with the driver.

They consider the mechanism of displaying/presenting information on the HMI using Apple CarPlay or Android Auto unfair. They argue that they should have the ability to communicate directly with the consumer and a method where data displayed for their applications will be real-time. Some stakeholders also viewed that certain applications are not allowed to run on the vehicle HMI, even if they do not in any way dictate or control any functions of the vehicle. Therefore, not granting access to these applications breaches the right to fair competition.

Some manufacturers have already started integrating applications to their proprietary infotainment systems, including voice assistants like Amazon's Alexa, Cortana for social media interactions, as a new way of interacting with the driver and maintaining close contact with the customer. If manufacturers can offer new and innovative ways to be in contact with the customers, then third party service providers would also like to have the same level of access to vehicle data and resources to enable competition with the manufacturers in terms of access to the customer and the ability to innovate.

3.4.4.1 TRL's analysis

To ensure fair competition, all market participants should have the same opportunity and access to this interface with the driver; this is the only way that there can be a level playing field for the market. At this important point in automotive evolution, where

manufacturers already control their digital dashboards and in-car experience, third party service providers must be given equal access to in-vehicle data and resources if the guiding principles agreed by WG6 are to be adhered to.

The only solution that provides truly equal access to the HMI is the on-board application platform, although other technical solutions can also make the HMI available to other market participants with the limitations of being accessible via mobile platforms. However, before access is made available to third parties enough testing and security measures should be put in place and/or implemented within the ECUs to prevent them from being hacked or being compromised. For example

- Hardware security module
- Secured hardware encryption
- Public key infrastructure
- Advanced encryption standard
- Embedded security

Consequently, we see access to the HMI via mobile platforms as being a pragmatic and practical position in the short term while the necessary security and technical improvements are being made to facilitate the in-vehicle data access and provided immediate steps are taken to commence these technical developments necessary for the on-board application platform.

We would also like to suggest implementation of central gateway modules, hypervisors, Domain Controller Units (DCU) and security session protocols (both for read and write access) must be implemented in the ECU's to make sure that no unauthorised access is granted. Following the developmental process as described in SAE 3061, this could add an extra cybersecurity layer while the ECU is in development and pave the way forward.

3.4.5 Futureproofing

The manufacturers view the data server solution (including Extended vehicle/neutral server model) as a future-proof concept because it involves upgrading of only the backend data servers, compared to upgrading the complete E/E architecture of millions of vehicles. Updating data servers maintains the backwards compatibility to the vehicle which essentially means that any software (SW) or firmware (FW) upgrades and changes to any ECU on the vehicle can be handled remotely. Changes made once on the data server can be implemented quickly, easily and cheaply on several vehicles. This is efficient in terms of cost and also enables critical bugs to be patched immediately and allows compelling new features to be added to the vehicle at any time during its lifecycle.

Manufacturers suggest it is easy and secure to access data from the data servers. The reason given is that when a third party requires access to additional data, they can approach the neutral server provider to negotiate their data needs. It is far easier for third party service providers to approach the neutral providers to request additional data (once consent is approved) than to have separated and multiple B2B contracts with the each manufacturer.

As already discussed in Task B4, under 'availability of data', not all data is available on the vehicle network. So, if a third party requests access to data which is not present on the CAN bus, but the data is present somewhere in the vehicle, vehicle manufacturers could find a way to extract and send the dataset to the data server. This would be a much easier task than to make separate B2B arrangements for multiple third parties who want access to the data. Making multiple contracts for various datasets could incur changes to the existing ECU software which the vehicle manufacturer has to make in order to make data available. Therefore, data communication channels which the vehicle manufacturers have established for data to flow from the ECU to the TCU and then to the servers, makes it a much easier task for the vehicle manufacturers to make data available at the data server, thus making the data server a futureproof technical solution.

The in-vehicle interface technical solution, which has limited scope and capabilities, is seen by manufacturers as a solution which is not future-proof compared to the data server solutions for the following reasons.

- The current OBD port provides restricted data sets to third parties and dealer repair garages.
- Malicious actions could present a real risk for on-board systems to be compromised.
- Some vehicle manufacturers were of the view that access to OBD will be blocked while driving and only left open for regulated areas like emissions, periodic technical inspection (PTI), security related repair and maintenance (SERMI). This is to prevent CAN hacking incidents which confer a real danger to the vehicle occupants while the vehicle is in motion.
- As vehicles become more autonomous, data generated by the on-board systems will also be enormous. Given the limited bandwidth of the current OBD ports, the amount of data generated by the on-board systems will be impossible to handle. Also, increasing safety and autonomous features not only puts extra components on the CAN bus but also adds to the complexity of the data availability on the OBD port in its current state.
- Given its current state, the plan to upgrade the OBD to a more sophisticated OBD which could handle more data was debated and kept aside by the WG6 members because OBD II is a standardised product and tools developed for accessing OBD data are in use worldwide. A project for a new standard connector that supports DoIP[26] was cancelled in ISO, due of lack of interest. Therefore, creating a new OBD-II and its associated tools would be rather challenging.

Since security challenges are always evolving, and all hardware needs to be encrypted and tested before deployment, significant effort, cost and time will is required to upgrade older systems to meet new cybersecurity requirements. This seems to be a major barrier for manufacturers as the hardware of the on-board application platform might become outdated and certain applications running on it will become incompatible.

Third party service providers do not consider the data server solutions to be future-proof since they do not allow access to real-time data and these types of data may become far more important for applications in the future compared with the current market.

Some third parties were of the view that the in-vehicle interface is only a partial solution due to its limited physical and data access conditions. It does not provide access to in-vehicle resources (i.e. they cannot implement embedded applications or access the in-vehicle display), which will be of significant importance in the future. Since remote access to some in-vehicle data (data which could be real-time or time critical in nature) will be limited, data may not be of the same quality and the lack of possibility to write data back in the vehicle, makes the in-vehicle interface a solution which is not future proof.

Third parties have the view that the on-board application platform will provide them direct and equal access to in-vehicle data and resources as compared to the vehicle manufacturers. This will allow them to provide value added services and state-of-the art digital services even in future.

Citing Apple CarPlay and Android Auto as platforms which are future proof, the repair and maintenance industry suggest having an Open telematics Platforms (OTP) which will provide them the access conditions and put them in the same position as vehicle manufacturers to offer digital services. The platform will be secure, encrypted by the

[26] Diagnostics over Internet Protocol

introduction of a hypervisor. It will be able to host several operating systems (OS) with their associated applications giving third parties full and secure access to in-vehicle data and resources. This paves the way for them to deploy trusted embedded applications developed in accordance with the manufacturer guidelines and empowers them to compete with applications that can access real time data. Considering the above facts the third party service providers endorse the on-board application platform as a future-proof platform.

3.4.5.1 TRL's analysis

Below is a comparison table which captures TRL's view on the three technical solutions.

Table 1 : TRL's view on future-proofing of the three technical solutions

Data server platform	On-board application platform	In-vehicle interface
Upgrade needed once in every approximately ten years to upgrade/add servers and solution which is something which is outside the vehicle.	Upgrade takes additional effort and time to be applied on millions of vehicles and something which is inside the vehicles.	Upgrade takes additional effort and time to be applied on millions of vehicles and something which is inside the vehicle.
Less investment required for upgrade	More investment required for upgrade	More investment required for upgrade
Backwards compatible	Specific hardware changes may render compatibility of applications	Changes to hardware may render compatibility of applications
Safe, secure, trusted and certified backend architecture	Changes on the platform could impact vehicle's safety and security.	Changes to the interface could impact vehicle safety and security.
Possibility to have a test and production environment	Needs to be production quality	Needs to be production quality
Easy to implement new APIs	Would take some time to implement new APIs.	Would take some time to implement new APIs.
Easy to implement requirements for new features and applications.	Requires additional effort to discuss and implement requirements	Requires additional effort to discuss and implement requirements
Low latency slightly delayed data (but not "real time" data) available but with technologies such as 5G,V2V,V2I real time data possible in future	Low latency data and "real time" data available inside the car	Low latency data and "real time" limited set of data available inside the car
manufacturers can monitor data	Level playing field	Level playing field
Standardised set of data availability in a secure manner.	Data could be available in different formats	Data could be available in different formats
Standardisation helps in converting raw data converted	Raw data may/may not be converted to meaningful	Raw data may/may not be converted to meaningful

to meaningful information for third parties	information	information

Based on **Table 1** the data server platform suggests being a future-proof solution. It creates a good balance between the safety and security of the vehicle and applies the principle of 'invent once, apply everywhere principle'.

On the other hand the on-board application platform also qualifies to be a future-proof platform but will cost money and time for development to the vehicle manufacturers.

TRL views ICT technologies such as Apple CarPlay and Android Auto as platforms that enable smartphone connectivity to the vehicle HMI. Although, they replicate the mobile screen on the vehicle HMI, the technology itself might still find hard to keep up pace with rapid developments in the areas of 5G and V2X in future. Secondly, not all applications installed on the smartphone can be mirrored on the vehicle HMI which further restricts the technology.

If vehicle manufacturers make their infotainment platforms more agile by integrating software solutions provided by companies like Qualcomm's connected car reference platform[27], Harman's Aha cloud platform [28]and Inrix Opencar [29] then this could become a future-proof platform. This process does not involve a complete overhaul of the existing EE architecture instead allows vehicle manufacturers to easily upgrade existing infotainment and audio systems to extend the lifespan of vehicles. Not only will these technologies allow vehicle manufacturers and drivers to upgrade in-car audio and infotainment systems, but also allow manufacturers and third parties to integrate applications and consistently improve embedded software features.

Recent automotive showcase events held in 2017 also suggest that some vehicle manufacturers have already started the process of preventing Android Auto access to vehicles. This clearly indicates that in general, the vehicle manufacturer's inclination towards Apple CarPlay or Android Auto poses an immediate challenge to their proprietary infotainment platforms. However, there are examples where some brands are integrating these platforms (e.g. SEAT). All of the above reasons suggest that the on-board application platform is a future proof platform.

[27]https://www.qualcomm.com/news/releases/2016/06/08/qualcomm-announces-connected-car-reference-platform-simplify-integration

[28] http://investor.harman.com/releasedetail.cfm?releaseid=817103

[29] http://inrix.com/products/inrix-opencar/

3.4.6 Contractual control

One of the frequent issues that arose in the stakeholder discussions was control of the data. While it may be unfeasible in practice for every party to have equal control or influence on the data, it is clear that to ensure that the guiding principle on fair and undistorted competition, no single of group of market participants, should have control that leads to significant detriment for these aspects.

Control of the data could arise in several ways; either by being the 'gatekeeper' to the data provided to other market participants, thereby having the potential opportunity to refuse, restrict, dilute or delay access to data, or by being first to the customer and steering the customer in the direction of particular services to the detriment of other service offerings in the market. The first of these issues is covered in Section 5 under the subheadings for Fair and Undistorted Competition for each technical solution..

During bi-lateral meetings with TRL, vehicle manufacturers stated that they are committed to providing their customers with a highest level of protection of their personal data. Manufacturers design their vehicles and services in way that customers can consent to share personal data or not. Customers are also able to revoke consent for example be able to de-activate the geolocation functionality of their vehicles and the services except where geolocation data must be processed to comply with contractual or legal obligations, such as in the case of eCall.

The Telematics Control Unit collects data from other modules on the CAN bus and sends data to an off-board server for further processing. Certain vehicle manufacturers issue a contract for telematics data transfer when a vehicle is sold (as part of packages or services) and collect data as they have their IT infrastructure that is already linked to the SIM card present inside the vehicle. This gives them the flexibility to offer more services in one transmission cost. In general terms, manufacturers prefer having a single contract for transmission and manage separate contracts for their services; they do not wish to combine the two.

Some stakeholders expressed concerns over the manufacturer's ability to obtain the first contract with the vehicle purchaser and could bundle activation of connected services with their own service offerings. It was expressed that this meant that the manufacturers were able to control the customer by steering or providing attractive bundled services at the outset. They expressed that this makes it challenging for the rest of the market, since although services could be offered, in practice the customer may have already purchased the same service and the pricing of services could be offset against other elements.

They argued that the provision of the communication services does not have to rest with the manufacturer (as is typically the case in the current market) and that other providers could offer this service. In this case the manufacturer would not be the data controller and this responsibility would pass to the party providing services. In the current situation it is possible to have multiple data controllers (i.e. the car manufacturer and the third party supplier).

3.4.6.1 TRL's analysis

In order to meet the guiding principle on fair and undistorted competition, no single of group of market participants should have control that leads to a material difference in the access to the customer.

At present the de facto supplier of the connected vehicle services is the car manufacturer and many purchasers of vehicles may not be aware that they could, for example, obtain services from another provider if the mechanisms were in place to allow this. If the vehicle was equipped with an external SIM holder this would allow the user to select the communications provider.

3.4.7 Read/write access to data

The question whether third parties could and should be given 'write access' to the vehicle or if the access to data should be restricted to read-only emerged as an important topic of discussion during the stakeholder consultations. The discussion appeared to be governed by two extreme positions, which fear that guiding principles would be violated by either decision: One side argues in favour of write access because the range of possible third party services and the means of access to the customer would be restricted (relevant with regard to fair and undistorted competition). The other side argues that giving third parties write access would compromise security of the vehicle and jeopardise the safety of the occupants (relevant with regard to tamper-proof access and liability). A more nuanced reflection on this topic is required to determine a potential compromise that does not violate any guiding principle.

Uncontrolled and unfiltered write access by third parties to the vehicle's bus systems (including, for example, chassis CAN etc.) is considered unsafe by OEMs: Safety critical components, including such as the brakes and airbags, are controlled via signals on the bus system. If these were activated by a third party, this could result indeed result in safety-relevant road incidents. Therefore, clearly safety critical functions, such as activating the brakes while driving, should be protected against access by third parties.

However, other levels of 'writing' to the vehicle could be considered. Three main aspects emerged as important to ensure fair competition:

A. Write access for diagnostics: Third parties do have the right to request stored diagnostic trouble codes and initiate a test in an ECU. These operations are write operations because a signal is sent on the bus to trigger the relevant ECU to broadcast the data. However, there are additional safeguards in place, such as PASS-THRU, when it comes to changing certain parameters or reprogramming ECUs.
B. Write access to infotainment system and comfort functions: Third parties could be allowed to project legitimate information on a vehicle's HMI and control associated aspects such as loudspeaker volume. This is critical for many third party services that wish to interact with the driver, for example for provision of location-related information (predictive repair suggestions and recommended garages nearby or deals from petrol stations in the area), for feedback (driving style feedback from insurers) or infotainment apps (music, navigation). Drivers cannot access other interfaces, such as their phone, while on the move which significantly delays the access to information through these routes.
C. Triggering legitimate events: Limited write access could be granted to third parties to control selected actuators for non-safety critical events, such as unlocking the doors under certain preconditions. This is relevant for third party services, such as car sharing (unlocking the car by a user), parcel delivery to the car (opening the boot by a delivery driver) or anti-theft services (remote engine shut-down).

With every form of write access there is a cybersecurity risk associated; for instance, third party software could overload the CAN bus by sending repeated signals or too many apps could write at the same time. This could be performed with a malicious intent or by simple programming errors. Furthermore, many actions are not per se safe or unsafe, but this depends on the circumstances. For example, could changing the temperature settings to excessively cold/hot settings cause discomfort or distract the driver.

3.4.7.1 TRL's analysis

Any safety incidents would entail liability risks for the OEM and arguably also reputational risks with customers, which would also apply if the liability is successfully passed on to another actor. This risk has to be mitigated by OEMs via technical

safeguards (e.g. firewall, hypervisor) and procedural safeguards (such as certifying software before it may be deployed to a vehicle on-board application platform).

This appears feasible: For requesting diagnostic data, OEMs have, for instance, reserved the right to restrict access to when the vehicle is stationary. The architecture employed for ICT platforms, such as Apple CarPlay, and in-vehicle application platforms such as Toyota T-Connect allows access to the vehicle's infotainment system including projection on the HMI with appropriate safeguards in place against unsafe operations or undue driver distraction. OEMs have also implemented functions such as door unlocking for car sharing together with selected business partners. While OEMs informed TRL that this is not a trivial technical procedure, the successful implementation nevertheless shows that with the right app certification and contractual arrangements in place a certain level of 'write' access can be given to third parties.

In conclusion, while free write access by any third party would indeed be safety critical, it should be acknowledged that the request from third parties of having the ability to display information via the vehicle HMI as a point-of-sale is a strong argument with regard to fair and undistorted competition. Based on the considerations above it appears fair to conclude that potential compromises exist that go beyond read-only access and still allow a safe implementation without forcing one standardised E/E architecture in all vehicles.

3.4.8 Methods of access and minimum set of data

Two alternative methods of accessing in-vehicle data were suggested by WG6:

- Access depending on pre-defined use-cases
- Application-dependent list of data (based on terms and conditions of each application)

TRL's initial technical analysis presented the advantages and disadvantages of either method in Section 3.1.1. It should be considered to combine both methods of access in order to minimise the disadvantages of either individual method. A solution with a range of data points defined in use-cases and access to a flexible part based on application-dependent terms and conditions appears feasible from a technical and procedural aspect.

WG6 has started to collate data needs, but categorising the relevant data fields in certain groups could make the necessary discussions easier and more structured. This, in effect, is a process of defining 'use-cases'. Defining these groups of data fields rather widely, which is sometimes referred to as 'use-case clusters' such as insurance, diagnostics, etc., appears beneficial because this could to an extent obfuscate the exact data use of third-party service providers who access want to access this data.

In-vehicle networks and sensors vary between OEMs (and also between models) and they cannot be changed at short notice. The nature of current vehicle E/E architectures with ECUs distributed across the vehicle and being connected via buses means that not all data measured by sensors somewhere in the vehicle is available at a central location, because some data remains on the private CAN of the module on which it was created. The required quality and update frequency of the data points is connected to the nature of the data, but can also vary depending on its intended use. For instance, the fuel level is a value that changes slowly, so it might not be necessary to update it more than every few minutes in order to provide related services. The required accuracy of location data could be quite low for services which only want to determine all cars within a certain geographical area, but might be higher for navigation services. These criteria could be defined per use-case class and this would therefore make standardisation more feasible.

The use-cases or use-case clusters as a whole could represent an agreed minimum set of data that is made available by OEMs in an agreed quality and format. However, third party service providers argue that having access only through defined use-cases would be restrictive because it is limited to what OEMs want to make available. Therefore it needs to be considered how any data outside defined use-cases/use-case clusters should

be made available to third parties. This could be based on individual B2B contracts or OEMs could be encouraged or obliged to make any data available to third parties, which they use themselves to offer services to customers that go beyond immediate driving functions. However, OEMs investing in specific in-vehicle sensors also have a commercial interest to profit from the data created which is why they argue in favour of making data outside defined use-cases available only available to selected third parties based on B2B contracts.

During the further technical analysis and stakeholder engagement activities for this project, further procedural and technical aspects of the two methods were considered:

The procedures for defining use-cases would likely involve a wide consortium made up of vehicle manufacturers and all interested third parties using data, such as suppliers and service providers. This would have to be a regular process (to define new and update existing use-case) and could be organised, for example, in the format of an ISO or CEN standards committee or another industry platform. The European Union could support this process by providing a legislative mandate for standardisation of use-cases or by soft measures such as facilitating and administering a suitable platform.

The timelines for defining use-cases appear to be a critical point of concern from side of the third parties. ACEA and CLEPA communicated in the stakeholder consultation that they were able to agree three trial use-cases between them within half a month. However, it was conceded that these were rather simple use-cases and there were no conflicts of commercial interests present between the parties involved. Other stakeholders expected much longer timescales. It is reasonable to expect that defining a new use-case in a wider consortium, such as a standards committee (ISO or CEN) would involve drafting and agreeing the use-case contents and followed by a wider comment period before finalisation. This process should be expected to take approximately one year as a minimum and, in case of a standards committee, would involve a vote (and therefore publication) of each use-case.

It could be considered to agree maximum timescales to set common expectations. Note that maximum timeframes exist, for example, in ISO standards committees and these can be (and are regularly) extended. This leads to the question what happens if parties cannot agree on the contents for a use-case in time or if a suggested use-case is not taken forward. This situation is to be expected where opposing commercial interests are involved. It might therefore be advisable to consider defining a procedure for arbitration that is followed in case a certain time limit is exceeded or if there are general disputes.

Other procedural questions remain that would need to be addressed to ensure fair and undistorted competition:

- Who has the right to formally suggest use-cases? What obligations arise for the parties involved if a use-case is suggested?
- Will OEMs be obliged to make data accessible as per all defined use-cases? If so, this could be expected to only apply if the relevant data is being generated by the vehicle (i.e. no obligation to equip the vehicle with new sensors). What if the data has to be converted/reformatted to comply with the format specified in the use-case (i.e. what level of burden is acceptable to OEMs)?

3.4.8.1 TRL's analysis

With regard to the consent of the data subject needed for data usage, the legal analysis in this report found that both methods (use-cases and application-dependent access) are possible; however, the consent given in the use-case model might be regarded as stronger. In this context it should also be considered that cars are often shared between individuals and consent to data usage given by the vehicle owner could therefore affect other people using the vehicle. Potential models to address this might be:

- Requesting consent from the driver at the beginning of each journey (engine-on). This appears more feasible with use-case-dependent consent where the list of use-cases would likely be smaller than a list of individual applications requesting consent for various data.
- Passing the obligation to inform all drivers on to the owner of the vehicle. The Terms and Conditions of telematics insurance services in the UK, for instance, request policyholders to confirm that all users have been made aware that data will be transmitted and used by the insurer.
- Identifying individual drivers by technical means and applying their stored consent profile. This could, for example, be based on the key fob used to start the car or the mobile phone connected to the vehicle's infotainment system. There is no notable difference between the two methods with this model.
- All of these models could be complemented by an easy to access switch or command in the vehicle that prohibits data transmission for a certain period (e.g. for the current journey).

4 Task C: Impact assessment

4.1 Approach to impact assessment for in-vehicle data

The aim of this task was to provide a quantified comparison of the direct and indirect economic, social and environmental impacts of the proposals developed by WG6 on the access to in-vehicle data and resources. In addition to the five proposals developed by WG6, the assessment also includes the extended vehicle/neutral server solution proposed by ACEA.

Following the EC guidelines for Impact Assessment[30] as far as possible within the constraints imposed by the data available, this approach consists of the following steps:

1. Identification of economic, social and environmental impacts
2. Qualitative assessment of the more significant impacts
3. In-depth qualitative and quantitative analysis of the most significant impacts

The review of literature and stakeholder consultation have provided only limited quantifiable data on the impacts, costs and benefits of the technical solutions for access to in-vehicle data and resources. The approach set out in the guidelines was therefore modified in consultation with the EC, with Step Three consisting of a comparative qualitative assessment, providing quantitative information where available.

Two types of impact can be identified from gaining access to in-vehicle data:

- Impacts of the services using the data
- Impacts of the technical solutions used to gain access to the data.

Access to in-vehicle data can be used to support a range of services, with data made available from the vehicle being used by a variety of stakeholders including fleet owners, the automotive industry, third party service suppliers, the repair and maintenance industry, road operators, emergency services, other public sector organisations as well as road users. In general terms, the various options for gaining access to in-vehicle data which are being considered in this study are expected to be capable of supporting the same range of services, so the impacts of services using the data are expected to be similar whichever technical solution is used to obtain the data. Although some concern was raised among stakeholders that access to data via a Data Server would introduce latency into the information chain, the majority of services being considered by stakeholders provide information and warnings to the driver (rather than intervening in vehicle control) and thus have only modest latency requirements. An exception to this is remote vehicle diagnostics and prognostics, where real time access to the data and communication with the driver to arrange repairs and maintenance is seen by the vehicle repair and maintenance industry as being crucial to maintaining their service offering. However, apart from information on the costs of setting up and running a data server supporting transport information services, no quantified data have been made available to enable a comparative assessment of the costs and benefits of the technical solutions to provide access to in-vehicle data for such services.

An indicative analysis of the societal benefits of a selection of services using in-vehicle data is provided in Section 4.2. The following sections (4.3 to 4.7) then present the assessment of the impact of the various technical solutions used to gain access to the data and the overall results are summarised in Section 4.8.

[30] http://ec.europa.eu/smart-regulation/guidelines/ug_chap3_en.htm

Section 5 then analyses implementation scenarios for the technical solutions, providing a comparative qualitative assessment of the solutions in terms of their compliance with the five guiding principles, timescales and proportionality of action at European level.

4.2 Socioeconomic benefit of services based on access to in-vehicle data

The scale of societal benefits which can potentially be realised through services using data obtained from vehicles is expected to dwarf the costs and benefits associated with the various architecture options that are being considered for gaining access to the data. This section provides indicative estimates of the scale of benefits associated with European implementation of a selection of services using in-vehicle data.

The societal benefits of a selection of five services based on in-vehicle data have been analysed at a European level:

1. Probe Vehicle Data (PVD) – Vehicles transmit a range of information, such as kinematics (speed, direction, position,…) or state (windscreen wiper status, air bag status, road surface condition,…). These data are then used for providing a range of services, for example, traffic flow management or roads maintenance.
2. Hazardous Location Notification (HLN) – Vehicle sensors and driver behaviour (which, for example, can be detected from the steering wheel or use of brakes) provide information about the presence of a hazard at a specific location. A warning is then sent to the vehicles nearby.
3. Traffic Jam ahead Warning (TJW) – Drivers are alerted when they are approaching the vicinity of a traffic jam in order to prevent rear end collisions.
4. Slow or Stationary Vehicle warning (SSV) – Drivers receive a warning when they are approaching a slow or stationary vehicle, allowing them to gradually adjust their driving or opting for an alternative route.
5. Emergency Brake Light (EBL) – If a vehicle brakes suddenly, a message is sent to following vehicles, giving them more time to react safely, thus avoiding rear end collisions.

Research on the potential impacts (Ricardo Energy & Environment, 2015) has identified that all these services contribute to improving safety; in addition, as summarised in **Table 2**, some of them have a positive impact on CO_2 emissions, fuel consumption or traffic efficiency (which, ultimately, can be quantified in terms of the time spent travelling). This table shows the main impacts, and does not include minimal impacts (such as the small improvement in fuel consumption and emissions over the approach to a traffic jam which may be realised if drivers use the warning to decelerate more economically).

Table 2 Main areas of benefit from five services based on in-vehicle data (Ricardo Energy & Environment, 2015)

Service	Fuel consumption	CO_2 emissions	Safety	Traffic efficiency
PVD – Probe vehicle data	✓	✓	✓	
HLN - Hazardous location information			✓	✓
TJW - Traffic jam ahead			✓	
SSV - Slow or stationary vehicle warning			✓	
EBL - Emergency electronic brake light			✓	

The monetised savings arising from the societal benefits of each service over the period to 2030 are reported here (discounted values); the procedure followed for deriving the

estimates and the data used are reported in Appendix D; further details about the results are also reported there.

4.2.1 Probe Vehicle Data

Figure 20 shows the estimated annual benefits arising from the implementation of the PVD service in Europe. Improved road safety is the main contributor, accounting for about 99% of the overall savings. Estimates of the avoided annual costs increase from approximately €170 million in 2017 to more than €930 million in 2030.

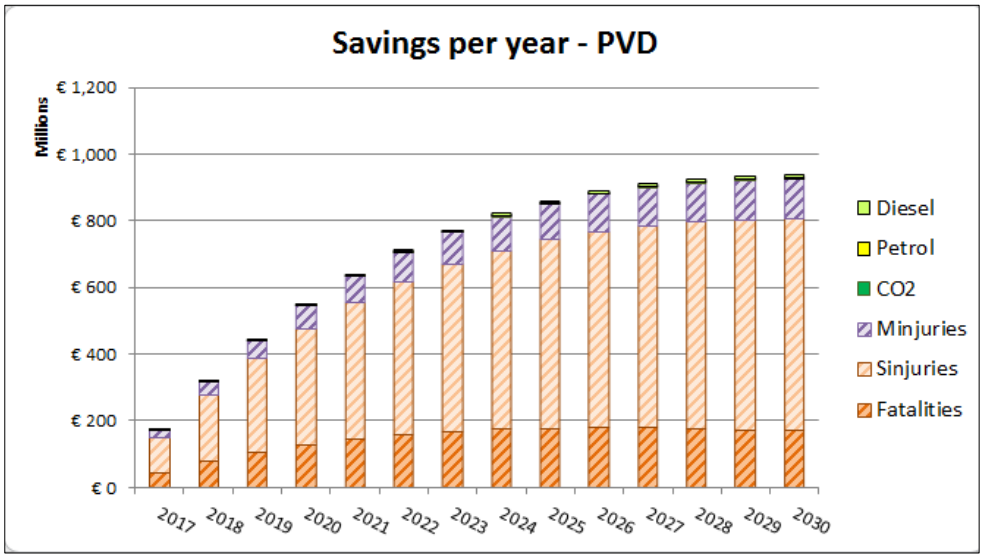


Figure 20: Annual savings for the PVD service due to prevention in road fatalities, serious injuries (light orange labelled 'Sinjuries'), minor injuries (purple labelled 'Minjuries'), diesel and petrol savings and reduction in the CO_2 emission.

4.2.2 Hazardous Location Notification

Of the services considered here, the HLN service has the highest impact on safety; its implementation could save more than 4,000 lives in 14 years, in addition to approximately 180,000 injuries (serious and minor). This service is also expected to improve traffic efficiency, quantified as a 2% improvement in speed (Ricardo Energy & Environment, 2015). This results in shorter travel times, which in turn can be linked to monetary values using the value of time for journeys for different purposes (for the procedure followed see Appendix D). The estimate of savings due to reduce travel times can be particularly significant; in particular for this service, it is also the predominant source of savings. As can be seen in **Figure 21**, annual benefits across Europe are estimated to grow from about €1.3 billion in the first year to almost €12 billion in 2030.

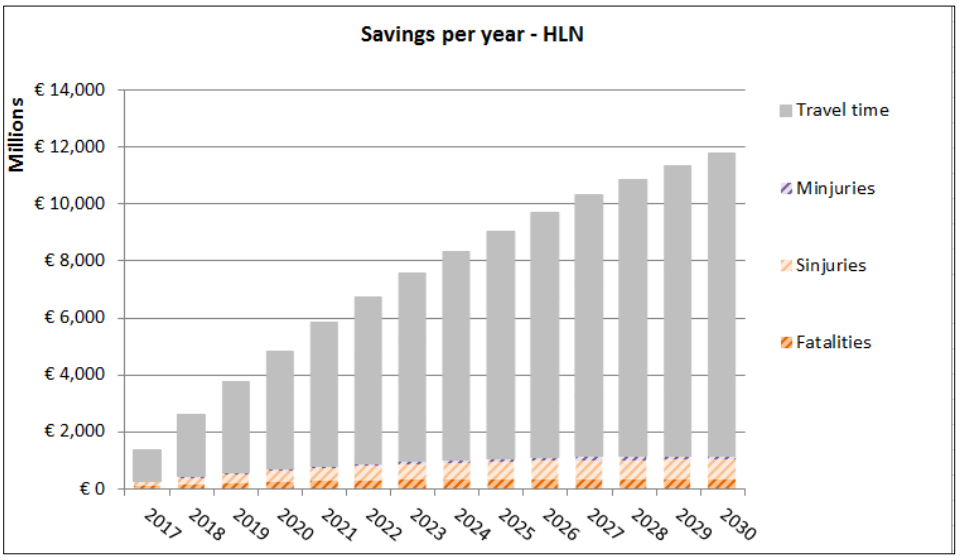


Figure 21 Annual savings for the HLN service due to prevention in road fatalities, serious injuries (light orange labelled 'Sinjuries'), minor injuries (purple labelled 'Minjuries') and reduced travel time (grey)

4.2.3 Traffic Jam ahead Warning

In fourteen years the TJW service could potentially save more the 1,800 fatalities, 30,000 serious injuries and almost 115,000 minor injuries across Europe. These figures correspond to savings of about €145 million in the first year, up to €800 million in 2030 (**Figure 22**).

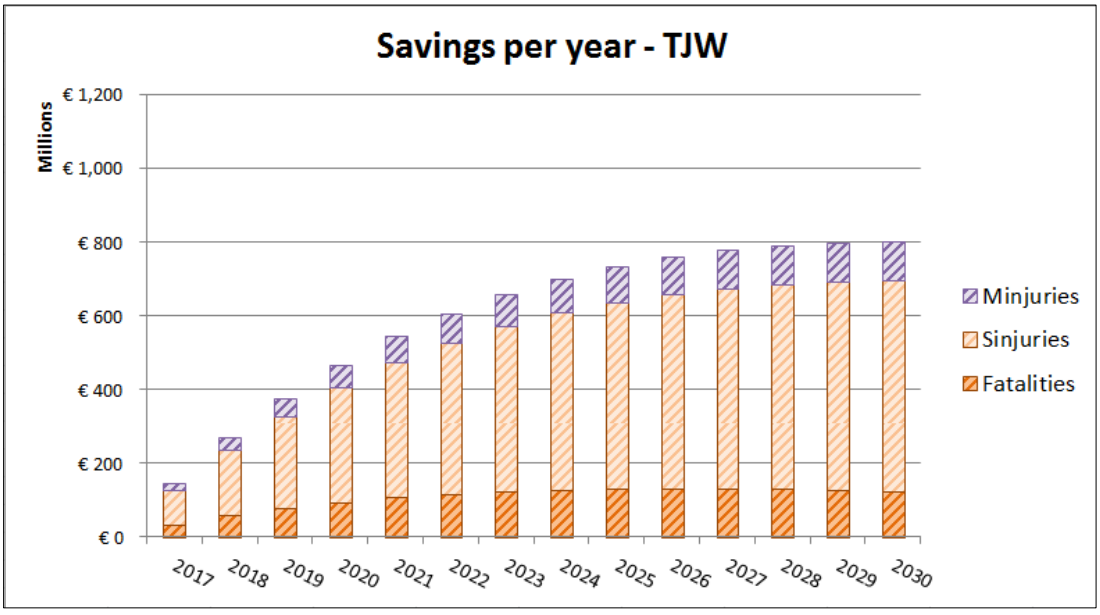


Figure 22 Annual savings for the TJW service due to prevention in road fatalities, serious injuries (light orange labelled 'Sinjuries') and minor injuries (purple labelled 'Minjuries')

4.2.4 Slow or Stationary Vehicle warning

The annual savings for the SSV service are estimated to increase from about €50 million in the first year to more than €250 million in 2030 (**Figure 23**), as a result of more than 1,100 saved lives and more than 40,000 injuries avoided (serious and minor).

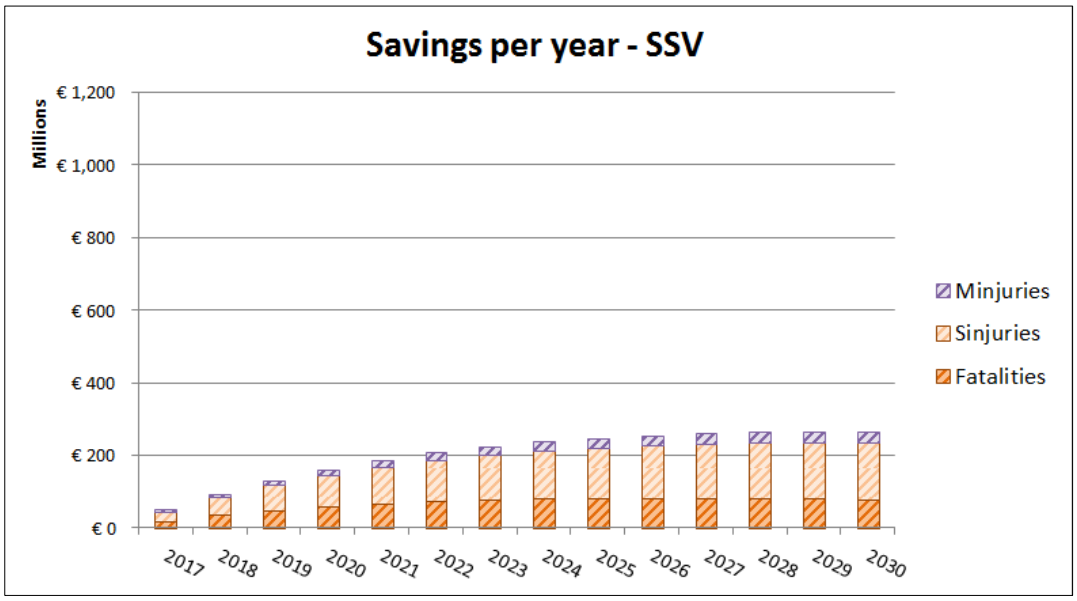


Figure 23 Annual savings for the SSV service due to prevention in road fatalities, serious injuries (light orange labelled 'Sinjuries') and minor injuries (purple labelled 'Minjuries')

4.2.5 Electronic Brake Light

The EBL service is estimated to prevent about 2,700 fatalities in road collisions and more than 30,000 and 115,000 serious and minor injuries respectively. **Figure 24** shows the corresponding annual cost savings; they are estimated to grow from around €160 million in 2017 to more than €850 million in 2030.

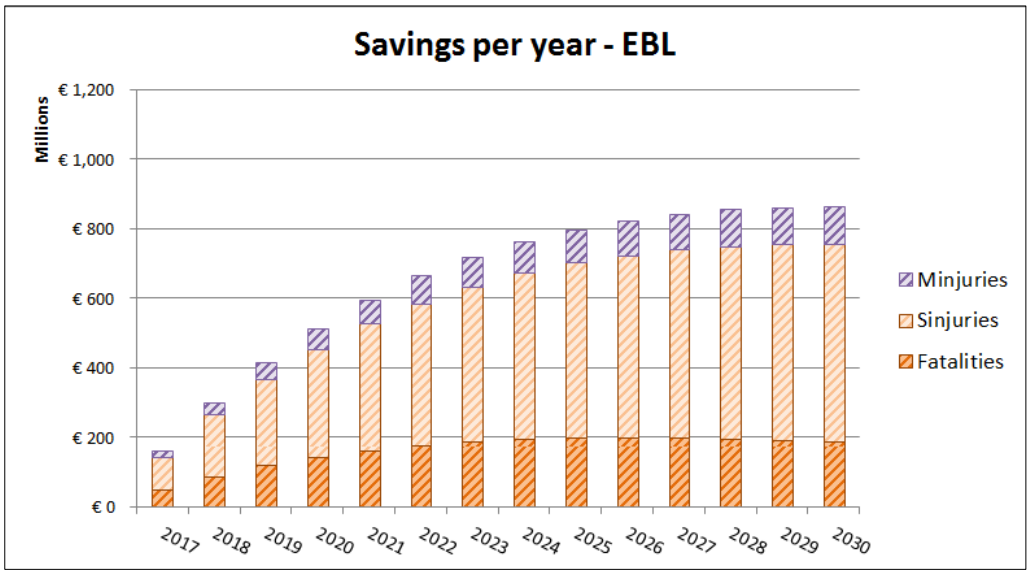


Figure 24 Annual savings for the EBL service due to prevention in road fatalities, serious injuries (light orange labelled '*Sinjuries*') and minor injuries (purple labelled '*Minjuries*')

Thus on a pan-European scale, and taking account of other potential benefits such as non-fatal injuries and travel time, the benefits of the services themselves, regardless of the architecture used to deliver the data from vehicles, are potentially very large.

4.3 Identification of economic, social and environmental impacts

The first step in the EC Impact Assessment Framework is to identify the scope of the assessment by identifying the expected impacts of the overall action to provide access to in-vehicle data. This involves identification of economic, social and environmental

impacts and assessment against fundamental rights. The results are summarised in the tables in Appendix E. These do not on the whole differentiate between the different options for gaining access to in-vehicle data.

The main elements which are of relevance to this set of technical solutions are as follows:

- Economic/Internal market – consumer choice
- Economic/Internal market – competitiveness of EU firms
- Economic/Operating costs SME – new or closing businesses
- Economic/Public authorities – additional government burden
- Economic/Property rights
- Economic/Innovations & research.

4.4 Quantifiable data

Using data from the literature review, known sources of data on the costs of ITS components and from stakeholders consulted during this project, the data on the costs of the various components of systems for access to in-vehicle data were compiled to provide as complete a picture as possible on the costs of the WG6 technical solutions. No information was found that enabled the benefits of gaining data through any of these solutions to be quantified.

This data were derived from the stakeholder survey responses, recent studies such as the Ricardo report[31], the US Department of Transportation database of Intelligent Transport System Costs[32] and direct contact with stakeholders. The limited amount of quantifiable data available is presented in Table 49 in Appendix F and summarised in **Table 3**. In order to compare the relative costs of the various technical solutions, the qualitative comparison summarised in Section 4.5 was also carried out. This review did not include the Extended vehicle/Neutral Server solution because it was not one of the WG6 solutions and at the time of investigation it had not been proposed. However, the costs are considered to be similar to those estimated for the Data Server – B2B Marketplace solution, plus one-off costs for establishing the neutrality of the server and ongoing costs for maintaining the neutral server. These latter costs have not been estimated

[31] RICARDO (2015). Study on the deployment of C-ITS in Europe: input data overview – cost data. Unpublished report to European Commission, DG MOVE.

[32] http://www.itscosts.its.dot.gov/

Table 3 Summary of cost estimates for the technical solutions

Cost	On-Board Application Platform	In-vehicle Interface	Data Server - Extended Vehicle	Data Server - Shared Server	Data Server - B2B Marketplace
One-off cost per vehicle manufacturer	€1m - €2.5m	€1m - €2.5m	€1m - €2.5m	€3m - €4.5m	€3m - €4.5m
One-off cost per vehicle	€115	€15	€15	€15	€15
Annual cost of database			€1m - €2m		
Annual cost per vehicle manufacturer				€1m - €2m	€1m - €2m
Annual cost per vehicle (maintenance and software updates)	€11				

4.5 Qualitative comparison of costs

A qualitative comparison of the costs involved in developing, setting up, operating and maintaining the various elements of the technical solutions was carried out. On the basis of the information obtained in the survey and from stakeholders and the literature, each technical solution was ranked high, medium or low on each cost element. The relative scale of each cost element was then allocated a value which was used to 'weight' the high/ medium/ low scores and the weighted scores were summed to produce an overall weighted score. The weighted scores are shown in **Error! Reference source not ound.** in Appendix F.

The results are summarised in **Table 4**. This shows similar, relatively low cost levels for each of the data server solutions. Higher cost levels were estimated for both the on-board application platform and the in-vehicle interface, largely because of the cost of technical development and the cost of equipping and maintaining 12 million new vehicles each year across Europe.

Table 4 Qualitative comparison of the relative cost of the technical solutions

Cost element	On-Board Application Platform	In-vehicle Interface	Data Server - Extended Vehicle	Data Server - Shared Server	Data Server - B2B Marketplace	Extended vehicle/Neutral Server
Technical development (including engineering & validation)	High	Medium	Low	Low	Low	Low
In-vehicle hardware	Medium	Medium	Low	Low	Low	Low
Maintenance in-vehicle hardware	High	High	Low	Low	Low	Low
Database development	None	Low	Low	Low	Low	Low
Database operation	None	Low	Low	Low	Low	Low
Database maintenance	None	Low	Low	Low	Low	Low
Server hardware	None	Low	Low	Medium	Medium	Medium
Server operation	None	Low	Low	Medium	Medium	Medium
Server maintenance	None	Low	Low	Medium	Medium	Medium
Administration & contracts	Low	Low	Low	Medium	High	High
App service set up	Low	Low	Low	Low	Low	Low
App service operation	Low	Low	Low	Low	Low	Low
Cellular communication	Medium	Medium	Medium	Medium	Medium	Medium
RAN/LAN/Wi-Fi communication	None	None	Low	Low	Medium	Medium
Overall weighted score	High	High	Low	Low	Low	Low

4.6 Qualitative comparison of technical solutions from the point of view of stakeholders

The qualitative information obtained from the stakeholders through the survey, workshop and bilateral discussions identified benefits and dis-benefits of the technical solutions from the point of view of the main types of stakeholder in the information chain.

Remote access to in-vehicle data and resources obtained using any of the architecture solutions provides some benefits that are applicable to all stakeholders. These include the ability to provide new and more efficient services which benefit all of the

stakeholders involved, as well as society in general such as safety and environmental benefits of driver training tailored to the individual and of independent testing of safety components and emissions as well as customer relationship management for industry and service providers.

Set against these overall benefits, some stakeholders warned that there are potential risks to security and safety involved in any method of obtaining in-vehicle data and that the system established to access in-vehicle data could have large effects in terms of market fairness and equality.

4.6.1 Benefits and dis-benefits to all stakeholders

Table 5 summarises the benefits and dis-benefits of the specific technical solutions (including the Extended vehicle/ Neutral Server) which affect all stakeholder groups involved. Benefits and dis-benefits to individual stakeholder groups are summarised in the following sections.

Table 5 Benefits and dis-benefits to all stakeholders

Technical Solution	Benefits	Dis-benefits
On-board application platform	Fair and non-discriminatory Enables all stakeholders to access data in real time (although real time access is not needed for many applications) A security layer with a connectivity control unit is required and provides reassurance to all parties involved that data is protected Remote assistance for eco driving and driving improvement	Need for implementation of security layer with a connectivity control unit. Potentially significant costs for some car manufacturers depending on readiness for solution and timing with respect to current design cycle for electrical architecture. Applications need validation to ensure compliance with safety and security requirements Potentially longer time scale for implementation.
In-vehicle interface	Technology is available (but requires update to security) Access to data is possible in real time, subject to control by vehicle manufacturer (although real time access is not needed for many applications) Provides direct access to the vehicle, with physical limitations and limited access to in-vehicle data	Additional features in vehicles are needed achieve appropriate security; these may impose significant costs on car manufacturers. Applications need validation to ensure compliance with safety and security requirements Only a partial solution - cannot implement embedded applications or access the in-vehicle display in all cases Potentially long timescale for implementation with improved security.
Data server/ extended vehicle	Secure system, already controlled by vehicle manufacturer Benefits can be realised immediately Access available to all stakeholders Standardised access to relevant data is possible without compromising security, safety or vehicle manufacturers' liability	Vehicle manufacturer controls the value chain, therefore potentially discriminatory Restricts access by aftermarket and third party service providers to data to support the minority of services requiring real time data and functions for time-critical services May involve third parties incurring additional costs to access the data; contracts required directly with manufacturers who can dictate terms

Technical Solution	Benefits	Dis-benefits
Data server/ shared server	Secure system, benefits can be realised immediately Supports competition If the server is run by a neutral party and has equal access to in-vehicle data then there is a basis for fair competition Could support multimodal transport management and new jobs in the mobility sector.	Restricts access by aftermarket and third party service providers to data to support the minority of services requiring real time data and functions for time-critical services and prevents them from implementing embedded applications May involve third parties incurring additional costs to access the data Contractual arrangements needed between car manufacturer, server operator and other stakeholders; manufacturer may dictate terms.
Data server/ B2B marketplace	Secure system, benefits can be realised immediately All stakeholders can access the data Supports competition	Restricts access by aftermarket and third party service providers to data to support the minority of services requiring real time data and functions for time-critical services and prevents them from implementing embedded applications Increased latency for the minority of services where real time data is needed May involve third parties incurring additional costs to access the data; manufacturer may dictate terms
Extended vehicle/Neutral server	Benefits can be realised immediately Standardised access to relevant data, including support of smartphone applications, without compromising security, safety or vehicle manufacturer liability Competition in downstream market One stop shop for service providers/SMEs who do not need to interface with each car manufacturer No interference in relationship between neutral server and clients Single point of data access/trading	Restricts access by aftermarket and third party service providers to data to support the minority of services requiring real time data and functions for time-critical services and prevents them from implementing embedded applications Increased latency for the minority of services where real time data is needed May involve third parties incurring additional costs to access the data; manufacturers may dictate contract terms.

The following sections summarise the benefits and dis-benefits of the technical solutions for the stakeholder groups. For each stakeholder group, a table is presented which summarises the role of that stakeholder in each architecture option and the advantages and disadvantages of that option for them.

The colour coding indicates anticipated key priorities for stakeholders as follows:

High	High- medium	Medium	Low	Will not consider

4.6.2 Benefits and dis-benefits for vehicle manufacturers

Advantages for vehicle manufacturers that were reported by stakeholders focused around the world-wide market for services that is enabled through access to in-vehicle data, with new functions, and improved quality of service and customer relationship management. Set against this were increased safety, security and liability risks.

Table 6 summarises the impacts on vehicle manufacturers, including the vehicle manufacturer-authorised repair and maintenance functions. The priorities for vehicle manufacturers are expected to be governed by the fact that the in-vehicle interface is being implemented for infotainment, but as an HMI interface not a data interface. Extending its scope to a bi-directional transfer of data is unacceptable to vehicle manufacturers (see Section 3.4.7). Thus the Data server – Extended vehicle option is the most favourable to vehicle manufacturers (along with the evolution of this solution to include a neutral server), but the shared server variant is also likely to be viewed favourably.

Table 6 Benefits and dis-benefits of architecture options for vehicle manufacturers

Architecture	Role	Advantages	Disadvantages
On-board application platform	Buy and integrate the platform. Write an interface from the vehicle to the platform. Retrieve the data and use it to provide user services e.g. diagnostics, arrange parts and maintenance	Potentially lower development costs with single platform. Little or no hardware. Can be integrated with existing functions. Can offer tailored solution to customers. Remote access to data, potentially in real-time, to support services. Easiest way to obtain consent from driver. Distraction issues can be managed by use of in-vehicle display. Customer relationship management.	Potentially higher equipment costs. Lack of control. Inability to differentiate and gain commercial advantage. Security issues. Type approval/ issues. Arrangements for approval of applications unclear. Potential risk of system instability from multiple interactions with vehicle. Product liability issues unless application platform controlled by vehicle manufacturer.
In-vehicle interface	Implement the interface if mandated. Contribute to the relevant standards	Integration of several in-vehicle applications into single HMI. Customer relationship management.	Security issues if security of in-vehicle interface insufficient, with risks for safety. Liability issues. Lack of control of the user experience and of data use. May be more inconvenient for users thanthe On-Board Application Platform (OBAP). Difficult for applications to manage system and data complexity. Potential for driver distraction (communication not integrated into in-vehicle display) unless using mobile platform.

Architecture	Role	Advantages	Disadvantages
Data server - extended vehicle	Design and manage the server platform, communications etc., and process the data. Export data to 3rd parties.	Technology already in use. No in-vehicle hardware. Control of data and easier data compliance. Retain the customer relationship over life of vehicle. In control of security. Very difficult 3rd party access to the vehicle. Data can be used for multiple purposes simultaneously without affecting vehicle performance. Supports innovation.	Applications limited to those which are not real time. Potential for driver distraction (communication not integrated into in-vehicle display) unless using mobile platform.
Data server - shared server	Provide data in standardised format to shared server.	Technology already in use. No in-vehicle hardware. Control of data and easier data compliance. Retain the customer relationship over life of vehicle. In control of security. Very difficult 3rd party access to the vehicle. Data can be used for multiple purposes simultaneously without affecting vehicle performance. Supports innovation.	Applications limited to those which are not real time. Loss of control. Responsibility for security shared between organisations. Need arrangements with shared server for liability, data protection, security Potential for driver distraction (communication not integrated into in-vehicle display).
Data server - B2B marketplace	Provide data in standardised format to marketplace	No in-vehicle hardware. Data can be used for multiple purposes simultaneously without affecting vehicle performance. Supports innovation.	Applications limited to those which are not real time. Loss of control. Responsibility for security shared between organisations. Need arrangements with marketplace for liability, data protection, security. Potential for driver distraction (communication not integrated into in-vehicle display).
Extended vehicle/ Neutral server	Provide data in standardised format to neutral server	Could co-exist with extended vehicle.	Applications limited to those which are not real time. Loss of control. Responsibility for security shared between organisations. Need arrangements with neutral server for liability, data protection, security. Potential for driver distraction (communication not integrated into in-vehicle display)

4.6.3 Benefits and dis-benefits for Tier 1 suppliers

Access to in-vehicle data is seen by stakeholders as benefitting Tier 1 suppliers by improving the range of services that can be provided, improving reliability of services and improving customer-relationship management.

Table 7 summarises the benefits and dis-benefits for Tier 1 suppliers. The on-board application platform is expected to be their favoured option due to the increased opportunities for business and the way in which it enables them to maintain a relationship with OEMs and service providers and to offer parts and components direct to customers.

Table 7 Benefits and dis-benefits of architecture options for Tier 1 suppliers

Architecture	Role	Advantages	Disadvantages
On-board application platform	Design and supply in-vehicle application platform	Increased business opportunities. Maintain a relationship with both vehicle manufacturers and service providers. Direct access to customers.	Slight increase in risk as a more complex device is implemented
In-vehicle interface	Implement interface to already existing in-vehicle unit/HMI (this assumes tier-1 is already supplying the In-vehicle Interface)	Small increase in supplied software, hence revenue. Customer relationship management.	Not much work involved, so little additional business opportunity. If dongle solution adopted, the installer would have exclusive access unless multi-dongle or smart dongle
Data server - extended vehicle	No additional role because this option does not change the data or the way it is communicated from the vehicle	None	No opportunity for increased business. Will not support real time, diagnostic or predictive services that are independent of vehicle manufacturer.
Data server - shared server	No additional role because this option does not change the data or the way it is communicated from the vehicle	Improved reliability.	No opportunity for increased business.
Data server - B2B marketplace	No additional role because this option does not change the data or the way it is communicated from the vehicle	None	No opportunity for increased business.
Extended vehicle/ Neutral server	No additional role because this option does not change the data or the way it is communicated from the vehicle	None	No opportunity for increased business.

4.6.4 Benefits and dis-benefits for the independent repair and maintenance industry

For the independent repair and maintenance industry, it is seen as vital to be able to access in-vehicle data in order to improve the efficiency of their operations. Remote

diagnosis can reduce the time spent in the workshop. It also enables the ordering of replacement parts to be streamlined, avoiding the 'speculative' ordering of spare parts and giving longer notice of the parts that will be required. Remote access to in-vehicle data also supports the development of new prognostic services, in which the driver is warned of issues before they become critical and the arrangements for vehicle servicing can be made, potentially giving those with access to the data a competitive advantage.

Table 8 shows that the on-board application platform is the priority for this group as it is the only technical solution which is seen to offer advantages. All of the other solutions were seen by the industry representatives interviewed as having significant disadvantages and no advantages.

Table 8 Benefits and dis-benefits of architecture options for the independent repair and maintenance industry

Architecture	Role	Advantages	Disadvantages
On-board application platform	Retrieve data from the vehicle and use it to provide users with diagnostics and prognostics services, arrange parts and maintenance in real time	Remote access to data, potentially in real-time, to support services which can be independent of the vehicle manufacturer and not monitored by the vehicle manufacturer. Easiest way to obtain consent from driver. Distraction issues can be managed by use of in-vehicle display. Customer relationship management.	Vehicle manufacturers control what data they allow to be taken from the platform.
In-vehicle interface	Retrieve data from the vehicle and use it to provide users with diagnostics and prognostics services, arrange parts and maintenance	None	Data available potentially limited, restricting the scope of services offered. Potential for driver distraction (communication not integrated into in-vehicle display)
Data server - extended vehicle	Retrieve data from the server and use it to provide limited diagnostics services, arrange parts and maintenance	None	Data available potentially limited, restricting the scope of services offered. Potential for driver distraction (communication not integrated into in-vehicle display)
Data server - shared server	Retrieve data from the server and use it to provide limited diagnostics services, arrange parts and maintenance	None	Data available potentially limited, restricting the scope of services offered. Potential for driver distraction (communication not integrated into in-vehicle display)
Data server - B2B marketplace	Retrieve data from the server and use it to provide limited diagnostics services, arrange parts and maintenance	None	Data available potentially limited, restricting the scope of services offered. Potential for driver distraction (communication not integrated into in-vehicle display)
Extended vehicle/ Neutral server	Retrieve data from the server and use it to provide limited diagnostics services, arrange parts and maintenance	None	Data available potentially limited, restricting the scope of services offered. Potential for driver distraction (communication not integrated into in-vehicle display)

4.6.5 Benefits and dis-benefits for testing and certification providers

For testing and certification bodies, access to in-vehicle data is seen as providing a guarantee of independent testing of emissions and safety related components during type approval and periodic technical inspections. Access to the data would enable additional checks to be carried out during type approval in a cost efficient manner, but would also necessitate additional tests, for example to ensure compliance with security standards.

Table 9 indicates that the on-board application platform would be the preferred solution assuming that IT security issues are solved, because it enables independent and direct access to the data and improved services under conditions of fair competition.

Table 9 Benefits and dis-benefits of architecture options for the testing and certification providers

Architecture	Role	Advantages	Disadvantages
On-board application platform	Retrieve data from vehicle and use it to provide independent testing and certification, in real time when needed.	If IT security issues are solved, this is the best solution, offering independent and direct access to data, and equal and fair competition. It enables improved service to customers.	Potential security risk but a standardised secure communication platform could meet requirements of data protection and security. Data is expected to be processed before leaving the vehicle.
In-vehicle interface	Retrieve data from vehicle and use it to provide independent testing and certification, in real time when needed.	Full control of data transfer by the owner. Independent access to data, supporting fair competition.	No specifications for IT security. Costly.
Data server - extended vehicle	Retrieve data from server to provide independent testing and certification	None	Vehicle manufacturers able to profile vehicle owners. High risk that vehicle manufacturers provide only limited data. Does not meet requirements for non-discrimination, privacy by design, guaranteed data transparency, freedom of choice for consumers and freedom for suppliers, data goes direct to selected provider, applications in vehicle software must be approved by third parties
Data server - shared server	Retrieve data from server to provide independent testing and certification	Vehicle manufacturers are liable for data transfer and in full control of data stream. Provides the basis for independent assessment e.g. type approval of environmental	Risk of latency due to bad internet connection

Architecture	Role	Advantages	Disadvantages
		compliance	
Data server - B2B marketplace	Retrieve data from server to provide independent testing and certification	None	Risk of latency due to bad internet connection. Specifications for IT security missing. No direct access to data from vehicle, vehicle manufacturer in full control of data; risk of market distortion and disruption of contractual relationships
Extended vehicle/ Neutral server)	Retrieve data from server to provide independent testing and certification	None	Risk of latency due to bad internet connection. Specifications for IT security missing. No direct access to data from vehicle, vehicle manufacturer in full control of data; risk of market distortion and disruption of contractual relationships

4.6.6 Benefits and dis-benefits for application service providers

For application service providers, the benefits of access to in-vehicle data are seen as focused around improved customer relationship management, more tailor-made services and enabling greater innovation. Potential risks associated with safety and security were identified as disadvantages.

Table 10 summarises the impacts on application service providers, including the insurance industry. The priorities for these service providers will depend on the applications they are delivering rather than the architecture options; hence all options are indicated as having 'medium' priority.

Table 10 Benefits and dis-benefits of architecture options for application service providers

Architecture	Role	Advantages	Disadvantages
On-board application platform	Develop and supply software to run on platform, providing services to users	Platform stimulates additional demand for services and if universal software development kit available and standardised platform, enables developers to create more innovative and competing services across all vehicles. Provides most direct access to raw data in real time. Easy to comply with data protection.	Existing hardware suppliers lose revenue from drop in hardware provision (e.g. navigation). Vehicle manufacturer becomes the gatekeeper, controlling what data they allow to be taken from the platform so lose control, and increased costs/reduced revenue. Vehicle manufacturers control what data they allow to be taken from the platform
In-vehicle interface	Implement the interface to use the HMI (and potentially get in-vehicle sensor data), process the data to provide services	Simplified development if a standardised interface is used. Potential for additional service provision on in-vehicle HMI? Direct access to raw data in real time. Easy to comply with data protection.	Same as above, plus Scope for many interfaces if not standardised interface. Not all of the current technologies allow real-time direct access to raw data. Data storage, ownership and privacy issues need to be dealt with.
Data server - extended vehicle	Retrieve data from server platform, possibly at a cost. Process this data, and provide service.	Data may be pre-processed to meet server requirements, so may be "cleaner"	Data not real time. Data not under their control Interface to customer via a different route Limited data sent to server loses detail. Vehicle manufacturer has advantage in holding real time data and could monitor service providers' data use
Data server - shared server	Retrieve data from server platform, possibly at a cost. Process this data, and provide service.	Less control from the vehicle manufacturers and minimal opportunity for vehicle manufacturer to monitor data use	Data is not real time. Data not under their control Interface to customer via a different route Limited data sent to server loses detail. Issue if real time data consent required for each transfer

Architecture	Role	Advantages	Disadvantages
Data server - B2B marketplace	Retrieve data from server platform, possibly at a cost. Process this data, and provide service.	None	Data is not real time. Data not under their control Interface to customer via a different route Limited data sent to server loses detail. Issue if real time data consent required for each transfer. Data storage, ownership and privacy issues need to be dealt with. Increased costs for data transfer and operation of marketplace
Extended vehicle/ Neutral server	Retrieve data from server platform, possibly at a cost. Process this data, and provide service.	Service providers remain anonymous. Start-ups can make contact easily with multiple vehicle manufacturers.	Data is not real time. Data not under their control Interface to customer via a different route Limited data sent to server loses detail. Issue if real time data consent required for each transfer. Data storage, ownership and privacy issues need to be dealt with. Third parties will need to make a strong case for gaining access to data in vehicle manufacturer proprietary APIs.

4.6.7 Benefits and dis-benefits for IT infrastructure providers

Access to in-vehicle data is seen as providing IT infrastructure providers with the tools for developing services based on analytics, prediction and prognostics. Some of the solutions provide other benefits for the IT industry: the On-board Application ensures that third party applications are deployed securely in the vehicle, while the in-vehicle interface provide a mechanism for them to improve customer-relationship management because services can be offered directly to the customer.

Table 11 summarises the impacts on IT infrastructure providers, including telecommunications providers. These are agnostic about the route for obtaining the data; their priority is to obtain more data.

Table 11 Benefits and dis-benefits of architecture options for IT infrastructure providers

Architecture	Role	Advantages	Disadvantages
On-board application platform	Ensure that 3rd party applications are deployed securely in the vehicle. Provide analytics, software and development tools. To carry data. Provide a repository for the vehicle-derived data and processing of this data on behalf of the service providers.	Increased business opportunities compared to no service provision.	None
In-vehicle interface	To carry data. Provide a repository for the vehicle-derived data and processing of this data on behalf of the service providers	Increased business opportunities compared to no service provision. Customer relationship management.	None
Data server - extended vehicle	To carry data. Provide a repository for the vehicle-derived data and processing of this data on behalf of the vehicle manufacturers	Increased business opportunities compared to no service provision. Bigger customer	None
Data Server - shared server	To carry data. Provide a repository for the vehicle-derived data and processing of this data on behalf of the shared server service provider	Increased business opportunities compared to no service provision. Bigger customer	None
Data server - B2B marketplace	To carry data. Provide a repository for the vehicle-derived data and processing of this data on behalf of the B2B service	Increased business opportunities compared to no service provision. Bigger customer	None
Extended vehicle/ Neutral server	To carry data. Provide a repository for the vehicle-derived data and processing of this data on behalf of the neutral server service provider	Increased business opportunities compared to no service provision. Bigger customer	None

4.6.8 Benefits and dis-benefits for road authorities and operators

Road authorities and operators benefit from a wide range of services using in-vehicle data that can be used to manage and maintain the road network more efficiently, which in turn have societal benefits in terms of safety, environment and economic impacts. Other public authorities such as law enforcement, emergency and security services can also benefit from using such data. Set against these advantages, one road authority saw additional operating costs and deterioration in the relationship with road users (trust, security and privacy) and unrealistically high expectations from road users about the quality of service they could expect.

Table 12 summarises the benefits and dis-benefits for road authorities and operators. For them, the data server solutions are expected to be the favoured options.

Table 12 Benefits and dis-benefits of architecture options for road authorities and operators

Architecture	Role	Advantages	Disadvantages
On-board application platform	Provision and collection of data.	Not clear.	May be complex to interface to multiple devices
In-vehicle interface	Provision and collection of data.	Single standardised interface	None
Data server - extended vehicle	Provision and collection of data.	None	Deal with multiple entities
Data Server - shared server	Provision and collection of data.	Deal with one entity. Supports applications competitive market	Not clear how relevant data gets to the shared server
Data server - B2B marketplace	Provision and collection of data.	Only deal with one entity	Only deal with one entity
Extended vehicle/ Neutral server	Provision and collection of data.	Only deal with one entity	Only deal with one entity

4.6.9 Benefits and dis-benefits for road user groups

For road user groups such as automobile clubs providing roadside assistance and representing end users, driver training and improvement programmes, access to in-vehicle data provides the opportunity for better quality of service, additional services and improved customer-relationship management. However if data access and use is not properly managed in accordance with the relevant regulation, there is potential for data protection issues.

Table 13 summarises the benefits and dis-benefits for road user groups such as automobile clubs providing roadside assistance and representing end users, driver training and improvement programmes. The On-Board Application Platform is the favoured option for this group due to the scope for providing real-time services for drivers and the ability of users to maintain control and to install their own apps.

Table 13 Benefits and dis-benefits of architecture options for automobile associations and road user groups

Architecture	Role	Advantages	Disadvantages
On-board application platform	Provide user services e.g. breakdown warning and assistance in real time. Provide apps for users.	Independent and direct access to data. New business opportunities and innovation will expand services available. Users can install apps. Users can retain control.	Vehicle manufacturers control what data they allow to be taken from the platform. Commercial organisations may be able to obtain data without consent, profiting without benefit to driver. Driver distraction if badly implemented. Security over vehicle lifetime needs to be clarified among all stakeholders.
In-vehicle interface	Process data from vehicle to provide services.	Independent access to in-vehicle data. Fair competition, if multi-client solutions are possible. Depending on configuration of back end server, data privacy and full control of the data transfer by vehicle owner/ driver ensured. New business opportunities and innovation will expand services available.	Inconvenient installation for customers if the retrofit device is connected to the OBD port. Security over vehicle lifetime needs to be clarified among all stakeholders. Vehicle manufacturers control what data they allow to be used. Driver distraction if can only send messages to drivers over mobile phone
Data server - extended vehicle	Retrieve data from server platform, possibly at a cost. Process this data, and provide service.	Data may be pre-processed to meet server requirements, so may be "cleaner"	Data not real time. Data not under their control. Interface to customer via a different route. Limited data sent to server loses detail. Vehicle manufacturer has advantage in holding real time data and could monitor data use. Vehicle manufacturers control what data they allow to be used.

Architecture	Role	Advantages	Disadvantages
Data Server - shared server	Retrieve data from server platform, possibly at a cost. Process this data, and provide service.	New business opportunities for service providers. Fair competition. Vehicle manufacturer does not monitor customers or services. Vehicle manufacturers are liable for the data transfer from/to the vehicle. Vehicle manufacturer is part of any business model related to in-vehicle-data over the lifetime of the vehicle	Data is not real time. Data not under their control Interface to customer via a different route. Limited data sent to server loses detail. Issue if real time data consent required for each transfer.
Data server - B2B marketplace	Retrieve data from server platform, possibly at a cost. Process this data, and provide service.	Vehicle manufacturers are liable for the data transfer from/to the vehicle.	Data is not real time. Data not under their control Interface to customer via a different route Limited data sent to server loses detail. Issue if real time data consent required for each transfer. Data storage, ownership and privacy issues need to be dealt with. Increased costs for data transfer and operation of marketplace Threat to future of independent aftermarket.
Extended vehicle/ Neutral server	Retrieve data from server platform, possibly at a cost. Process this data, and provide service.	Anonymity and ease of contact with service providers.	Data is not real time. Data not under their control Interface to customer via a different route Limited data sent to server loses detail. Issue if real time data consent required for each transfer. Data storage, ownership and privacy issues need to be dealt with. Threat to future of independent aftermarket. Driver distraction if can only send messages to drivers over mobile phone

4.6.10 Benefits and dis-benefits for vehicle rental and fleet managers

For vehicle rental and fleet managers, remote access to the in-vehicle data offers the opportunity for working more efficiently, with improved productivity for operators and vehicles out of use for shorter times and improved protection of vehicle assets. Services for users could also be improved.

Table 14 summarises the benefits and dis-benefits for vehicle rental and fleet managers. The On-Board Application Platform is the favoured option for this group due to the scope for providing real-time services for fleet management and driver monitoring and improvement and the ability to arrange servicing in real time.

Table 14 Benefits and dis-benefits of architecture options for vehicle rental and fleet managers

Architecture	Role	Advantages	Disadvantages
On-board application platform	Retrieve data from vehicle to monitor fleet and drivers. Provide services to improve driver behaviour and fuel efficiency. Arrange servicing, including in real time.	Improved productivity and fleet management. Improved services for users	
In-vehicle interface	Retrieve data from vehicle to monitor fleet and drivers. Provide services to improve driver behaviour and fuel efficiency. Arrange servicing, including in real time.	Asset protection	Support for one service provider at a time causes difficulties for fleets with more than one brand of vehicle. Possible source of driver distraction.
Data server - extended vehicle	Retrieve data from server platform, possibly at a cost. Process this data, and provide limited service.		Lack of real time access to raw data results in inefficiencies, reduced range of services and higher costs with more complicated arrangements for obtaining data. Loss of competitive advantage.
Data Server - shared server	Retrieve data from server platform, possibly at a cost. Process this data, and provide limited service.	Eliminates market distortion if all have access to the same server as the vehicle manufacturer	Lack of real time access to raw data results in lower overall quality of data, reducing efficiency and functionality of services

Architecture	Role	Advantages	Disadvantages
Data server - B2B marketplace	Retrieve data from server platform, possibly at a cost. Process this data, and provide limited service.		Lack of real time access to raw data results in lower overall quality of data, reducing efficiency and functionality of services Disadvantage to small businesses with less bargaining power, which in the worst case scenario could result in business failure.
Extended vehicle/ Neutral server			Lack of real time access to raw data results in lower overall quality of data, reducing efficiency and functionality of services Vehicle manufacturer can control the market and eliminate competition.

4.6.11 Summary of priorities for stakeholders

The stakeholder preferences indicated by their responses to the consultation are summarised in **Table 15**. This shows that for several stakeholder groups there is a preference for the On-Board Application Platform, but the vehicle manufacturers would prefer the data server extended vehicle while the road authorities would prefer any of the other server solutions.

Table 15 Summary of stakeholder preferences for architecture options

Stakeholder groups	On-Board Application Platform	In-vehicle Interface	Data Server - Extended Vehicle	Data Server - Shared Server	Data Server - B2B Marketplace	Extended vehicle/ Neutral Server (ACEA proposal)
Vehicle manufacturers			Preferred			Preferred (later proposal)
Tier1 suppliers	Preferred					
Independent repair and maintenance	Preferred					
Testing and certification	Preferred					
Application service providers	No preference	No preference	No preference	No preference	No preference	No preference
IT infrastructure providers	No preference	No preference	No preference	No preference	No preference	No preference
Road authorities and operators				Preferred	Preferred	Preferred
Road user groups	Preferred					
Vehicle rental and fleet managers	Preferred					

4.7 Qualitative assessment of the more significant impacts

Based on the overall assessment of the impact of social, economic and environmental impacts of access to in-vehicle data that was summarised in Section 4.3, the following impacts were identified as the more significant impacts for further analysis of the individual technical solution because the expected impacts vary between technical solutions:

- Economic/Internal market – consumer choice
- Economic/Internal market – competitiveness of EU firms
- Economic/Operating costs SME – new or closing businesses
- Economic/Public authorities – additional government burden
- Economic/Innovations & research.

In addition, the solutions are compared on the basis of their compliance with the principles of the ITS Directive.

Using the information from stakeholders, the technical solutions were rated on the scale of impact on each of these factors, with the results summarised in **Table 17**.

In these qualitative assessments, the rating scale ranges from --- (most negative) to +++ (most positive). So for example, the highest level of costs are rated --- and the highest level of benefit are rated +++.

4.7.1 Consumer choice

The on-board application platform has the most positive impacts on consumer choice in the long term because it enables all stakeholders to access the data in real time and on a fair and equal basis, supporting the development of new services for consumers. Compared with this solution, consumer choice is restricted in the case of solutions where the vehicle manufacturer controls the value chain or the data (in-vehicle interface and data server - extended vehicle, although the in-vehicle interface is an interoperable solution giving third parties access to the data, so this supports a higher level of consumer choice than the extended vehicle solution). The other data server solutions support competition and therefore foster consumer choice but because a limited set of data is expected to be provided to the server (due to restrictions such as network capacity and load), the range of services that can be made available is somewhat more restricted than in the case of the On-Board Application Platform.

4.7.2 Competitiveness

The in-vehicle interface and the data server/extended vehicle solutions are potentially detrimental to competition between service providers as a result of the control which the vehicle manufacturer is in a position to exert over the data set that is available to service providers. The On-Board Application Platform is fair and non-discriminatory in so far as the same data set would be available to all service providers, and because data could be made available in real time it supports productivity improvements in sectors using the data such as the repair and maintenance industry.

4.7.3 Small and Medium Enterprises

Any solutions providing a one-stop shop for service providers or other data users are likely to reduce the effort required by SMEs to obtain in-vehicle data (potentially the shared server and the extended vehicle/neutral server) although they may incur additional costs to access the data in this way. In contrast, the need to make bilateral agreements with individual OEMs to obtain data from On-Board Application Platforms, In-vehicle Interface and Extended Vehicle solutions is likely to discourage SMEs from entering the market for providing services.

4.7.4 Public authorities

Public authorities will incur additional effort in the case of solutions requiring compliance checking of additional in-vehicle equipment (the On-Board Application Platform and In-vehicle Interface solutions). Additional administration will also be involved in the case of governance of the neutral server (or shared server).

4.7.5 Innovation and research

The availability of unprocessed data from vehicles potentially in real time is expected to stimulate the innovation and research to support new services. Thus, the On-Board Application Platform and the In-vehicle Interface are expected to have the most positive impact on innovation compared with the other solutions. The data server solutions also have the potential to stimulate innovation but to a lesser extent, given that it is restricted by the fact that only processed data will be made available.

4.7.6 Principles of the ITS Directive

The European Commission ITS Directive 2010[33] sets out the principles for specifications and deployment of ITS in Annex II. The extent to which the individual technical solutions comply with these principles is an indication of the extent of their compliance with the principles of the ITS Directive. The results of this assessment are summarised in **Table 16** and explained below.

The on-board application platform and the in-vehicle interface are potentially more effective in their contribution to societal objectives relating to safety, environment and traffic efficiency because they enable in-vehicle data to be provided in real time.

On the basis of the estimates of the relative costs of developing, building, operating and maintaining the technical solutions summarised in **Table 4**, the server-based solutions are expected to be more cost-efficient than the on-board application platform and the in-vehicle interface.

The data server solutions which are readily available for implementation are those which score highly for appropriate levels of achievable service quality and deployment.

Similarly, the data server solutions, which are based on existing technologies and services, provide greatest support for backward compatibility.

All solutions support continuity of services and seamless travel across the EU as they can be used to provide data for improved traffic information services, but the shared server options are more potentially favourable for their ability to support innovative independent services for travellers.

The solutions are all expected contribute equally to interoperability, enabling data to be exchanged and shared in order to deliver services.

Similarly, the solutions are all expected to contribute equally to equality of access by vulnerable road users.

The shared and extended vehicle/neutral server solutions contribute most to the objective of respecting existing infrastructure because these servers could potentially be those used for Access Points for road safety, traffic and travel information.

The data server – shared server and B2B marketplace are expected to contribute most to the objective of maturity on the basis of robust systems backed by R&D and operational experience, with the in-vehicle solutions contributing least to this objective.

The contribution to quality of timing and positioning and inter-modality is expected to be greater in the case of the on-board application platform and in-vehicle interface than in the data server solutions, because the data is provided immediately and without processing, whereas the data sent to servers is expected to be pre-processed.

The extended vehicle and extended vehicle/neutral server options support coherence as they provide standardised access to data, without compromising security, safety or vehicle manufacturers' liability.

[33] European Commission 2010. Directive 2010/40/EU of the European Parliament and the Council on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport. Official Journal of the European Union, L207 6 August 2010.

Table 16 Rating of compliance of technical solutions with the principles of the ITS Directive

Principles of the ITS Directive	On-Board Application Platform	In-vehicle Interface	Data Server - Extended Vehicle	Data Server - Shared Server	Data Server - B2B Marketplace	Extended vehicle/ Neutral Server (ACEA proposal)
Effective	+++	+++	+	+	+	+
Cost-efficient	---	--	+++	+++	+++	+++
Proportionate	+	+	+++	+++	+++	+++
Support continuity of services	+	+	+	+++	++	+++
Deliver interoperability	+++	+++	+++	+++	+++	+++
Support backward compatibility	0	+	++	++	++	++
Respect existing national infrastructure and network characteristics	0	0	0	+	0	+
Promote equality of access for VRUs	0	0	0	0	0	0
Support maturity	+	+	++	+++	+++	++
Deliver quality of timing and positioning	++	++	0	0	0	0
Facilitate inter-modality	++	++	0	0	0	0
Respect coherence	0	0	+++	0	0	+++

These principles were rated in isolation from each other and their scope is very broad; the relative importance of each element is likely to very different. Since it is difficult to determine the weighting for each of these, it was considered most appropriate to present the information without an overall total for each technical solution.

4.8 Summary of impacts of architecture options

The results of the qualitative assessment of the impact of the architecture options are summarised in **Table 17**.

Table 17 Summary of impacts of architecture options

Impacts	On-Board Application Platform	In-vehicle Interface	Data Server - Extended Vehicle	Data Server - Shared Server	Data Server - B2B Marketplace	Extended vehicle/ Neutral Server
Component costs	---	---	+++	+++	+++	+++
Consumer choice	+++	+	---	++	++	++
Competitiveness	+++	---	---	++	++	++
SMEs	--	--	--	++	+	++
Public authorities	---	---	0	-	0	-
Innovation and research	+++	+++	+	+	+	+

In addition to **Table 17**, the reader should also refer to **Table 16** to consider the compliance of each technical solution with the principles of the ITS Directive.

5 Task D: Scenario-based analysis

5.1 Technical solutions

For each of the possible technical solutions proposed in WG6 for the access to in-vehicle data and resources, the extent to which they meet the five guiding principles, both from a technical and legal perspective, is a necessary first step. Compliance with the guiding principles may not be 'black and white' and this section is intended to identify and to describe the extent of compliance, extract the key issues and risks associated with each solution, and provide an overview of the most relevant cost-benefit aspects; this then forms the building blocks for determining a toolbox of possible 'soft' and 'hard' measures, the Commission could choose to employ in order to achieve implementation of a solution and to ensure its compliance with the five guiding principles.

Note that in some cases a compromise may need to be made between the technical requirements of the solution and compliance with the guiding principles in order to balance the overall demands of the solution. For some technical solutions, the guiding principles are in conflict – i.e. solutions which have a solution that provides good agreement with safety and security requirements may be less likely to ensure fair and undistorted competition.

5.1.1 Solution 1: On-board application platform

5.1.1.1 Technical and legal compliance with the five guiding principles

5.1.1.1.1 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."

For the on-board application platform, the application using in-vehicle data would be running inside the vehicle and the interface with the driver would be provided via the vehicle HMI. The driver would be able to provide consent to use the data required by any application via the HMI.

The technical solution does not specify how consent is given by the user. In legal terms, where consent is required, the data subject must consent before any data pertinent to that data subject is provided from the vehicle to the application. For example, in practice, different journeys may be undertaken by different drivers. Each driver is a different data subject, and consent would be need to be attained for each data driver; this could be provided via different 'driver profiles' in the vehicle or, more simply, by using a request for consent at the start of each journey. The consent should be capable of being revoked after being initially provided by a data subject. The precise details of how any required consent could be obtained would depend on the specific circumstances, but in any event this technical solution provides a plausible mechanism for obtaining consent (and permitting the data subject to revoke consent) via the vehicle HMI. The guiding principle of consent can therefore be met fully by the on-board application platform.

5.1.1.1.2 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."

The on-board application platform is, by definition, a technical solution that allows applications that have been appropriately certified by the car manufacturer to run inside the vehicle, accessing an agreed dataset. This solution allows all market participants access to the same dataset at the same time. It also allows the same interface with the driver (the vehicle HMI) regardless of the party providing the application. In these respects it provides equitable access to both in-vehicle data and resources and therefore complies with the guiding principle for fair and undistorted competition.

However, several points should be reiterated. Firstly, although this is an "open" on-board application platform, the car manufacturer should be responsible – and indeed is responsible for the ultimate safety and security of the system – only applications that are certified by the manufacturer should be deployed to the platform. The car manufacturer must be the party responsible for approving applications on the basis that they have designed the system and delivered the platform from a technical perspective. Therefore, car manufacturers theoretically have the ability to preferentially certify and deploy applications to the platform. Secondly, the data interface between the vehicle and the platform where the data is made available would be designed and controlled by the car manufacturer. Therefore, there is a potential risk that the market could be distorted by access being provided to a greater range of data, or data at lower latency or at a superior quality, to preferred market participants.

Both of these considerations could result in discrimination of applications from different third parties or more rapid implementation of preferred applications, especially in areas where car manufacturers may be directly engaged in the same competitive markets.

This technical solution, notwithstanding the considerations above, theoretically allows all market participants to access the same dataset at the same time with equitable access to the driver/data subject via the car's HMI. It is therefore, at least in principle, the best candidate to facilitate fair and undistorted competition.

5.1.1.1.3 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."

The Article 29 Working Party has issued guidance on the concept of personal data[34], which clarifies that the intention of EU regulation is to adopt a broad (but not unlimited) definition of personal data. The objective of the rules contained in the Directive is to protect the fundamental rights and freedoms of individuals, in particular their right to privacy, with regard to the processing of personal data. These rules were therefore designed to apply to situations where the rights of individuals could be at risk and hence in need of protection.

For data used by applications (with the consent of the data subject) this will, using this approach, include data which is personal. Working Group 6 concluded that in-vehicle data would be considered personal data and our legal assessment is also in line with this conclusion. This is because the in-vehicle data could be used in conjunction with other information likely to be in possession of the user to identify a living individual. In-vehicle data also relates to the identifiable individual because it is used to learn or record something about that individual. In the context of applications, these are likely to be

[34] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

tailored to the data subject's location, preferences etc. and therefore will log or learn various aspects particular to the specific user.

In this respect, Directive 95/46/EC and the forthcoming General Data Protection Regulation (GDPR) provide requirements that must be met for parties dealing with personal data. Therefore, in this respect an appropriate legal framework exists to protect and ensure data privacy and data protection; these obligations are the same regardless of the specific technical solution. How these obligations are met will vary depending on the precise implementation of each technical solution. However, our legal assessment has concluded that none of the proposed technical solutions is in principle incompatible with these obligations.

5.1.1.1.4 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."

It is a fundamental requirement that the technical solution to access in-vehicle data and resources is safe and secure. The system must be resilient to malicious intent and it is the responsibility of the car manufacturers to deliver a system that is safe and secure by design. From a technical perspective, achieving a safe and secure on-board application platform is feasible and some examples from specific manufacturers exist today that demonstrate this (e.g. General Motors, Toyota). It is apparent that car manufacturers may be in different states of readiness to deliver a safe and secure platform as described by this technical solution. This group of stakeholders indicate that manufacturers employ different electrical architectures that transfer data that is encoded differently. As the electrical architecture is this is a fundamental aspect of a car's design cycle (7-10 years) the cost and complexity of a change to deliver an on-board platform is likely to be significant for most manufacturers and unless coinciding with the established design cycle, could have particularly large effects for some manufacturers if they have only recently updated the electrical architecture that is to be used across current models.

Manufacturers rightly cite concerns about unauthorised access to safety critical aspects (e.g. braking, steering) of vehicle functionality and also that the communications network (CAN) could be overloaded with messages from applications that could impede or prevent other safety critical messages being processed correctly. These concerns are valid and are an integral part of the safety solution that must be developed if the on-board application platform is to be implemented. It is considered that as part of good design practices (e.g. ISO 26262) functional safety risks should be identified and measures that would mitigate the risk implemented. In this case, this might involve separating CAN access to safety critical components from other areas of the vehicle CAN (as is believed to the current approach in some cases) and implementing a 'hypervisor' to control and distribute messages appropriately around the vehicle that could also avoid buffer overflows created by repeated messages being sent to the CAN.

Therefore, for the on-board application platform there is a technical challenge to make such a technical solution acceptably safe. The burden of this activity will fall on car manufacturers and is likely to be significant. In this study, no estimated costs were received from car manufacturers, but indications are that costs would be significant and that the costs would vary between individual manufacturers depending on their particular electrical architecture design and also on the synchronisation of any changes with their current design cycle.

Liability for the vehicle and its safety lies (at least initially) with the car manufacturer. The manufacturer must ensure that the system implemented is safe and not exposed to malicious or unintentional effects that increase safety risk. Again, this comes back to good design practices and ensuring that the car's electrical architecture is designed with safety and risk mitigation in mind; this is an approach that should be employed currently

as well as in any future technical solution for access to in-vehicle data and resources. Applications running on the on-board platform would need to be certified by the manufacturer before installation. Theoretically, applications that posed a safety risk not detected at certification would be extremely rare because the technical issues that might reasonably lead to safety issues would have been tested and either passed or rejected. If the application achieved certification, a mechanism could be put in place such that liability could be passed along the chain from the car manufacturer to the third party, provided the manufacturer could demonstrate reasonable measures to protect safety (i.e. evidence that they had not acted negligently with respect to allowing access to third parties). This assumes that the fault for any failure could be diagnosed and traced; the system should store messages to allow this ability. The explicit transfer of liability could form part of the certification procedure for applications, either contractually or under a regulatory framework dealing with the requirements for such certification. In practice, the identification of fault and liability in such circumstances may not always be clear cut.

5.1.1.1.5 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."

As highlighted in the previous section, current vehicles have different electrical architectures between brands (and according to stakeholders, between models of the same brand) and also carry data that is encoded differently. Therefore the types of data and the way in which it is encoded are incompatible between vehicles of different manufactures. The only exception to this are regulated data types (e.g. emissions) that are standardised and presented via the OBD-II port in the same way by all manufacturers. This proves the principle that data can be made available in a way that would allow interoperability between applications using the data.

However, in practice, this is likely to be a significant undertaking for the same reason described in 5.1.1.1.4 relating to the proprietary electrical architectures implemented by different manufacturers. Even though current electrical architectures and data encoding are different between manufacturers, the provision of data mandated by regulation shows that this can be provided in a standard manner on a small scale. The technical challenge of providing a larger set of data in a common format on an on-board application platform is unknown. Again the issues in terms of cost that will fall on the car manufacturers are unknown. Standardising the on-board platform so that there is one interoperable platform between vehicle manufacturers will result in additional timescale and cost compared with a possible short-term solution whereby application developers would be required to design different versions for each manufacturer-specific platform.

In terms of remaining relevant in the light of developing technology and the data needs of applications that cannot be envisaged yet, the on-board application platform allows access to data with a low latency and would therefore support real-time applications that may become more important in the future.

5.1.1.1.6 Overview

Table 18: Compatibility of the on-board application platform with the WG6 guiding principles

Technical solution	Data provision conditions – consent	Fair and undistorted competition	Data privacy and data protection	Tamper-proof access and liability	Data economy
On-board application platform					

Assessment of compliance with WG6 guiding principles	Rating
Compatible with guiding principles	
Minor issues with compatibility or issues that could be addressed with low cost/impact	
Issues with compatibility or issues that could be addressed with medium cost/impact	
Significant issues with compatibility or issues that could be addressed with high cost/impact	
Incompatible with guiding principles in current form	

5.1.1.2 Risks and issues

Potential risks and issues have been identified in the areas of fair and undistorted competition, tamper-proof access and liability, and data economy (Table 19).

Table 19: Risks and issues from a technical and legal perspective associated with the on-board application platform

Area	Risks and issues	Comments on potential mitigation
Fair and undistorted competition	Risk of discrimination of third parties in areas where manufacturers are directly engaged in the same competitive markets: The market could be distorted by access being provided to a greater range of data, or data at lower latency or at a superior quality, to preferred market participants.	Mitigation appears possible via agreements or legislative interventions.
Tamper-proof access and liability	Safety risks: Concerns about unauthorised access to safety critical aspects (e.g. braking, steering) of vehicle functionality and that communications network (CAN) could be overloaded with messages from third party applications.	Mitigation appears possible but there are technical challenges and potentially high costs to achieve safety.

Area	Risks and issues	Comments on potential mitigation
	Liability: Concerns that manufacturers would be liable for incidents caused by third party code. Liability for the vehicle and its safety lies initially with the car manufacturer, who must ensure that the system implemented is safe and not exposed to malicious or unintentional effects that increase safety risk.	If an application achieved certification by the manufacturer, We consider that liability may be passed along the chain from the car manufacturer to the third party. This is likely to require the manufacturer to demonstrate reasonable measures to protect safety (i.e. evidence that they had not acted negligently with respect to allowing access to third parties).
Data economy	Compatibility of data: Current electrical architectures and data encoding are different between manufacturers (and between models).	The technical challenge of providing a larger set of data in a common format on an on-board application platform and the issues in terms of cost that will fall on the car manufacturer are unknown; in practice, providing a larger set of data in a common format between manufacturers is likely to be a significant undertaking.

5.1.1.3 Cost-benefit aspects

The cost data available for this solution indicated:

- One-off costs per vehicle manufacturer of €1m - €2.5m
- One-off costs per vehicle of approximately €115
- Annual costs per vehicle of approximately €10 (excluding communication costs).

Compared with other solutions the costs are expected to be relatively high, as a result of high costs of developing and maintaining the in-vehicle hardware for 12 million new vehicles each year (see Table 20).

Table 20: Relative scale of component costs for On-Board Application Platform

Technical development	In-vehicle hardware	Maintenance in-vehicle hardware	Database development	Database operation	Database maintenance	Server hardware	Server operation	Server maintenance	Administration and contracts	App service set up	App service operation	Cellular communication	RAN/ LAN/ WiFi communication	Overall weighted score
H	M	H	0						L	L	L	M	0	H

H = High

M = Medium

L = Low

The comparative impact assessment showed that this solution has the most positive impacts on consumer choice, competitiveness and innovation and research. It enables all stakeholders to access the data in real time and on a fair and equal basis, supporting the development of new services for consumers. Because data could be made available in real time it supports productivity improvements in sectors using the data (see Table 21).

There are negative impacts in terms of component costs (this is expected to be the most costly solution), on SMEs due to the need to make bilateral agreements with each vehicle manufacturer and on public authorities to carry out compliance checking.

The compliance with the principles of the ITS Directive is relatively low: while effective and interoperable, the relatively high component costs mean that this solution is less effective than others.

Table 21: Relative impacts of On-Board Application Platform

Component costs	Consumer choice	Competitiveness	SMEs	Public authorities	Innovation & research	ITS Directive principles
---	+++	+++	--	---	+++	+

5.1.1.4 Toolbox of measures at EU level

Table 22 contains a set of 'soft' and 'hard' measures, the Commission could choose to employ in order to achieve implementation of the on-board application platform and to ensure its compliance with the five guiding principles. The analysis of Scenario 3 (5.2.5) expands more on the measures employed in the scenario.

Table 22: Toolbox of possible measures at European level for on-board application platform (OBAP)

Implementation of the technical solution	
Encourage	**Enforce**
Instigate and support standardisation working groups.	Mandate an open OBAP for every connected car.
	Mandate an open OBAP (i.e. a platform that is open to any market participant) if an OBAP of any type is implemented in a car.

Compliance with the five guiding principles	
Encourage	**Enforce**
Suggest standard procedures for providing consent to data usage and suggest model contract clauses.	
Suggest model compliance guidelines for applications (those checked by OEMs before deployment), which are non-discriminatory for third-parties.	Prescribe that compliance guidelines have to be non-discriminatory.
	Specify rules on equal access to HMI.
	Require the availability of a documented API and SDK.
Facilitate a voluntary agreement on equal quality of the data available to third party- and OEM- or selected partner-applications.	Specify rules on equal quality of the data available to third party- and OEM- or selected partner-applications.
Facilitate an agreement on a minimum dataset that covers (initially) at least the data needs of existing and short term use-cases.	Define a mandatory minimum dataset.
Support the development of commonly accepted automotive cybersecurity standards.	

Compliance with the five guiding principles	
Encourage	**Enforce**
Provide safety performance guidelines in regard to distraction and HMI design.	
Encourage the development of a single, interoperable platform by facilitating a suitable platform of technical experts and setting maximum timeframes to achieve standardisation.	

5.1.2 Solution 2: In-vehicle interface

5.1.2.1 Technical and legal compliance with the five guiding principles

5.1.2.1.1 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."

For the in-vehicle interface, the application is either running on a nomadic device, other resource external to the vehicle system, or hosted on a layer of the interface itself, with the interface providing access to the in-vehicle data. The user (data subject) must consent before any data pertinent to that data subject is provided to the application. The data subject can, in this technical solution, provide consent using either the application – in this instance likely to be running on a smartphone or external resource. Consent can be given for each data subject and this could be given at the start of each journey, or for a particular device, authorised for each user as is currently the practice for applications running on smartphones. Similarly, the data subject would have the ability to revoke approval. However, for consent provided using an external device, this has safety implications because, for some examples at least, the use of the external device cannot be easily or safely operated in practice (i.e. when driving the car).

For implementations using the in-vehicle interface to send data back to a server or other resource, the provision of consent for specific data subjects is more difficult since there is not a facility that allows interaction with the driver (usually the data subject). This may create situations, where data is collected for a data subject who has not consented to that collection of that data. For example, if one driver has consented via an external device, but another person drives the vehicle. In this case, there is no interface to allow the second driver to either consent or revoke the existing consent because to the application there is no differentiation between the different data subjects.

The guiding principle of consent can therefore be theoretically met by the in-vehicle interface for some implementations of the solution but not for others; there are practical issues that need to be considered.

5.1.2.1.2 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."

The in-vehicle interface technical solution allows access to in-vehicle data but the latency of the data is greater than that of the on-board application platform because of the time incurred in sending data out of the vehicle. This means that other parties using a proprietary on-board application platform could have an advantage if both systems were in use simultaneously. Although the scale of this advantage might not be significant, it may mean that the driver is presented with outcomes or offers sooner with the on-board application platform. Furthermore, the importance of true real-time data could increase in the future, making this distinction more critical in terms of the effect on competition.

Due to the lack of access to the vehicle HMI, the access to the customer is also facilitated in a different way and this means that access to the customer is inferior to the on-board application platform and if different market participants are using these solutions, it has the potential to distort the market in favour of those with direct or easier access to customer and access to data with lower latency.

In addition, the OBD-II port could be occupied by a dongle for a specific provider; this would prevent access to other third party providers unless the customer removed the existing dongle and replaced it with another.

5.1.2.1.3 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."

The issues in relation to data privacy and data protection apply equally to all technical solutions are outlined in Section 5.1.1.1.3. In summary, Directive 95/46/EC and the forthcoming General Data Protection Regulation (GDPR) provide requirements that must be met for parties dealing with personal data. Therefore, for this, and all technical solutions, an appropriate legal framework exists to protect and ensure data privacy and data protection. Our legal assessment has concluded that none of the proposed technical solutions is in principle incompatible with this legal framework. Provided the relevant stakeholders comply with their obligations, this technical solution is therefore compatible with the WG6 guiding principles in this respect.

5.1.2.1.4 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.

As described in Section 5.1.1.1.4, it is a fundamental requirement that the technical solution to access in-vehicle data and resources is safe and secure. The system must be resilient to malicious intent and it is the responsibility of the car manufacturers to deliver a system that is safe and secure by design. From a technical perspective, achieving a safe and secure in-vehicle interface is feasible and some stakeholders of WG6 proposed a phased technical approach that included the addition of an improved security layer and a 'hypervisor' to deal with requests on the vehicle CAN bus.

The current OBD-II port used to access regulatory data on emissions and repair and maintenance has been shown to have security flaws. Most, if not all, of the examples of 'vehicle hacking' have utilised accessing the vehicle data via the OBD-II port and there are numerous examples that have been reported where vehicle functionality (including safety critical functionality such as the steering and brakes) could be interfered with. This highlights the importance of action to improve the security of the OBD-II interface, a step that would be necessary to make the legitimate access to in-vehicle data feasible. It also provides some evidence that suggests that some vehicle architectures are not currently designed in a way that appropriately mitigates security and safety risks if access to the CAB-bus is allowed.

As outlined in Section 5.1.1.1.4, it is a technical challenge to make the in-vehicle interface platform acceptably safe. The burden of this activity will fall on car manufacturers and is likely to be significant. In this study, no estimated costs were received from car manufacturers, but indications are that costs would be significant and that the costs would vary between individual manufacturers depending on their particular electrical architecture design and also on the synchronisation of any changes with their current design cycle. The requirements for improved safety and for a 'hypervisor' to provide management of messages to the CAN-bus would be similar to the on-board application platform.

While the imposition of an improved security layer and hypervisor functionality could have large cost implications for car manufacturers, especially if any mandatory action was imposed at a time that required a complete redesign of the vehicle's architecture, a view was often expressed that with the increase in automation, design and security of the vehicle should be robust with considerations of system failures as well as overall safety and security.

The liability issues relating the in-vehicle interface would be as described in Section 5.1.1.1.4. However, the applications would be running outside the vehicle system

(although they could be running on the device plugged into the interface) and therefore would not be certified by the manufacturer. This might be considered to result in greater risk because the functionality of the application has not been tested by the vehicle manufacturer directly and highlights the importance that the car manufacturer has architectures designed with functional safety in mind and has the capability to prevent communication with safety critical aspects of the vehicle unless specifically authorised and that messages on the CAN-bus are actively managed to prevent buffer overflows that could impede or crash vehicle systems.

5.1.2.1.5 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."

Regulated data types (e.g. emissions) are presented via the OBD-II port in the same way by all manufacturers. This proves the principle that data can be made available in a way that would allow interoperability between applications using the data. Therefore, it seems feasible that a larger dataset could be provided at this interface that would remain interoperable.

The technical challenge of providing a larger set of data in a common format via the in-vehicle interface is unknown. These cost burdens will fall on the car manufacturer and information from ACEA indicated that different car manufacturers use different electrical architectures and encode data in different ways. This means that the cost burden to enable the agreed dataset to be available via an in-vehicle interface may vary between vehicle manufacturers. However, examples exist of standardised data being provided (repair and maintenance for example) so this appears feasible.

5.1.2.1.6 Overview

Table 23: Compatibility of the in-vehicle interface with the WG6 guiding principles

Technical solution	Data provision conditions – consent	Fair and undistorted competition	Data privacy and data protection	Tamper-proof access and liability	Data economy
In-vehicle interface					

Assessment of compliance with WG6 guiding principles	Rating
Compatible with guiding principles	
Minor issues with compatibility or issues that could be addressed with low cost/impact	
Issues with compatibility or issues that could be addressed with medium cost/impact	
Significant issues with compatibility or issues that could be addressed with high cost/impact	
Incompatible with guiding principles in current form	

5.1.2.2 Risks and issues

Potential risks and issues have been identified in the areas of fair and undistorted competition, tamper-proof access and liability, and data economy (Table 24).

Table 24: Risks and issues from a technical and legal perspective associated with the in-vehicle interface

Area	Risks and issues	Comments on potential mitigation
Fair and undistorted competition	Limited access to real-time data: The latency of the data is greater than that of an on-board application platform (a proprietary version of which is likely to be available to vehicle manufacturers in parallel) because of the time incurred in sending data out of the vehicle. This has the potential to limit the functionality of certain applications, for example in RMI, whereas those with access to real time data will not be constrained.	This is a technical limitation that cannot be mitigated by legislative interventions.
	No access to the vehicle HMI: This could limit the range of applications that can be offered and offers third-parties reduced access to the customer for selling new services compared to the manufacturer.	Technical limitation that could be partially mitigated by offering access to HMI via other channels (e.g. smartphone projection technologies).
	Single OBD-II port could be occupied by a dongle for a specific provider: this could prevent access to other third party providers.	Technical solutions possible that allow applications from various providers although there is only one interface.
Tamper-proof access and liability	Safety risks: The current OBD-II port is not secure enough to ensure safe operation when applications have free access via this port.	Mitigation is technically feasible by updating the safety and security of the interface but might create significant costs for some manufacturers.
	Liability: Concerns that manufacturers would be liable for incidents caused by third party applications. These would not be certified by the manufacturer before deployment.	Liability would be limited if the manufacturer could demonstrate reasonable measures to protect safety (i.e. evidence that they had not acted negligently and that allowing access to third parties did not make the car in effect a defective product).
Data economy	Compatibility of data: Current electrical architectures and data encoding are different between manufacturers (and between models).	It seems feasible that a larger dataset could be provided at this interface that would remain interoperable. The costs, which will fall on the car manufacturers, are unknown and may vary between vehicle manufacturers.

5.1.2.3 Cost-benefit aspects

The cost data available for this solution (excluding communication costs) indicated:

- One-off costs per vehicle manufacturer of €1m - €2.5m
- One-off costs per vehicle of approximately €15.

Compared with other solutions the costs are expected to be relatively high, as a result of high costs of developing and maintaining the in-vehicle hardware for 12 million new vehicles each year (see Table 25, where L=Low, M=Medium and H=High relative cost).

Table 25: Relative scale of component costs for In-Vehicle Interface

Technical development	In-vehicle hardware	Maintenance in-vehicle hardware	Database development	Database operation	Database maintenance	Server hardware	Server operation	Server maintenance	Administration and contracts	App service set up	App service operation	Cellular communication	RAN/ LAN/ WiFi communication	Overall weighted score
M	M	H	L	L	L	L	L	-	L	L	L	M	0	H

The comparative impact assessment showed that this solution has the most positive impact on innovation and research as a result of the availability of data in real time to support the development of new services. This interoperable solution gives third parties access to the data with some positive impact on consumers, but the vehicle manufacturer controls the data so consumers benefit less than in some of the other solutions (see Table 26).

There are negative impacts in terms of component costs (this is expected to be a relatively costly solution), on SMEs due to the need to make bilateral agreements with each vehicle manufacturer and on public authorities to carry out compliance checking.

The compliance with the ITS Directive principles is relatively low: while effective and interoperable, the relatively high component costs mean that this solution is less effective than others.

Table 26: Relative impacts of In-Vehicle Interface

Component costs	Consumer choice	Competitiveness	SMEs	Public authorities	Innovation & research	ITS Directive principles
---	+	---	--	---	+++	+

5.1.2.4 Toolbox of measures at EU level

Table 27 contains a set of 'soft' and 'hard' measures, the Commission could choose to employ in order to achieve implementation of the in-vehicle interface and to ensure its compliance with the five guiding principles.

Table 27: Toolbox of possible measures at European level for in-vehicle interface

Implementation of the technical solution	
Encourage	**Enforce**
Instigate and support standardisation working groups for a suitable interface specification.	Develop a technical specification for the in-vehicle interface and mandate its fitment to new cars.

Compliance with the five guiding principles	
Encourage	**Enforce**
Suggest standard procedures for providing consent to data usage and suggest model contract clauses.	

Compliance with the five guiding principles	
Encourage	**Enforce**
Facilitate a voluntary agreement on equal quality of the data available to third party-applications via the in-vehicle interface and those available to applications running on a potential proprietary on-board application platform.	Specify rules on equal quality of the data available via in-vehicle interface to third party-applications.
Facilitate an agreement on a minimum dataset that covers (initially) at least the data needs of existing and short term use-cases.	Define a mandatory minimum dataset.
Seek voluntary industry agreements against dongle solutions that would 'block' the OBD-II port for proprietary applications from only one provider or limit data transmission to the servers of only one provider.	Develop and mandate a technical specification for dongles that would prevent this issue.
Support the development of commonly accepted automotive cybersecurity standards.	

5.1.3 Solution 3.1: Data server – Extended vehicle

5.1.3.1 Technical and legal compliance with the five guiding principles

5.1.3.1.1 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."

The data subject (in most cases the driver) must consent before any data pertinent to that data subject is provided from the vehicle to any party wanting to use that data. For the 'extended vehicle' data server solution proposed by ACEA, the data from the vehicle is sent via a mobile connection to the manufacturer back end server.

Consent would need to be provided for each data subject; this could be provided via different 'driver profiles' in the vehicle or, more simply, by using a request for consent at the start of each journey. Consent for each journey would be required since each journey may have a different driver and the driver should always have the option to revoke permissions already given. In this technical solution, the only feasible mechanism of providing consent is via the HMI. However, only the car manufacturer has access to the HMI for this technical solution, excluding all other market participants from being able to attain consent in the same way.

The guiding principle of consent can therefore be met by all market participants, but the way in which consent could be met in practice means that the car manufacturer is likely to have an advantageous position with respect to contact with the driver and in the overall 'user friendly' implementation of applications. For others, consent would need to be given using the application which would need to be running on another device; this would mean the mechanism to provide consent is likely to be more onerous than that enjoyed by the car manufacturer.

5.1.3.1.2 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."

The extended vehicle data server solution means that consent to use the data can be achieved preferentially by the car manufacturer using the vehicle HMI; a method which no other market participant has access to. Lack of access to the resource (the car HMI) for other market participants also means that the interaction with the customer in general is considered to place the car manufacturer in a privileged position with regard to the provision of services. This technical solution also means that the data could be available at superior quality and with lower latency on the car manufacturer's server compared with the interface available to other market participants. This also has the potential to place the car manufacturer in a privileged position in the market where the car manufacturer is competing for the same services.

Furthermore, the car manufacturer may be able to identify the third party accessing data from the car manufacturer's server and would also have visibility of the data being used. Some stakeholders argued that this would mean that the car manufacturers would have a competitive advantage in that it would allow car manufacturers to oversee the innovation made by competitors in the same market. The same stakeholders also said that the car manufacturer could (without any oversight) have control over who had access to the data and, combined with the knowledge about the party accessing the data would have the opportunity to distort the market.

Therefore, the extended vehicle is considered to have multiple features that confer risks of unfair competition, with the potential to distort the market for existing and future services using vehicle data to the detriment of consumers.

5.1.3.1.3 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."

The issues in relation to data privacy and data protection apply equally to all technical solutions are outlined in Section 5.1.1.1.3. In summary, Directive 95/46/EC and the forthcoming General Data Protection Regulation (GDPR) provide requirements that must be met for parties dealing with personal data. Therefore, for this, and all technical solutions, an appropriate legal framework exists to protect and ensure data privacy and data protection. Our legal assessment has concluded that none of the proposed technical solutions is in principle incompatible with this legal framework. Provided the relevant stakeholders comply with their obligations, this technical solution is therefore compatible with the WG6 guiding principles in this respect.

5.1.3.1.4 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.

As described in the preceding sections, it is a fundamental requirement that the technical solution to access in-vehicle data and resources is safe and secure. The extended vehicle prevents any direct access to the vehicle and vehicle systems by third parties and in this respect, provides clear security and safety responsibility on the car manufacturer. The car manufacturers assert that this reduces the risk. Other stakeholders however, view this as a safety risk precisely because the system is opaque and only accessible by the manufacturer. This may mean that the security is provided primarily by limiting access rather than by different layers of protections, including robust design and other technical safety and security measures (e.g. firewalls).

Car manufacturers state that this system allows safety and security to be maintained and ensures that the system is protected by preventing access to other parties and clearly leaving safety and security liability wholly with the manufacturer. This situation is

continuation of the status quo and so, provides safety and security in line with the level experienced today.

Considering the whole system, all data server concepts could be argued to pose a greater risk because should a malicious hacker gain access to the server, they could influence all vehicles. This security at the server must be appropriate and the security layer and hypervisor must prevent writing to safety critical components.

5.1.3.1.5 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 extended vehicle provides the data to a standard interface so that the data agreed is available to other market participants. This implies that the data agreed is provided in a format that is interoperable among all manufacturers. However, third parties wanting to access the data would need to establish contacts with each manufacturer to access the data for their vehicles. This would add significant contractual burden to third parties trying to deliver services across the market. Although in this respect the barrier would be the same for all participants, the ability and resources necessary to overcome this might favour larger organisations and in effect be a larger barrier for SMEs.

Additionally, all data server solutions are subject to increased latency compared with data accessed directly inside the vehicle. This means that data server solutions cannot support real-time applications, but perhaps – with improvements in communication speed – could be near real-time. However, feedback from stakeholders indicated that these solutions would not be compatible with real-time solutions. In the future, more and more services may require real-time data so these technical architectures may not be as futureproof as solutions accessing data directly from the vehicle.

5.1.3.1.6 Overview

Table 28: Compatibility of the data server (extended vehicle) with the WG6 guiding principles

Technical solution	Data provision conditions – consent	Fair and undistorted competition	Data privacy and data protection	Tamper-proof access and liability	Data economy
Data server (extended vehicle)					

Assessment of compliance with WG6 guiding principles	Rating
Compatible with guiding principles	
Minor issues with compatibility or issues that could be addressed with low cost/impact	
Issues with compatibility or issues that could be addressed with medium cost/impact	
Significant issues with compatibility or issues that could be addressed with high cost/impact	
Incompatible with guiding principles in current form	

5.1.3.2 Risks and issues

Potential risks and issues have been identified in the areas of fair and undistorted competition, tamper-proof access and liability, and data economy (Table 29).

Table 29: Risks and issues from a technical and legal perspective associated with the extended vehicle data server solution

Area	Risks and issues	Comments on potential mitigation
Fair and undistorted competition	Mechanism to provide consent: The manufacturer could request consent via the vehicle HMI (third parties via another device, e.g. phone), which could put him in an advantageous position with respect to contact with the driver and overall 'user friendly' implementation of applications.	This can partially be mitigated by definition of suitable procedures.
	No access to real-time data: The latency of the data is greater than that of an on-board application platform (a proprietary version of which could be offered in parallel) because of the time incurred in sending data to the extended vehicle server, re-formatting it if required, and sending it on to the service provider. This means that data server solutions cannot support real-time applications, for example in RMI.	This is a technical limitation that cannot be mitigated by legislative interventions.
	No access to the vehicle HMI: This could limit the range of applications that can be offered and offers third-parties reduced access to the customer for selling new services compared to the manufacturer.	Technical limitation that could be partially mitigated by offering access to HMI via other channels (e.g. smartphone projection technologies).
	Monitoring of third parties: The manufacturer may be able to identify a third party accessing data from the extended vehicle server and would also have visibility of the data being used. Vehicle manufacturers may have better access to data (greater range of data, lower latency etc) via proprietary on-board application platforms.	Technical solutions such as the extended vehicle/neutral server model could mitigate this issue.
Tamper-proof access and liability	Safety risks: The fact that the car is only accessible to manufacturers appears per se beneficial for safety but it could mean that the security is provided primarily by limiting access rather than by different layers of technical protections, which would incur security risks.	Mitigation is technically feasible.

Area	Risks and issues	Comments on potential mitigation
Data economy	Contractual burden: Third parties wanting to access data would need to establish contacts with each manufacturer to access the data for their vehicles. This might favour larger organisations and in effect be a larger barrier for SMEs.	Mitigation by legislative measures seems possible to an extent.

5.1.3.3 Cost-benefit aspects

The cost data available for this solution (excluding communication costs) indicated:

- One-off costs per vehicle manufacturer of €1m - €2.5m
- One-off costs per vehicle of approximately €15
- Annual cost of database €1m - €2m.

Compared with other solutions the costs are expected to be relatively low, as a result of low costs of developing and maintaining the in-vehicle hardware and relatively low server costs (see Table 30).

Table 30: Relative scale of component costs for Data Server – Extended Vehicle

Technical development	In-vehicle hardware	Maintenance in-vehicle hardware	Database development	Database operation	Database maintenance	Server hardware	Server operation	Server maintenance	Administration and contracts	App service set up	App service operation	Cellular communication	RAN/ LAN/ WiFi communication	Overall weighted score
L	L	L	L	L	L	L	L	L	L	L	L	M	L	L

The comparative impact assessment showed that this solution has the most positive impact on component costs (as a result of the costs being low relative to other solutions). It is anticipated to have a positive compliance with the principles of the ITS Directive as a result of it being interoperable, cost-efficient, proportionate and respecting coherence. There is a limited positive impact on innovation and research as a result of the availability of data to support the development of new services, but since limited data is made available, this impact is less than in the case of some other solutions.

Because a limited set of data is expected to be provided and the vehicle manufacturer controls the value chain, the range of services available to consumers is expected to be less than in the case of other solutions and the contribution to competitiveness is also expected to be lower (see Table 31). There are also negative impacts in terms of SMEs due to the need to make bilateral agreements with each vehicle manufacturer before they can enter the market.

The compliance with the principles of the ITS Directive is 'medium': while cost-efficient, proportionate and delivering interoperability and respecting coherence, it is expected to be less effective and provide less support to continuity of services than other solutions.

Table 31: Relative impacts of Data Server – Extended Vehicle

Component costs	Consumer choice	Competitiveness	SMEs	Public authorities	Innovation & research	ITS Directive principles

+++	---	---	--		+	++

5.1.3.4 Toolbox of measures at EU level

Table 32 contains a set of 'soft' and 'hard' measures, that could be used as part of measures at EU level to firstly achieve implementation of the extended vehicle and secondly, to improve its compliance with the five guiding principles.

Table 32: Toolbox of possible measures at EU level for extended vehicle

Implementation of the technical solution	
Encourage	**Enforce**
Not applicable: ISO standards are being defined and industry is working towards implementation.	Mandate data access via an extended vehicle server for new cars.

Compliance with the five guiding principles	
Encourage	**Enforce**
Suggest suitable standard procedures for providing consent to data usage, e.g. procedures that allow giving consent via the vehicle HMI at the start of each journey that covers all apps that have previously had access to data via the extended vehicle server (including third parties).	
Facilitate a voluntary agreement on equal quality of the data available to third party-applications via the extended vehicle server and those available to applications running on a potential proprietary on-board application platform. This cannot solve the latency/real-time limitation of this solution.	Specify rules on equal quality of the data available via the extended vehicle server to third party-applications. This cannot solve the latency/real-time limitation of this solution.
Facilitate an agreement on a minimum dataset that covers (initially) at least the data needs of existing and short term use-cases.	Define a mandatory minimum dataset.
Encourage technical safeguards against the monitoring of third parties' data usage (such as neutral servers).	Create legal safeguards against the monitoring of third parties' data usage.
Support the development of commonly accepted automotive cybersecurity standards.	
Suggest model contract clauses in order to reduce the contractual burden.	Define default contract rules to reduce the contractual burden

5.1.4 Solution 3.2: Data server – Shared server

5.1.4.1 Technical and legal compliance with the five guiding principles

5.1.4.1.1 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."

In terms of consent, the compliance with the guiding principles is as described in Section 5.1.3.1.1. In summary this is that the guiding principle of consent can be met in practice by all market participants, but the car manufacturer can obtain consent via the HMI, but this mechanism is not available to other market participants. For others, consent would need to be given using the application which would be running on another device; this would mean the mechanism to provide consent would be more onerous than enjoyed by the car manufacturer. For all market participants, this solution enables the requirements of consent to be met, but the way in which consent could be met in practice means that the car manufacturer is likely to have an advantageous position with respect to contact with the driver and overall 'user friendly' implementation of applications.

5.1.4.1.2 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."

The shared server solution means that consent to use the data can be achieved preferentially by the car manufacturer using the vehicle HMI; a method which no other market participant has access to. Lack of access to the resource (the car HMI) for other market participants also means that the interaction with the customer in general is considered to place the car manufacturer in a privileged position with regard to the provision of services.

This solution would allow data to be available at the same quality and latency for all market participants. The shared server is envisaged in different ways by the stakeholders; either as a server that shares data required for services for all market participants or a shared server that receives the same data in parallel to the car manufacturer's server, but with a separate data link directly to the vehicle. In either arrangement, the data is provided with the same quality and latency at the shared server. In this respect, this architecture supports fair competition. Furthermore, in this solution, the car manufacturer would not be able to identify the third party accessing data.

The Shared Server (in common with all data server solutions) cannot give access to real-time data because of the time incurred in sending data to the server, re-formatting it if required, and sending it on to the service provider. Hence, the latency of the data is greater than that of an on-board application platform (a proprietary version of which could be offered in parallel) and so certain market participants could be in an advantageous position compared to others.

The shared server is considered to have some features that confer risks of unfair competition relating to the access to HMI that have the potential to distort the market for existing and future services using vehicle data.

5.1.4.1.3 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.

The shared server concept is considered capable of being implemented in a way that is compliant with data privacy and data protection requirements.

5.1.4.1.4 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.

As described for the 'extended vehicle' solution and in common with all technical solutions, it is a fundamental requirement that the system that enables access in-vehicle data and resources is safe and secure. As with other data server concepts, direct access

to the vehicle and vehicle systems by third parties is prevented, providing clear security and safety responsibility on the car manufacturer. This provides a way of preventing access to the vehicle by design.

It is important that any car architecture is well designed with respect to functional safety standards and includes multiple layers (preventing access to safety critical ECUs, security to prevent unauthorised writing or repeated messages on the CAN bus). The exact design and security arrangements in place by the car manufacturers are unknown. There are examples of unauthorised access being possible via the OBD port which includes writing to safety critical components. However, this may be an issue for only a small proportion of vehicles, but this could indicate a larger issue that might affect a larger proportion of vehicles. This indicates that, for some vehicles at least, revisions to vehicle architecture and security arrangements might be required and highlights a potential issue with independent oversight of the design and security concepts in place.

On one hand the shared server provides an approach that could be effective in terms of preventing third party access to the vehicle and could be implemented in short timeframe, but it retains the security arrangements as a 'black box' with no oversight of the adequacy of any design or security arrangements. Furthermore, access using this (and other) data server concepts will mean that it will place the car manufacturer in a privileged position with respect to access to resources (i.e. the car HMI).

5.1.4.1.5 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 issues for the data economy for the shared server are similar to that of the extended vehicle; see Section 5.1.3.1.5.

5.1.4.1.6 Overview

Table 33: Compatibility of the data server (shared server) with the WG6 guiding principles

Technical solution	Data provision conditions – consent	Fair and undistorted competition	Data privacy and data protection	Tamper-proof access and liability	Data economy
Data server (Shared server)					

Assessment of compliance with WG6 guiding principles	Rating
Compatible with guiding principles	
Minor issues with compatibility or issues that could be addressed with low cost/impact	
Issues with compatibility or issues that could be addressed with medium cost/impact	
Significant issues with compatibility or issues that could be addressed with high cost/impact	
Incompatible with guiding principles in current form	

5.1.4.2 Risks and issues

Potential risks and issues have been identified in the areas of fair and undistorted competition, tamper-proof access and liability, and data economy. The items are similar to the extended vehicle solution (provided in Table 29) less the risk of monitoring of third parties' data usage by manufacturers.

5.1.4.3 Cost-benefit aspects

The cost data available for this solution (excluding communication costs) indicated:

- One-off costs per vehicle manufacturer of €3m - €4.5m
- One-off costs per vehicle of approximately €15
- Annual cost per vehicle manufacturer €1m - €2m.

Compared with other solutions the costs are expected to be relatively low, as a result of low costs of developing and maintaining the in-vehicle hardware and 'medium' server costs (see Table 34).

Table 34: Relative scale of component costs for Data Server – Shared Server

Technical development	In-vehicle hardware	Maintenance in-vehicle hardware	Database development	Database operation	Database maintenance	Server hardware	Server operation	Server maintenance	Administration and contracts	App service set up	App service operation	Cellular communication	RAN/ LAN/ WiFi communication	Overall weighted score
L	L	L	L	L	L	M	M	M	M	L	L	M	L	L

The comparative impact assessment showed that this solution has the most positive impact on component costs (as a result of the costs being low relative to other solutions). It is anticipated to have a positive compliance with the principles of the ITS Directive as a result of it being interoperable, cost-efficient, proportionate, respecting coherence and supporting continuity of services. The shared server also has a positive contribution to consumer choice, competitiveness and SMEs, and there is a limited positive impact on innovation and research as a result of the availability of data to support the development of new services; however since limited data is made available, this impact is less than in the case of some other solutions.

A degree of negative impact on public authorities is anticipated as a result of the need to ensure governance of the shared server (see Table 35).

The compliance with the principles of the ITS Directive is 'medium': while cost-efficient, proportionate and delivering interoperability and respecting coherence, it is expected to be less effective and provide less support to continuity of services than other solutions.

Table 35: Relative impacts of Data Server – Shared Server

Component costs	Consumer choice	Competitiveness	SMEs	Public authorities	Innovation & research	ITS Directive principles
+++	++	++	++	-	+	++

5.1.4.4 Toolbox of measures at EU level

The toolbox of 'soft' and 'hard' measures, which could be employed in order to achieve implementation of the shared server solution and to ensure its compliance with the five

guiding principles, is in effect identical to that for the extended vehicle solution (as provided in Table 32).

5.1.5 Solution 3.3: Data server – B2B marketplace

5.1.5.1 Technical and legal compliance with the five guiding principles

5.1.5.1.1 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."

In a similar way to the other data server concepts, the B2B marketplace solution would provide a way for consent to be sought and provided for all market participants and in this respect the requirements of consent could be met for all market participants. However, despite meeting the requirement for consent, since the car manufacturer can solicit consent from the vehicle HMI and third parties cannot, this creates the risk of unfairness. This could be significant especially as consent may be requested for each driver or each journey. This would be user friendly to implement on the vehicle HMI, but third parties would need to do this via an application running elsewhere. Although on a personal mobile device consent could be provided specific to that individual (i.e. always consent to this), it would require interaction with the device to commence or revoke access that might be less 'user friendly' than using the vehicle HMI.

5.1.5.1.2 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."

This solution is similar to the shared server (see Section 5.1.4.1.2) in this respect.

5.1.5.1.3 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."

As with other technical solutions, this requirement can be met. The B2B marketplace concept is considered capable of being implemented in a way that is compliant with data privacy and data protection requirements, and the relevant safeguards that exist in European law apply to all market participants

5.1.5.1.4 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."

The issues for the B2B marketplace with respect to tamper-proof access and liability are similar to that of the shared server (see Section 5.1.4.1.4) and the extended vehicle (see Section 5.1.3.1.4).

5.1.5.1.5 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 issues for the data economy for the B2B marketplace are similar to that of the shared server (see Section 5.1.4.1.5) and the extended vehicle (see Section 5.1.3.1.5).

Table 36: Compatibility of the data server (B2B marketplace) platform with the WG6 guiding principles

Technical solution	Data provision conditions – consent	Fair and undistorted competition	Data privacy and data protection	Tamper-proof access and liability	Data economy
Data server – B2B marketplace					

Assessment of compliance with WG6 guiding principles	Rating
Compatible with guiding principles	
Minor issues with compatibility or issues that could be addressed with low cost/impact	
Issues with compatibility or issues that could be addressed with medium cost/impact	
Significant issues with compatibility or issues that could be addressed with high cost/impact	
Incompatible with guiding principles in current form	

5.1.5.2 Risks and issues

Potential risks and issues have been identified in the areas of fair and undistorted competition, tamper-proof access and liability, and data economy. The items are similar to the extended vehicle solution (provided in Table 29) less the risk of monitoring of third parties' data usage by manufacturers.

5.1.5.3 Cost-benefit aspects

The cost data available for this solution (excluding communication costs) indicated:

- One-off costs per vehicle manufacturer of €3m - €4.5m
- One-off costs per vehicle of approximately €15
- Annual cost per vehicle manufacturer €1m - €2m.

Compared with some other solutions the costs are expected to be relatively low, as a result of low costs of developing and maintaining the in-vehicle hardware and 'medium' server costs (see Table 37).

Table 37: Relative scale of component costs for Data Server – B2B Marketplace

Technical development	In-vehicle hardware	Maintenance in-vehicle hardware	Database development	Database operation	Database maintenance	Server hardware	Server operation	Server maintenance	Administration and contracts	App service set up	App service operation	Cellular communication	RAN/ LAN/ WiFi communication	Overall weighted score
L	L	L	L	L	L	M	M	M	H	L	L	M	M	L

The comparative impact assessment showed that this solution has the most positive impact on component costs (as a result of the costs being low relative to other solutions). It is anticipated to have a positive compliance with the principles of the ITS Directive as a result of it being interoperable, cost-efficient, proportionate, respecting coherence and supporting continuity of services. The B2B marketplace also has a positive contribution to consumer choice and competitiveness, and there is a limited positive impact on SMEs and innovation and research as a result of the availability of data to support the development of new services; however since limited data is made available, this impact is less than in the case of some other solutions. No impact on public authorities is anticipated in the case of the marketplace (see Table 38).

The compliance with the principles of the ITS Directive is 'medium': while cost-efficient, proportionate and delivering interoperability and respecting coherence, it is expected to be less effective and provide less support to continuity of services than other solutions.

Table 38: Relative impacts of Data Server – B2B Marketplace

Component costs	Consumer choice	Competitiveness	SMEs	Public authorities	Innovation & research	ITS Directive principles
+++	++	++	+		+	++

5.1.5.4 Toolbox of measures at EU level

The toolbox of 'soft' and 'hard' measures, which the Commission could choose to employ in order to achieve implementation of the shared server solution and to ensure its compliance with the five guiding principles, is in effect identical to that for the extended vehicle solution (as provided in Table 32).

5.1.6 Overview of compliance with the guiding principles

Table 39 summarises the findings of this section with a graphical representation of the extent to which the WG6 solutions comply with the five guiding principles.

Table 39: Level of compatibility of the WG6 solutions with the five guiding principles

Technical solution	Data provision conditions – consent	Fair and undistorted competition	Data privacy and data protection	Tamper-proof access and liability	Data economy
On-board application platform					
In-vehicle interface					
Data server – Extended vehicle					
Data server – Shared server					
Data server – B2B marketplace					

Assessment of compliance with WG6 guiding principles	Rating
Compatible with guiding principles	
Minor issues with compatibility or issues that could be addressed with low cost/impact	
Issues with compatibility or issues that could be addressed with medium cost/impact	
Significant issues with compatibility or issues that could be addressed with high cost/impact	
Incompatible with guiding principles in current form	

In general terms, the data server platform solutions could be delivered in a shorter timeframe compared with the in-vehicle solutions. This is because the data server solution are already developed and the safety and security issues can be more rapidly addressed as a large portion of the risk is removed by excluding access to the vehicle by third parties. For in-vehicle solutions it is considered likely that a larger body of technical development is required to ensure safety and security for all car manufacturers, but examples exist in the market that also indicate that for some manufacturers this would not be a significant timeline.

5.2 Scenarios

5.2.1 Definition of scenarios

Section 5.1.6 provided an overview of the compliance of each of the technical solutions proposed by WG6 to access in-vehicle data and resources. It can be seen that no single

solution is wholly compliant with all of the guiding principles. The preceding analysis has highlighted areas where action is required to either make the solution compliant or to improve the degree of compliance to mitigate against the risks identified and has determined a toolbox of possible 'soft' and 'hard' measures of intervention.

In addition to possible actions to improve the compliance for each of these technical solutions with the guiding principles, it is clear that all technical solutions currently exist in parallel and any implementation scenario must consider actions across all technical solutions, account for the timescale in which acceptable compliance with the guiding principles of the system can be achieved and the overall long-term objectives for the arrangement of the market in place to access in-vehicle data and resources.

This section sets out a series of four scenarios, starting with describing the baseline, i.e. a 'no action' scenario, and further scenarios with various interventions combined from the measures available in the toolbox to improve compliance with the five guiding principles and to mitigate the risks that have been identified.

The scenarios assessed comprised:

- Scenario 0 – no action (Extended vehicle/neutral server; the baseline scenario)
- Scenario 1 – Scenario 0 with measures at European level to accompany market development and address risks
- Scenario 2 – Short term: Shared server
- Scenario 3 – Long term: On-board application platform

We believe that the extended vehicle/neutral server model is the technical solution that will be available for the wider market to access vehicle data if there is no intervention at EU level, since the car manufacturers are already working to deliver this solution and have clearly stated an intention to deliver a data server solution. Scenario 1 has been proposed to provide options for 'soft' intervention at EU level designed to accompany the development of the market with the intention of delivering improvements in terms of compliance with the guiding principles. The shared server has been proposed as Scenario 2 because this solution rated highest in the impact analysis and can be implemented in a shorter timescale than the other in-vehicle solutions, therefore providing an intermediate step that to the market. Scenario 3 – the on-board application platform – has been selected as Scenario 3. This solution provides strong compliance in terms of fair and undistorted competition and allows access to real-time data. Therefore, based on the information currently available and on stakeholder contributions this is judged to be most probably the best long-term solution for delivering an interoperable, standardised, secure and open-access platform for access in-vehicle data and resources. Although this solution places financial burden on the car manufacturers to develop improved security and hypervisors, there are examples in the market that suggest this is already happening and we consider that such development is necessary in the longer term and that any requirements could be appropriately phased to allow manufacturers to synchronise updates with their existing design cycles.

5.2.2 Scenario 0 – no action

This is the baseline scenario and is considered to be the situation that will become established if there is no market intervention. TRL believe that this is the case because ACEA has proposed this approach and the solution utilises the 'extended vehicle' solution which the car manufacturers are developing, and which itself draws on to a large extent the existing system in place used by manufacturers. Furthermore, car manufacturers indicated that this technical solution would be implemented in the absence of European action on the subject. However, it should also be noted that without any formalisation of the neutral server model, it is a possibility that the position of the car manufacturers could revert to their original position of the 'extended vehicle' solution.

The extended vehicle/neutral server model is a technical solution using a data server concept based on the extended vehicle with the modification that data is provided from

the car manufacturer's server to another server which is maintained by a neutral service provider (see Section 3.2.2.4). Furthermore, it is suggested that third parties could utilise mobile platforms such as Apple CarPlay and Google Android Auto (see Sections 3.2.5.5 and 3.2.5.6) to access the vehicle HMI and interact with the driver if the application in question required this functionality.

In this baseline case, TRL see this as the solution that is available for the market but this is likely to co-exist in practice with proprietary on-board platforms. The in-vehicle interface is expected to exist but may be closed to communication while the vehicle is in motion.

5.2.2.1 Compliance with five guiding principles

5.2.2.1.1 Data provision conditions – consent

Consent can be solicited and obtained from the data subject (usually the driver) by all market participants. For the car manufacturer, this is likely to be provided by using the vehicle HMI as this is the most convenient mechanism and the request for consent could be given for each driver or each journey. For other parties, access to the vehicle HMI would be possible if the application could be used in conjunction with Apple CarPlay or Google Android Auto (or another platform accepted and integrated into the vehicle by the car manufacturer). This may provide some limitations on the third parties – i.e. they are dependent on compatibility with these platforms and on car manufacturers integrating the platforms into their vehicles. However, where this was possible, it would allow third parties to access the driver using the same resources as the car manufacturer.

5.2.2.1.2 Fair and undistorted competition

This would allow access for the car manufacturer to their back end server and provide the agreed data to the neutral server for access by the rest of the market. This solution is therefore similar to that previously described for the WG6 data server technical solutions (see Section 5.1.5.1.2). In summary, this solution means that the car manufacturer has access to data that may be at a differing quality and lower latency that might be available to the rest of the market. This in itself introduces the possibility of market distortion, but in addition the data provided to the neutral server is under the control of the car manufacturer. Although the neutral server prevents the car manufacturer from knowing the identity of the third party requesting data, it does not prevent them knowing which data is requested. Therefore, in markets for which the car manufacturer is in direct competition with other market participants, this arrangement although capable of delivering fair and undistorted competition, relies on the car manufacturer providing data to the neutral server for which a contract will be required between the neutral server operator and the car manufacturer. For this solution in isolation, the features of the neutral server model are an improvement over other data server platform solutions but do not solve all of the risks relating to possible market distortion.

Furthermore, since in practice, multiple technical solutions will exist in parallel, the car manufacturer is also likely to have access to a proprietary on-board application platform and this means that there is the risk of an unfair market because other market participants only have access via a data server solution.

As with all solutions, the types of data and how this is made available also could have large effects on fair and undistorted competition. The main issues arising from this aspect is covered in Section 3.4.8. Without specific action in this area, agreement of data is likely to be on the basis of use-cases and could be under the control of the car manufacturers. This may limit the timeliness of the use-cases (and therefore the data) being agreed and made available to other market participants. It could also provide car manufacturers with a veto on any data being provided. The treatment of these aspects is unclear at present, but can be identified as risks that unless appropriately addressed,

could result in the distortion of the market in favour of car manufacturers. As competitors in some markets, they would continue to have access to data at their own servers and potentially also on the in-vehicle platform.

5.2.2.1.3 Data privacy and data protection

This technical solution would be capable of being implemented in a way that is compliant with this guiding principle, and the existing European regulation that effectively requires such compliance would apply to all market participants.

5.2.2.1.4 Tamper-proof access and liability

In terms of safety, this technical solution is similar to that described previously for the other data server solutions (see Section 5.1.3.1.4). In summary these are that it provides a level of safety and security by virtue of the fact that it excludes third party access to the vehicle. This is a reasonable step to introduce the system safe and secure, but it does not allow independent oversight of the safety and security arrangements and delegates the strategy of safety and security to the car manufacturer. Other market participants are of the view that a closed system might be more vulnerable as it relies on this exclusion and may not have other safeguards in place; the access to safety critical ECUs via the OBD port suggests that some vehicles may not have adequately secure electrical architecture.

However, this solution has distinct advantages in that car manufacturers are doing this already so the cost to develop this arrangement has already been spent and the system could be operational in a short timeframe. This arrangement also delivers a good level of safety and also means that the car manufacturer is solely liable for the safety and security of the system, therefore providing clear responsibility on this aspect.

5.2.2.1.5 Data economy

The issues for the data economy for this model are similar to that of the shared server (see Section 5.1.4.1.5) and the extended vehicle (see Section 5.1.3.1.5).

In summary, if the data agreed to be provided at the neutral server is in a format that is interoperable between manufacturers, third parties accessing data would only need one contract with the neutral service provider.

Additionally, all data server solutions are subject to increased latency compared with data accessed directly inside the vehicle. This means that data server solutions cannot support real-time applications, but perhaps – with improvements in communication speed – could support applications that were near real-time. However, the latency will always be inferior to accessing the data inside the vehicle. In the future, more and more services may require real-time data, so this technical architecture may not be as futureproof compared with solutions accessing data directly from the vehicle.

5.2.2.2 Timeline and impact of implementation

Based on information collected from stakeholders, many believe that a data server solution could be implemented in the shortest timescale (e.g. 1 to 3 years). This model is considered to have similar timeframes and provides a treatment of safety and security aspects in line with current developments being undertaken by manufacturers. This scenario is therefore less burdensome on manufacturers than the in-vehicle architectures and the costs have already been invested. However, this proposal includes the option for the car manufacturer to close access to the OBD port while driving. This is arguably a valid course of action to improve the safety of the vehicle and prevent unwanted control of safety critical ECUs. **However, it will affect other market participants who have developed business models based on accessing data via the OBD port while the vehicle is in motion. For these, the closure of the OBD port is a very significant issue. These market participants would be able to access the data via the neutral sever, but with increased latency that they argue would not support**

their needs. Therefore, it is possible that their businesses will be catastrophically affected with the action of the car manufacturers to close the OBD port while driving.

At the same time as this technical solution is being established, the car manufacturers will also have access to their own in-vehicle platform to develop applications and this is likely to place them at a competitive advantage compared to other market participants. For applications using vehicle specific data, access to data inside the vehicle will provide an advantage over accessing data at the neutral server and these market participants may be competing for the same services.

5.2.2.3 Scenario outcome (baseline)

Main risks of not intervening in accordance with this scenario
The features of the extended vehicle/neutral server model are an improvement over other data server platform solutions but do not solve all of the risks relating to fair and undistorted competition because manufacturers are still in control of the data; there is still a risk of discrimination of third parties in areas where manufacturers are directly engaged in the same competitive markets (e.g. RMI industry). Proprietary application platforms (open or closed) would likely be developed in parallel to this model. There is a risk of discrimination associated with closed platforms and, even for open platforms, a risk of market fragmentation making the on-board platforms unattractive to developers. For applications requiring real-time data (e.g. in predictive maintenance) and those applications requiring access to vehicle resources (such as HMI or unlocking doors) third parties need to rely on on-board platforms or smartphone mirroring technologies. The fact that the car is only accessible to manufacturers appears per se beneficial for safety but it could mean that the security is provided primarily by limiting access rather than by different layers of technical protections, which would incur security risks.

Table 40 provides an overview of the expected outcome of the baseline scenario (no action at European level) in regard to compliance with the five guiding principles.

Table 40: Compatibility of the extended vehicle/neutral server model with the five guiding principles (colour-coding as per Table 39)

Technical solution	Data provision conditions – consent	Fair and undistorted competition	Data privacy and data protection	Tamper-proof access and liability	Data economy
Data server – Extended vehicle/neutral server model					

5.2.3 Scenario 1 – Scenario 0 with measures at European level to accompany market development and address risks

5.2.3.1 Actions at European level for implementation

Scenario 1 is the previously described baseline scenario with the addition of a range of possible actions that could be implemented to mitigate against the risks identified in the compliance of the baseline situation with the guiding principles. The central technical solution of this scenario is, therefore, again the extended vehicle/neutral server model. No action might be necessary to achieve implementation of this solution, considering the current volition of the industry. However, **it should be noted that without any formalisation of the extended vehicle/neutral server model in voluntary agreements or legislative requirements, it is a possibility that the position of**

the car manufacturers could revert to their original position of the 'extended vehicle' solution.

5.2.3.2 Actions at European level for compliance with the five guiding principles

5.2.3.2.1 Data provision conditions – consent

No initial intervention may be required but **the implementation of the technical solution should be monitored to ensure that all market participants have the ability to gain consent and allows this to be given for a specific user or for each journey and that these can be revoked by the user at any time**. From the information available, there seems to be reasonable access for all market participants in this respect, assuming that third parties can access a suitable mobile platform to link to the vehicle's HMI. If this is not available, then this is a significant barrier and will place the car manufacturers at a competitive advantage.

The Commission could support the emergence of a standardised and customer-friendly approach for providing consent by suggesting legally acceptable standard procedures and making available suitable standard contract clauses. These standard procedures could also include a recommendation to provide an easy to access means to switch-off data transmission for a certain period (e.g. for the current journey).

5.2.3.2.2 Fair and undistorted competition

A range of options are presented in order to mitigate the risks identified with respect to fair and undistorted competition.

Should the Commission wish to ensure that market participants have equitable access to data, **measures to clarify *which data* is made available and the *timescales in which it is made available* may be required.** These could be **established via encouraging voluntary agreements, although it is considered that a mandatory requirement or specification would be more effective**.

- Equal quality of data (update frequency, resolution, latency etc.) available to third party applications and apps provided by OEM or selected partners. No latency or reduction in frequency should be put on data before it is forwarded to third-party apps (so that it is the same data as OEM-provided apps would use).
- A large harmonised minimum dataset, covering at least the data needs of existing and short term use-cases (see Section 3.4.8). This could be standardised in analogy to 'if fitted' requirements, i.e. if certain data which falls in the definition of the minimum dataset is created somewhere in the vehicle, it must be made accessible via the API, but it is not necessary to equip a vehicle with additional sensors to populate the minimum dataset.
- A requirement that a reasonable request for data could not be rejected by any vehicle manufacturer.

Consideration should also be given to the equality of access to the vehicle resources; while this will be predominantly visual HMIs (screens and control elements, or touchscreens), other modes are conceivable in the future, such as gesture control, voice control or voice feedback. If third parties can adapt their current systems to use existing mobile platforms, this could provide access to the HMI, but it is currently unclear to what extent this would be feasible for other market participants and what costs would be necessary to achieve this.

Third party businesses currently using the OBD port to access data could be significantly affected if this is closed while the vehicle is in motion. While there are strong safety

arguments for this approach, **measures at European level could mandate timescales for access to the OBD port for all market participants to allow users that would be affected by its closure to adapt their business models.** It is not clearly stated in the legislation that the OBD port should be left open exclusively for repair and maintenance while the vehicle is stationary; it may also remain open for remote diagnostics support. The specific technical solution, data required and data access timescales for that purpose shall be defined in a new CEN standard under the mandate set out in RMI legislation.

5.2.3.2.3 Data privacy and data protection

This technical solution would be capable of being implemented in a way that is compliant with this guiding principle, and the existing European regulation that effectively requires such compliance would apply to all market participants.

5.2.3.2.4 Tamper-proof access and liability

The safety and security risks of this technical architecture are essentially devolved to the car manufacturer and they take full responsibility for the safety and security of the vehicle and access to the in-vehicle data. **Measures at European level could consider methods to verify that the design of the vehicle E/E architecture delivers an appropriate level of functional safety and cyber security.** Any agreements should be developed in conjunction with the vehicle manufacturers before any mandatory technical requirements are implemented.

In addition, car manufacturers communicated a concern about being liable for safety risks resulting from driver distraction by third party apps running on vehicle HMI. Acceptance guidelines for applications should therefore be agreed which cover the aspect of permissible and non-permissible levels of distraction. **This could be supported by the Commission by providing specific safety performance guidelines for HMI design (as is the case in the US)**. Any agreements should be developed in conjunction with the vehicle manufacturers before any mandatory technical requirements are implemented.

5.2.3.2.5 Data economy

In order to ensure that the data is interoperable and standardised, the data available on the neutral server should be in a standard format from all car manufacturers. **Measures at European level could encourage the standardisation of data by setting guidance in this respect** so that the data from multiple car manufacturers can be used by apps and market fragmentation can be avoided. This is also likely to stimulate the market since it will possible to develop apps for a larger market and it will not be necessary to develop manufacturer-specific applications.

5.2.3.3 Timeline

Under the assumptions as described above, i.e.:

- A data server solution is implemented;
- Measures are taken to encourage the development of one interoperable and standardised platform/API; and
- Third parties will have, as a minimum, access to a minimum dataset,

TRL expects the following timelines as a reasonable minimum:

- Standardisation of a minimum dataset based on use-case clusters could take approximately 1 year.
- In a parallel timeframe, the technical architecture could be developed and implemented. This would utilise the development made by the work at ISO on the extended vehicle and the systems already in place. This is considered to take approximately 1 year.

- Establishing the neutral server provision (hardware and supplier of service overall) and negotiating the contracts necessary with car manufacturers to enable the flow of data to the market is estimated to take approximately 1 year although this might not be possible until after system was in place.

This leads TRL to the conclusion that a minimum timespan of approximately 1-2 years should be expected from an intervention that starts the necessary procedures (i.e. measures to support the implementation of the 'Extended vehicle/neutral server' solution) to the implementation of a neutral server that facilitates access to in-vehicle data.

5.2.3.4 Scenario outcome

Cost-benefit aspects	Scale of potential effects of an intervention according to this scenario	Risks of intervention according to this scenario
The benefits of measures to address competition issues seem likely to outweigh the cost of additional effort in standardisation and harmonisation of data, improving the overall impact.	The potential magnitude of effects of the intervention is ranked lowest among the three analysed scenarios.	Even with the interventions described, not all of the risks relating to fair and undistorted competition can be solved because manufacturers are still in control of the data; there is still a risk of discrimination of third parties in areas where manufacturers are directly engaged in the same competitive markets (e.g. RMI industry). There is a risk of hampering innovation if a minimum dataset is standardised prematurely and this is treated as a de facto standard, rather than a minimum. As in the baseline scenario, proprietary application platforms (open or closed) would likely be developed in parallel to the extended vehicle/neutral server model. There is a risk of discrimination associated with closed platforms and, even for open platforms, a risk of market fragmentation making the on-board platforms unattractive to developers. For applications requiring real-time data (e.g. in predictive maintenance) and those applications requiring access to vehicle resources (such as HMI or unlocking doors) third parties would still need to rely on on-board platforms or smartphone mirroring technologies.

Table 41 provides an overview of the potentially achievable outcome of Scenario 1 in regard to compliance with the five guiding principles, should interventions at European level achieve the desired effect.

Table 41: Potential favourable outcome of Scenario 1 (colour-coding as per Table 39)

Technical solution	Data provision conditions – consent	Fair and undistorted competition	Data privacy and data protection	Tamper-proof access and liability	Data economy
Scenario 1					

5.2.4 Scenario 2 – Short term: Shared server model

5.2.4.1 Actions at European level for implementation

Scenario 2 is a data server concept (see Section 5.1.4) but has the key advantage that the 'data used for applications' is shared, such that all market participants accessing data at the server have access to the same data at the same time, thus supporting a level playing field for this route of data access. The other key advantage of this solution is that it could be implemented in a shorter timeframe compared with in-vehicle solutions.

This scenario includes the addition of a range of possible actions at European level that could be implemented to mitigate against the risks identified in the compliance of the baseline situation with the guiding principles. **Action at European level is considered necessary to achieve the implementation of this solution over the baseline extended vehicle/neutral server model**.

5.2.4.2 Actions at European level for compliance with the five guiding principles

5.2.4.2.1 Data provision conditions – consent

No initial intervention may be required but **the implementation of the technical solution should be monitored to ensure that all market participants have the ability to gain consent and allows this to be given for a specific user or for each journey and that these can be revoked by the user at any time**. From the information available, there seems to be reasonable access for all market participants in this respect, assuming that third parties can access a suitable mobile platform to link to the vehicle's HMI. If this is not available, then this is a significant barrier and will place the car manufacturers at a competitive advantage.

The Commission could support the emergence of a standardised and customer-friendly approach for providing consent by suggesting legally acceptable standard procedures and making available suitable standard contract clauses. These standard procedures could also include a recommendation to provide an easy to access means to switch-off data transmission for a certain period (e.g. for the current journey).

5.2.4.2.2 Fair and undistorted competition

A range of options are presented in order to mitigate the risks identified with respect to fair and undistorted competition.

Should the Commission wish to ensure that market participants have equitable access to data, **measures to clarify *which data* is made available and the *timescales in which it is made available* may be required.** These could be established via encouraging voluntary agreements, although **it is considered that a mandatory requirement or specification would be more effective**.

- A large harmonised minimum dataset, covering at least the data needs of existing and short term use-cases (see Section 3.4.8). This could be standardised in analogy to 'if fitted' requirements, i.e. if certain data which falls in the definition of the minimum dataset is created somewhere in the vehicle, it must be made accessible, but it is not necessary to equip a vehicle with additional sensors to populate the minimum dataset.
- A requirement that a reasonable request for data could not be rejected by the car manufacturer.

Consideration should also be given to the equality of access to the vehicle resources; while this will be predominantly visual HMIs (screens and control elements, or touchscreens), other modes are conceivable in the future, such as gesture control, voice control or voice feedback. If third parties can adapt their current systems to use existing mobile platforms, this could provide access to the HMI, but it is currently unclear to what extent this would be feasible for other market participants and what costs would be necessary to achieve this.

The shared server could be maintained by a consortium or by a single service provider and costs would be involved in establishing such a group or organising a contract. **Measures at European level could encourage the formation of a consortium of all stakeholders to put in place the necessary architecture to deliver the shared server.**

There is a risk of hampering innovation if a minimum dataset is standardised prematurely and this is treated as a de facto standard, rather than a minimum. **Measures at European level could ensure that there is the facility to add elements to any minimum dataset.**

Third party businesses currently using the OBD port to access data could be significantly affected if this is closed while the vehicle is in motion. While there are strong safety arguments for this approach, **measures at European level could mandate timescales for access to the OBD port for all market participants to allow users that would be affected by its closure to adapt their business models.**

5.2.4.2.3 Data privacy and data protection

This technical solution would be capable of being implemented in a way that is compliant with this guiding principle, and the existing European regulation that effectively requires such compliance would apply to all market participants.

5.2.4.2.4 Tamper-proof access and liability

The safety and security risks of this technical architecture are essentially devolved to the car manufacturer and they take responsibility for the safety and security of the vehicle and access to the in-vehicle data. **Measures at European level could consider methods to verify that the design of the vehicle E/E architecture delivers an appropriate level of functional safety and cyber security.**

In addition, car manufacturers communicated a concern about being liable for safety risks resulting from driver distraction by third party apps running on vehicle HMI. Acceptance guidelines for applications should therefore be agreed which cover the aspect of permissible and non-permissible levels of distraction. **This could be supported by the Commission by providing specific safety performance guidelines for HMI design (as is the case in the US)**.

5.2.4.2.5 Data economy

In order to ensure that the data is interoperable and standardised, the data available on the shared server should be in a standard format from all car manufacturers. **Measures at European level could encourage the standardisation of data by setting guidance in this respect** so that the data from multiple car manufacturers can be used by apps and market fragmentation can be avoided. This is also likely to stimulate the market since it will possible to develop apps for a larger market and it will not be necessary to develop manufacturer-specific applications.

5.2.4.3 Timeline

Under the assumptions as described above, i.e.:

- A shared server solution is implemented;

- Measures are taken to encourage the development of one interoperable and standardised platform/API; and
- Third parties will have, as a minimum, access to a minimum dataset,

TRL expects the following timelines as a reasonable minimum:

- Standardisation of a minimum dataset based on use-case clusters could take approximately 1 year.
- In a parallel timeframe, the technical architecture could be developed and implemented along with the establishment of a consortium and service provider to run the shared server model.
- Establishing the shared server provision (hardware and supplier of service overall) and negotiating the contracts necessary with car manufacturers to enable the flow of data to the market is estimated to take approximately 1 year although this might not be possible until after system and/or shared server service provider was operational.

This leads TRL to the conclusion that a minimum timespan of approximately 2 years should be expected from an intervention that starts the necessary procedures to the implementation of a shared server that facilitates access to in-vehicle data.

5.2.4.4 Scenario outcome

Cost-benefit aspects	Scale of potential effects of an intervention according to this scenario	Risks of intervention according to this scenario
The benefits of measures to address competition issues seem likely to outweigh the cost of additional effort in standardisation and harmonisation of data, improving the overall impact.	The potential magnitude of effects of the intervention is ranked lowest among the three analysed scenarios.	Even with the interventions described, not all of the risks relating to fair and undistorted competition can be solved because manufacturers still have superior access to the vehicle HMI; there is still a risk of discrimination of third parties in areas where manufacturers are directly engaged in the same competitive markets (e.g. RMI industry). There is a risk of hampering innovation if a minimum dataset is standardised prematurely and this is treated as a de facto standard, rather than a minimum. As in the baseline scenario, proprietary application platforms (open or closed) would likely be developed in parallel to the shared server model. There is a risk of discrimination associated with closed platforms and, even for open platforms, a risk of market fragmentation making the shared server unattractive to developers. For applications requiring real-time data (e.g. in predictive maintenance) and those applications requiring access to vehicle resources (such as HMI or unlocking doors) third parties would still need to rely on on-board platforms or smartphone mirroring technologies; a barrier not in place for car manufacturers and under their control.

Table 42 provides an overview of the potentially achievable outcome of Scenario 2 in regard to compliance with the five guiding principles, should interventions at European level achieve the desired effect.

Table 42: Potential favourable outcome of Scenario 2 (colour-coding as per Table 39)

Technical solution	Data provision conditions – consent	Fair and undistorted competition	Data privacy and data protection	Tamper-proof access and liability	Data economy
Scenario 2					

5.2.5 Scenario 3 – Long term: On-board application platform

5.2.5.1 Actions at European level for implementation

Scenario 3 describes a scenario with a longer term view where connected cars would provide an open, interoperable on-board application platform that allows third-party applications running on the vehicle HMI to access certain in-vehicle data and resources via an API. Given the current inclination of vehicle manufacturers and suppliers towards data server solutions and the fact that manufacturers have stated that they will not, of their own accord, develop an open and interoperable on-board application platform, it appears reasonable to assume that this scenario would only materialise if measures of market intervention are taken. Potential alternative levels for this intervention could be:

1) Make the provision of an open on-board application platform mandatory for every connected car. This intervention could be seen as overly intrusive because it could entail large sums of development costs for OEMs who are in early stages of adapting their E/E architecture to connectivity and it would limit the design choices of OEMs who might not wish to offer aftermarket services to their customers.
2) **Mandate that an on-board application platform should it be implemented in a new vehicle model, be used by the OEM to offer aftermarket services based on in-vehicle data to customers, and has to be open for applications of third-party service providers on a non-discriminatory basis.** This 'if fitted' requirement would aim to prevent the development of closed application platforms, the use of which is limited to the OEM itself and their selected partners.

It should be noted that any on-board application platform would need to compete or co-exist with existing mobile platforms and mirroring technologies, such as Apple CarPlay or Android Auto, and data server solutions being implemented by OEMs (Extended Vehicle, Neutral Server Concept).

5.2.5.2 Actions at European level for compliance with the five guiding principles

5.2.5.2.1 Data provision conditions – consent

As described in Section 5.1.1.1.1, an on-board application platform can be designed in a way that customers provide consent via the vehicle HMI. This can be done either at the beginning of each journey, once when installing an application or signing up to a service, or only once per vehicle owner before activating connectivity initially (consent to certain use-cases). **The Commission could support the emergence of a standardised and customer-friendly approach for providing consent by suggesting legally acceptable standard procedures and making available suitable standard contract clauses.** These standard procedures could also include a recommendation to provide an easy to access means to switch-off data transmission for a certain period (e.g. for the current journey).

5.2.5.2.2 Fair and undistorted competition

As described in Section 5.1.1.1.2, an on-board application platform is a system that can be implemented in a way that allows all market participants to access the same dataset at the same time with equitable access to the customer via the vehicle's HMI; itis therefore well-placed to facilitate fair and undistorted competition. Assuming an intervention according to 2) above, i.e. an intervention that requires that an on-board application platform must be open for third-party applications if the OEM uses it to sell aftermarket services to customers, **rules on the following aspects should be considered to ensure fair and undistorted competition**:

- Equivalent channels of access to the customer: Should third parties be given the right to access the customer through the same channels as the OEM does for aftermarket services? Currently, this will be predominantly visual HMIs (screens and control elements, or touchscreens), but other modes are conceivable, such as gesture control, voice control or voice feedback.
- To be open to third parties an application platform would require a documented API and an SDK for software developers.
- Non-discriminatory compliance guidelines that clearly define the process, timelines and acceptance criteria (safety, security, technical performance, content, design, commercial and legal aspects) applied for the pre-deployment application check and approval by the OEM. This could be supported by defining a fair process for arbitration in case of disputes.
- Sufficiently large harmonised minimum dataset, to cover at least the data needs of existing and short term use-cases initially (see Section 3.4.8). This could be standardised in analogy to 'if fitted' requirements, i.e. if certain data which falls in the definition of the minimum dataset is created somewhere in the vehicle, it has to be made accessible via the API, but it is not necessary to equip a vehicle with additional sensors to populate the minimum dataset.
- Equal quality of data (update frequency, resolution, latency) available to third party applications and apps provided by OEM or selected partners. No latency or reduction in frequency should be put on data before it is forwarded to third-party apps (so that it is the same data as OEM-provided apps would use).

5.2.5.2.3 Data privacy and data protection

This technical solution would be capable of being implemented in a way that is compliant with this guiding principle, and the existing European regulation that effectively requires such compliance would apply to all market participants.

5.2.5.2.4 Tamper-proof access and liability

The effort (cost and time) required to secure an on-board application platform will vary depending on the functionality that is required, in particular the level of 'write access'. In TRL's view it is *not* necessary for fair competition to provide third parties with entirely uncontrolled and unfiltered write access to the vehicle's bus systems. However, in order to achieve fair and undistorted competition it appears reasonable that third parties are able to:

- gain certain write permissions to the infotainment system and comfort functions that allow interaction with the customer via an in-vehicle HMI; and
- trigger legitimate access to selected actuators for non-safety critical events, e.g. unlocking the doors under certain preconditions.

The cyber-security risks associated with this functionality appear manageable, considering that some OEMs have already implemented such functionality for selected aftermarket partners in production vehicles and that applications could be reviewed by OEMs before being allowed onto the vehicle. **The OEMs' concerns around liability might be alleviated by supporting the development of commonly accepted automotive cyber-security standards (in analogy to the functional safety standards).**

In addition, OEMs mention a risk of being liable for safety risks resulting from driver distraction by third party apps running on the OEM platform. Acceptance guidelines for applications should therefore be agreed which cover the aspect of permissible and non-permissible distraction. **This could be supported by the Commission by providing**

specific safety performance guidelines in regard to HMI design (as the US also provide).

5.2.5.2.5 Data economy

Soft measures could be used to facilitate the development of a single platform rather than fragmentation of the market, which might prevent the development of a sufficient number of apps being developed to really create a data economy.

In order to successfully deliver benefits to customers and the economy it is not sufficient that an open platform is merely available in the car. It also has to be commercially sensible for third parties to develop applications for this platform and attractive for the customer to use them. Currently, OEMs develop and implement on-board application platforms which are not interoperable and use different APIs. Even if these platforms are open for third party app developers (such as with the General Motors NGI SDK), it can be argued that this fragmentation would result in relatively small customer target groups which reduces the commercial attractiveness for service providers and might hence lead to a reduced choice of services. The eCall Regulation also stipulates a platform that is '*interoperable'* and '*standardised'*. **Appropriate measures should be considered to encourage the development of a single, interoperable platform and avoid fragmentation.** These should aim to foster the development of appropriate technical standards (API and standardisation of minimum dataset) without leading to a standardised, commoditised vehicle architecture that would prevent innovation. Measures might include facilitating, administering and chairing a suitable platform of technical experts and setting maximum timeframes to achieve standardisation.

Any new on-board application platform will also have to compete, for developers and for users, with other technical solutions for access to in-vehicle data (Extended Vehicle, Natural Server Concept) and mobile app platforms (iOS, Android). Even if an interoperable on-board application platform is created that provides an attractive offering to developers and users, there is potential for other vehicle solutions to enter the market quicker and create a very strong market presence. Considering that OEMs have stated that they will not, of their own accord, develop an interoperable on-board application platform, there is a possibility of a data server solution combined with smartphone mirroring (Apple CarPlay, Android Auto) becoming the de facto standard in the meantime. Therefore, any action taken should aim at achieving quick implementation of standards in order to allow deployment soon. **It might be warranted, to an extent, to prioritise quick implementation over a large scope of initial mandatory functionality; i.e. defining a pragmatic minimum dataset based on the most important use-case clusters and limited access to in-vehicle resources initially and considering to expand these requirements later.** With regard to in-vehicle resources, the ability to interact with the customer via the vehicle HMI appears to be the most essential for fair competition. Focussing on this aspect initially could reduce the technical challenges for safe implementation and liability concerns voiced by OEMs.

OEMs are currently working on proprietary in-vehicle platforms and it is reasonable to assume that they do have an interest to offer in-vehicle apps to their customers and not rely on mobile platforms, because:

- The scope of the functionality that can be offered is larger (deeper integration and access to real-time data), and
- OEMs would not be dependent upon mobile platform providers and be subjected to their commercial decisions.

An 'if fitted' requirement, as mentioned above, might encourage OEMs to redirect these R&D efforts to developing an interoperable solution instead. However, any 'if fitted' requirement can have the perverse consequence of discouraging the fitment of a technology. If the changes to the vehicle architecture required for a standardised platform are too extreme**, there is a risk that an intervention does not achieve its**

aims because OEMs decide to not offer any in-vehicle platform and rely on other solutions as described above. It is not possible to predict the likelihood of such a commercial decision being taken.

5.2.5.3 Timeline

Under the assumptions as described above, i.e.:

- An on-board application platform, if fitted, is mandated to be open for third-parties;
- Measures are taken to prevent fragmentation and encourage the development of one interoperable and standardised platform/API; and
- Third parties will have, as a minimum, access to a minimum dataset and the ability to interact with customers via the vehicle HMI,

TRL expects the following timelines as a reasonable minimum:

- Standardisation of a minimum dataset based on use-case clusters could take approximately 1 year.
- In parallel, the platform architecture, API, and security requirements could be agreed and standardised. Considering the timescales of the extended vehicle ISO standards, this process could be expected to last approximately 3 years.
- The timespan for technical implementation in vehicles appears to depend largely on the state of readiness of an OEM's electrical/electronic architecture and where in the development lifecycle each manufacturer is with respect to the architecture used in current and forthcoming models. Relevant aspects include:
    - Method to apply an open-modular approach to the underlying software written for the infotainment systems.
    - Faster adoption of the Open Web Platform specifications for HTML5/JavaScript application developers enabling web connectivity through in-vehicle infotainment systems and vehicle data access protocols as described by the W3C consortium.
    - Faster development of vehicle information API and vehicle data API.
    - Introducing Hypervisors.

  In the most favourable cases, development, implementation and validation might be completed in approximately 2 years. This timespan could be much longer if a large upgrade to the electrical/electronic architecture is required.

This leads TRL to the conclusion that a minimum timespan of approximately 5 years should be expected from an intervention that starts the necessary procedures to the implementation of an open, interoperable and standardised on-board application platform in the first customer vehicles.

5.2.5.4 Scenario outcome

Cost-benefit aspects	Scale of potential effects of an intervention according to this scenario	Risks of intervention according to this scenario
Additional costs are anticipated for OEMs. However if intervention could achieve a single interoperable platform, the benefits for service providers and consumers would be considerable in the long term	The potential magnitude of effects is ranked highest among the three analysed scenarios. This scenario has the potential to result in high costs for vehicle manufacturers, lead to significant changes in the E/E architecture of vehicles and introduce certain safety risks.	Risks of high costs for OEMs, vehicle architecture changes that hamper innovation and safety issues. Despite an intervention, the interoperable open on-board application platform might not be successfully taken up by the market (e.g. because other solutions are available quicker and dominate the market).

Table 43 provides an overview of the potentially achievable outcome of Scenario 3 in regard to compliance with the five guiding principles, should interventions at European level achieve the desired effect.

Table 43: Potential favourable outcome of Scenario 3 (colour-coding as per Table 39)

Technical solution	Data provision conditions – consent	Fair and undistorted competition	Data privacy and data protection	Tamper-proof access and liability	Data economy
Scenario 3					

6 Conclusions

Vehicles are generating and recording increasing amounts of data as technological development continues. These data enable intelligent decisions to be made by vehicle systems, but also generate information that can be used to offer enhanced or new services to consumers. There has been a need for the way in which in-vehicle data are made available to be defined and integrated for some time and this was included in the eCall type-approval Regulation (Regulation (EU) 2015/758) which included provisions and empowerments regarding an interoperable, standardised, secure and open-access platform.

This report assesses the legal, technical, and cost-benefit implications of the most likely scenarios for access to in-vehicle data and the associated resources in the near future (next two to five years), with the objective to address the risks related to the baseline scenario and to ensure the materialisation of an interoperable, standardised, secure, and open-access platform.

Concerning any possible policy measure, in a currently highly evolving market, the study recommends firstly monitoring how the eventual technical solutions selected by the market comply with the five guiding principles agreed by WG6. If any action by the Commission is deemed necessary for a specific technical solution, such action should be subject to an exhaustive impact assessment. The assessment must include a thorough cost-benefit analysis of several policy options; one of them covering the inclusion of specific technical requirements and administrative provisions in relevant EU legislation(s).

The main conclusions of this study are as follows:

Legal

- Each of the WG6 solutions could in principle work within the existing legal framework. However, each option is likely to give rise to a range of legal obstacles that will need to be navigated by market participants and there is a risk that the current legal framework may allow the market to develop in a way that is inconsistent with the five guiding principles agreed by WG6 and with the relevant European legislation in general (e.g. competition legislation).

- From a strictly legal perspective, there are no significant differences between providing access to data based on use-cases or providing access to data depending on the terms and conditions in the applications. However, the legal analysis is more supportive of access to data on the basis of use-cases, because the purpose of the data is well defined, meaning that it may be easier for data subjects to give consent that is more specific as to the purposes for which the data can be used.

- The primary legal challenge of the negotiation model is its interaction with competition law. Existing law should in theory be sufficient to ensure fair and undistorted competition. However, although legal protection against anti-competitive behaviour exists, the practical application of this law is very complex. The model of access to in-vehicle data should ideally mitigate the concentration of power with one group of market participants to prevent the situation where, before competition law can be effectively applied, the market has already been distorted to the detriment of consumers.

Technical

- This study found that all solutions proposed by WG6 are technically feasible, but no one solution satisfied all guiding principles agreed by WG6.

  - The data server platform derivatives cannot support real-time data, whereas in-vehicle interface and on-board application platform have access to real-time data. This could be an increasing issue in the future as more applications demand real-time data.
  - Data server platforms result in access to the Human Machine Interface (HMI) in the vehicle being more limited, although a level of access is possible if accesses to the HMI via mobile platforms are relied upon. However, the on-board application platform provides equal access to the vehicle HMI and is most compliant with the guiding principle on fair and undistorted competition.
  - The investment required for safety and security, while being a pre-requisite for all technical solutions, is greater for the on-board application platform and in-vehicle interface than it is for the data server solutions. Key areas for safety and security are development of a security layer and the implementation of a hypervisor[35].
  - Largely due to the effort required to improve security, data server solutions are estimated to be able to be implemented sooner (1-2 years) than the in-vehicle solutions (approximately 5 years)
  - All technical solutions currently exist in the market with advantages to specific stakeholder groups; therefore although the technical solutions were assessed individually, the later scenario analysis also considered the effects of the existence and development of different systems in parallel.

- The main challenge is in balancing the demands of safety and security with fair and undistorted competition, whilst ensuring that any interventions are proportionate and do not inflict unreasonable burdens on market participants.
  - Key areas for safeguarding fair competition are ensuring equal access to resources (HMI) and data (both in terms of types of data available and timeliness) and avoiding the ability of any one participant to delay, dilute or deny access to data.
  - Safety and security is required for all solutions and was cited by some stakeholders as a reason to favour a data server technical solution. This is because the development of a suitably secure in-vehicle interface could have potentially large impacts on the automotive industry.

- Irrespective of the specific in-vehicle data access model implemented, several 'horizontal issues' can be identified:
  - Standardisation of data so that data from all manufacturers can be used by the wider market to encourage innovation.
  - Whether data is accessed by the market on the basis of a list of application-dependent data (i.e. the application provider has access to all available in-vehicle data and the user consents to access particular data elements depending on the application) or on the basis of use-cases (i.e. specific pre-defined data is available for applications with a particular purpose), both these approaches could be served by a minimum data set (i.e. a list of data parameters that allow the majority of services to be developed).

[35] A hypervisor manages the separate execution of software tasks; in this context allowing the management of messages to vehicle ECUs and the prevention of unauthorised access to safety-critical ECUs or to functions that are not authorised for the application.

- TRL note examples of the minimum dataset concept being successfully established in regulation elsewhere (e.g. CPR 49 Part 563 in the US[36]) and this approach would be favoured by certain stakeholder groups. However, even with such an approach, a mechanism to establish access on the basis of new use-cases or the addition of data elements to the agreed dataset would also be required in parallel so that innovation is not stifled by being limited to a specific dataset.
- Ensuring actions on standardisation, the timely agreement of data and/or a minimum dataset is considered to require measures at European level to bring these about.

Impact Assessment

- Overall socio-economic benefits of each of the technical architectures are dependent on the specific application(s) implemented that use the data and the effectiveness of these at bringing about improvements in safety and/or environmental performance. Access to in-vehicle data could support a large number of existing and new services; for example remote diagnostics and prognostics, pay as you drive insurance, incentives to the driver to access particular automotive services based on location etc. These services have massive potential benefits, many times greater than costs required to implement access to data in the market. From this perspective, the action to implement access to in-vehicle data is proportionate because the estimated benefits far outweigh the costs of implementing any model of accessing the data.

- An assessment of the costs of the various components of systems for access to in-vehicle data were compiled from the literature review, known sources of data on the costs of ITS components and from stakeholders consulted during this project. A qualitative comparison of the costs involved in developing, setting up, operating and maintaining the various elements of the technical solutions resulted in similar, relatively low cost levels for each of the data server solutions. Higher cost levels were estimated for both the on-board application platform and the in-vehicle interface, largely because of the cost of technical development and the cost of equipping and maintaining 12 million new vehicles each year across Europe.

- Remote access to in-vehicle data and resources obtained using any of the architecture solutions provides some benefits that are applicable to all stakeholders. These include the ability to provide new and more efficient services, which benefit all of the stakeholders involved, as well as society in general. Examples are safety and environmental benefits of driver training tailored to the individual and customer relationship management. Set against these overall benefits, some stakeholders warned that there are potential risks to security and safety involved in any method of obtaining in-vehicle data and that the system established to access in-vehicle data could have large effects in terms of market fairness and equality.

- The stakeholder preferences, which were indicated by their responses to the consultation, showed that for several stakeholder groups there is a preference for the On-Board Application Platform. Whereas vehicle manufacturers would prefer a data server solution combining the 'extended vehicle' concept with a neutral

[36] US minimum specification for data recorded by Event Data Recorders (EDRs)

server, and road authorities (according to their stakeholder responses) would prefer any of the other data server solutions.

- Directive 2010/40/EU[37] (the ITS Directive) sets out the principles for specifications and deployment of ITS in its Annex II. The extent to which the individual technical solutions comply with these principles is an indication of the extent of their compliance with the principles of the ITS Directive. These and a number of other important factors were rated based on the information available to provide the overall impacts. In these qualitative assessments, the rating scale ranged from --- (most negative) to +++ (most positive).

Impacts	On-Board Application Platform	In-vehicle Interface	Data Server - Extended Vehicle	Data Server - Shared Server	Data Server - B2B Marketplace	Extended Vehicle/ Neutral Server
Component costs	---	---	+++	+++	+++	+++
Consumer choice	+++	+	---	++	++	++
Competitiveness	+++	---	---	++	++	++
SMEs	--	--	--	++	+	++
Public authorities	---	---	0	-	0	-
Innovation and research	+++	+++	+	+	+	+

[37] Directive 2010/40/EU of the European Parliament and the Council on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport. Official Journal of the European Union, L207 6 August 2010.

Compliance with the principles of the ITS Directive	On-Board Application Platform	In-vehicle Interface	Data Server - Extended Vehicle	Data Server - Shared Server	Data Server - B2B Marketplace	Extended vehicle/ Neutral Server (ACEA proposal)
Effective	+++	+++	+	+	+	+
Cost-efficient	---	--	+++	+++	+++	+++
Proportionate	+	+	+++	+++	+++	+++
Support continuity of services	+	+	+	+++	++	+++
Deliver interoperability	+++	+++	+++	+++	+++	+++
Support backward compatibility	0	+	++	++	++	++
Respect existing national infrastructure and network characteristics	0	0	0	+	0	+
Promote equality of access for VRUs	0	0	0	0	0	0
Support maturity	+	+	++	+++	+++	++
Deliver quality of timing and positioning	++	++	0	0	0	0
Facilitate inter-modality	++	++	0	0	0	0
Respect coherence	0	0	+++	0	0	+++

The technical solutions proposed by Working Group 6 were assessed against the guiding principles in order to identify the degree of compliance and to highlight areas that might warrant measures to mitigate any risks identified.

Technical solution	Data provision conditions – consent	Fair and undistorted competition	Data privacy and data protection	Tamper-proof access and liability	Data economy
On-board Application Platform					
In-vehicle Interface					
Data Server – Extended Vehicle					
Data Server – Shared Server					
Data Server – B2B Marketplace					

Assessment of compliance with WG6 guiding principles	**Rating**
Compatible with guiding principles	
Minor issues with compatibility or issues that could be addressed with low cost/impact	
Issues with compatibility or issues that could be addressed with medium cost/impact	
Significant issues with compatibility or could be addressed with high cost/impact	
Incompatible with guiding principles in current form	

Scenario-based Analysis

Four scenarios were assessed based on assumptions about the current market and possible measures to implement short and long term architectures to provide an interoperable, standardised, secure and open-access platform for access in-vehicle data and resource. These scenarios and their rationale are as follows:

Scenario	Rationale
Scenario 0 – No action (Extended vehicle/neutral server; the baseline scenario)	If there is no market intervention, the 'Extended Vehicle/Neutral Server' is expected to become established (alongside proprietary on-board application platforms) as the predominant technical solution.
Scenario 1 – Scenario 0 with measures at European level to accompany market development and address risks	Supporting measures to ensure that the neutral server aspect of the technical solution is implemented and a range of further measures designed to mitigate the risks of market distortion.
Scenario 2 – Short term: Shared server	The Shared Server solution could be encouraged in preference to the extended vehicle/neutral server concept. This maintains the short-term security of the vehicle and does not place large additional burdens on the automotive industry while on the other hand providing, with the addition of interventions at European level, features more aligned to delivering fair competition than the Extended vehicle/neutral server.
Scenario 3 – Long term: On-board application platform	For this solution to be implemented and to result in an interoperable system, it is strongly recommended that legislation will be necessary. In the longer term (up to 5 years before it is accessible to the market), the On-board Application Platform could be encouraged because this provides all market participants with access to real time data and vehicle HMI and therefore the solution with features most aligned to delivering fair and undistorted competition. We acknowledge the safety and security challenges of this solution (the burden of which lies with the vehicle manufacturers), but measures could focus on limiting access to non-safety critical data and using an "if fitted" approach. This could also be implemented in phases to provide adequate time for manufacturers to integrate the required technical development into their existing E/E versions/model cycles.

For each of the four scenarios considered, options for interventions at European level were described that could improve compliance with the five guiding principles and mitigate the risks identified. These measures can be summarised as follows:

Scenario	Measure	Rationale
1, 2 and 3	Monitoring of how consent is obtained and managed	To ensure that all market participants have the ability to gain consent and this can be given for a specific user, or for each journey, and that consent can be revoked by the user at any time
1, 2 and 3	Supporting the emergence of a standardised and customer-friendly approach for providing consent	To suggest legally acceptable standard procedures and making available suitable standard contract clauses
1, 2 and 3	Clarification of which data is made available to the market and the timescales in which it is made available in terms of: 1. Equal quality of data (update frequency, resolution, latency etc.) available to all market participants ; 2. A harmonised minimum dataset, covering at least the data needs of existing and short term use-cases could be standardised; and 3. A requirement that a reasonable request for data could not be rejected by any vehicle manufacturer. A system similar to the SERMI scheme could be used to ensure that requests originate from appropriate third parties.	To ensure that as far as is allowed by the characteristics of the specific technical solution that the relevant data is available at the same quality and timeliness to all market participants
1, 2 and 3	Mandating timescales for access to the OBD port while the vehicle is in motion for regulated parameters and remote diagnostics for all market participants	To allow market participants that would be affected by the closure of the OBD port while the vehicle is in motion or restriction on the data parameters available sufficient time to adapt their business models
1, 2 and 3	Measures to verify that the design of the vehicle electric/electronic (E/E) architecture delivers an appropriate level of functional safety and cyber security	To ensure that the security of the E/E system has been appropriately designed with functional safety and cybersecurity risks in mind
1, 2 and 3	Provision of specific safety performance guidelines for HMI design	To address risks resulting from driver distraction
1, 2 and 3	Measures to encourage the standardisation of data	To ensure that the data is interoperable
1	Formalisation of the 'Extended Vehicle/Neutral Server' solution in voluntary agreements or legislative requirements	To guard against a 'roll back' to the Extended Vehicle solution which does not include the neutral server that makes the party accessing data anonymous to the vehicle manufacturer
2	Legislation to achieve the implementation of the Shared Server solution	It is considered that legislation is required to fully implement this technical solution in the market over and above the baseline extended vehicle/neutral server model.
2	Encourage the formation of a consortium of relevant stakeholders	To put in place the necessary architecture to deliver the shared server

3	Legislation to achieve the implementation of the On-board Application Platform	This could be achieved by making the provision of an open on-board application platform mandatory for every connected car or mandated if an on-board application platform is implemented in a new vehicle model and used by the OEM to offer aftermarket services.
3	Ensure equal access to the vehicle HMI	To support fair competition and reduce the risk of the market being distorted, the access to the vehicle HMI should be ensured for all market participants
3	Support the provision of a documented API and an SDK for software developers	To ensure that the programming interface is clearly defined and that a software development kit is available to facilitate the offline development of applications in the same environment as that when installed on the on-board platform
3	Non-discriminatory compliance guidelines that clearly define the process, timelines and acceptance criteria (safety, security, technical performance, content, design, commercial and legal aspects) applied for the pre-deployment application check and approval by the OEM. This could be supported by defining a fair process for arbitration in case of disputes	To ensure that the certification process for applications is defined in a transparent way and that there is a mechanism to deal appropriately with disputes
3	Supporting the development and implementation of automotive cyber-security standards	Development of effective and standard approach to cybersecurity to mitigate against this risk and ensure that a common design requirement is met
3	Encourage the development of a single, interoperable platform	To standardise the platform such that developers could deploy applications across brands thereby avoiding fragmentation of the market and maximising exploitation potential

All technical solutions currently exist in parallel. Therefore, any implementation scenario should:

- take account of the characteristics of the market and the timescales within which the desired objectives should be achieved;
- consider actions across all technical solutions such that if measures are implemented for one solution, measures should also be applied to other technical solutions where this is appropriate; and
- be compared against other policy options through a detailed impact assessment, including a cost-benefit analysis.

The potentially achievable outcome of each scenario in regard to compliance with the five guiding principles, should interventions at European level achieve the desired effect are predicted to be as follows:

Technical solution	Data provision conditions – consent	Fair and undistorted competition	Data privacy and data protection	Tamper-proof access and liability	Data economy
Scenario 0					
Scenario 1					
Scenario 2					
Scenario 3					

Assessment of compliance with WG6 guiding principles	Rating
Compatible with guiding principles	
Minor issues with compatibility or issues that could be addressed with low cost/impact	
Issues with compatibility or issues that could be addressed with medium cost/impact	
Significant issues with compatibility or could be addressed with high cost/impact	
Incompatible with guiding principles in current form	

7 References

ACEA & CLEPA. (2016). Automotive industry joins forces on access to vehicle data. Retrieved February 09, 2017, from http://www.acea.be/press-releases/article/automotive-industry-joins-forces-on-access-to-vehicle-data

ACEA. (2016a). ACEA Strategy Paper on: Connectivity. Brussels. Retrieved November 17, 2016, from https://www.acea.be/uploads/publications/ACEA_Strategy_Paper_on_Connectivity.pdf

ACEA. (2016b). ACEA Position Paper: Access to vehicle data for third-party services. Brussels. Retrieved February 7, 2017, from https://www.acea.be/uploads/publications/ACEA_Position_Paper_Access_to_vehicle_data_for_third-party_services.pdf

AEA. (2012). *EU transport GHG: Routes to 2050 II.* EC.

AECC. (n.d.). *Introduction to the technology for emissions control, Catalytic converters*. Retrieved from Association for emisssions control by catalyst: http://www.aecc.be/en/Technology/Introduction.html

AFCAR. (2016). Fair and Equal Access to Vehicles: Implementing the eCall mandate on the 'interoperable telematics platform' in line with the principles for fair competition and free consumer choice. Brussels. Retrieved November 17, 2016, from http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwiy95SP9_3RAhXpB8AKHbHWBGYQFggaMAA&url=http%3A%2F%2Fwww.iaaf.co.uk%2F_literature_137987%2FFigiefa_Manifesto&usg=AFQjCNGWezAUV0NPRTdQTrT3e_EDdW_BKw

Apple Inc. (2017). *Apple Developer* . (Apple Inc) Retrieved 03 15, 2017, from https://developer.apple.com/videos/play/wwdc2016/722/

BASF. (2012, 09 01). *SCR on Filter*. Retrieved from http://www.catalysts.basf.com/: http://www.catalysts.basf.com/p02/USWeb-Internet/catalysts/en/content/microsites/catalysts/prods-inds/mobile-emissions/scr-filter

BASF. (2014). *Catalyzed Soot Filter (CSF)*. Retrieved from BASF: http://www.catalysts.basf.com/p02/USWeb-Internet/catalysts/en/content/microsites/catalysts/prods-inds/mobile-emissions/csf

CLEPA. (2015). Open Telematics paper. Brussels. Retrieved November 17, 2016, from http://clepa.eu/wp-content/uploads/2015/08/20150722_CLEPA_PP_Open_Telematics_Platform.pdf

Continental. (2017). *Continetnal press release*. (Continental) Retrieved 03 16, 2017, from http://www.continental-corporation.com/www/pressportal_com_en/themes/press_releases/3_automotive_group/interior/press_releases/pr_2016_11_28_psa_connect_en.html

de Bruyn, W. (2014). *Review of the Impact Assessment for a 2030 climate and energy policy framework.* Delft.

DfT. (2016). *TAG data book.*

DieselNet. (2005, 06). *Catalyzed Diesel Filters*. Retrieved from DieselNet: https://www.dieselnet.com/tech/dpf_cat.php

Directive. (2010). *Official Journal of the European Union*, 13.

Directorate-General for Energy. (2014). *Subsidies and costs of EU energy.* EC.

E3M-Lab. (2003). *EU-15 energy and transport outlook to 2030 - PART II.* Directorate-General for Energy and Transport, National Technical University of Athens . Luxembourg: EU.

E3M-Lab. (2016). *EU Reference Scenario - 2016 - Energy, transport and GHG emissions, Trends to 2050.* Institute of Communication and Computer Systems at the National Technical University of Athens, Directorate-General for Energy, the Directorate-General for Climate Action and the Directorate-General for Mobility and Transport . EC.

E4tech. (2013). *A harmonised Auto-Fuel biofuel roadmap for the EU to 2030.* London: E4tech.

EC Energy policy. (2017). *EC Energy policy 6/3/2017.*

EC. (2016). *European strategy on C-ITS.* Brussels: European Commission.

EC RMI. (2016). *Access to Vehicle Repair and Maintenence Information .* European Commission. Brussels: EC.

EC, Directorate-General for Mobility and Transport. (2016). *Transport in figures - Chapter 2.7 Saftey.* EU.

ETSC. (2016). *RANKING EU PROGRESS ON ROAD SAFETY - 10th Road Safety Performance Index Report.* Brussels: ETSC.

European Commission. (2014). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'Towards a thriving data-driven economy'.*

European Commission. (2015). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'A Digital Single Market Strategy for Europe'.*

European Commission. (2017a). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Building a European data economy".*

European Commission. (2017b). *Commission Staff Working Document on the free flow of data and emerging issues of the European data economy - Accompanying the document Communication Building a European data economy .*

Eurostat. (2017, 03 16). *Summary of annual road freight transport by type of operation and type of transport (1 000 t, Mio Tkm, Mio Veh-km)* . Retrieved 03 17, 2017, from ec.europa.eu: http://ec.europa.eu/eurostat/web/transport/data/database

FIA. (2016). Policy position on car connectivity. Brussels. Retrieved November 17, 2016, from http://www.fiaregion1.com/download/20160412fia_policy_brief_on_car_connectivity_fin.pdf

FIGIEFA. (2016). *Commission Communication on "Free Flow of Data" - Input from the Independent Automotive Aftermarket .*

FIGIEFA. (2017). *Security Concept for an Open Telematics Platform (unpublished).*

FMS Standard. (2016). *Technical Specification - rFMS.* HDEI Working Group.

GENIVI . (2016). Retrieved 03 01, 2017, from https://at.projects.genivi.org/wiki/pages/viewpage.action?pageId=11568933

Green Car Congress. (2014, 06 23). *Cummins progressing with lightweight downsized T2B2 diesel for pickup; 40% improvement in fuel economy over gasoline V8*. Retrieved from Green Car Congress: http://www.greencarcongress.com/2014/06/20140623-cummins.html

Hsieh, M.-F., & Wang, J. (2011). Adaptive and Efficient Ammonia Storage Distribution Control for a Two-Catalyst Selective Catalytic Reduction System. *Journal of Dynamic Systems, Measurement, and Control*.

IBM. (2015, August 24). C-ITS EU Platform, WG6 Technical Proposal B2B Marketplace. p. 39.

IBM. (2017). *IBM press release*. (IBM) Retrieved 03 16, 2017, from http://www-03.ibm.com/press/us/en/pressrelease/50838.wss

IDC. (2017). *European Data Market - SMART 2013/0063 - Final Report.*

IEA. (2016, 06 01). *Energy Technology Perspectives 2016 - Towards Sustainable Urban Energy Systems.* Retrieved 03 17, 2017, from Framework assumptions: https://www.iea.org/etp/etpmodel/assumptions/

Isuzu. (2014). *Technology for cleaner diesel, other technologies for cleaner diesel*. Retrieved from Isuzu: http://www.isuzu.co.jp/world/technology/clean/cleaner05.html

ITS Directive. (2017). *European Commission*. Retrieved 03 17, 2017, from https://ec.europa.eu/transport/themes/its/road/action_plan_en

Jaguar. (2017). Media Information. Retrieved 03 02, 2017, from http://media.jaguar.com/news/2017/02/jaguar-and-shell-launch-worlds-first-car-payment-system-just-fill-and-go-your-car-pays

John Deere. (2010). *Off-Highway Diesel Engines, Interim Tier 4/Stage III B.* Retrieved from John Deere: http://www.deere.co.uk/common/docs/products/equipment/industrial_and_agricultural_engines/interim_tier_4_stage_3_b/brochure/it4_brochure.pdf

Majewski, W. A. (2005). *Selective Catalytic Reduction.* Retrieved from DieselNet Technology Guide: https://www.dieselnet.com/tech/cat_scr.php

Nitsche, E. S. (2017). *ANACONDA D4.1 - Report on data collection and processing.*

otp. (2014). *open telematics platform* . Retrieved 03 15, 2017, from http://otp.systems/what-is-otp-subpage/tpl_subpage33

PSA Peugeot Citroen. (2015). Driving Automation and Connectivity. Retrieved November 17, 2016, from https://polcms.secure.europarl.europa.eu/cmsdata/upload/45934def-772e-4150-a609-d4cd7aa7da4b/Presentation_JFH.pdf

Ricardo Energy & Environment. (2015). *Study on the Deployment of C-ITS in Europe: input data overview – impacts data .* DG MOVE.

SAE. (2002). Recommended practice for Pass-Thru vehicle programming - SAE J2534. 25. Retrieved 03 10, 2017, from https://law.resource.org/pub/us/cfr/ibr/005/sae.j2534.2002.pdf

Scheiblich, C., & Raith, T. (2014). The extended Vehicle(ExVe) – New Standardization Project ISO. Retrieved November 17, 2016, from http://taysad.org.tr/uploads/dosyalar/18-12-2014-01-26-5-Extended-Vehicle---a-proposal-for-sharing-diagnostics-data-in-the-future-Scheiblich-ve-Raith-Daimler-27-11-2014.pdf

SERMI. (2017). *http://www.vehiclesermi.eu/*. Retrieved 03 09, 2017, from http://www.vehiclesermi.eu/about-sermi/

SMMT. (2017, 02). *Connected and Autonomous Vehicles Position Paper*, p. 46.

Thatcham Research, AZT, ADIG. (2016). *The identification of automated driving systems and the provision of data recording and storage suitable fo rhte insurance industry.* Thatcham Research, Allianz Center for Technology (AZT), Automated Driving Insurer Group (ADIG), Association of British Insurers (ABI), German Insurance Research Association (GDV). Thatcham: Thatcham Research.

Tina Grady, B. (2010, 04 21). *John Deere Power Systems shows entire Interim Tier 4/Stage III B diesel engine lineup.* Retrieved from Aggrigates Manager: http://www.aggman.com/john-deere-power-systems-shows-entire-interim-tier-4stage-iii-b-diesel-engine-lineup/

Toyota. (2017). *Toyota Global Newsroom* . (Toyota Motor Corporation) Retrieved 03 21, 2017, from http://newsroom.toyota.co.jp/en/detail/3203921

VDA. (2016). Position: Access to the vehicle and vehicle generated data. Berlin. Retrieved February 7, 2017, from https://www.vda.de/en/topics/automotive-industry-and-markets/aftermarket/the-open-telematics-platform-in-the-aftermarket.html

VdTÜV. (2017, January 26). Requirements for the telematics interface in vehicles. p. 5.

Appendix A. LEGAL ANALYSIS REPORT

Legal Background and General Analysis: Data Protection and Privacy

Legislative background

The Data Protection Directive (Directive 95/46/EEC) and the General Data Protection Regulation in April 2016 (Regulation (EU) 2016/679, the GDPR)

EU data protection legislation is currently based on the Data Protection Directive (Directive 95/46/EEC). This provides a framework for the protection of personal data which is implemented across the EU in national laws. Implementation within the UK, for example, is through the Data Protection Act 1998. While it provides a high degree of protection for individual privacy and extensive harmonisation between member states, it was written before many of the current uses of personal data were anticipated. In addition, divergence between member states in some areas, such as what constitutes valid consent and how the interests of the data subject and the data processor should be balanced, can present difficulties as cross-border communication and data use proliferates.

The legislation is consequently due to be strengthened and updated through the introduction of the General Data Protection Regulation in April 2016 (Regulation (EU) 2016/679, the GDPR). This is to apply from 25 May 2018, and so is likely to be of greater relevance to the current project than the existing legal regime.

At the heart of both systems, however, is the protection of personal data about individuals by organisations who control and process that data. In contrast with data "ownership" laws, data protection laws give rights to the individual subjects of the personal data rather than any organisations that may use that data. In general, data protection laws regulate the way that organisations can use the data rather than mandating particular uses of the data.

Controllers, those who determine how and why personal data is processed, and processors, who act on behalf of controllers, must comply with the principles set out in the legislation when carrying out processing activities (for example by putting in place appropriate security for the data).

In order to be lawful, processing must normally satisfy one of a limited number of conditions, such as consent of the data subject or processing necessary for the performance of a contract with the data subject.

e-Privacy Directive (Directive 2002/58/EC on privacy and electronic communications, as amended and as proposed to be reformed)

The e-Privacy Directive complements the Data Protection Directive and concerns the protection of privacy and personal data in the electronic communications sector. While much of the e-Privacy Directive deals with the provision of public communications services, it also addresses the use of location data for the provision of value added services. Information about the processing of the data and transmission to third parties must be provided to the data subject, their consent must be obtained and they must be able to withdraw consent temporarily or permanently.

The e-Privacy Directive is currently under review in the light of the changes to the wider data protection regime.

General analysis

Data protection laws give rights to the subjects of personal data. We have addressed below some key questions in terms of the use of personal data in the context of accessing in-vehicle data.

Do data protection laws apply?

Data protection laws only apply to personal data. Personal data includes any information that relates to an identifiable natural person. This includes any information that can be used to evaluate, influence the status or behaviour of that person or that is otherwise likely to have an impact on the individual's rights or interests. The use of in-vehicle information that relates to an identifiable individual (more obviously the driver/vehicle owner/passenger) will therefore be subject to data protection laws.

In the context of the three technical solutions, a significant proportion of the services envisaged by Working Group 6 will be targeted at specific individuals based on features about their activity and/or their vehicle. It is highly likely therefore that the majority of the data used will constitute personal data and that the use of the data will engage data protection laws.

Data that has been aggregated or anonymised in such a way so as to prevent an individual being identified will not constitute personal data and so its use will not engage data protection laws. So, for example, the use of aggregated data collected by an OEM during vehicle servicing about the performance of a particular engine type would not be subject to data protection laws.

Who has rights under data protection laws in respect of the use of in-vehicle data?

As set out above, data protection laws give rights to the data subjects. Those rights can be enforced either by the individuals themselves or by regulators responsible for ensuring compliance with data protection laws.

In the context of in-vehicle data, data subjects will clearly include drivers/vehicle owners but also potentially passengers who use on-board services and other individuals who interact with the vehicle (e.g. other road users and pedestrians whose data is collected by vehicle safety technology or who may use on-board wireless technology). Data subjects of in-vehicle data may also include people who provide services in respect of a vehicle (e.g. identifiable mechanics).

Which stakeholder groups need to comply with data protection laws?

Data protection laws apply to the processing of personal data. This "processing" is broadly defined to cover any operation or set of operations on the data, including, for example, collection, storage or transfer. Any entity that determines how or why this processing takes place will be a data controller and so be required to ensure that the processing complies with data protection laws.

Stakeholder groups likely to be acting as data controllers in respect of in-vehicle data include each of the operators identified in Working Group 6's proposed technical solutions. OEMs and vehicle retailers and service providers may already be acting as data controllers in respect of in-vehicle data. Under the anticipated models of data storage and access, other data controllers are likely to include platform providers, application providers, insurers and public authorities using the data in the course of carrying out functions (e.g. law enforcement, provision of medical services in emergencies).

Under the Data Protection Directive, service providers acting purely on the instructions of data controllers only have obligations where they are expressly passed on by terms included in contracts with the data controllers. Under the General Data Protection Regulation, service providers will also become liable for their use of personal data even where used solely on the instruction of the data controllers. This will mean that service providers such as software vendors will also be directly subject to data protection laws.

Do data controllers need consent of data subjects to make use of the data?

Working Group 6 has made consent a "guiding principle" for this project. This goes beyond the requirements of data protection laws, under which consent is only one of the

means by which a data controller can justify the processing of personal data. Under data protection laws, consent to the processing of in-vehicle data may not be necessary in a number of scenarios, such as where:

- **the processing is necessary to carry out a contract** – so, for example, vehicle servicing providers may need to process in-vehicle personal data about a vehicle owner (such as information about the way and distance that the vehicle owner has driven the vehicle) in the course of carrying out maintenance on the vehicle;
- **the processing is necessary to protect the vital interests of the data subject** – for example, where emergency services wished to access in-vehicle data about the data subject at the scene of an accident; and
- **the processing is necessary to carry out a public function** – for example, if a law enforcement agency were mandated to collect and analyse information about the way that vehicles were being driven – we note that Working Group 6 says that consent is "without prejudice to the requirements of regulatory applications", though this oversimplifies the position under the data protection laws.

The position in the case of in-vehicle personal data is that consent will be generally necessary where that personal data is to be used for a commercial purpose. There are a limited number of exceptions (most notably, where the processing is necessary to carry out a contract with the data subject, as noted above), but a significant proportion of the applications considered by Working Group 6 will require data subject consent. For example, if an OEM collects in-vehicle data about the driver/vehicle owner and wishes to use that data to offer services to the data subject that are not very closely related to their existing commercial relationship (i.e. as the provider and user/owner of a vehicle, respectively), the data subject's consent is likely to be needed. Equally, if an OEM wishes to disclose in-vehicle data to a third party service provider (such as an insurer), the data subject's consent is likely to be needed. Where consent is necessary, it must be freely given, specific, informed and unambiguous.

What do stakeholders acting as data controllers need to do to comply with data protection laws?

Arguably the most onerous obligation is to ensure that appropriate technical and organisational security measures are taken to prevent unauthorised and unlawful processing – certainly this is where data protection authorities (such as the Information Commissioners Office in the UK) have imposed most monetary penalties and focused their other enforcement efforts.

The GDPR also introduces a number of other obligations that are likely to affect any data controllers handling personal data as part of any of the three technical solutions. The GDPR brings in a requirement for **"privacy by design"** – this means that as well as complying with their privacy obligations as a matter of fact, the design of any application platform and associated infrastructure will have to ensure privacy is ensured by default.

The GDPR introduces rights for data subjects to require that the data is made "portable" by being provided in a format that enables the data to be given to a replacement service provider. It also allows data subjects to request their personal data be deleted when they withdraw their consent or it is no longer necessary for the purpose for which it was collected. These changes mean that the solutions may need to be able to cope with the transfer of data from one service provider to another at a data subject's request. If a vehicle owner sells their car or changes their vehicle-servicing provider, they may be entitled to request that their personal data is deleted by their previous service provider (and potentially from the car's in-vehicle systems and any external databases) and transferred to their new service provider. Data controllers would need to consider how to effect such a process in practice.

Will downstream users of personal data (such as application providers) be limited in their use of personal data?

The data subject must be given information about the identity of the data controller and their purposes in processing the personal data, so far as is practicable. Unless consent is not required as explained above, data controllers will be limited in their processing to the extent of the original consent given by the data subject. Where a downstream data controller (such as an application provider) seeks to make use of the personal data, they will only be able to do so where the data subject has been informed of their identity and the purposes for which they are processing the data and has consented to such processing. Where their intended processing goes beyond the information given to and consent originally provided by the data subject, the relevant further information will be required to be provided and the relevant further consent given before such further processing can be carried out.

How will data controllers provide information to data subjects or obtain consent where necessary?

The mechanism for informing data subjects about the use of their data and obtaining consent where necessary is likely to vary according to who is the data controller. We have provided more commentary on this in relation to each technical solution below.

What are the risks of breaching data protection laws?

Currently, the risks of breaching data protection laws are limited – though data subjects have certain rights and regulators can impose penalties, these are not generally substantial when compared to other regulatory regimes such as competition law (though they do vary significantly across member states).

Under the General Data Protection Regulation, the exposure of data controllers will increase significantly, potentially including fines of up to 4% of worldwide turnover. Given the rapid increase in the number of reported cyber-attacks, the risks associated with processing personal in-vehicle data will increase significantly.

Will data protection laws distort competition or hamper the deployment of interoperable systems?

Data protection laws give rights to data subjects rather than service providers. They are unlikely in themselves to distort competition because data subjects are unlikely to be able to influence the development of a market for services.

However, the increasing scope of the data protection laws and the increasing risks associated with non-compliance may dissuade service providers from entering markets dependent on the use of in-vehicle personal data unless the opportunities justify the risks and they are able to control the factors giving rise to risk (e.g. security of data, particularly when it is being transferred between vehicle/platform/application).

Data Ownership

Legislative background

Database Directive (Directive 96/9/EC)

The Database Directive requires member states to provide protection for collections of data which are arranged in a systematic or methodical way and individually accessible by electronic or other means. There must have been substantial investment in obtaining, verifying or presenting the contents of the database. We refer to the "Legal study on Ownership and Access to Data (SMART 2016/0085)" for more detail on this right.

Trade Secrets Directive (Directive (EU) 2016/943)

The Trade Secrets Directive, adopted in June 2016 and to be implemented by June 2018, harmonises the definition of trade secrets. We refer to the "Legal study on Ownership and Access to Data (SMART 2016/0085)" for more detail on this Directive.

General analysis

As discussed in pages 6 for 42 of the "Legal study on Ownership and Access to Data (SMART 2016/0085)", the concept of ownership as it relates to data is a complex issue. We have addressed the key questions in the context of the access to and use of in-vehicle data below.

What ownership rights can exist in data?

Broadly, ownership rights in data can arise in two ways:

- **rights in the data itself** – data can potentially be protected by the entities that created the data through the law of confidence and/or as a trade secret. If a third party uses confidential information without permission or misappropriates a trade secret, the "owner" of the information may be able to bring an infringement claim against the third party. However, there is considerable variation in approach across member states here, for example in terms of whether data can give rise to property rights;
- **rights in the database in which the data is stored** – which may be protected through copyright or database rights. Owners of rights in databases can restrict the ability of third parties to use/extract the contents of the database or reproduce the database. Though there is more harmonisation here across member states under the Database Directive, the application of the law by the courts has shown that the scope of legal protection offered to database "owners" is uncertain.

Who owns any rights in data?

Under the existing legal position regarding data ownership, drivers/vehicle owners are unlikely to "own" the in-vehicle data generated by their vehicles. The holder of the relevant ownership rights will typically be:

- **data** – the party who creates/holds the data may argue that the data is confidential and/or a trade secret. On that basis, they could argue that they "own" the data and that another party wishing to access/use the data would need their permission (which may be dependent on granting a right, typically under a contract).
- **database** – database rights arise only where a party has invested in obtaining, verifying or presenting the contents of the database. Copyright in databases only arises where the selection or arrangement of the contents make it the creator's own intellectual creation. In both cases, the database owner would need to show that the database was more than a by-product of another process (e.g. engine management).

On that basis, OEMs may argue that they own the relevant rights in the in-vehicle data created by their vehicles both because (a) the data is confidential and only made available to third parties under contract and (b) they have invested in obtaining the content of the databases containing the data. In both cases, these arguments may be vulnerable. If in truth the data is not confidential (for example if the data is held in an industry-standard format) then it may be difficult to bring a claim for use of the data by a third party for breach of confidence. If there has been no separate investment in obtaining the data (e.g. because it is a by-product of an existing process) it may not be possible to bring a claim for use/extraction of data from the database by a third party on the basis of database rights infringement.

Other stakeholders may also argue that they hold various ownership rights in data – we have addressed this in respect of each of the solutions below.

Will data ownership laws distort competition or hamper the deployment of interoperable systems?

The existing legal position regarding data ownership is in itself unlikely to prevent any of the solutions or data access models put forward by Working Group 6 from operating successfully. However, as discussed in pages 6 to 42 of "Legal study on Ownership and Access to Data (SMART 2016/0085)", there is currently uncertainty both in terms of (a) the lack of harmonisation across member states in terms of proprietary rights in data and (b) the extent to which any proprietary rights in data will arise in respect of in-vehicle data (for example depending on how the data are obtained, verified and presented). That uncertainty could in theory affect the development of an open market for the use of in-vehicle data because stakeholders (e.g. OEMs) may not feel that they have a commercial incentive for collecting and making the data available if they cannot obtain a commercial benefit from doing so.

In practice, as discussed below, the uncertainty over the application of data ownership laws here is in practice unlikely to be significant because those with control/possession of the data can restrict access to/use of the data through the use of contracts. As described in the Commission's Communication "Building a European Data Economy" COM (2017) 9, this would effectively make them "*de facto* owners" of the data.

To the extent that any rights in data do arise, there is the potential for the owners of those rights to distort the market and hamper the provision of services based on the usage of in-vehicle data because they would be in a position to restrict the use of data that would infringe those rights. As discussed in the Competition Law and Contract sections below, the principal check on such behaviour would be through existing competition laws.

If the EU wanted to ensure rights-holders did not restrict access to/use of data then it would need to consider whether competition law is sufficient or whether an intervention is necessary (e.g. mandating data access, standardising terms of data access). However, the issues around data ownership are not specific to automotive sector (as discussed in "Legal study on Ownership and Access to Data (SMART 2016/0085)"). Our view is that the problems with the existing legal position regarding data ownership are unlikely to determine the success or otherwise of any of the solutions or data access models under consideration by Working Group 6.

Competition Law

Legislative background

Treaty on the Functioning of the European Union (TFEU)

The TFEU sets out the detailed basis of EU law as established in 1957 and revised in 1992 and 2007. Articles 101 and 102 provide the basis for competition law.

Article 101(1) of the TFEU (mirrored in the UK's Competition Act 1998, s2) prohibits agreements between undertakings (that is, businesses), decisions by associations of undertakings or concerted practices which may affect trade between EU member states and which have as their object or effect the prevention, restriction or distortion of competition within the EU.

Article 102 of the TFEU (mirrored in the UK's Competition Act 1998, s18) prohibits the abuse by one or more undertakings of a dominant market position within the EU (or a substantial part of it) in a way which may affect trade between EU member states.

Application of competition law, and particularly Art. 101 TFEU, is fleshed out in Block Exemption Regulations and associated guidance. These give information on the types of structures and arrangements that are and are not acceptable. The Technology Transfer

Block Exemption Regulation 316/2014, for example, while unlikely to be directly applicable to the way that in-vehicle data is accessed, is accompanied by Guidelines that includes a discussion of technology pooling arrangements.

General legal analysis

Fair and undistorted competition is one of the guiding principles identified by Working Group 6. This principle broadly reflects the position in the current applicable competition law. As a result, current competition law (such as Articles 101(1) and 102) is in principle sufficient to prohibit any anti-competitive behaviour taking place during the implementation or operation of any of the three technical solutions. From this perspective, the market envisaged by the three technical solutions will be like any other and competition authorities will be able to rely on their existing powers to bring enforcement action for any anti-competitive behaviour.

There is nothing inherently anti-competitive about any of the elements of any of the three solutions (or indeed any purely technical solution), but in so far as any operators find themselves in a position where they are able to affect the proper functioning of a competitive market, there will be an increased risk that competition law may be breached. The potential for *de facto* ownership or control of data in general to engage competition law is discussed in the European Commission Study SMART 2016/0085. This indicates that whether a particular arrangement complies with competition law will be highly fact sensitive. However a broad analysis of the relevant themes that would apply to the proposed solutions is given below.

Any OEM that exercises control over data generated by the vehicles it manufactures is likely to be in a dominant position with respect to the market for services that make use of that data offered to owners or users of that make of vehicle. Although the holding of a dominant position is not in itself a breach of competition law, any refusal to provide access to the data on non-discriminatory terms to third parties may constitute an abuse of this dominant position and so infringe Article 102. This could be on the basis that access to the data constitutes an "essential facility" for the provision of services in the relevant market.

In principle, therefore, existing competition law may be sufficient to require the sharing of in-vehicle data in accordance with one or more of the solutions considered by this study. In order to guide practice in this area and reduce the risk of abuses of a dominant position by a single data owner/controller, guidelines or regulations could be issued to ensure that data is shared equitably. Suitable models covering similar areas already exist: for example, Euro 5 regulation on Vehicle Diagnostic, Repair and Maintenance Information, as noted in the Working Group 6 Report (December 2015), requires that vehicle management data (principally environmental) is made available to independent servicers of vehicles in a non-discriminatory and standardised way. This allows independent mechanics to service vehicles as well as authorised OEM service centres. This ensures a competitive market to the benefit of consumers.

As discussed below in respect of the "use-case" model of data access, there may be a benefit to the market in standardising the way that data is made available. Producing that technical standard will require discussions between OEMs (and potentially other stakeholders), who will be competitors. There is a risk that any discussions between such competitors would fall foul of the prohibition under Article 101(1). Therefore it is important that discussions with and between OEMs deal only with technical matters and not with commercial issues. Participation in standard setting should be unrestricted and transparent. The resulting standards should be objective and non-discriminatory. As well as standardised data, the means of accessing data may also need to be standardised. Competition law is likely to require licences for use of the necessary technology to be on fair, reasonable and non-discriminatory terms. Ideally there should be "ground rules" or "terms of reference" agreed by all participants that govern any standardisation discussions.

Although existing competition laws should already restrict any anti-competitive behaviour that arises from the three solutions, one potential issue is that any limitations placed on anti-competitive behaviour will in part undermine the incentive for entities to make the investment required to generate the market. For example, the motivation for an OEM to develop the infrastructure for the data server platform may be reduced if that OEM is not then in a privileged position to exploit that data or is not otherwise able to generate sufficient return on its investment. This is a particular issue given the complexity of the legal position regarding data ownership set out above. OEMs are likely to seek to rely on contractual control in order to determine the ways in which third parties are able to make use of the data rather than relying on proprietary rights in the data (such as database right). This approach is likely to require complex contractual arrangements in order to restrict how the data is used or passed on. Such arrangements would be at risk of breaching competition law if the correct balance is not struck by the OEM between seeking a fair return on its initial investment and unfairly leveraging its privileged position in the market.

In addition, the impact of competition law is highly dependent on the details of how a specific market operates in practice. This means there is a risk of initial uncertainty before the limits of the data holders freedom to determine the terms of any arrangement are determined in practice. Competition law sanctions are typically retroactive and therefore even where anti-competitive behaviour is ultimately found to be a breach of competition law, by the time this finding has been made and the appropriate interventions made, a significant negative impact on the functioning of the market may have already occurred. This is exacerbated by the tendency of digital markets to be dominated by a few key providers. Even where these providers are found to have acted anti-competitively in establishing their position, competition law sanctions are unlikely to entirely counteract the ongoing benefits of their initial advantage. This risk is also touched upon in the Commission's Communication "Building a European Data Economy" COM (2017) 9.

Contract

General legal analysis

We have noted above that the concept of data ownership is problematic and so a data holder is unlikely to seek to rely on just any inherent rights it may hold with respect to the data (for example, database rights, copyright, or trade secret protection). Instead, a data holder is likely to rely on contractual arrangements to control access and use of the data.

There is a wide variety of different approaches in terms of national contract laws across the EU. Differences between member state contract laws generate additional cost and legal uncertainty when operating across different jurisdictions. Notwithstanding the differences in national contract laws, generally speaking the basic position in contract law is that parties are free to agree terms between themselves. This is restricted and controlled to a certain extent by certain EU and national laws, but, as a general concept, contract law is the law that governs the commercial relationship between two parties.

The general legal analysis above holds true for any of the contractual relations required under any of the three technical solutions. Contractual terms can be used to regulate access to and use of the data, but can also be used to address liability as between the parties. Contract laws will tend to allow data holders to exploit the data or restrict its usage by others. The key points in relation to contract law are that (i) regardless who is the data subject or the data holders, the issues applying to each of the technical solutions are the same and (ii) we are not aware of any contract law which would necessarily impede or prevent the implementation of any of the three technical solutions.

The wider question is whether there is any particular advantage or disadvantage associated with any of the three technical solutions from a contract law perspective. In

other words, do any of the three technical solutions lend themselves to the creation of a clear, certain and flexible contractual matrix between the parties concerned? A brief analysis of the likely contractual structure for each of the three technical solutions is given in the next main section. A detailed analysis of each of these contractual relationships is beyond the scope of this report.

Liability

Legislative background

Rules on liability vary considerably between member states and there is a lack of harmonisation at EU level. The law relating to liability to consumers is harmonised more than that as between organisations. We will address the following EU consumer legislation:

- Unfair Terms in Consumer Contracts Directive (93/13/EEC)
- The Product Liability Directive (85/374/EEC).

General analysis

Liability from access to and use of in-vehicle data could arise in three main ways: (a) through contract, (b) through negligence or (c) through strict liability particularly under the Product Liability Directive. Elements (a) and (b) are not closely harmonised across the EU and so the detailed analysis will vary from one member state to another.

The potential for injury or damage arising from access to in-vehicle data, and particularly where this involves read/write access, is considerable. Services involving maintenance of vehicle equipment and safety features need to be reliable and consistent. Services involving influencing the vehicle's movements and controls need to be tightly restricted in order to prevent injury and damage to the vehicle's occupants and others. Even mapping and route-finding services could expose a driver to danger where an unsafe route is presented. Clearly participants in the system, and particularly OEMs, will have concerns about exposure to additional liability that should be addressed in the implementation of a new system.

We discuss in our analysis of contract law some of the possible contractual arrangements between the different parties. Each of these contractual relationships may address the allocation of liability arising from particular situations, and the limitation of the liability attaching to a particular party. The parties' freedom to establish contractual arrangements concerning the allocation of liability will, to some extent, be limited by EU and member state law. Contracts between businesses and consumers are heavily circumscribed, for example by the Unfair Terms in Consumer Contracts Directive (93/13/EEC). Controls on contracts between businesses/organisations are primarily dealt with under national law and not harmonised. In English law, for example. The Unfair Contract Terms Act 1977 places limits on the exclusion or restriction of liability resulting from negligence, whether in performance of the contract or a wider duty to take reasonable care or exercise reasonable skill. There are also detailed rules based on jurisprudence built up through case law as to the limits on parties' freedom to exclude or allocate liability and the wording needed to achieve this.

Liability arising through negligence does not require there to be a contractual relationship between the parties. It can arise where injury or damage is caused because the conduct of a person or organization falls below a reasonable standard. While EU member states all provide for some form of fault-based liability, there are differences between jurisdictions as to the principles and procedures that are applied. In English law, a claimant must prove:

- that a duty of care to the injured party existed;
- that the duty of care was breached by conduct falling below a reasonable standard;

- that damage was caused by the negligent conduct; and
- that loss was suffered by the claimant.

Variations exist among the laws of other EU member states, for example, in relation to:

- the burdens of proof (who must establish what in order to pursue or defend a claim);
- limitation periods (the period of time after which a claim may no longer be compensated); and
- defences to negligence claims, such as the voluntary assumption of risk by the claimant, contributory negligence by the claimant, and the fact that harm was caused by some intervening event.

In complex, multi-party situations such as those under consideration, it is often extremely difficult to establish the extent to which fault rests with a particular party. Litigation may be required to establish the degree of negligence attributable to each actor in the system, and this is time-consuming and expensive. For this reason, statutory rules may be introduced to provide an additional form of liability in a particular set of relationships.

The EU product liability regime is an example of a set of rules that avoid the need to rely on contractual or fault-based liability by providing an additional route to claim for damage. The Product Liability Directive (85/374/EEC) establishes the principle of liability without fault applicable to EU producers. Where a defective product causes damage to a consumer, a producer may be liable without negligence or fault on their part. The Product Liability Directive applies to damage in the form of death or personal injury, and damage to property. A product is defective if it does not provide the safety that a person is entitled to expect, taking into account all the circumstances, such as the reasonable use of the product.

The producer of a product is widely defined, and can mean the manufacturer of a finished product or of a component part, the importer of a product, any business or organisation that puts their name or trade mark on a product and any person supplying a product where the producer or importer cannot be identified. While the arrangements under consideration primarily relate to the supply of services, the supply of a vehicle to a consumer, or of a separate communication device to a consumer, could engage the strict liability rules of the Product Liability Directive and member state rules implementing it.

While the injured person is required to prove the damage, the product defect and the causal link between the two, courts in a number of member states have shown some flexibility in this. For example, the requirement to prove a defect has been relaxed to the extent that the injured person need not prove the exact flaw in the product that caused the injury. An unexpected failure in a product with no obvious alternative explanation can be sufficient (e.g. *Ide v ATB Sales Ltd* [2008] EWCA Civ 424). In some cases the burden of proving a causal link between the defect and the damage has also been relaxed.

Defences to this form of liability are available. These include:

- that the defect did not exist at the time the product was put into circulation;
- that the defect is due to compliance of the product with mandatory regulations issued by public authorities;
- that the state of scientific and technical knowledge at the time when the producer put the product into circulation was not such as to enable the existence of the defect to be discovered; and
- in the case of a manufacturer of a component, that the defect is attributable to the design of the product in which the component has been fitted or to the instructions given by the manufacturer of the product.

The Product Liability Directive is implemented in the UK by the Consumer Protection Act 1987. There is a degree of flexibility given to member states in how the Directive is implemented but this is limited and so the system is fairly well-harmonised across the EU.

While liability arising through contract and negligence is largely within the control of the parties that may become liable, whether through negotiating the terms of a particular contract or through actively providing for and constantly updating the safety for users of their systems and products, the strict liability regime may be a cause for concern. In order to address these concerns it will be important for the implementation of the system to take account of where liability might arise and how to avoid inappropriate exposure of OEMs and other producers to litigation. Use of a mandatory regime, or set of regimes, under which access to in-vehicle data must be provided in specified ways, will help to address this concern as it will enable reliance on a defence to strict liability. This applies in respect of each of the different technical solutions and models for access.

We have not considered in this report the potential for liability in non-EU jurisdictions arising from the sale or use of vehicles containing data access technology outside the territory of the EU. The United States, in particular, provides a sophisticated product liability system with the potential for large compensation awards. Any system that is likely to be made available outside the EU would need to be considered in the light of the relevant jurisdiction's liability rules.

The Three Technical Solutions

On-Board Application Platform

Data protection and privacy

As discussed above, data protection laws are unlikely to prevent the development of a market based on the use of in-vehicle data or the use of in-vehicle data by regulators/authorities where necessary, but they will impact the way that any model for accessing/using data is implemented.

In particular, data controllers processing personal in-vehicle data will be taking on the responsibilities and risks associated with processing personal data so will need to consider how to provide information to data subjects about their use of the data and how to obtain their consent where appropriate. We have given some key examples of this in the context of the on-board application platform solution below:

- **The OEM as data controller:** OEMs are likely to be a data controller in so far as they determine how and why personal data are provided into the on-board application platform. Though OEMs may argue that some uses of personal data are necessary to carry out their contract with vehicle owners (e.g. as part of providing a warranty service), as discussed above, OEMs will need to consider how they obtain consent to any disclosure of the data to application platform providers and potentially to application providers (to the extent not handled by a separate platform provider). We would expect this to affect the terms that OEMs provide to data subjects (e.g. in purchase and registration documents).

- **The on-board application platform provider as data controller:** Although it is possible that the on-board application platform provider will be the same entity as the OEM, we understand that this is not necessarily the case. For example, an OEM may enter into an arrangement with a third party to provide the necessary infrastructure for the inbuilt device. In this scenario, this third party may also be a data controller and so obliged to comply with data protection laws. Any

separate platform provider would need to consider how to provide appropriate information to data subjects and how to obtain any necessary consents to disclosure (e.g. to application providers). This could either be handled by the OEM as above or the platform provider may engage directly with data subjects (e.g. through an on-board interface or online portal).

- **The application provider as data controller:** Each application available on the on-board application platform has the potential to make use of the personal data in a way not explained and consented to at the point of collection. Where this is the case, further consent may be required. For example, a driver may download an application to the platform and at the point of installation agree to the terms on which the application provider can use the data.

Data ownership

As discussed above, the existing legal position regarding data ownership would not prevent the on-board application model from operating but may affect the way that it would operate. In particular, proprietary rights in data would potentially allow anyone who holds those rights to distort competition among application providers – for example, by allowing rights holders to limit access to the data to certain categories of provider or by using the threat of legal action for infringement to persuade or coerce providers to accept onerous licensing terms.

As discussed above, proprietary rights (if any) in the in-vehicle data on the on-board platform are likely to be held by the OEM or (where separate) the application platform provider. They could potentially use those rights to limit the access to/use of the data by other application providers (either those hosted in the vehicle or that could otherwise access the data in the vehicle from outside the vehicle). However, competition law would apply to any such restrictions.

Competition

As discussed above, arrangements between stakeholders may breach the prohibition on preventing, restricting or distorting competition. For example, any arrangement between OEMs to agree to limit access to data or to standardise the basis on which data is made available or used may give rise to competition law issues. Similarly, arrangements between platform providers (if they are not OEMs) may give rise to concerns.

Those with control/possession of data (in this case, likely to be OEMs or platform providers) are prohibited from abusing a dominant position in the market. They would need to be careful not to abuse their position by, for example, requiring onerous contractual terms as basis for making data available, such as in terms of exclusivity, price, liability, limitations on the onward disclosure of the data.

Contract

In our view, the following contractual relationships are likely to be particularly relevant:

- Contract between OEM and on-board application platform provider
- Contract between on-board application platform provider and third party application providers
- Contract between on-board application platform provider and authorities
- Contract between on-board application platform provider and customer

We anticipate that the on-board application platform provider might well be the OEM. If so, there would be no particular contract law concern as the contractual arrangement (if any) between the OEM (as OEM) and the OEM (as on-board application provider) would be intra-group and not therefore commercially negotiated.

In the event that the on-board application provider is not the OEM, the relationship between the OEM and the on-board application provider will be of critical importance to the OEM. Such contract could be the subject of detailed and, potentially lengthy, negotiations. This in itself does not cause any particular legal issues although the fact that such contractual arrangement is detailed and lengthy, may result in a degree of inflexibility which could hinder innovation.

Subject to the method of access chosen (see the Different Methods of Accessing Data section below), we would anticipate the on-board application provider determining the terms on which third party application providers could develop applications and the terms on which users could install such applications on the platform. Where the on-board application provider is distinct from the OEM, it is likely that the OEM will still have a large influence on these terms by including in its contract with the on-board application provider a requirement that the on-board application provider pass on particular terms to the third party application provider and the ultimate user. Again, whilst not causing any particular legal issues, this may have the effect of allowing the on-board application provider and/or the OEM to stifle innovation and restrict the interoperability across different platforms (though see above about the competition law implications of doing so).

In addition (again depending on the method of access granted), we would expect the on-board application platform provider to determine the access granted to customers and for each third party application provider to determine the terms on which the customer or user has access to the application.

As previously stated, whilst some of the contractual arrangements for the on-board application platform may be complex, there is no reason why contract law would prevent the adoption of an on-board application platform solution.

Liability

With this solution there is a potential concern for OEMs in relation to liability attaching to them as producers of the vehicle. If the system within the vehicle can expose the vehicle as a whole to a safety risk, then the OEM could become the subject of consumer claims under the Product Liability Directive. A particular concern may arise where there is read/write access to the vehicle's systems. In order to reassure OEMs that liability will not attach to them in this way it may be necessary to introduce legislation that mandates a system to provide access to vehicle data such that they have a clear defence to strict liability. This could be included in legislation that mandated the technical solution or through separate legislation like the type approval system. Detailed rules addressing the safety of data-access systems would offer a defence to an allegation of liability arising from the inclusion of the system in the vehicle, or permitting access to the vehicle's information. Careful use of warnings and information addressed to vehicle users may also be needed in order to ensure that access is only given in ways and to third party organisations that will not put the vehicle user at risk.

In-Vehicle Interface

Data protection and privacy

The legal obligations placed on the data controllers under the relevant data protection legislation will be the same for the in-vehicle interface as for the on-board application platform. To this extent, the earlier analysis on this topic will also apply here. Where the two solutions are likely to differ is in the identity and relationship between the various data controllers.

- **The external device provider as data controller:** As the in-vehicle interface solution requires an external device, the provider of that external device may act like the application platform provider discussed in relation to the on-board platform model above. Accordingly, the same issues around disclosure of personal

data to/by the external device provider and informing data subjects about the use of their data will apply here.

- **The OEM and application provider as data controllers:** From a privacy and data protection perspective, the status of the OEM and the application provider as data controllers will be the same for this solution as for the on board application platform, so the analysis given that section will also apply here.

Data ownership

Arguably under this model it is less likely that proprietary rights will arise in relation to the in-vehicle data because no single party (e.g. OEM) is making a separate investment in obtaining, verifying or presenting the contents of a database containing all in-vehicle data. However, it is still possible that the providers of each external device that connects and collects data will itself own rights in the data/database created.

For example, arguably the OEMs' investment in collecting the data is for operational reasons and the valuable data that is passed onto the external device is a by-product of this process. If this were the case, database rights would be unlikely to arise in the data collected within the vehicle system and passed to external device.

If the in-vehicle interface model is unlikely to involve a contractual relationship between the OEM as data-collector and the external device provider, this would mean that the two most viable means by which the OEM might seek to derive a return on its investment in making data available to third parties are unlikely to work in the case of the in-vehicle interface. Therefore, there is a risk that the in-vehicle interface as a universal interoperable means of access to in-vehicle data may not arise from market forces alone without regulatory intervention. This is because OEMs may have insufficient incentive to carry out the significant investment to facilitate the implementation of the interface (though in practice, if OEMs are also offering other services that rely on collecting in-vehicle data, there may be other incentives here). The need to protect such investment and the associated assets is also recognised in the Commission's Communication "Building a European Data Economy" COM (2017) 9.

Again, if any rights in the data do arise, the owner of those rights could potentially use them to limit the access to/use of the data by application providers and on that basis distort the market by restricting the provision of services based on the usage of in-vehicle data. However, competition law would apply to any such restrictions.

Competition

Again, arrangements between stakeholders may breach the prohibition on preventing, restricting or distorting competition. Accordingly, any arrangement between OEMs to limit access to data by the interface or by external devices and any standardisation of the basis on which data is made available or used by external devices would need to be compliant with competition law.

As with the on-board platform, those with control/possession of data (OEMs, device owners or operators of applications on those devices) would be prohibited from abusing a dominant position in the market (e.g. requiring onerous contractual terms as the basis for making data available).

Contract

In our view, the following contractual relationships are likely to be relevant:

- Contract between OEM and external device provider (if different)
- Contract between external device provider and application provider
- Contract between application provider and consumer

One concern in relation to the in-vehicle interface solution is that it is not clear to us that there will be a contractual arrangement between the OEM and the external device provider. We have assumed that this model will enable users of the vehicle to introduce their own external device. On that basis, whilst the OEM may make available the data feed via the interface, the OEM will not necessarily have a contractual arrangement with the external device provider. This gives rise to liability concerns, although it might encourage innovation and interoperability. From a contract law perspective, this is not ideal as it generates a degree of uncertainty as a result of the lack of clear terms. This is not insurmountable and could be overcome by mandating the terms that would apply between the OEM and the external device provider. An analysis of the specific terms that such an arrangement might involve is beyond the scope of this report.

In relation to the contractual arrangements between the external device provider and the application provider and between the application provider and the consumer, we have the same comments as in relation to the on-board application platform (with the external device provider in the in-vehicle interface solution effectively acting in the same capacity as the on-board application platform provider in the on-board application platform solution).

In general and as noted above, whilst some of the contractual arrangements for the in-vehicle interface solution may be complex, there is no reason why contract law would prevent the adoption of the in-vehicle interface solution.

Liability

With this technical solution the OEM and the provider of the external device could potentially be exposed to liability should injury or damage be caused. Again, the prospect of strict liability due to either the vehicle itself, the in-vehicle interface or the external device becoming exposed to interference or misuse is potentially concerning. The introduction of a mandatory system setting forth how data is to be made available and used would help to address these concerns.

Data Server Platform

Data protection and privacy

Again, the legal obligations placed on the data controllers under the relevant data protection legislation will be the same here as for the other two technical solutions. To this extent, the analysis presented above on this topic will apply. Where this solution is likely to differ is in the identity of and relationship between the various data controllers. Similarly, the data protection obligations placed on the various data controllers across the three different implementations of the data server platform will be the same. Any entity that processes personal data on its own behalf will generally have an obligation to ensure the relevant data subject is appropriately informed and that consent has been obtained where applicable.

- **OEM as data controller** – as with the previous two solutions, where it acts as the data controller in respect of the data stored in the data server platform, the OEM would need to consider the basis on which it allows disclosure of personal data to application providers and other third parties and how it discloses information about disclosures to/obtained consent from data subjects.
- **Data server provider as data controller** – the data server provider may either act as a data controller in its own right or act on behalf of a third party. If it acts as a data controller then data subjects would need to be told about how and why it process their personal data and potentially to be asked to consent to the storage of their data on the data server and/or to the disclosure to third party application providers.

Another key additional privacy and data protection issue with this solution (over and above those issues identified in relation to the "on-board application platform" and "in-vehicle interface" solutions) relates to the resilience of the security measures put in place to prevent unauthorised access to the personal data.

Issues relating to the security of databases that contain personal information are well documented and in our view those issues would apply equally and no differently to data that had been produced in-vehicle and transmitted to the data server.

Data ownership

As with the in-vehicle interface, there is uncertainty over whether the OEM will hold any proprietary rights here but in practice this may not prevent the OEM from restricting access to the data through contracts.

The platform provider may hold rights in the data/database and so, depending on who the platform provider is, may be able to distort competition/prevent the provision of services based on the usage of in-vehicle data – for example by requiring application providers to agree to onerous licence terms. However, competition law would apply to any attempt to distort competition.

Competition

As for the in-vehicle interface, arrangements between stakeholders may breach the prohibition on preventing, restricting or distorting competition. Accordingly, any arrangement between OEMs to limit access to data by the platform provider and any standardisation of the basis on which data is made available or used would be subject to restrictions in competition law.

Again, those with control/possession of data (OEMs, platform providers) will be prohibited from abusing any dominant position in the market (e.g. requiring onerous contractual terms).

Contract

In our view, the following contractual relationships are likely to be relevant:

- Contract between OEM and platform provider (shared/B2B)
- Contract between platform provider and application providers
- Contract between application provider and consumer

We would anticipate a key contractual arrangement for the data server solution being between the OEM and the platform provider. We would expect the OEM to attempt to control the flow of data from the vehicle, not least because the OEM will wish to protect its reputation in terms of the data generated by its vehicle.

On this basis, the terms of engagement between the OEM and the data server platform provider will be a matter of complex negotiation. This in itself does not give any particular cause for concern but careful thought should be given to the likely terms of such contractual arrangement so as to ensure that each party involved in the provision of the data server solution is aware of its responsibilities and so that the consumer and general public are adequately protected from any risk associated with this solution. A full analysis of the likely terms of such relationship is beyond the scope of this report.

In relation to the contractual arrangements between the platform provider and the application provider and between the application provider and the consumer, we have the same comments as in relation to the on-board application platform and in-vehicle interface solutions.

As noted above, the adoption of a solution based on the data server platform model is not prevented by any contract law concerns. However, it would be important to make clear, and possibly mandate through legislation and regulation, the terms of the contract between the OEM and the platform provider. This is because without a clearly structured

contractual relationship, the allocation of responsibility between the OEM and the platform provider may not be sufficiently clear. Although this should not affect their collective responsibilities to third parties (such as the consumer), if each thinks the other is responsible for a particular element (e.g. the resilience of the means of the in-vehicle data passing between them), there is a risk it may not be adequately addressed by either of them.

Liability

With this technical solution there is once again the possibility of concern among OEMs that enabling access to in-vehicle data could expose them to liability to vehicle users in the event that injury or damage resulted from such access. If this solution is selected, then the introduction of mandatory rules to require data sharing in this way, and clarification as to the extent of liability of OEMs, should allay these concerns.

Different Methods of Accessing Data

Relevance of "read" when compared to "read/write" access

The concept of "access to data" is itself complex quite separately to whether this access is in accordance with pre-defined use-cases or the terms and conditions of each application. "Access to data" could cover a range of different forms of access. For example, it could cover access to data generally transmitted by the vehicle (e.g. to nearby vehicles and infrastructure), access to data not generally transmitted by the vehicle but otherwise made available to external operators (e.g. through an in-vehicle interface or directly to a remote server), data or commands transmitted directly from external sources to the specific vehicle that the vehicle then implements, or data transmitted generally from external sources that the vehicle may pick up on its in-vehicle systems (e.g. RDS signals picked up and displayed by the infotainment system). A legal analysis that considers each of these different forms of access in detail is beyond the scope of this report. However, it is clear that access to in-vehicle data in its broadest sense will involve more than a single form of access, regardless of whether that access is based on use-cases or terms and conditions.

From a legal perspective, the most significant dimension of difference between these various forms of access is whether the access is on a "read only" basis or alternatively on a "read and write" basis. In our view this is a critical question when determining the method of access to the data as the liability and risk profile associated with access on a read only basis is an order of magnitude different to the liability and risk profile associated with access on a read and write basis. For example, there is a very different liability and risk profile associated with having read access to data relating to a vehicle's acceleration and braking (for example for usage based insurance) when compared with the risk and liability profile where read and write access to the data allows the application to control the vehicle's acceleration and braking (for example smart cruise control). This consideration does not only apply to what may be seen as safety critical systems; for example, the ability to manipulate a vehicle's internal temperature settings (i.e. a read/write access to the vehicle's climate control system) could have safety implications if the climate control system was operated by the application in a manner that could cause discomfort or distraction to the driver.

Whilst a detailed analysis of the use-cases identified by Working Group 6 is beyond the scope of this report, it is our view that the provision of access to data on a "read/write" basis would tend towards being best supported by the "access depending on use-cases" method. This is not due to a theoretical legal reason but due to the liability and risk profile associated with read/write access.

Whereas, if the access to the data is solely on a read only basis, it is our view that allowing that read only access on the basis of terms and conditions should be sufficient in most cases (although the points highlighted below relating to the sufficiency of acceptance of those terms and conditions would still apply).

Legal analysis of the "access depending on use-cases" method

Data protection and privacy

The processing of personal data relating to a data subject (whether the data subject is the operator of a vehicle, a passenger in the vehicle or a third party outside of the vehicle) requires either legal authority (for example the processing of personal information by governmental law enforcement agencies) or the consent of the data subject itself.

In the event that a definitive set of "use-cases" was determined (which we assume would be a precursor to the adoption of a method allowing "access depending on use-cases"), it may be that the processing of personal information in relation to certain of those "use-cases" would be exempt from the need to obtain consent from the data subject. Appropriate legislation or regulation could be put in place so as to achieve this.

Whilst there would be significant benefits in undertaking an analysis of the "use-cases" to establish which of those "use-cases" might benefit from such an exemption, such an analysis is beyond the scope of this report.

From a legal perspective, the certainty given by determining a definitive set of use-cases and then applying exemptions from the data protection regime to certain of those use-cases is attractive as it avoids the need to obtain consent of the data subject on an application by application basis for certain of the use-cases.

Where a "use-case" did not carry such an exemption, the consent of the data subject would usually need to be obtained in the usual way through an appropriate data processing consent.

Data ownership

In our view there are no additional data ownership issues worthy of particular mention in relation to the "access depending on use-cases" method.

Competition Law

As referred to earlier, the ability of a party to control access to data has the potential to prevent open and undistorted competition. To the extent the "access depending on use-cases" method would mandate the circumstances when the data holder would be required to provide access to a third party (and thus limit the potential for them to leverage their control to distort the market), this method would appear to have merit from a competition law perspective.

However, there are other ways to achieve fair and undistorted competition and therefore we do not think that the advantage noted should determine which of these methods is preferred.

Contractual

Adoption of the "access depending on use-cases" method would negate the need to determine (either in a mandatory form or on a case by case basis) a separate contractual relationship between the party with the data and the party accessing the data. The reason for this is that we would envisage the terms of such relationship being mandatory as part of the regulations determining the "use-cases" and the "access to those use-cases" (an integral part of mandating access depending on specific use-cases is likely to be mandating the terms on which that access is to be granted).

Whilst dispensing with the need for determining separate contractual relationships would appear attractive, the effort taken to determine, regulate and update the various "use-cases" (and the terms on which such access would be granted) would appear to outweigh this benefit. As a result, we do not believe that this advantage of the adoption of the "access depending on use-cases" method is significant from a contractual perspective.

Liability

Adoption of the "access depending on use-cases" method may be preferable from a liability perspective. The definition of a series of defined uses and the data that is to be made available in each case may provide a clearer situation in relation to liability on the part of an OEM, particularly if the provision of data in support of each use-case is mandatory.

Legal analysis of the "access depending on the terms and conditions of the applications" method

Data protection and privacy

The earlier privacy and data protection analysis in relation to the "access depending on use-cases" method is relevant here.

In general, unless a legal exemption exists from the need to obtain the consent of the data subject in relation to the processing of their personal information, consent will need to be obtained from the data subject in relation to the processing of their information.

Such consent is often obtained through the express acceptance of terms and conditions. Whilst this is often cumbersome, it is a process understood by data subjects.

It is however questionable whether adopting a method which generally requires consent of each data subject through terms and conditions risks missing out on some of the public interest benefits of being able to access and process the data without a specific consent (as seemingly offered by the access depending on use-cases method).

Data ownership

In our view there are no additional data ownership issues worthy of particular mention in relation to the "access depending on use-cases" method.

Competition Law

We do not consider there to be any particular competition law concerns with the "access depending on terms and conditions" method that are not also relevant to the "access depending on use-cases" method.

Whilst mandating the use of particular terms and conditions and the circumstances in which they must be used might assist in preventing the data holder from anti-competitive behaviour, we do not think this should be used to determine which of these methods is preferred.

Contractual

An "access depending on terms and conditions" method is a pure contractual method. The success or failure of this method would depend on whether the terms and conditions were clear, satisfactory and achieved a fair legal relationship between the respective parties.

However, an "access depending on terms and conditions" method is limited by the degree to which the parties to the terms and conditions comply with and understand those terms and conditions. Careful consideration should therefore be given to the circumstances in which access to in-vehicle data will be granted and the use of such data

so as to determine whether the terms and conditions and the acceptance of those terms and conditions are adequate in the circumstances.

As noted above, the adequacy of the terms and conditions is potentially less important in the context of "read only" data but far more important in the context of "read/write" data.

Liability

Adoption of the "access depending on the terms and conditions of the applications" method may expose an OEM or device provider to a greater degree of liability than the "access depending on use-cases" method. However, the inclusion of detailed consumer information and appropriate warnings in the terms and conditions to which a consumer agrees would assist in reducing the risk. In addition, if the making available of data access in this way is mandatory, the exposure of OEMs and device providers will be reduced.

The Negotiation Model

Legal analysis of the "negotiation model"

Data protection and privacy

The issues around privacy and data protection discussed above in relation to the data server platform generally will also apply to the sharing of data under the negotiation model. As both the OEM (in its capacity as the data collector) and any service provider are both likely to be data controllers, they will need to comply with the obligations described earlier. Each data controller would need to ensure that the data subject is appropriately informed about what is happening to their personal data and that appropriate consent has been obtained where necessary.

Data ownership

The issues with data ownership discussed above in relation to the data server platform generally will also apply to the sharing of data under the negotiation model. The ability of the OEM to control access to the data by any third party service providers is likely to be subject to the limitations on data ownership highlighted above. It is likely that the OEM will seek to rely on controlling access contractually rather than by exercising proprietary rights in the data. Subject to contract and competition law, this would allow the OEM to leverage its privileged position when negotiating with third parties.

Competition Law

There are two major potential competition issues arising from the negotiation model, both of which arise from each OEM's possible status as the sole source of in-vehicle data from its make of cars. Firstly, this model effectively leaves it up to the OEM as data holder to decide whether and on what terms it will allow third party service providers to access the data. Secondly, the OEM itself may also be a service provider in direct competition with other service providers and so it would be free to effectively "agree" more favourable terms for its own use of the data to provide services. Each of these has the potential to engage both the "abuse of a dominant position" and the "agreements between undertakings" aspects of competition law described above. Whether this is the case in practice will depend on the actual behaviour of the relevant market participants. If this model is adopted, its implementation and the development of the associated market will therefore require close monitoring by competition authorities.

As well as potentially distorting the market by allowing different services providers to access in-vehicle data under different terms, the negotiation model also has the potential to increase the barrier to entry for new service providers. To the extent an OEM has the potential to act as gate keeper to data generated by users of its vehicles, well-established service providers are likely to be at a significant advantage relative to new

entrants. New entrants will need to separately negotiate the terms of access to data with each OEM before they are able to compete on an equal footing with established service providers. Even where an OEM is not seeking to act in an anti-competitive matter, the uncertainty and period of time involved in such negotiations could act as a significant impediment to new market entrants and increase the risk associated with any speculative investment by prospective service providers to the ultimate disadvantage of consumers.

Contract

At the core of the negotiation model is the ability of OEMs and service providers to freely negotiate the terms under which data is shared. Subject to the limitations of contract discussed above, there will be a huge range of potential differentiators between the agreements reached between OEMs and service providers. As well as reaching an agreement on the range of data and the purposes for which it can be used, the parties will be free to negotiate, for example, how risk is apportioned.

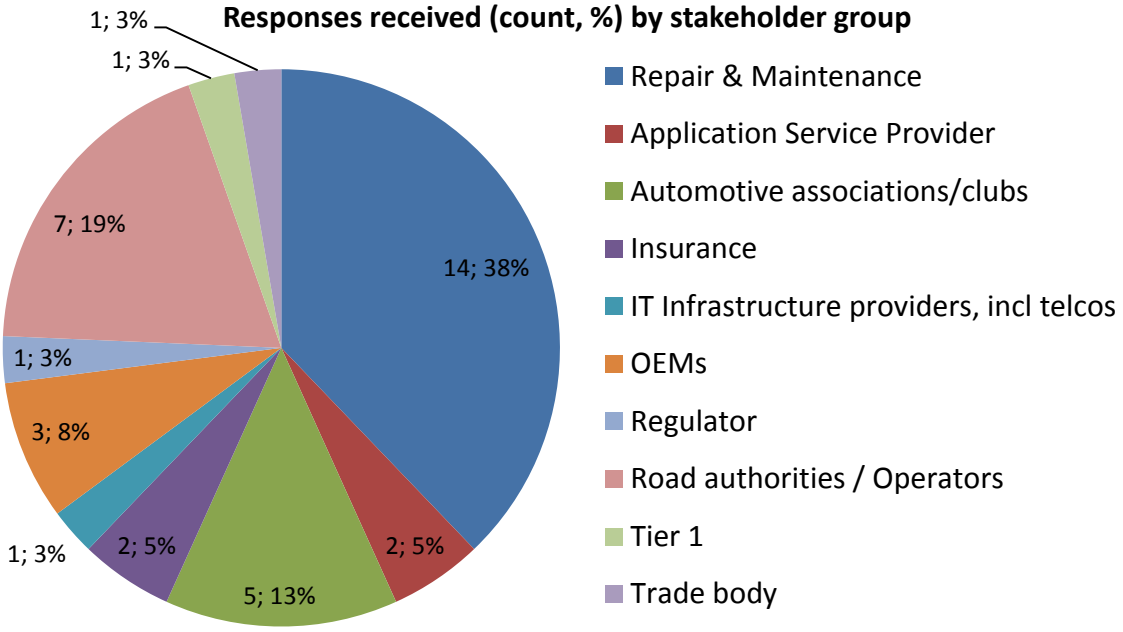
Liability

In the "negotiation model" there is potentially greater control for OEMs and service providers in relation to the data they provide and the use that it is put to. While this may expose them to greater liability should something go wrong, it may also reduce the concern that they will be exposed to liability arising from the data being made available more widely and for purposes that they cannot control. However, in a situation where the data is held by a party other than the OEM, the concerns over liability for injury and damage arising from providing access to data remain. Again, the introduction of a mandatory system that defines what data must be provided and in what circumstances will help to reduce these concerns.

Appendix B. RESPONSES TO ONLINE QUESTIONNAIRE

Based on the on-line questionnaire hosted by TRL, responses from different stakeholders were reviewed and a synthesis of these is presented below.

There were 37 responses received, from a variety of stakeholders. Each of the stakeholders was assigned to one of ten groups, for example OEMs, Repair and Maintenance, Insurance etc. A simple points weighting mechanism was used to allow a fairer comparison between the responses, which was important because for example there were 14 responses in the repair and maintenance group, and only two for insurers. Each of the ten stakeholder groups was assigned an equal amount of points. The points were used to distinguish between those stakeholders that represented only one country/company versus those that represented Europe or an association of companies. If there were multiple organisations at the same level within a group, then their points were shared equally. The final points were then scaled to 100%.



	Application Service Provider	Automotive associations/clubs	Insurance	IT Infrastructure providers, incl telcos	OEMs	Regulator	Repair & Maintenance	Road Authorities / Operators	Tier 1	Trade body	**Grand Total**
Austria		1					1	2			**4**
Europe		1	1	1	3	1	7		1		**15**
Germany		1	1				3				**5**
Italy		1					1				**2**
Netherlands	1							2			**3**
Norway	1							1			**2**
Poland							1				**1**
Spain							1				**1**
Sweden								1			**1**
Switzerland								1			**1**
UK		1								1	**2**
Grand Total	**2**	**5**	**2**	**1**	**3**	**1**	**14**	**7**	**1**	**1**	**37**

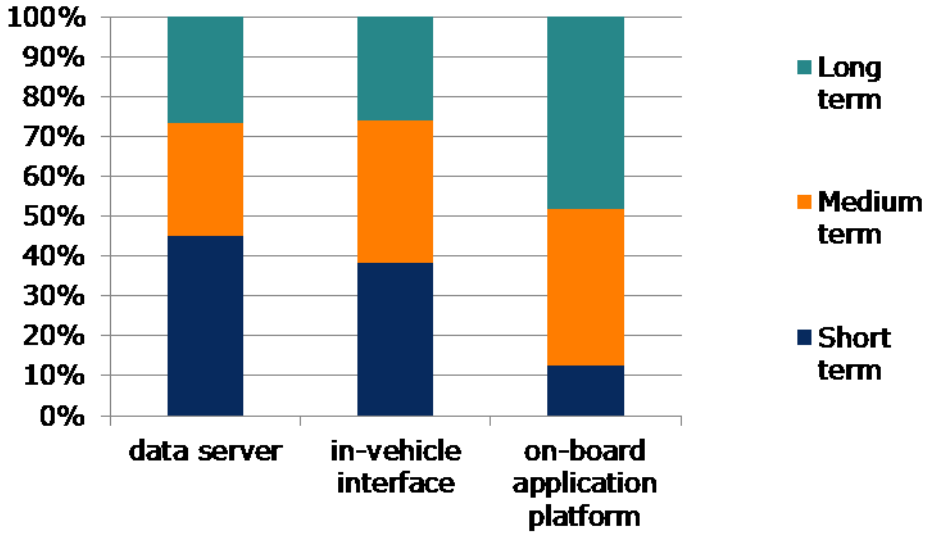
Since questions 1, 2 and 3 were not technical questions, the analysis commences at question 4.

Limitations:

1 The questionnaire surveyed people's thoughts and opinions to try and gain their insight. In some cases we can use quantitative analysis to draw conclusions, for example that the majority of respondents all gave a certain response. However, just because many respondents gave that answer it doesn't actually mean it is actually technically correct, nor if it's a prediction for the future that it will actually happen in that way or at that time. The responses provide insight from the state of the market opinion at this time only.

2 The responses given are often quoted or summarised below, and those responses may be technically correct or incorrect. In some cases, an additional technical note is given by TRL for clarification purposes.

4 Please can you indicate which of the three technical solutions (on-board application platform, in-vehicle interface and data server platform) you most support/prefer in the short term (2-3 years), medium term (4-7 years) and long-term (over 7 years)?



Generally, respondents favoured the data-server platform in the short-term and the on-board application platform the in long term. This reflects the general outcome of the C-ITS WG6 report.

5 Please explain your choice of preferred method for the short-term. Please consider benefits and costs as well as legal and liability issues.

Generally, respondents indicated that the Data server platform was the preferred short term solution because the technology and system is already in place, so benefits can be attained immediately using a secure system. Most respondents for this solution referred to the shared server concept as being the only acceptable data server platform solution.

One stakeholder indicated that they do not believe any of the proposed technical solutions can be implemented in a manner that complies with all five guiding principles within next 2-3 years (but that this would be possible in next 5 years).

Some respondents indicated a road-map approach whereby the short-term solutions of data server platform and in-vehicle interface would ultimately result in the on-board application platform. Commenting specifically on some of the stakeholder groups, those indicating a 'road map' approach were the Automotive associations/clubs, Insurance, and IT Infrastructure providers groups. However the Tier 1 supplier stakeholder said the exact opposite, which highlights that the future predictions are somewhat unclear.

The OEMs indicated that the data server platform would be the solution in the short, medium and long term; i.e. that there would be no progression or development.

6 Please explain your choice of preferred method for the medium-term. Please consider benefits and costs as well as legal and liability issues.

The majority view that the On-board application platform is the preferred option as it allows direct access to raw data in real time for all stakeholders. For data security, the implementation of a security layer with a connectivity control unit (CCU) is necessary. However, the time required to develop this should be much shorter than the time to

reach the next generation of cars in which the CCU should be implemented, not only for accessing data but also for ITS functionality and autonomous driving.

Some stakeholder views were that OEMs currently allow third party service providers the access to the vehicle by way of an on-board application platform (e.g. Google and Apple). The early systems would have not have accessed the vehicle data, and would only have linked the phone processing to the car HMI. However there is now more integration, with the connections being made to the vehicle data itself.

7 Please explain your choice of preferred method for the long-term. Please consider benefits and costs as well as legal and liability issues.

Responses for this question were the same as medium term responses

Please can you explain your view of the specific advantages and disadvantages of each of the three technical solutions (on-board application platform, in-vehicle interface and data server platform)?

8 Advantages of on-board application platform:

- Little or no hardware
- Apps can be installed by users
- Fair competition/non-discriminatory access
- Direct access to raw data in real time
- Easiest way to gain consent of driver
- Already exists (google/apple play) (TRL note: we are not sure that this is really the OB platform)
- Low latency
- Distraction issues can be managed effectively

9 Disadvantages of on-board application platform:

- Security risks – applications causing vehicle fault
- Malicious applications/viruses
- Not clear who would approve applications and on which criteria
- Longer lead time than the data server platform (some refute this and maintain that this is available immediately)

10 Advantages of in-vehicle interface:

- Real time
- No over the air data (Note: it can be if the connected device sends out data to e.g. an external server)
- Not monitored by OEMs

11 Disadvantages of in-vehicle interface:

- No access to car HMI – limitations on use/ potential increases in safety risk
- Requires hardware – cost and convenience (depends on connection type)

- Distraction from driving task
- Security – vulnerability to hacking. Malware could influence the performance of the electronic architecture and therefore the whole vehicle, resulting in potential risks for road safety and passenger safety.
- Vehicle manufacturers cannot fulfil their product liability obligations if third parties are (re-) designing the vehicle (TRL note: we cannot see how this would affect the OEM liability obligations as there are distinct responsibilities in the data chain)
- Vehicle manufacturers are unable to answer questions about the data that are accessed and processed by third parties. It is not clear who will be liable when issues arise. TRL do not agree and anticipate that the responsibilities can be clearly allocated.
- Specifications would be forced on vehicle manufacturers, who would need to fit them into their development plans. We think that it is likely that a minimum dataset would need to be specified (including its format) to allow access to the data for all the stakeholders. A specification for the interface would also be needed to allow connection from difference devices. The downside of the specification for an interface is that it might limit future development of systems, and a regulated specification might struggle to keep pace with technological developments, putting the end consumer at a disadvantage).
- Fair and equal communication with the customer is not possible because the manufacturer communicates using the in-vehicle display (HMI) and controls, while service providers using the in-vehicle interface would be restricted to smartphone communication (which is prohibited whilst driving) (Note: unless the vehicle HMI can be used by connection with the phone).

12 Advantages of data server platform:

- Short lead time, access for all stakeholders
- Security issues already controlled by OEM
- Monitoring issues/competitive advantage can be addressed by Shared or B2B derivatives

13 Disadvantages of data server platform:

- Limited number of participants can control prices (TRL note: competition law protects this area, but there are risks in terms of the effects of market distortion; see legal analysis)
- Data transmitted over air
- Costs for transmission
- High latency
- More difficult to gain consent

Extended vehicle

- Vehicle Manufacturers control all access to in-vehicle data, information and resources and consequently become the controller of the complete value chain of competing vehicle related service providers

- No direct access to the real-time in-vehicle generated data, functions and resources needed for time-critical services
- Excludes the possibility of providing 3rd party in-vehicle applications, limiting possible services, innovation, entrepreneurship and competition
- Data and services provided according to the policy of the Vehicle Manufacturer meaning that they control the development of new/competitive services
- Latency issues possible, due to poor internet connection (Note: also due to poor telecom network availability)
- Vehicle Manufacturers are able to profile the automotive aftermarket/business models
- Only the Vehicle Manufacturer has the ability to directly display services to the consumer via the vehicle HMI
- Additional costs and delays of accessing data

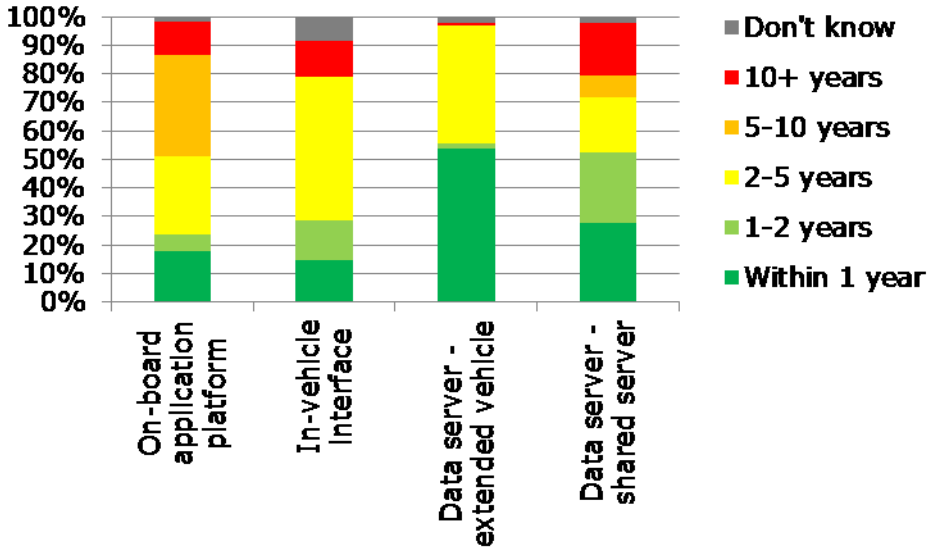
B2B Marketplace

- As extended vehicle
- One stakeholder responded "We see no benefits for third party service providers, as the access and content/quality of the data to provide services to the customer is controlled by the Vehicle Manufacturer"
- B2B platform may introduce additional market surveillance by the platform operator
- Also comments that this solution enhances the problems of Data Server Platform / Extended Vehicle because it adds another server and additional latency to the communication

Shared Server

- No direct access to the vehicle to implement 3rd party applications that can access real-time data or display services to the driver via the in-vehicle display (HMI). Only the Vehicle Manufacturer has the ability to directly display services to the consumer via the vehicle HMI
- Latency issues possible
- Data and services will be provided according to the policy of the vehicle manufacturer
- Additional costs of accessing data

14 Please provide estimates of the timescales for when each of the proposed technical solutions could be implemented at the earliest, i.e. how long after one of the technical solutions was selected could service providers expect to get access to the data?



The data server solution was most commonly expected within one year of selection, although a few thought it might take a few years longer. Although the data server platform already exists from purely the technical solution position, there are significant additional requirements from the contractual, legal, competition, and legislative position which will mean these solutions would not provide data until at least the 2-5 year window. The automotive associations and insurance groups, plus some of the OEMs and some of the road authorities thought it would take within a year. The remainder of the OEMs and road authorities thought it would take 2-5 years, along with the application service provider, trade body and repair & maintenance stakeholder groups.

On-Board Application Platform - 5-10 years; the current technology of hypervisors must be opened for 3rd party applications to access in-vehicle data, information, and resources. As additional features for IT security are increasingly necessary for today's vehicles (firewall, updates, automated systems, connection to backend servers) the costs and the development time for an On-board Application Platform can be significantly reduced.

The most common response was 5-10 years, although 2-5 years was a close second; this is seen as a mid-term solution by most respondents. The repair & maintenance, and trade body groups saw this as 2-5 years; IT infrastructure providers saw this as 5-10 years. The rest of the stakeholders were a mixture within the 2-10 year period. The OEMs thought it would be 10+ years.

In-Vehicle-Interface - 2-5 years; although the basic technology (dongles, e.g. connected to the OBD interface) is currently available, additional features for IT security are increasingly necessary for today's vehicles (firewall, updates, automated systems, connection to backend servers). The OEMs indicated that they thought it would take 10+ years to implement the in-vehicle interface solution after it was selected.

Data Server Platform / Extended Vehicle - 2-5 years; the technology is state of the art and already used by vehicle manufacturers; but note, that is not acceptable for many stakeholders, as it cannot provide compliance with the basic principles agreed in the C-ITS platform.

The responses here were split between implementation within one year, and in 2-5 years. The OEM response from ACEA was 2-5 years, with one other manufacturer indicating within one year.

Data Server Platform / Shared Server - 2-5 years; the data server platform technology is state of the art and already used by vehicle manufacturers; the private data are already separated in the Vehicle Manufacturer back-end servers today, so this could be migrated to the shared server.

The responses on timescale for implementation were evenly spread for this solution, ranging from within a year to 10+ years. The OEM response was 10+ years. The Repair & maintenance group though 1-5 years, whereas the automotive associations and clubs thought within 1 year. So there are some vastly differing responses from those groups involved with the vehicles.

15 In your view what are the main benefits (in terms e.g. of economic, societal, environmental, liability, and effects on small and medium-sized enterprises) arising from each of the three technical solutions for the following groups of stakeholders?

Main benefits to society / the public / service users of…

Many respondents produced similar or identical responses indicating collaboration. In particular, the 'repair & maintenance' respondents had produced an agreed response. Specific (monetised) benefits were not provided by any of the stakeholders. However, areas of benefit were identified as follows:

On-board application platform

- Economic: Allow independent entrepreneurship and new business innovation opportunities for all app developers and all existing and new service providers to develop service offers and present them to the driver via the in-vehicle display of the vehicle (HMI).
- Societal: Multimodal transport management and interoperability, public health, driving improvement programmes, reduction in road hazards/accidents and geo-fencing.
- Environmental: Remote assistance for eco-driving and ensuring minimum vehicle emissions and support independent assessment of type approval environmental compliance.
- Effects on Small and Medium Enterprises: Independent development of new business models and services, direct access to customers; fair competition, no monitoring of customers and service providers by the vehicle manufacturer as a competing service provider, with the possibility to display competing services to the driver via the in-vehicle display (HMI). Independent aftermarket ensures customer rights to choose from competing service providers.
- Main benefits to society/public/service users: Affordable mobility and convenience through the choice of competitive service providers (even in remote areas), including the ability to continue to support independent innovation, without being dependent on your competitor.

In this solution, every service provider would be liable for their own product or service and would follow Vehicle Manufacturer SDK guidelines, verified applications and trusted servers and 'state of the art' security strategies (https, VPN etc.) for data exchange

between the server and vehicle. Additionally, the in-vehicle functionality would include 'hypervisor' functions that silo operating systems and applications, as well as using constant monitoring of the application implementation. Vehicle manufacturer (or their designated test centres) would remain responsible for the validation of 3rd party applications.

In-vehicle interface

Respondents indicated the same benefits as for the On-board application platform.

Some views that this was the "second best" solution with respect to competitiveness because there was no access to the HMI of the vehicle (TRL note: there could be access to the HMI under certain circumstances).

Data server platform

Respondents indicated that this solution could be implemented in the short term as the Vehicle Manufacturers use this method currently.

One respondent indicated that it provided standardised access to data, including support of smartphone applications, without compromising security, safety or the vehicle manufacturers' liability. They indicated that the model complies with the five guiding principles agreed in the C-ITS final report of phase 1 (data provision conditions, fair and undistorted competition, data privacy and protection, tamper-proof access and liability, and data economy). This contradicts answers to question 14 from other stakeholders.

16 Main benefits to vehicle manufacturers of…

On-board application platform: Offering the customer a tailored solution.

In-vehicle interface: The In-Vehicle-Interface may be provided by using the OBD plug. The benefit for the Vehicle Manufacturers is that the consumer may prefer the OEM solution offered via the dashboard of the vehicle rather than the more 'inconvenient' OBD connection.

Data server platform (Extended Vehicle): Low implementation costs as the technology is already in use. Control of vehicle data and access to the customer.

Data Server Platform (Shared Server) Low implementation costs, as the technology is already in use. Full control of the data from-/to the vehicle. Vehicle Manufacturer is part of any business model related to in-vehicle-data over the lifetime of the vehicle

Data Server Platform (B2B Marketplace) No additional implementation costs, as the B2B Marketplace is financed by the independent repair & maintenance sector. Full control of the data from-/to the vehicle. Vehicle Manufacturer is part of any business model related to in-vehicle-data over the lifetime of the vehicle. Direct and exclusive access to the customer over the lifetime of the vehicle

17 Main benefits to Tier 1 suppliers of…

On-board application platform: benefit from implementing additional hard- and software for the on-board application platform into each vehicle, thereby getting direct access to the customers to offer parts and components directly.

In-vehicle interface: benefit from offering the retrofit devices that need to be installed in each vehicle using an in-vehicle-interface, such as the OBD port. By getting direct access to the customers, suppliers have the possibility to offer parts and components directly.

Data server platform: **Data Server Platform / Extended Vehicle** no benefits for Tier 1 suppliers, as the access to the customer is controlled by the Vehicle Manufacturer. **Data Server Platform / Shared Server** The Tier 1 suppliers are able to offer services via smartphone apps direct to the customer using the shared server.

Data Server Platform / B2B Marketplace Similar benefits to the shared server.

18 Main benefits to third party service providers of…

On-board application platform:

- Access not restricted by OEM
- Direct communication channel with the customer, fair competition on level playing field between OEM and other service providers, easiest way to develop and offer new services (app-based), low cost level if the software development kit (SDK) is standardised for all OEMs.

In-vehicle interface:

- Assuming continued direct access via the standardised connector and the in-vehicle data, 3rd party service provider's suppliers can offer their services to the customer. The in-Vehicle-Interface is inconvenient to be used and therefore less attractive to customers, compared to the on-board application platform. Fair and equal communication with the customer is not possible because the manufacturer communicates using the in-vehicle display (HMI) and controls, while service providers using the in-vehicle interface would be restricted to smartphone communication (prohibited whilst driving).

Data server platform:

- Only receive data so limits innovation [Note: there could be a write access as well]
- No benefits for third party service providers, as the access and content/quality of the data to provide services to the customer is controlled by the Vehicle Manufacturer and there is no possibility to communicate with the customer using in-vehicle display (HMI) and controls
- **Data Server Platform / Shared Server** As services are made anonymous and therefore unknown to the vehicle manufacturer, the third-party service providers may offer their products via smartphone apps to the customer. However, the content/quality of the data to provide services to customers is controlled by the vehicle manufacturer, limiting innovation and competitive service offers.
- **Data Server Platform / B2B Marketplace** Perhaps greater problems compared with the Extended Vehicle because it adds another server and additional latency to the communication, adds additional costs to all third-party businesses.

19 Main benefits to any other groups of stakeholders of… (please specify which other groups of stakeholders may benefit)

On-board application platform:

In-vehicle interface:

Data server platform:

No further groups of stakeholders identified.

20 Any other comments relating to the above?

Some detailed comments were received in response to this question. One stakeholder set out a series of principles that should be met:

- The driver / owner must be in control of the data transfer from / to the vehicle
- The financial contribution to get access to vehicle data must be on a cost-oriented base
- All service providers must have non-discriminatory access to the data at the same time
- The FIA Region I asked 12.000 European consumers on their views on connected vehicles. 90% of the vehicle owners say, it´s their data; 91% like to switch connectivity on/off; 83% want to decide for how long and with whom they share data; 78% want to choose, who will repair their car. 95% want legislation to protect user data when it comes to connected vehicles
- All data and all services that the Vehicle Manufacturers offer as an aftersales service provider, must be accessible for the independent repair & maintenance sector. A limit or a reduction to a "day1" set of data or "emission related data" is not acceptable
- The independent repair & maintenance sector must reach the customer/vehicle driver in the same way as the Vehicle Manufacturer. Therefore, the access to the infotainment system for independent third-party service providers must be included in the scope of this "access to in-vehicle-data" campaign
- There are millions of connected vehicles already in the market. The interim solution via Shared Server needs to include these vehicles, too, if technically possible

Another responded commented:

"Comments on Data Server Platform / Extended Vehicle - Vehicle generated data – especially combined with user information – has become increasingly important for the entire automotive value chain. The market position of a company is significantly influenced by its access to data and the functionalities inside the vehicle that operate using this data. Consequently, it is necessary to find solutions to ensure equal opportunities for all market players on the digitalised market. European legislation identified this necessity early on and created with the eCall Regulation (EU) 2015/758 the basis for the legal basis for an interoperable, standardised, secure and open-access telematics platform (article 12 (2)). From the Independent Aftermarket's point of view it is inevitable to stipulate precise legal requirements and standards for such a platform (on-board telematics system). There is an urgent need for a framework granting standardised and direct unrestricted access to vehicle generated data and functionalities/resources for all market players. The Extended Vehicle concept however does not meet these requirements. It treats the vehicle manufacturers and their chosen partners as privileged parties and provides them with an objectively unjustified competitive advantage over

other market players whose business models include services of the same kind. Only balanced and fair competition between all market players will provide consumers with the greatest possible advantage when using digital services. - -

2. Competitive effects of the Extended Vehicle concept - Access to data and functionalities/resources already represent today decisive factors for companies when it comes to maintaining their market positions and to establishing innovative, digital business models for the benefit of the consumer. It is needless to say that the quantity of data and functionalities/resources will grow rapidly in the future and thus increase the dependence of entrepreneurs on such innovations. Any access barriers or restrictions concerning the access to data functionalities and resources that complicate a direct and independent communication with a vehicle will therefore significantly influence free competition and the competitiveness of the digital single market players. This however is exactly the key aspect of the Extended Vehicle concept which implies a transfer of the telematics platform to an external server held by the respective vehicle manufacturer outside the vehicle. The implementation of the Extended Vehicle concept would treat vehicle manufacturers as privileged players in many respects over other competing parties and thus lead to considerable competition restrictions. - The following severe restraints on competition are mentioned by way of example:

a) Access to data functionalities/resources exclusively via the vehicle manufacturer (a competitor). The vehicle manufacturer has unrestricted access to all vehicle generated data, functionalities and resources at any time – directly via the on-board telematics system. Third parties (especially diagnostic tool manufacturers) however are not granted equal access conditions. Instead, they have to access the data via a server of their competitor (the vehicle manufacturer) in order to receive the data they need. Since vehicle manufacturers offer their own competing products for numerous telematics services, exclusive control of access to vehicle generated data via the vehicle manufacturer has in principle an immediate and significant negative competitive relevance. It is immediately evident this would cause an unjustified disadvantage to competing market players whilst expressly benefitting the vehicle manufacturer at the same time - vehicle manufacturers cannot be the service generator and the service provider at the same time! - -

b) Third parties without equal access to the same data/functionalities/resources - Due to the privileged access to all vehicle generated data and the possibility to process this data in the telematics system, vehicle manufacturers have 100 percent of the data available at any time (data quantity and quality). In comparison, third parties (their competitors, such as diagnostic tool manufacturers) only have access to some of the vehicle data via the server of the vehicle manufacturer. On the way from the vehicle to the server of the vehicle manufacturer and from that server to the server of the third party, the data is inevitably subject to technical restrictions (e.g. additional latency) which is why third parties only have access to a limited data quantity (limited amount of bandwidth using mobile communication) and data quality – completely insufficient to run diagnostic test routines. In addition to these technical restrictions vehicle manufacturers would moreover be able – due to the data collection on their own servers – to decide on access, waiting times, nature, quality and offered extent of access to in-vehicle data, functionalities and resources. This would complicate the development of services for third parties – if not make it entirely impossible. If the access to data is denied, limited (data packets) or only delayed, this represents a clear restriction of competition at the expense of third parties who need certain data swiftly to carry out their business activities efficiently, if it all, but do not have the required access.

c) Freedom of choice for the customer - This would be to the detriment of third parties which are looking forward to innovate but also, and above all, of the customers who would lose their freedom of choice for competitive services.

d) No access to real-time in-vehicle generated data - The Extended Vehicle concept makes it impossible for other market players to access real-time data, such as time-critical or highly available vehicle data needed by diagnostic tool manufacturers. Only vehicle manufacturers have this opportunity as they are not restricted by the Extended Vehicle concept but have direct access to the on-board telematics system and in-vehicle data and algorithms and can therefore implement their own diagnostic test routines directly in the vehicle. The usability of time-critical data is highly dependent on an immediate transmission. High availability means that a multitude of new data is created in rapid succession. The engine speed typically fulfils both of these criteria. In this example, vehicle manufacturers would exclude all service providers depending on a real-time transmission of engine speed information from competition. Furthermore, real-time data will play a

central role in the future, e.g. for the further development of road safety. Examples include information about traffic light phases, construction sites and accidents. The same applies to telematics services concerning trip convenience, such as information about the search for a parking place and for anticipatory driving. Access to this data is of critical importance for providers of such services.

e) Exclusion of market players by means of telematics contracts - Concluding a so-called telematics contract with the vehicle manufacturer is the precondition for using all telematics services. If the user does not sign this contract, the external communication of the vehicle is deactivated by the vehicle manufacturer. Having to sign a contract with the vehicle manufacturer forms the pre-cursor basis of unfair competition and market monitoring. These telematics contracts are presented to the customer for signature along with the sales contract and often include various mandatory services. Due to the link with services offered by the manufacturer – requested by the customer or not – third parties have effectively no more opportunity to afterwards offer their comparable services to the consumer. The initial contact to the customer and the content of the telematics contract thus represent a considerable competitive advantage for vehicle manufacturers. They are for example able to send offers and invitations to the on-board information display. Third parties are unable to do that. Via information on the display, the driver could be specifically routed to a manufacturer-owned workshop in case of a breakdown instead of to a franchised dealer, or - if requested by the driver - an independent workshop. As a result, consumers are effectively dependent on a monopolistic offer by the vehicle manufacturer. Consequently, innovation and competitiveness in the aftermarket are significantly restricted.

f) Exclusion of market players by means of exclusivity agreements - Vehicle manufacturers could moreover conclude exclusivity agreements with single providers which would make it impossible for competitors to access certain-vehicle data. Third parties would thus be substantially dependent on the commercial policy and the business models of vehicle manufacturers and would have to adapt their business activities accordingly. The consequence would be a significant restriction of the competitiveness in the aftermarket. -

g) Control and supervisory options of the vehicle manufacturer - According to the Extended Vehicle concept third parties only have access to the vehicle via an external server held by the vehicle manufacturer. A direct and unlimited communication between these providers and the vehicle owners would as a result be impossible. This would represent a clear distortion of competition in favour of the vehicle manufacturer. If vehicle manufacturers can constantly control all details regarding the performance and use of the services of their competitors, this as well represents a massive distortion of competition. Vehicle manufacturers could not only analyse the customer and competitors' behaviour but also see their prices and react accordingly. Moreover, they could analyse the customers' buying habits and their willingness to pay for certain products and services. On that basis, they could establish adaptive pricing models tailoring prices to certain groups of customers, locations services and strength of competition. The afore-mentioned examples clearly emphasise how competition would be substantially restricted in case of the implementation of the Extended Vehicle concept. Additionally, the market-dominating position of the vehicle manufacturers regarding vehicle generated data would be manifested.

3. One difference identified between the inside-the-vehicle and outside-the-vehicle technical solution is in their support for "real time applications."

To help us to understand these differences, please could you explain what you mean by 'real time'? (i.e. what is the likely actual technical performance of typical solutions such as latency?)

There were very diverse views/definitions of "real time" within the stakeholder group which indicates that different participants have very different ideas about the systems which require data termed as 'real time'. These definitions ranged from "real-time can be seen as up to 5 minute old data" to "whilst there is always some level of latency, 'real time' should be understood to mean any time in the sub-second range".

One stakeholder reiterated that the latency issue is only for "data server platform" solution and not for in-vehicle interface or on-board application platform.

Another stakeholder was of the view that 'real time' date was not required and that 90%+ of use-cases could be satisfied without real-time data.

21 Please give any specific examples of services that cannot be supported by outside-the-vehicle solutions:

A range of examples were provided and there were differing views on whether any services would be excluded by data server solution. The following examples were provided of services that could not be supported:

- Insurance-related guidance to the driver based on the way the vehicle is being driven because Insurers should receive the data from the vehicle, process this data and send the feedback to the driver in less than 1 second.
- One stakeholder referenced RMI information
- Any application that is recognised in the list of Day 1 services of the ITS-platform. Also a large amount of those in the services recognised for Day 1.5 and beyond
- Safety critical systems (platooning, crossing AEB etc.) were also mentioned by a few stakeholders (TRL note: we feel it is very unlikely that these would ever be implemented via this approach and would be responsibility of OEM only)

One stakeholder commented that "the extended vehicle as defined in draft ISO standard 20077 contains not only a web interface (or data server platform, draft ISO standard 20078) but also other interfaces, one or more of which could be used for real-time applications. Consequently, the extended vehicle can support all possible use-cases." [Note: certainly, but then it is no longer an outside-the-vehicle solution only.]

22 The C-ITS report states 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 the vehicle manufactures at least for as long as these security issues persist". What practical steps are required to solve these security issues?

A range of responses were received; these included the following:

- Implementation of a gateway and security layer including authentication function. For future cars, which will be connected to take advantage of C-ITS functionalities or autonomous driving functions, this gateway and security layer is necessary.
- The Extended Vehicle concept is based on proprietary links between vehicle and OEM cloud and there is no standardisation for this interface. This makes it impossible to protect, and it will remain a major security gap.
- Liability - We do not share the view of Vehicle manufacturers, that they are solely liable for the access to in-vehicle-data. Anybody who offers services is liable for those services. This should be transferred from today´s business to Internet of Things (IoT) business. The vehicle manufacturer is responsible for the safe and secure operation of the vehicle. He needs to set a transparent protection profile for any service developer in a standardised SDK. The service developer is then liable for the service he offers. - - 2. Practical steps required to solve the security issues - a) all stakeholders should develop a risk analysis, starting from the in-vehicle-network to the infotainment system and Apps and ending after the Over-The-Air (OTA) to the end user of the information - b) Define a protection profile,

that is required to fulfil all risks discovered - c) Define a type approval process, according to which the authorities can check the evaluation target of each single manufacturer against the protection profile - d) Define an update process, for security updates of the vehicle and the platform - e) Define a process on how to handle security gaps that are detected and need to be closed asap - f) Define an "end of life" process for the on-board application platform - d) Define a registration, authentication and authorisation process for vehicle owners, in order to secure that only the right person can steer the data transfer from/to the vehicle -

23 Do you have an estimate on the timescale of security issues being addressed?

Respondents provided a range of responses from "solutions are already available" (three responses) and "We estimate a timescale of three years, after an agreement on a methodology (standardisation-process) and further two years for the implementation into vehicles" (13 responses) and "we estimate a timescale of two to four years, for agreement on a methodology (standardisation-process) and implementation into vehicles." (2 responses)

24 Can you estimate the cost (please specify currency if different from Euros) for adding a security layer for each of the proposed technical solutions?

Very few quantitative costs were received for adding the security layer to each of the proposed technical solutions. The responses included:

- Experience collected in the e-Call were costs of approx. 140 EUR per vehicle covering all involved cost for the e-Call technology in the vehicle. For the Access to Data discussion a detailed estimate is not available. A first indication at the commission assumed costs of 100 EUR per new vehicle for a secure e-Call connection.
- This is difficult to estimate as it might be different from OEM to OEM. Security is already integrated part for OEM data server platforms.
- The cost varies depending on the level or scale of measures to be taken, making it difficult to estimate it at this stage. However, the security level is expected to be raised years after year, which will affect profitability.
- Next to the costs for the standardisation, we see costs for developing and implementing hard- and software into the vehicles, as well as keeping them up to date over the lifetime of the vehicle. We see a medium invest for vehicle manufacturers as the technologies are available on the market (Security layers, HSM, Firewall, Hyper Visor Technologies), but not yet adapted to vehicle technology. Next to that the automation of vehicles and the connectivity will lead to higher IT-Security in-vehicles. This can compensate the costs for an on-board application platform.

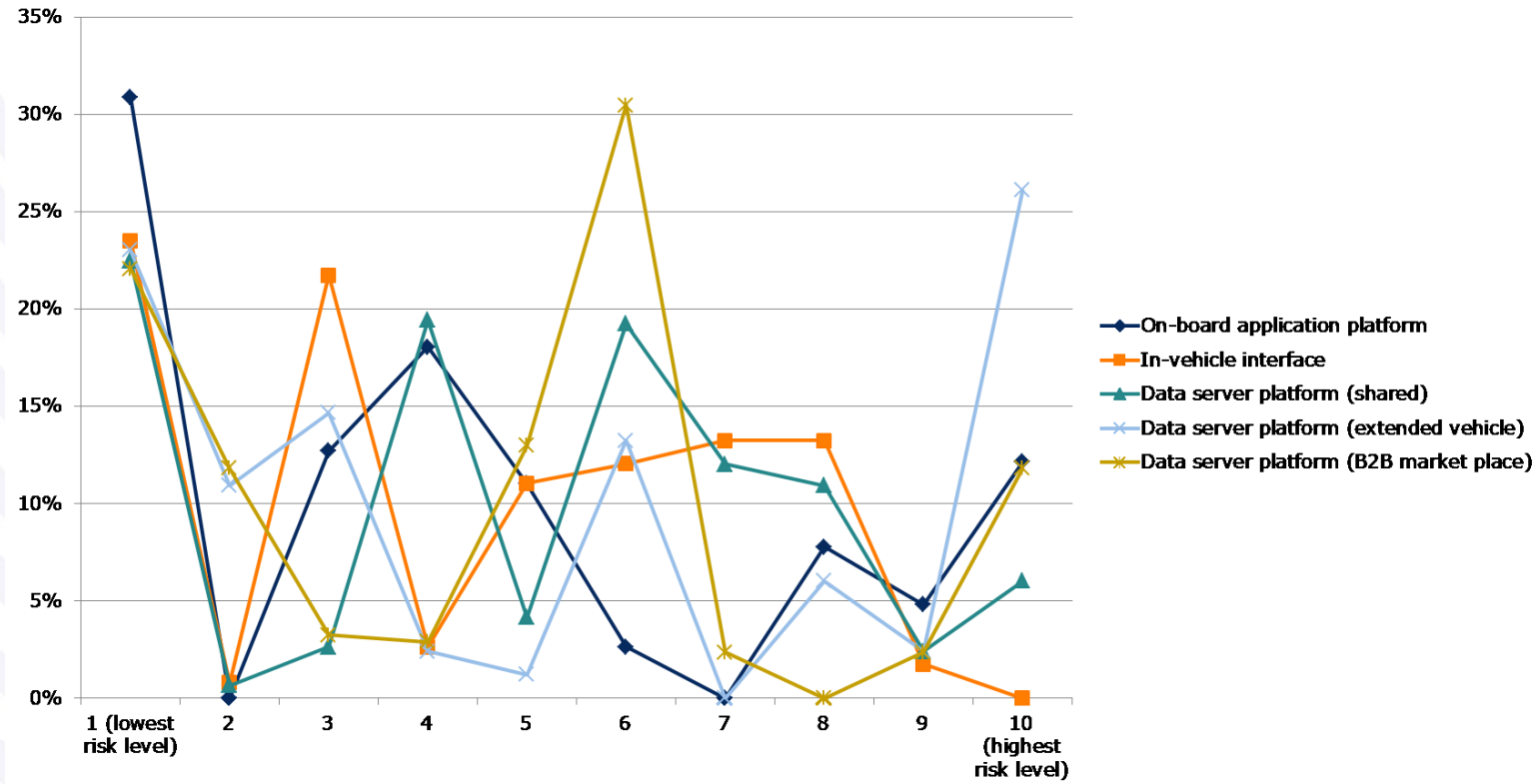
25 What are the benefits, if any, of adding a security layer to each of the technical solutions?

Each of the technical solutions has to come with a complete security concept. If this requires an additional security layer, then the original technical concept is not correct. Each of the technical solutions has to have a proper security concept, including, but not limited to the usual key components: Access control, Identity management, communication encryption, public key infrastructure and use of hypervisor layers for proper and safe runtime execution checks.

26 Please try to quantify the relative risks of the three technical solutions in terms of cyber security on the following scale, where 10 is the highest risk:

The responses to this question were varied and exhibited diverging responses; the same technical solution was perceived to have low risk by some stakeholders and high risk by others. The table below provides the perceived risk level of each technical solution on a scale of 1 to 10, where 10 is the greatest risk. The variation in the responses meant that it was difficult to draw conclusions about the risk conferred by each solution and it is considered that the more general views of the stakeholders on the technical solutions may have influenced the rating of risk.

	1 (lowest risk level)	2	3	4	5	6	7	8	9	10 (highest risk level)	Grand total
On-board application platform	30.88%	0.00%	12.69%	18.04%	11.03%	2.64%	0.00%	7.76%	4.81%	12.14%	100.00%
In-vehicle interface	23.51%	0.79%	21.73%	2.65%	11.04%	12.04%	13.25%	13.25%	1.76%	0.00%	100.00%
Data server platform (shared)	22.48%	0.66%	2.64%	19.43%	4.16%	19.24%	12.03%	10.93%	2.41%	6.01%	100.00%
Data server platform (extended vehicle)	23.03%	10.93%	14.67%	2.41%	1.21%	13.23%	0.00%	6.01%	2.41%	26.10%	100.00%
Data server platform (B2B market place)	22.07%	11.81%	3.24%	2.90%	12.99%	30.46%	2.36%	0.00%	2.36%	11.81%	100.00%



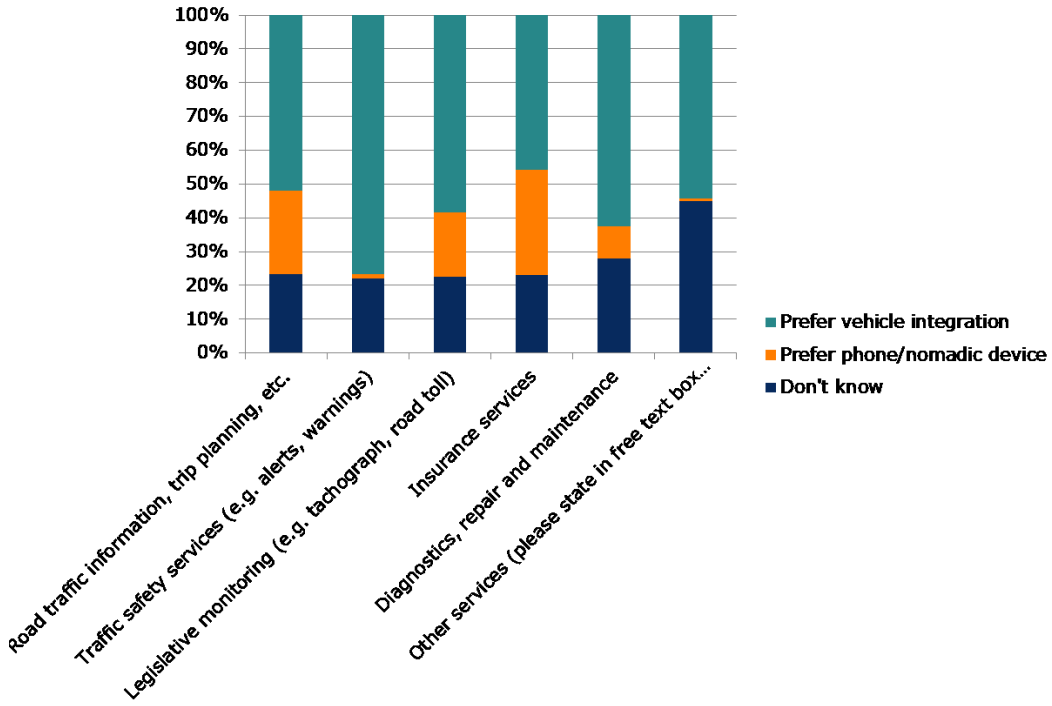
Please provide a rationale for your ratings:

- *Generally: same risk for all solutions should security measures (including authentication) which are state of the art being implemented in all connected cars this will be (besides the question of connectivity) essential for autonomous driving.*
- *All these solutions have the same risk level in terms of cybersecurity. This level will be lowest provided security by design is ensured for any solution.*
- *Only a standardised security concept with security targets and key components set out by external authorities can guarantee an independent and high level of security. Thus, the on-board application platform with its end2end-concept has the highest, level of security, independent of the vehicle manufacturer. Applications undergo a defined testing process at the vehicle manufacturer following standardised best practise test procedures. During run time of the third-party application in the vehicle, the vehicle security system (e. g. hypervisor) makes sure that no harmful function calls or data request are issued against electronic control units (ECUs).*

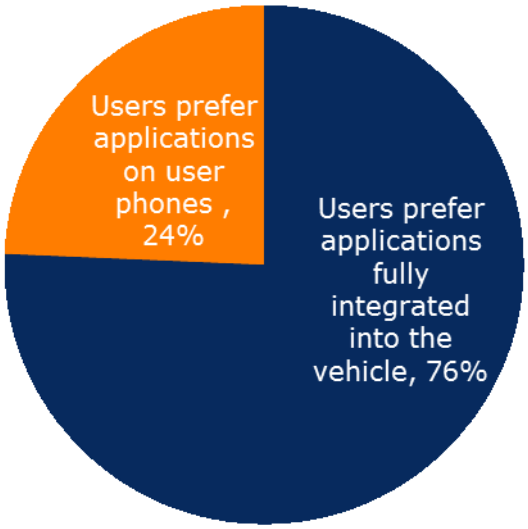
27 What are your views on whether users would prefer applications on their phones or fully integrated into the vehicle, for the following types of applications?

	Prefer vehicle integration	Prefer phone/nomadic device	Don't know
Road traffic information, trip planning, etc.	☐	☐	☐
Traffic safety services (e.g. alerts, warnings)	☐	☐	☐
Legislative monitoring (e.g. tachograph, road toll)	☐	☐	☐
Insurance services	☐	☐	☐
Diagnostics, repair and maintenance	☐	☐	☐
Other services (please state in free text box below)	☐	☐	☐

Respondents indicated that overall, vehicle integration was preferable in all instances although some stakeholders acknowledged that some users may use a phone/nomadic device for road traffic information and trip planning, insurance, and road tolls. There was a strong preference for traffic safety services to be integrated into the vehicle.



28 **What are your views on whether, in general terms, users would prefer applications on their phones or fully integrated into the vehicle?**



Comments:

General comments were that functionality would be safer if controlled within the vehicle. Use of mobile devices/HMI whilst driving should be prevented.

Comments were also made that both options should be possible with transfer between the mobile device and the car HMI. So when the user is in the vehicle and driving, then the in-vehicle application version is displayed on the HMI with a potentially extended functionality and using in-vehicle controls. When not driving the user can control parts of the application using a smartphone. This stakeholder also noted that users prefer having

the same Graphical User Interface (GUI) and the same applications running on the phone as well as in the infotainment systems.

Use-cases / minimum data set

Working Group 6 of the C-ITS platform summarised the position on two approaches to define specific data made available to applications, with this being defined on the basis of specific 'use-cases' (the data required for the specific application) or a harmonised minimum dataset (a larger sub-set of data covering the majority of applications). The data made available to applications is independent of the three technical solutions. That is, data provided using specific use-cases or a minimum data set can be used with the data server platform, in-vehicle interface or the on-board application platform.

In your view, what are the benefits (e.g. economic, societal, environmental, liability, effects on small and medium-sized enterprises) of access to data on the basis of...

29 ...specific use-cases:

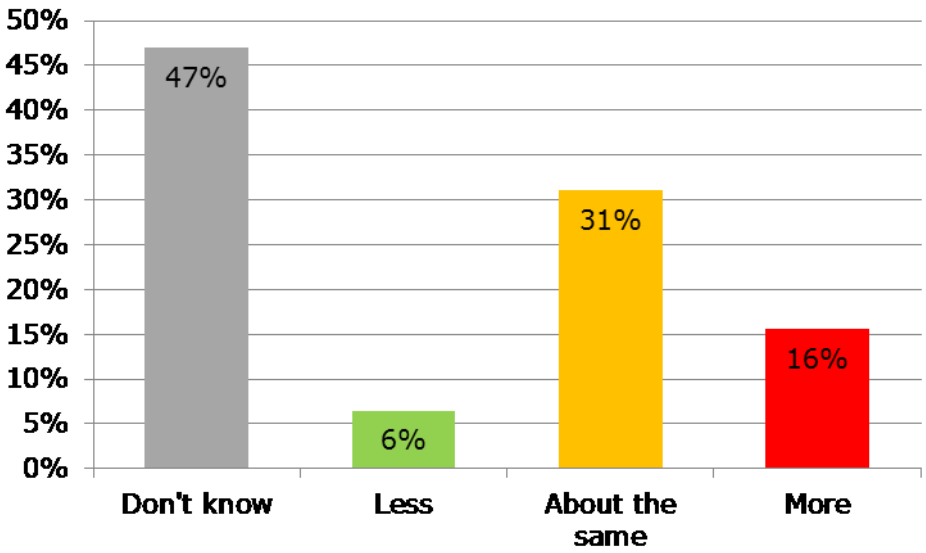
- Privacy and control over data usage
- The dataset can be specified exactly for each use-case. One good example is the draft ISO standard 20080 which specifies the information for remote diagnostic support. It is also easy (Note: but may be lengthy if 2-3 years of standardisation are need for each new use-case) to add new use-cases with potentially new datasets as and when new use-cases or types of applications are developed. Another important advantage is that providing data access on the basis of specific use-cases makes it considerably easier to comply with EU data protection legislation. This is necessary whenever the dataset contains personal data such as the vehicle identification number (VIN). Legally, such personal data can be transmitted to third parties only with the consent of the vehicle user provided he or she knows who the recipient is and for which purpose the recipient will use the data. Making information available for specific use-cases will ensure that the purpose for which the data will be used is clear in every case.
- There were also views that this option would encourage innovation, differentiation between the various players, but that this should be an add-on to a minimum accessible data set which is fully transparent to all players.
- Stakeholders also mentioned disadvantages of use-case approach because by describing the use-case to the OEM, information on the new business model is also transferred to the biggest competitor. Furthermore, if each use-case must be approved individually, innovation is restricted.

30 ...a harmonised minimum dataset:

- Larger potential for developing innovative applications as data is available and can be used in the creative process.
- Maximum freedom of choice for the customer; no monitoring or potential interference in the development of new /advanced services.

31 Is the cost of providing access to data on the basis of specific use-cases more, less, or about the same compared with costs for a minimum dataset?

Most respondents indicated that costs were considered about the same:



Please explain your response:

- Some views that the use-case approach would be more costly because it is subject to each vehicle manufacturer's interpretation and that these are bound to differ, thus making this process more onerous to all stakeholders involved.
- Others thought that the use-case approach would be cheaper because the agreement of data for a use-case would require less negotiation than agreeing an entire minimum dataset.

Overall, the split between 'don't know' and another answer (less, same, more) was about 50:50. This indicates that the respondents were not sure, and this response should be used with caution.

32 Please can you estimate the cost (please specify currency if different from Euros) for providing access to in-vehicle data via use-cases (for example remote diagnostics) for applications in the…Short term (2-3 years):

No specific cost estimates were received. The general response was that the costs would be "low" because the technology is already available.

33 Long term (4-7 years):

Similar to responses to Q33

34 Please can you provide estimates of the costs (please specify currency if different from Euros) and staff time for providing access to in-vehicle data via use-cases in terms of hardware, software, and yearly operation

Responses to this question were not well answered with many respondents not providing cost estimates. The only figures received were:

- Hardware –100 Euro: comment that this is already available
- Software - Already available at 'marginal cost'

- Annual operating costs – no estimates received

Rationale:

General feedback was that it was not possible to quantity costs without significant work. Many factors are needed to provide results.

35 Please can you estimate the cost (please specify currency if different from Euros) of providing access to in-vehicle data on the basis of a harmonised minimum data set in the…

Short term (2-3 years):

No specific costs, indications that these would be "low"

36 Long term (4-7 years):

No specific costs, indications that these would be "low"

37 Please can you estimate the cost (please specify currency if different from Euros) and staff time for a harmonised minimum dataset in terms of hardware, software, and yearly operation

Hardware – already available 100 Euro. Other answers that costs could not be provided or were not possible to determine.

Software and annual operating costs: no values provided

Data server platform

38 What technical issues, if any, do you see with the data server platform?

- Any kind of data server platform should not be under the control of only one stakeholder (i.e. vehicle manufacturer). Such a platform should be operated by an independent trusted third party or a consortium of the platform users.
- Comments that technically and commercially feasible to set up one or more "neutral" servers operated by third parties independent from the vehicle manufacturer. The operator(s) of such a neutral server would need to conclude a B2B agreement with one or more vehicle manufacturers. This agreement should include clear arrangements regarding matters such as data availability and quality, transmission costs, security and the protection of personal data. Views that it is not practicable to set up a shared server operated by a consortium of stakeholders because this would lead to lengthy discussions between stakeholders with different interests, which could cause problems when rapid action is required, for example to deal with security issues.
- Also comments in general that the type of model is not so much a technical question, but an issue of business models.

Please can you indicate the benefits (in terms of economic, societal, environmental, liability, and effects on small and medium-sized enterprises) of...

39 Data server platform – the shared server?

- No monitoring of business models by OEM; no difference in data access between all stakeholders, thus guaranteeing fair competition.
- The availability of the neutral server should facilitate data access in particular for small and medium-sized companies by offering multi-brand data access on one server rather than obliging them to use multiple servers of individual manufacturers

40 Data server platform – the extended vehicle?

- Liability, the OEM has clear responsibility for the data and for the user it is clear who to communicate with for questions regarding data usage.
- No benefits for the repair and maintenance sector, as data is controlled by the vehicle manufacturer who has a direct conflict of interest as a competitor in the vehicle related services market.

41 Data server platform – the B2B marketplace?

- The availability of the neutral server should facilitate data access in particular for small and medium-sized companies by offering multi-brand data access on one server rather than obliging them to use multiple servers of individual manufacturers.
- Some views that there would be no benefits for the repair & maintenance sector, as private data of vehicle owners are still under the control of vehicle manufacturer. Difficult to implement as all stakeholders would need access.

42 Please can you list the components required for the data server platform?

The responses included:

- Proprietary links from vehicle to OEM cloud. Simple database for operations. CRM for billing and invoicing users
- The components of the data server platform (extended vehicle web services) are described in the draft ISO standard 20078. The other components of the extended vehicle are described in draft ISO standard 20077.

43 What would be your best estimate of the costs (please specify the currency if different from Euros) for staff, hardware, software, maintenance, operation, security and hosting for...

	The shared server	The 'extended vehicle'	The B2B marketplace
Staff cost	_____	_____	_____
Hardware	_____	_____	_____
Maintenance	_____	_____	_____
Software	_____	_____	_____
Operation	_____	_____	_____
Security	_____	_____	_____

	The shared server	The 'extended vehicle'	The B2B marketplace
Hosting	_____	_____	_____
Other (please specify in text box below)	_____	_____	_____

Low for all

Comments:

No cost information received. Comment that 'Backend solutions' require much less cost compared to in-vehicle solutions, as one server connects many vehicles. Even multiple servers will not raise the costs significantly compared with costs for changes to each vehicle.

44 Please could you outline your intended charging policy for providing access to in-vehicle data?

General view that any charging policy should be non-discriminatory and purely cost-based. The charging policy should simply provide fair compensation to the vehicle manufacturers for the actual costs incurred (investment, connectivity and data operating).

45 Would the charge closely reflect the actual costs?

The respondents responded yes to this question in line with guiding principles agreed in the C-ITS WG 6 which include fair and undistorted competition.

46 Can you describe the process you would follow to derive the charge?

Responses were sparse and where a response was given, generally indicated that this was not the responsibility of the stakeholder providing the response. No specific method or process to derive the appropriate charge was identified.

One response indicated that the process should be guided by the guiding principles agreed in the C-ITS Platform's WG 6 which include fair and undistorted competition: "all service providers should be in an equal, fair, reasonable and non-discriminatory position to offer services to the data subject". This respondent also indicated that an independent entity would need to be consulted to review the charge in light of the operational costs.

47 Cybersecurity is stated as an advantage of the data server solution. If possible, can you quantify the risk or explain the cyber concerns in greater detail?

Some views that all the solutions have the same risk level in terms of cybersecurity and therefore improved cybersecurity is not necessarily an advantage of the data server platform. Regardless of the solution envisaged, security by design should be the starting point.

Repair and maintenance stakeholders indicated that they don't see an extended vehicle having an advantage in terms of cybersecurity over other approaches. If it is limited to read-only-access to data, then it is not a viable option in terms of fair competition. If it is enhanced and offers read and write access, then the Extended vehicle offers a single point of failure. Furthermore, the Extended vehicle currently doesn't adhere to neutral security standards, instead, the security is only in the responsibility of the vehicle manufacturers with known limitations and various hacks in the past. Are there any applications that you think will not be supported with the data server platform approach? If yes,

please list these specific applications and state why you think will not be supported with the data server platform approach:

Stakeholders provided the following examples:

- Accident notification, driver coaching, information to driver, contact to customer via display. Reasons: no real time access, no access to raw data, no access to on-board screen.
- Diagnostic tests that need real-time data access. Eco Driving apps including CO2 and NOx measurement. Apps using dynamic related data like PAYD, PHYD. Safety related apps that are highly time critical. All apps that do not meet the policy of the VM. C2C-communication applications, for e.g. collision avoidance, platooning . CIC-communication applications for e.g. inner city traffic optimization at crossroads.
- Application that requires a latency of several 100 ms for an event leading to an accident which takes a few seconds to occur - Ex: crossing collision prevention, right/left turn collision prevention, rear-end collision prevention, motorcycle approaching indication.

(TRL note: we do not find these examples convincing on the available evidence; either these are not real time and do not exclude the possibility of the data server, or they are functionalities so critical to the control of the vehicle that there are doubts that these may ever be implemented by anyone other than the vehicle manufacturer).

48 For the data server platform how many servers would there be?

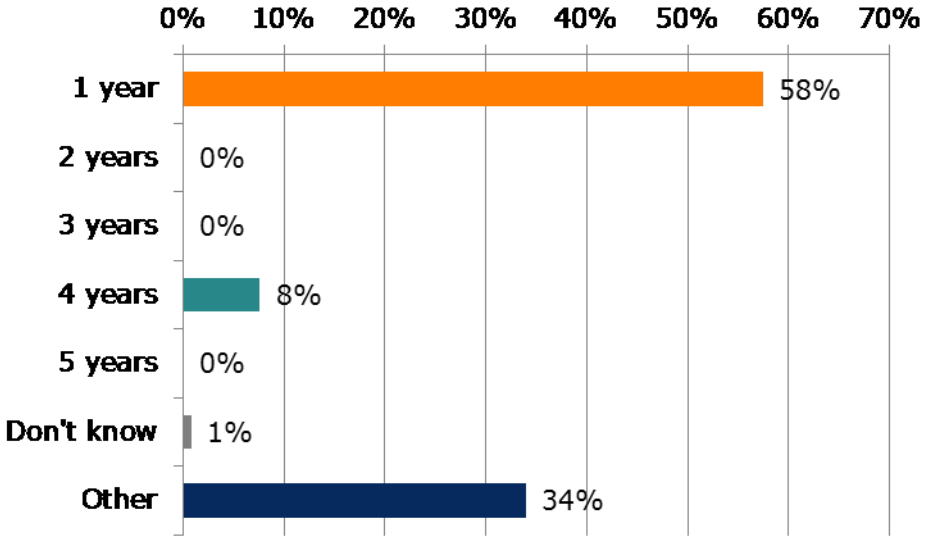
- ☐ One server per vehicle manufacturer
- ☐ One shared server for all vehicle manufacturers
- ☐ One server per vehicle manufacturer and one shared server
- ☐ Don't know

Those that responded other than "don't know" indicated that there would be one server per vehicle OEM.

Comments:

One stakeholder proposed a "neutral" server that would be operated by a third party that is totally independent from the vehicle manufacturer. This third party would operate that server on a commercial basis and conclude a B2B agreement with one or more vehicle manufacturers with due regard for security and the protection of personal data. In reality, it is not possible to estimate how many physical servers a vehicle manufacturer would have, nor how many neutral servers there would be.

49 Can you estimate a timeframe ranging from a period of 1 to 5 years when data encryption between the vehicle and data server platform will be assured?

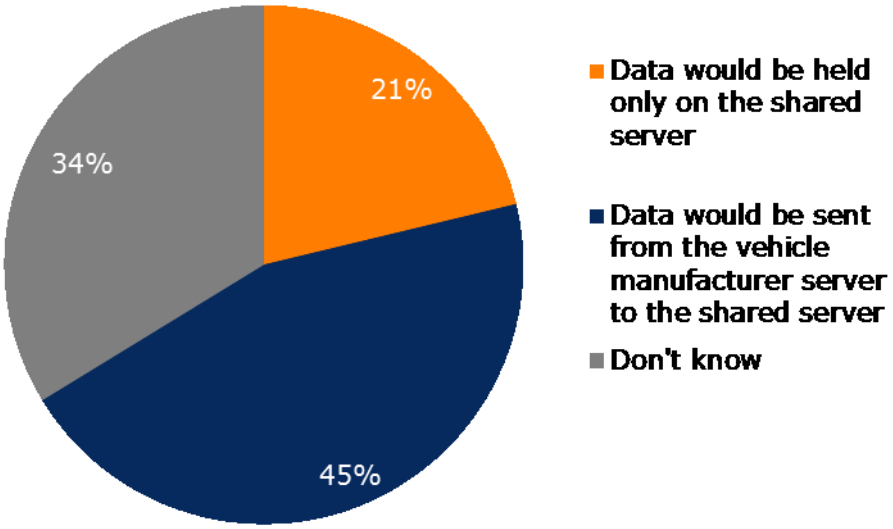


Comments:

- The timeframe when such data encryption will be assured will depend on each vehicle's technology, with some vehicles already able to handle such communication.
- Encrypted data transmission between the vehicle and the vehicle manufacturer's server is current state of the art and already widely used. Encryption is a pre-requisite for the functioning of the extended vehicle and will therefore be available from day one.

50 With the shared server, will data be sent from an existing vehicle manufacturer server onto a shared server or be held only on the shared server?

Stakeholder views differed, with most of the opinion that data will be sent from an existing vehicle manufacturer server to a shared server



Comments:

- Shared server provides data to all stakeholders in the same manner, including OEM. Only this option will ensure compliance with the guiding principles of fair and undistorted competition.
- The objective of a shared server is to separate vehicle data from competitive and private data of the vehicle owners. The shared server is in series behind the Extended Vehicle. An additional solution that should be considered is a second IP address. It follows all of the principles for the shared server. The significant difference is that the same data that is sent to the VM server from the vehicle is also sent in parallel directly to a third-party service provider server using a second IP address. We consider that the following definition would apply: Second IP address: To address the concerns of business model monitoring and personal data privacy, a 2nd IP address sends the same data at the same time directly from the vehicle to both the VM and a third-party backend server. Data is provided based on the vehicle manufacturer's in-vehicle data sets.

If a certain set of data was sent from a vehicle manufacturer server to a shared server:

51 What effect, if any, would this have on latency or other aspects?

Likely to have an effect but no specific quantifiable values were received. Stakeholders reaffirmed that the data server was not compatible with real time data. This question was specifically asking what effect the extra layer from the OEM server to a shared server would have on latency; no responses on this aspect were received.

52 To what extent would this solve the liability issues for the vehicle manufacturers?

- If the neutral server has data access through the interface on the vehicle manufacturer's server only, the vehicle manufacturer could effectively secure the end-to-end communication and therefore assume product liability obligations. This would not be the case if the shared server, as conceived by other stakeholders, has a direct connection to the vehicle.
- Other stakeholders thought the shared server solved all liability issues for all stakeholders because in case of liability, the vehicle manufacturer can get the real name of the vehicle owner and the name of the workshop from the shared server operator
- However, other views were that the shared server does not solve the liability issues presented from the vehicle manufacturers. "There is a shared liability (vehicle manufacturer/service provider) as it is today the case where an independent workshop changes the brake pads using aftermarket parts. In every technical solution each party is responsible for their component (soft- or hardware) in the service chain for the end user. In case of the Extended Vehicle the vehicle manufacturer has to make sure that all data retrieved using the web services is correct and that no write operations, triggered by a web service call to the Extended Vehicle, threatens the security and safety of the car in operation. In case of the On-board application platform, the vehicle manufacturer stays responsible for his implementation of the standardized On-board application platform in-vehicles of his brand. The defined processes of testing an application in combination with his On-board application platform implementation gives him a possibility to not only test the new application for conformance, but also if his

implementation might still have problems. So only tested combinations of application and On-board application platform implementations hit the road. In no case however is the VM responsible for the services realized in the various applications. If e. g. a prognostic application asks the driver to change brake pads far too early and thus too costly for the driver: that's the responsibility and liability of the application provider. However, the vehicle manufacturer has to ensure via his pre-deployment testing and his runtime security measures like the hypervisor that no application can threaten the safety and integrity of the vehicle in operation."

53 Are you aware of any other potential issues with this approach?

- Who will pay for the shared server
- "Beyond the technical considerations, the principle concerns relate to the legal compliance concerning the extended vehicle concept, such as latency, possible monitoring, no possibility to implement 3rd party applications in the vehicle etc., all of which do not allow true competition between vehicle-related service providers. The shared server is considered as an interim solution. While private data and company data are 'pseudonymised', the vehicle manufacturer still knows the VIN and the location of the vehicle and can misuse these data for market surveillance and distortion of the automotive repair & maintenance sector."

54 In the case of the shared server, vehicle manufacturers ask for the ability to identify specific vehicles. Please explain specifically what "liability and type approval" issues might arise if this ability is not present.

No responses to the question posed were received.

55 In the case of the shared server, who would be liable for the communication cost for the data transfer between vehicle and server?

Range of responses from "the user" to comments that this would depend on the business model.

The contract between the vehicle owner and the VM covers the costs of communication between the vehicle and the extended vehicle server. A second contract exists between the vehicle manufacturer and the shared server provider that would cover the costs of communication of data between the extended vehicle server and the shared server (the terms would be agreed in a B2B contract). A third contract exists between the vehicle owner and the service provider that is using vehicle data via the shared server. This creates an unnecessarily complicated and burdensome process to access data that is only needed to address the basic competition concerns created by the shared server solution.

56 Can you estimate the communication costs (please specify currency if different from Euros) between the vehicle and shared server?

- No. This is directly related to the amount of data per time unit and the chosen payment model with regard to data availability and roaming fees.
- This is commercially sensitive information which ACEA cannot collect from its member companies under EU competition law.
- Other responses indicated:

- Less than 1 euro per month
- Should be below 5 EUR per month and in-line with standard cost for connected other mobile devices.

57 Are there any specificities / difficulties with setting up or maintaining a server controlled by a neutral stakeholder? If so, please describe:

- One stakeholder indicated that this is likely to lead to lengthy discussions between stakeholders with different interests, which could cause problems when rapid action is required, for example to deal with security issues.
- Trust issues and issues related to the determination of contracts

This agreement should include clear arrangements regarding matters such as data availability and quality, transmission costs, security and the protection of personal data.

On-board application platform

58 What technical issues, if any, do you see with the on-board application platform?

The platform needs to be designed according to standards used by all vehicle manufacturers and must also have the capacity to support all types of applications, through a common application programming interface.

"First of all, we do not see any technical issue with the on-board application platform. The on-board application platform is designed to fulfil all requirements for the implementation of applications that have the ability to directly communicate independently between the vehicle and the service provider, using direct access to real-time in-vehicle generated data, functionalities and resources in a complete safe and secure process. - Today a wide range of vehicle manufacturers (VMs) implement in their vehicles in-vehicle on-board application platforms with the ability to install their own and their chosen partners third party applications (software programs such as Android Auto or Apple Car Play). By using these on-board application platforms it is possible, under the full agreement of the vehicle manufacturer, to safely and securely (VM-Security-Layer (Hypervisor + Firewall)) run multiple applications. Currently, the condition for installing the chosen partner third party applications in the in-vehicle telematics system are the following:

1. The VM makes the agreement about which third party applications can be implemented in the vehicle telematics system (B2B-contract)

2. The VM defines and controls through the VM-Security-Layer the level of access to the vehicle data (amount of vehicle data per application) and with whom this data is exchanged.

3. The vehicle manufacturer is also now allowing deeper access to in-vehicle data for their chosen third party partners, but which is being used by the vehicle manufacturer for their own services (e.g. Android Auto) developed using the standardised third party API.

Of course, the VMs install their own applications with full access to all in-vehicle data functionality and resources through the VM-Security-Layer. To ensure equal access to in-vehicle data, functionalities and resources for competitive third party service providers, legislation and standardisation will be necessary."

59 Please can you indicate the benefits (in terms of economic, societal, environmental, liability, and effects on small and medium-sized enterprises) of the on-board application platform?

No quantitative benefit information received.

60 Please can you list the components required for the on-board application platform?

Security Layer for different levels of access, Application Level (API), On-Board Operating Systems - Gatekeeper e.g. a standardised open vehicle interface, Automotive Firewall between the Extended Gateway and the E/E architecture.

61 For the on-board application platform, please can you estimate the cost (please specify currency if different from Euros) of:

Research and Development of the application platform

Standardisation of the platform

Implementation in each vehicle

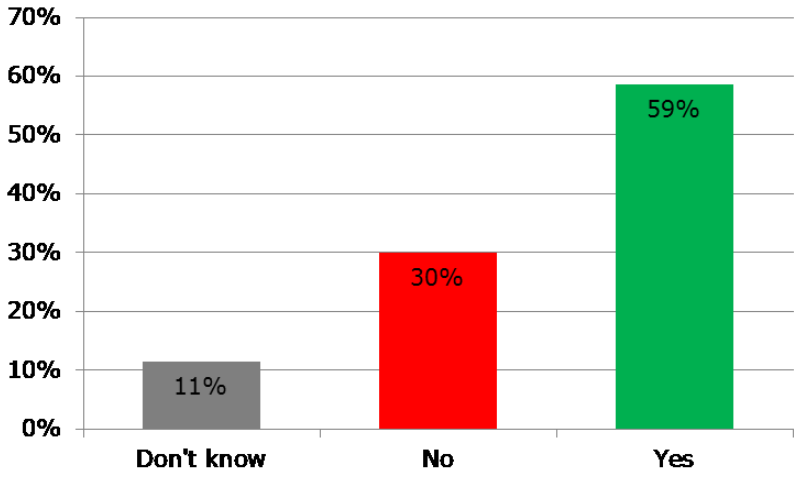
Components (broken down as far as possible)

Respondents indicated that the cost for all categories was "medium"; this was not further specified or benchmarked against known values.

Comments:

In practical terms, on-board application platform already exists; - components: data-interface, CPU, in-vehicle display, communication module, GPS module, security layer including authentication process, API (all components beside security layer already exist).

62 Do you think there will be an open application platform (software development kit) used by all manufacturers?



ACEA responded that they did not believe that there would be a standard SDK applicable to all car manufacturers. A small number of other respondents covering a range of stakeholder groups also supported this view. Generally, the automotive aftermarket and insurance stakeholders held the opposing view that there would be a standard SDK.

Comments:

Such a software development kit is in fact necessary to avoid a fragmented market. There are two emerging standards, but in the absence of a single effective standardisation process, no real shared solution to access to data could be reached.

A standardised Software Development Kit (SDK) should be a target, it is not realistic as of today. Vehicle manufacturers with standardised SDKs profit from higher number of services running in their vehicles

63 Will there be one software development kit per manufacturer? Please explain.

It is essential to have one software development kit suitable for use with all OEMs. This would ensure the possibility of being able to offer multibrand solutions and the widest range of possible services.

Some stakeholders were somewhat sceptical about possible collaboration between manufacturers to determine a common SDK. Other respondents indicated that "probably more than one" would be developed.

64 We consider that if a single SDK is a desired outcome, then regulation will be required to bring about the necessary standardisation Can you estimate the cost for the vehicle manufacturer and/or application owner for the certification process (please specify currency if different from Euros)? Please state the context of any stated costs and benefits of the certification process. (To whom do these costs apply and does this include or exclude any elements for profit?)

The costs for the development of applications and their certification are small, if e.g. one standardised development kit is available to cover all OEMs. Processes which are implemented today are e. g. the Apple certification process for different third party applications. These applications are tested using state of the art processes and standards. The goal of this certification process is that the application can be downloaded from e. g. the App-Store of Apple and can run without any problem on the iPhone. - The costs depend on a range of points. From our experience the costs are approximately 5.000 Euro per application.

65 What process to identify "certified applications" would you regard as fair and reasonable?

- Process comparable to Apple app certification.
- Transparent Common Criteria like e.g. ISO 15408.
- The OEM is responsible for the process

66 Please can you describe the steps that would be required to enable certification?

Responses included the following:

"The process should be as follows:

- *Develop the application using the software development kit for an on-board application platform*
- *Submit the application with all necessary information to the respective vehicle manufacturer*
- *Tested by the respective vehicle manufacture according to state of the art processes*
- *Have the application admitted to the vehicle manufacturer's app store. This application can be implemented on customer request in the vehicle.*
- *To avoid any unacceptable burdens, costs, delays or other barriers that would impair the approval and implementation of 3rd party applications, a detailed legislative process description will be necessary."*

Several responses also referred to the answer provided to the previous question that the OEM should be responsible for the process; although without describing how.

In-vehicle interface

67 What technical issues, if any, do you see with the in-vehicle interface?

- The primary issue is standardisation of interfaces, security and data definitions. - Standardisation has begun in CEN TC278(ITS) WG16(C-ITS)
- No standardisation of the interface
- Multiple SDKs for each OBD plug mean cannot design application for whole market

68 Please can you describe and quantify the benefits (in terms of economic, societal, environmental, liability, and effects on small and medium-sized enterprises) of the in-vehicle interface?

No quantified costs received. Some stakeholders provided comments:

- *Will allow SMEs to grow new business models. This is totally different from the other two methods, since this is the only method that avoids full control by the OEMs*
- *In-vehicle interface, security layer (Hypervisor and firewall like in the on-board application platform solution to prevent potentially damaging request in unsafe driving conditions or when the bandwidth on the bus is not sufficient. Because there is no final testing of a single application possible for the vehicle manufacturer in this scenario, security measures would need to be higher and therefore more expensive compared to the on-board application platform approach, where the possibility of black- and white-box-testing of every application prior to the admission to the app store and deployment to the car makes it easier to detect potentially harmful applications.*

69 Please can you list the components required for the in-vehicle interface?

Many respondents stated that they could not. However, a few did respond and they suggested:

- Position location system
- Communication system
- CPU
- HMI (via phone or in-vehicle)
- In-Vehicle secure and open interface / A secure gateway and information gathering unit / function to obtain vehicle information
- Data storage and management systems
- Applications

70 **For the in-vehicle interface, please can you estimate the cost (please specify currency if different from Euros) of…**

Research and Development of the in-vehicle interface

Standardisation of the interface

Implementation in each vehicle

Components (broken down as far as possible - please use comments box below)

No cost information was received.

Comments:

- The interface itself will cost the OEMs minimal, probably less than ten cents if the current OBD-II extension standards are used. The external device may cost from 10€ upwards to several hundred depending on a lot of factors.
- Costs similar to existing OBD connector. In-vehicle gateway or switch as well as physical plug/socket in the vehicle needed.

71 Please can you estimate the cost (development, standardisation, implementation in-vehicle etc) of adding a state of the art security layer to the upgraded on-board diagnostics interface including gatekeeper and central gateway to the in-vehicle network (please specify currency if different from Euros)?

Few cost values were received. Stakeholders indicated that the situation was too complex and too many unknowns to provide cost information. "The cost varies depending on the level or scale of measures to be taken, making it difficult to estimate it at this stage.

- One stakeholder provided the value of "around 400k"
- Another commented "the in-vehicle interface (IVI) needs the same or even higher security concepts in the vehicle as the on-board application platform. It has to be aware of the various applications that could be released to the plugged in box without these having been checked prior to installation in the car. So the amount is unknown, but should be similar to the amount for the in-car security components of the on-board application platform.

72 Will the in-vehicle interface be tested against a specific cyber security standard? If so which one?

- For the in-vehicle interface solution we suggest to develop a new security concept following the common criteria approach of the German BSI. - This approach enables the easy re-use of proven security elements and components that adhere to established standards. –
- We propose to test it against a whitelist and against a protection profile (develop via e.g. Common Criteria ISO 15408)

73 Can you provide any experiences associated with the Fleet Management System standard access to the Controller Area Network for trucks and buses?

"The FMS interfaces are in the market since 2004 (trucks) and 2007 (buses) respectively. As the interface provides data needed in a fleet management system in a standard way, most suppliers use the FMS interface for receiving data for their systems. We estimate that more than 1 million FMS gateways are in the market today. However, the existing FMS interface will

not be further developed due to technology reasons. It has been succeeded by the rFMS (remote Fleet Management Standard) since 2012. The rFMS delivers a defined set of data from the vehicle to the vehicle manufacturer's server. Those data are then sent via the rFMS interface to the server of the freight forwarder. Conceptually, the rFMS is a web interface that is part of the extended vehicle. Since 2016, rFMS is available in version 2.0 and provides several standardized interfaces at each vehicle manufacturer's server. Access is granted by providing typical IT credentials (password + login) for the fleet manager, who can either connect through an application running in his private IT, through a web server or through an own app on a device connected to the internet. In addition, the fleet manager can easily integrate the vehicle data into his commercial IT infrastructure. The rFMS uses vehicle manufacturer-specific hardware and software. Access to the in-vehicle network and the communication to and from the vehicle is out of scope of the rFMS. The data are "downloaded" from the vehicle and stored on the vehicle manufacturer's server. The rFMS gives access to this information in a standard way for all vehicle manufacturers. As the rFMS is only now beginning to be implemented, there is no real experience to report for the moment. However, initial reactions from some user groups (DOIT, Telematics Valley) are positive."

74 For Fleet Management System standard access, how long did it take to establish the minimum dataset and standard interface?

"The first version of the FMS standard was published in 2003. The definition work started in 2001. The first activity for rFMS started in 2010. Definition work took place in 2011. Version 1 was published at the end of 2014. It defines how to get access to information that is already available from vehicles equipped with FMS hardware/software in the vehicle manufacturers' back offices. Version 2 was published in September 2016. It defines how to access information from the vehicle manufacturers' back offices. Implementation is vehicle manufacturer-specific."

75 Is any cost information available for the development of the Fleet Management System standard access?

No cost information forthcoming.

76 Can you please give a breakdown of the costs involved in the Fleet Management System standard access (please specify currency if different from Euros)?

No information forthcoming.

77 Can you please give a breakdown on the benefits of the Fleet Management System standard access?

Respondents provided the following benefits of the FMS standard:

- Compliance with safety and environmental standards and requirements
- Enables the owner to select who has access to vehicle data, when, and to which extent.
- Vehicle data and services can be accessed in a standard way by everybody who has the given access to the information
- Applications can be developed without knowledge of the in-vehicle structure/network
- Access to the vehicle data and services are independent of the vehicle hardware.
- Easy use of different Fleet Management Services from different suppliers
- Fleet Management Service suppliers are able to provide software/information to any customer independent of the hardware installed in the vehicle
- Fleet Management Service suppliers can change their systems without influencing the vehicle manufacturers' systems

- Change of the internal (vehicle manufacturer) technology is possible without influencing third- party systems
- Protection of the in-vehicle network against abuse
- No stand-still cost for installing hardware in the vehicle as the necessary hardware is part of the delivery of the vehicle

Appendix C. LITERATURE REVIEW SOURCES

	Author	Year	Title	Survey No	Included/ Not included	Reasoning
1	BVRLA	ND	http://www.bvrla.co.uk/policy/update/connected-vehicles-driver-and-vehicle-data	1	Not included	Relevant background reading but nothing specific to extract
2	Squarell	X	FLEX: Multi Source Vehicle Data Interface	1	Not included	N/A
3	Kranz M and Weber E	2009	Open Vehicular Data Interfaces for In-Car Context Inference	1	Not included	Too old
4	Yun H and Lee S	2008	The Fully Networked Car: Standards for Vehicle Gateway	1	Not Included	Too old
5	C-ITS	Dec-15	C-ITS Platform - Final report	1	Not Included	Relevant background reading but nothing specific to extract
6	C-ITS	Jan-16	C-ITS Platform - Access to in-vehicle reources and data	1	Not Included	Relevant background reading but nothing specific to extract
7	SAE		SAE J1939	1	Not Included	Relevant background reading but nothing specific to extract
8	ISO	tbc -2017-8	ISO/DIS 20077 - ISO/DIS 20077-1 Road Vehicles -- Extended vehicle (ExVe) methodology -- Part 1: General information	1	Not Included	Relevant background reading but nothing specific to extract
9	ISO	tbc -2017-8	ISO/NP 20078 - ISO/NP 20078-1 -Road vehicles -- Extended vehicle (ExVe) 'web services' -- Part 1: ExVe content	1	Not Included	Relevant background reading but nothing specific to extract
10	ISO	tbc -2017-8	ISO/DIS 20080 - ISO/DIS 20080-1 - Road vehicles -- Information for remote diagnostic support -- General requirements, definitions and use cases	1	Not Included	Relevant background reading but nothing specific to extract
11	BSI	X	BS EN 15722 - Ecall	1	Not Included	Relevant background reading but nothing specific to extract
12	Chan B	X	In-Car Gateway Software for Internet-of-Vehicles (IoV)	1	Not Included	Relevant background reading but nothing specific to extract
13	Scheiblich C and Raith T	2014	The Extended Vehicle (ExVe) – New Standardization Project ISO 20078	1	Included	Mercedes-Benz
14	HERE	2015	Vehicle Sensor Data Cloud Ingestion Interface Specification (v2.0.2)	1	Not included	
15	Reininger M, Miller S, Zhuang Y and Cappos J	2015	A First Look at Vehicle Data Collection via Smartphone Sensors	1	Not Included	Relevant background reading but nothing specific to extract
16	Maerien J, Michiels S, Van Baelen S, Huygens C and	2010	A Secure Multi-Application Platform for Vehicle Telematics	1	Not Included	Relevant background reading but nothing specific to extract
17	Yoo J W, Lee Y, Kim D and Park K	2013	An Android-based Automotive Middleware Architecture for Plug-and-Play of Applications	1	Included	
18	Freshfields Bruckhaus	2015	From connected to self-driving vehicles: the regulatory	1	Not included	No suitable information
19	BT	2014	The Connected Car	1	Not Included	Relevant background reading but nothing specific to extract
20	Kollaikal P, Ravuri S and Ruvinsky E	2015	Connected Cars	1	Not included	N/A
21	X	X	Web API for Vehicle Data RI: Reference implementation of Web API for Vehicle Data	1	Not included	N/A
22	Isenberg S, Harbel W, Goebel M, Michel Mand Baumgarten U	2012	Enabling Rich Web Applications for In-Vehicle Infotainment	1	Not included	No suitable information
23	Balasubramanian J, Beiker S, Chauhan S, Colombo T, Hansson F, Inampudi S, Jaarsma R and Kasser M	2016	Car data: paving the way to value-creating mobility. Perspectives on a new automotive business model	1	Not Included	Relevant background reading but nothing specific to extract
24	Akiyama S, Nakamoto Y, Yamaguchi A, Sato K and Takada H	2015	Vehicle Embedded Data Stream Processing Platform for Android Devices	1	Not included	No suitable information
25	PSA	2015	PSA Peugeot Citroen: Driving Automation and Connectivity	1	Included	PSA
26	Apvrille L, El Khayari R, Henniger O, Roudier Y, Schweppe H, Seudié H, Weyl B and Wolf M	2010	Secure Automotive On-Board Electronics Network Architecture	1	Not included	No suitable information
27	Schweppe H and Roudier Y	2015	Security and Privacy for In-Vehicle Networks	1	Not Included	Relevant background reading but nothing specific to extract
28	Smart Automotive	2016	Catalyzing Connected Car Proliferation	1	Not included	No suitable information
29	Squarell	X	SOLID: Vehicle Data Interface	1	Not Included	N/A
30	VDA	2014	Data Protection Principles for Connected Vehicles	1	Not included	No suitable information
31	BMW	2012	Enabling Rich Web Applications for In-Vehicle Infotainment: Using the Webinos Platform inside the Automotive Domain.	1	Not Included	Relevant background reading but nothing specific to extract
32	Intel Corporation	2012	What is a connected car?	1	Not included	No suitable information
33	CLEPA	2015	CLEPA Position Paper: Open Telematics Platform	2	Included	Position paper
34	FIA	2016	Policy position On Car Connectivity	2	Included	Position paper
35	ACEA	2016	ACEA Strategy Paper on: Connectivity	2	Included	Position paper
36	Axway	2016	Axway API Gateway and the Connected Car	2	Not Included	No suitable information
	VDA	2014	Data Protection Principles for Connected Vehicles		Not Included	Relevant background reading but nothing specific to extract
37	Leaseurope	2012	Car Leasing: Supporting sustainable mobility in Europe	2	Not Included	Relevant background reading but nothing specific to extract
38	Mai A and Schlesinger D (CISCO)	2011	A Business Case for Connecting Vehicles Executive Summary	2	Not Included	Relevant background reading but nothing specific to extract
39	KPMG	2015	Connected and Autonomous Vehicles - The UK Economic Opportunity	2	Not Included	Relevant background reading but nothing specific to extract
40	BVRLA	2016	Statement of Best Practice: Key principles in respect of data collected from vehicles	2	Not included	N/A
41	AFCAR/Leaseurope	X	Why the eCall legislation should address the need for an interoperable, open-access platform, and what does that mean?	2	Not Included	Relevant background reading but nothing specific to extract
42	McClure D, Forestieri F and Rooke A	2016	Achieving a Digital Single Market for Connected Cars eCall – implementation status, learnings and policy recommendations	2	Not Included	Relevant background reading but nothing specific to extract
43	Insurance Europe	2013	Insurance Europe's position on the EC's proposal on a Regulation for the deployment of the eCall in-vehicle system	2	Not Included	Relevant background reading but nothing specific to extract
44	European Parliament	2016	Breifing: Automated vehicles in the EU	2	Not included	N/A
45	Ericsson	X	Connected vehicle cloud: Under the hood	2	Not Included	Relevant background reading but nothing specific to extract
46	everis	X	everis Connected Car Report	2	Not Included	Relevant background reading but nothing specific to extract
47	Berends M	2013	Car Data – New access via telematic systems	2	Not Included	Relevant background reading but nothing specific to extract
48	FPF	2014	The Connected Car and Privacy: Navigating New Data Issues	2	Not Included	Relevant background reading but nothing specific to extract
49	IET	2015	Automotive Cyber Security: An IET/KTN Thought Leadership Review of risk perspectives for connected vehicles	2	Not Included	Relevant background reading but nothing specific to extract
50	Bongartz M, Chen H, Fricke V, Gerstenberger V, Koehn M, Kohler A and Scherzer	2016	IT Security for the Connected Car	2	Not Included	Relevant background reading but nothing specific to extract
51	CECRA	2016	Car dealers and repairers need equal access to vehicle data	2	Not Included	Relevant background reading but nothing specific to extract
52	AFCAR		Fair and Equal Access to Vehicles in a Digital Single Market	2	Included	Position paper
53	Leaseurope	2016	The Connected Car	2	Not Included	Relevant background reading but nothing specific to extract
54	Saed M, Bone S and Robb J	2014	Security Concepts and Issues in Intra-Inter Vehicle Communication Network	2	Not Included	Relevant background reading but nothing specific to extract
55	Bose R, Brakensiek J and Park K Y	2010	Terminal Mode – Transforming Mobile Devices into Automotive Application Platforms	2	Not Included	Relevant background reading but nothing specific to extract
56	Crocker P	2015	The In-Car App Experience: Convergence and Integration	2	Not Included	Relevant background reading but nothing specific to extract
57	VDA	2016	Access to the vehicle and vehicle generated data	2	Included	Position paper
58	Datta S K, Ferreira Da Costa R P, Bonnet C and Harri J	2016	Web of Things for Connected Vehicles	2	Not Included	Relevant background reading but nothing specific to extract

Appendix D. Socio-economic Benefit Analysis – Data and Methodology

Steps in the assessment

In order to quantify the societal benefits arising from the implementation of a range of services based on in-vehicle data across Europe in the time frame from 2017 to 2030, the following steps were followed:

1) **Impact factors estimation** - estimate the magnitude of the impacts per year on the four areas considered: safety, CO_2 emissions, fuel consumption and time spent travelling.

2) **Baseline scenario forecast** – prediction of the plausible trends in the four areas under the hypothesis that the services are not introduced; that is, how many annual fatalities and injuries are expected, what is the yearly projection of the CO_2 emitted by road vehicles, how much fuel is going to be used and how much time is likely to be spent on road journeys per year if these services are not introduced?

3) **Societal impact calculation -** use the impact factors on the forecast values to quantify the impact of the services; that is, calculate the magnitude of the variation from the baseline scenario. Depending on the service, the expected effects are (see Table 44):
    - Reduced number of fatalities and injuries due to road accidents
    - Reduced CO_2 emissions
    - Reduced fuel consumption
    - Reduced travel time.

For the economic evaluation it was also necessary to:

4) Assign the unit cost values to the indicators analysed (fuel cost per litre, travel time cost per hour, etc.). Values derived from future projections were used when possible.

5) Multiply the unit costs by the annual variations obtained in step 3. A discount rate of 4% has been used for calculating the discounted values of future costs to represent them in current monetary terms.

Impact factors estimation

The impact factors employed derive from a study commissioned by DG MOVE and prepared by RICARDO-AEA, where the percentages of the reductions expected for 2030 for different C-ITS services were estimated based on the findings of a wide literature review (Ricardo Energy & Environment, 2015). It was assumed that the impacts increase linearly from 2017 to reach the maximum values indicated in the RICARDO-AEA report in 2030 (Table 44).

The reductions in the number of fatalities and injuries were reported in the source document for specific roads (motorways, non-motorways and urban roads) and as an overall estimate. The latter were used for this calculation. It must be noticed though, that, since an overall value was not available for the TJW service, an approximation was

made based on the figures provided for the different types of roads (see asterisk in Table 44).

Table 44 Impact factors of the services (Ricardo Energy & Environment, 2015)

Service	Area	Reductions (2030, impacts at 100%penetration)		
			Fatalities	**Injuries**
PVD - Probe vehicle data	Fuel consumption	0.006%		
	CO2 emissions	0.006%		
	Safety		2.40%	2.80%
HLN - Hazardous location notification	Traffic efficiency	2%		
	Safety		4.10%	3.10%
TJW - Traffic jam ahead warning	Safety		1.80%(*)	2.51%(*)
SSV - Slow or stationary vehicle warning	Safety		1.13%	0.69%
EBL - Emergency brake light	Safety		2.70%	2.50%

(*) Assumptions. The percentages from the original source were: 2.40%, 2.00% and 1.20% reduction in the number of fatalities on Motorways, non-motorways and urban roads respectively; 4.40%, 3.70% and 1.80% reduction in the number of injured on Motorways, non-motorways and urban roads.

Forecasts

Safety

The projections about the number of road fatalities, serious injuries and slight injuries have been obtained by extrapolating from historical data trends. The sources used for these were:

- Number of fatalities in EU28 from 2001 to 2015: a European Transport Safety Council (ETSC) report (ETSC, 2016)
- Number of seriously injured in EU24 from 2005 to 2015: a European Transport Safety Council (ETSC) report (ETSC, 2016)
- Number of road accidents involving personal injury from 2005 to 2015: EU-transport in figures 2016 (EC, Directorate-General for Mobility and Transport, 2016)
- Number of slightly injured from 2005 to 2015: difference between the number of road accidents involving personal injury and the number of seriously injured

CO_2 Emissions

The forecast of the CO_2 emitted by road transport were taken from a report commissioned by the EC in 2016 (E3M-Lab, 2016). Figure 25 shows the emission trend from 2017 to 2030.

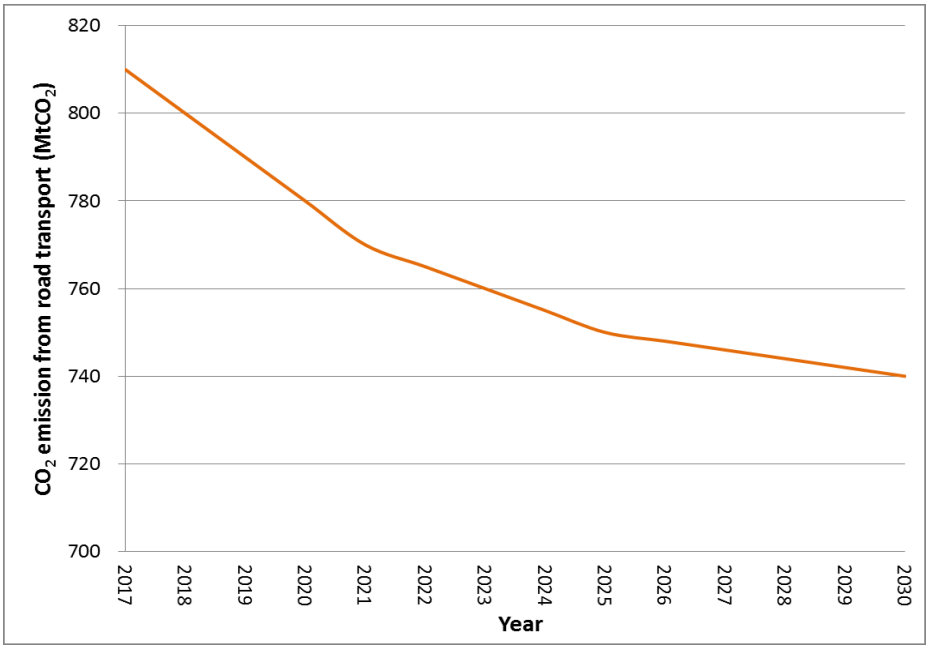


Figure 25 Forecast values for the CO_2 emitted by road transport (E3M-Lab, 2016)

Travel time

1. Cars

   The average travel time spent travelling by car in Europe was estimated by multiplying the total number of cars in a year by the average annual distance travelled, the average speed and the average vehicle occupancy. The number of cars was obtained by interpolating the 2015 figure and the projected value for 2030. The other parameters were assumed to remain constant over time. The following figures and sources have been used:

- Number of cars in 2015: 251,095,313 – from the SULTAN model (AEA, 2012)
- Number of cars in 2030: 283,160,774 – from the SULTAN model (AEA, 2012)
- Average annual distance travelled by car: 11,800 km (Department for Transport, 2016[38])
- Average speed: 45km/h assumed
- Car occupancy: 1.5 (Department for Transport, 2017[39])

2. Freight transport

The yearly time travel for freight transport in Europe has been calculated by multiplying the average annual vehicle kilometres by the average speed. The vehicle occupancy has been assumed to be one. The vehicle kilometres value in 2014 was a Eurostat figure

[38] Department for Transport, 2015. National Travel Survey Table 0901.

[39] Department for Transport, 2017. Webtag databook, March 2017. https://www.gov.uk/government/publications/webtag-tag-data-book-march-2017 .

(Eurostat, 2017), while the data projection has been calculated using an annual increase of 2.10% (E3M-Lab, 2003).

The result of the calculations is shown in Figure 26.

Since the time spent travelling has a different cost value according to the purpose of the trip (see next section), the amount of hours calculated was assumed to be divided into three categories: business, commuting and other purposes. All the freight time travel has been assumed to be business journeys; the car fleet has been divided into the three categories with the proportions calculated using an average of the percentages estimated for the ANACONDA project (Nitsche, 2017), namely 8%, 25% and 67%, for business trips, commuting and other trips, respectively.

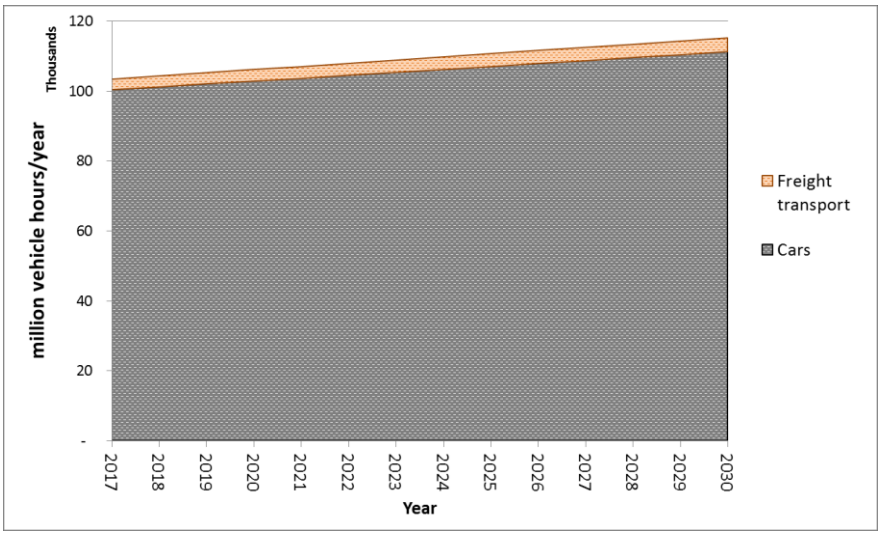


Figure 26 Cars and freight transport forecast in Europe

Fuel consumption

The petrol and diesel demand for road transport from 2017 to 2030 was the estimated by interpolation of three values provided by an E4tech report commissioned by a consortium of car manufacturers (E4tech, 2013). The three figures refer to 2010, 2020 and 2030. The result of the interpolation is shown in Figure 27.

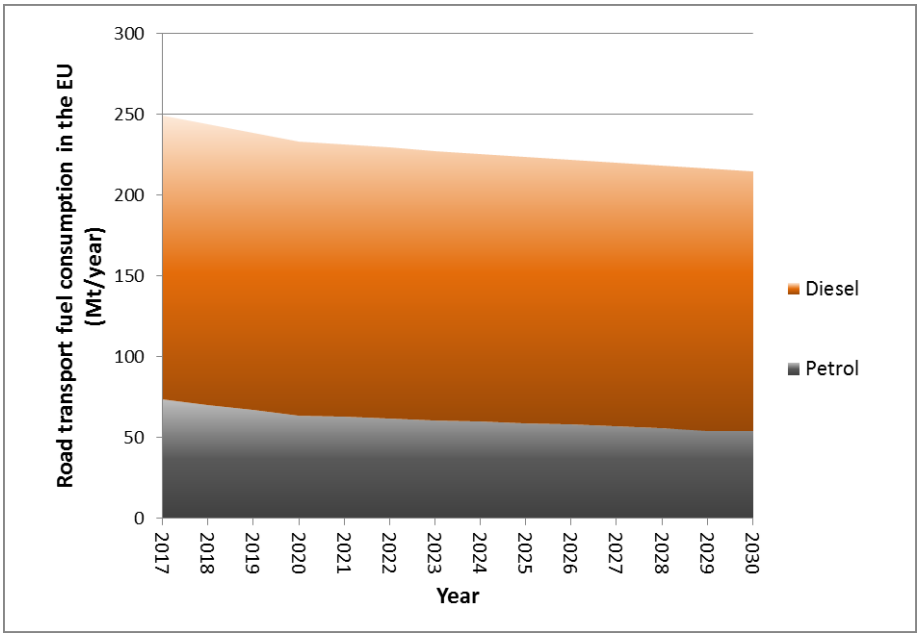


Figure 27 Projection of diesel and petrol consumption by road transport in Europe (E4tech, 2013)

Monetary values

The unit costs used and the corresponding sources are listed below.

1. Safety

   The costs associated with road fatalities and to serious or slight injuries were derived from the average of the values for five European countries used in the ANACONDA project (Nitsche, 2017); namely, UK, Austria, Finland, Germany and The Netherlands. In consideration of the fact that there can be significant differences among the economies of the EU constituent countries, and in order to maintain a conservative approach, a reduction of 25% was applied to those figures. This procedure led to the following (approximated) unit costs:

   - Fatality €1.2 million per person
   - Seriously injured €272,000 per person
   - Slightly injured €13,600 per person

   The values have been kept constant in time.

2. CO_2 emissions

   For the external cost, the value provided by a study commissioned by the European Commission in 2014 (Directorate-General for Energy, 2014) was used.

   - External cost per tonne of CO_2 emitted (2012 value): €43/tonne

   This value is likely to increase in time (de Bruyn, 2014); however, a conservative estimate was selected so the cost has been assumed to be the same over the assessment period.

3. Travel time

The monetary value of one hour spent on road journeys during the 2017- 2030 time period have been estimated as follows (DfT, 2016):

- Business trips €17/hour
- Commuting journey €11.4/hour
- Other personal purposes (holidays, shopping, etc.) €5.2/hour

4. Fuel price

The EU-28 weighted average price of fuel (EC Energy policy, 2017) was adjusted to reflect the trend in the crude oil import price forecast by the International Energy Agency (IEA, 2016). The projections are displayed in Figure 28.

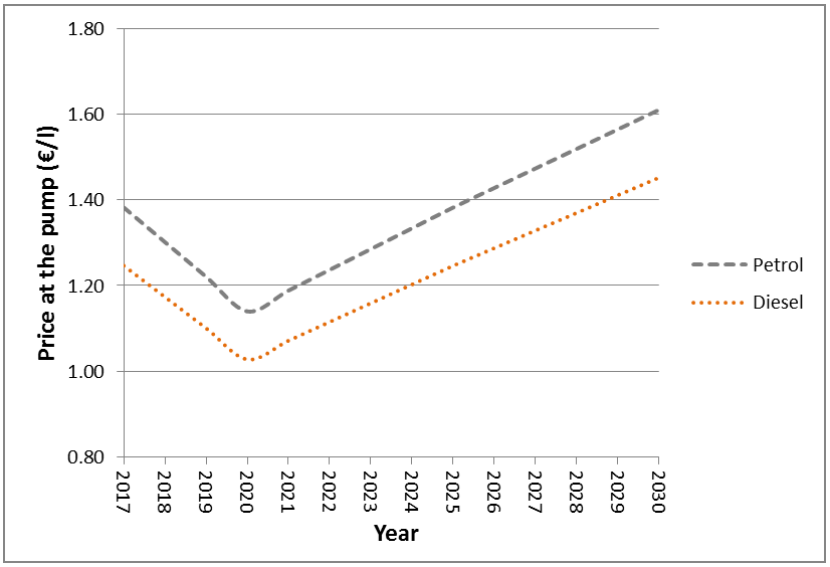


Figure 28 Forecast of petrol and diesel price at the pump

Socioeconomic benefit analysis – results and further details

All of the five example services analysed have a positive impact on road safety. The outcome in monetary terms for all the services is summarised in Figure 17. Even in the first year the savings are of the order of magnitude of millions of euros for all the services.

It is important to note that these figures refer to the single services; implementing multiple services would not result in impact factors equal to the sum of the single impact factors, since there would be overlaps in the functionalities to take into account. Therefore, even though the activation of multiple services would likely result in higher benefits, these cannot be calculated as the simple sum of the benefits accrued by the individual services.

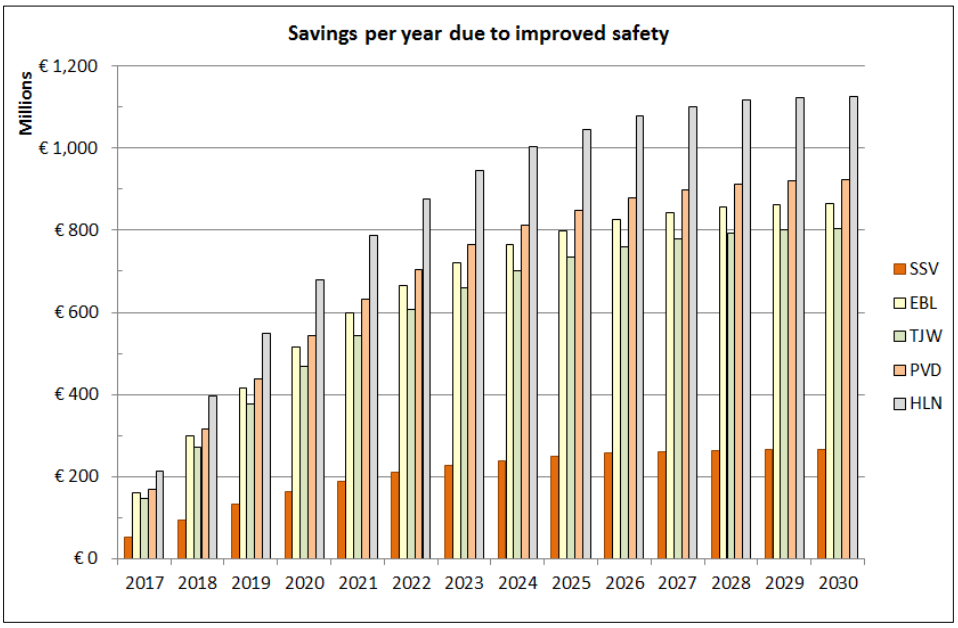


Figure 29 Annual savings associated with five services due to avoided fatalities and injuries

Prevention of serious injuries is the main contributor to the cost savings in the safety field, with percentages that go from about 50% to more than 60%. Cumulative savings derived from the prevention of serious injuries are reported in Figure 30; as shown in the chart, the impacts on safety would lead to overall savings of the order of billions of euros.

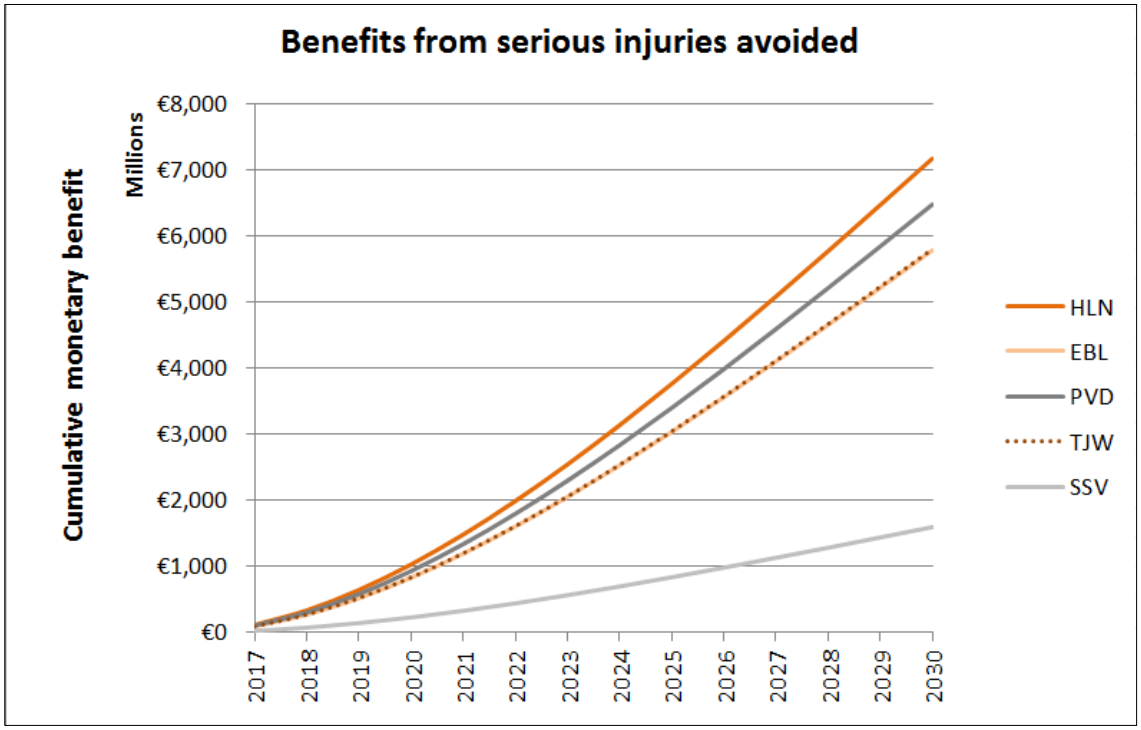


Figure 30 Cumulative benefits accrued in preventing serious injuries by each service

Fuel consumption and CO2 emissions – PVD service

In addition to the benefits deriving from improved road safety, the PVD service is associated with fuel savings and, consequently, to emissions reductions. The Ricardo report indicates 0.006% of fuel saved from this service (Ricardo Energy & Environment, 2015); CO_2 emissions are directly linked to the burnt fuel, therefore the same percentage represents the reduction in carbon dioxide emissions. Further benefits would arise from the reduction of particulate matter (PM) and nitrogen oxides (NOx) emissions; however, they are not discussed here. This is because the health hazards strongly depends on the distance from the PM or NOx source; therefore, to quantify the impacts it would be necessary to consider the population within a certain range by the road traffic and such data is not readily available.

Approximately 34 million litres of petrol and 81 million litres of diesel is the estimation of the fuel that can be saved in 14 years, corresponding to about 330,000 tonnes of CO_2. Figure 31 shows the estimated annual cost savings in these three fields, derived from the PVD implementation. The calculations took into account that future technology improvements will bring about reductions anyway; therefore, the values reported here can be attributed to the implementation of the service only. The savings in the first year are estimated to be in the range of €1.6 million; they then gradually grow up to almost €14 million in 2030.

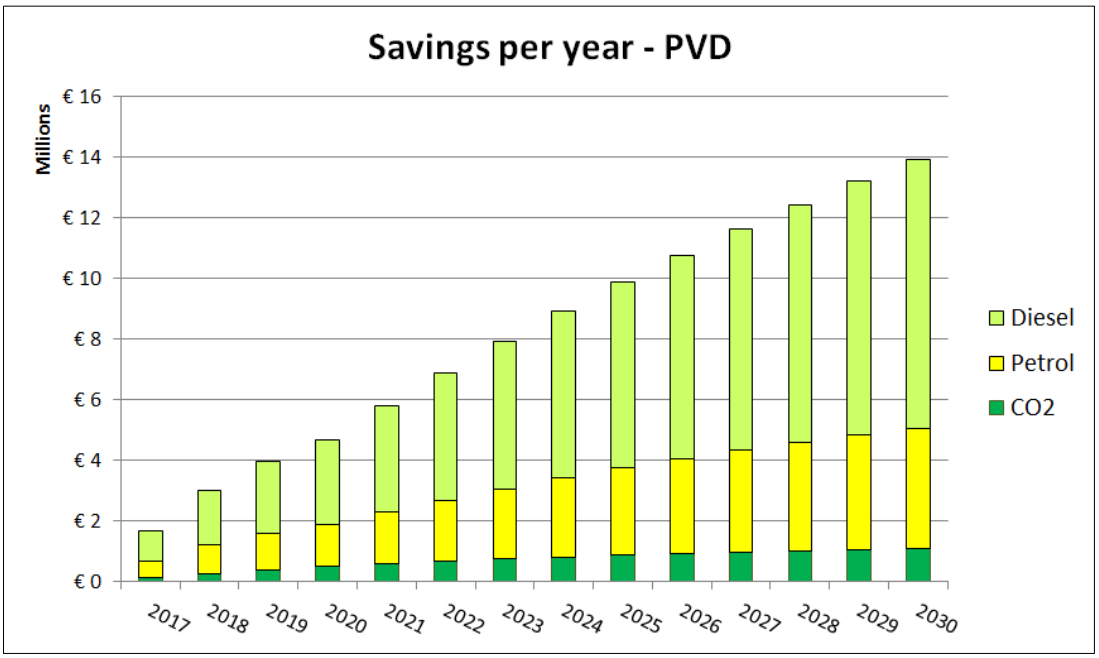


Figure 31 Annual benefits derived from fuel savings and CO_2 reductions due to the PVD service

Appendix E. Identification of Potential Economic, Social and Environmental Impacts and Fundamental Rights

Table 45, Table 46 and

Table 47 below identify the areas and expected impacts of access to in-vehicle data in general, whichever technology is used to obtain the data from the vehicle). Table 48 summarises the assessment against fundamental rights.

Table 45 Identification of potential economic impacts

Area	Key Questions	Expected impacts
Functioning of the internal market and competition	What impact (positive or negative) does the option have on the free movement of goods, services, capital and workers?	None
	Will it lead to a reduction in consumer choice, higher prices due to less competition, the creation of barriers for new suppliers and service providers, the facilitation of anti-competitive behaviour or emergence of monopolies, market segmentation, etc.?	The actions proposed have the potential to stimulate new services to consumers based on the wider availability of data from vehicles; this may lead to increased consumer choice for services.
Competitiveness, trade and investment flows	What impact does the option have on the global competitive position of EU firms?	The actions proposed have the potential to stimulate new services to consumers based on the wider availability of data from vehicles. A properly functioning market would reduce the dominance of the two principal US-based providers of mobile ecosystems (Google and Apple) in the European market.
	Does it impact on productivity?	Potential for improvement in productivity in sectors which benefit from remote access to in-vehicle data.
	What impact does the option have on trade barriers?	None
	Does it provoke cross-border investment flows (including relocation of economic activity)?	No
Operating costs and conduct of business/Small and Medium Enterprises	Will it impose additional adjustment, compliance or transaction costs on businesses?	A fully functioning market would remove the need for bilateral agreements but there will be an adjustment cost involved in developing a standard approach to accessing data from vehicles.
	How does the option affect the cost or availability of essential inputs (raw materials, machinery, labour, energy, etc.)?	N/A
	Does it affect access to finance?	No
	Does it impact on the investment cycle?	No
	Will it entail the withdrawal of certain products from the market?	No products will have to be withdrawn but there will be market adjustments in the products that are available and the way they are made available, based on choices made by consumers
	Is the marketing of products limited or prohibited?	No
	Will it entail stricter regulation of the conduct of a particular business?	No additional requirements are expected unless new legislation is introduced.
	Will it lead to new or the closing down of businesses?	There will be market adjustments based on choices made by consumers, which could involve new businesses as well as business closures.
	Are some products or businesses treated differently from others in a comparable situation?	No

Area	Key Questions	Expected impacts
Administrative burdens on businesses	Does it affect the nature of information obligations placed on businesses (for example, the type of data required, reporting frequency, the complexity of submission process)?	No
	What is the impact of these burdens on SMEs in particular?	No.
Public authorities	Does the option have budgetary consequences for public authorities at different levels of government (national, regional, local); both immediately and in the long run?	No
	Does it bring additional governmental administrative burden?	There will be a requirement for compliance checking in the case of any mandate for specific in-vehicle equipment. If a neutral data server is included in one of the options selected, the governance of the server will be an additional administrative burden.
	Does the option require the creation of new or restructuring of existing public authorities?	No
Property rights	Are property rights affected (land, movable property, tangible /intangible assets)?	No
	Is acquisition, sale or use of property rights limited?	No
	Or will there be a complete loss of property?	No
Innovation and research	Does the option stimulate or hinder research and development?	Making in-vehicle data available will stimulate R&D.
	Does it facilitate the introduction and dissemination of new production methods, technologies and products?	Greater availability of in-vehicle data may lead to the development of new products due to the lower costs of data discovery and data access.
	Does it affect intellectual property rights (patents, trademarks, copyright, other know-how rights)?	No
	Does it promote or limit academic or industrial research?	It will promote research.
	Does it promote greater productivity/resource efficiency?	It will promote greater efficiency.
Consumers and households	Does the option affect the prices consumers pay?	A well-functioning market should reduce the prices paid by consumers for services.
	Does it impact on consumers' ability to benefit from the internal market?	No
	Does it have an impact on the quality and availability of the goods/services they buy, on consumer choice and confidence? (cf. in particular non-existing and incomplete markets – see Annex 8)	The policy actions are intended to stimulate the market and improve the range of services and their quality, and should provide more choice for consumers.
	Does it affect consumer information and protection?	No
	Does it have significant consequences for the financial situation of individuals / households, both immediately and in the long run?	No

Area	Key Questions	Expected impacts
	Does it affect the economic protection of the family and of children?	No
Specific regions or sectors	Does the option have significant effects on certain sectors?	Yes – the automotive industry and third party providers of information services will be affected by the proposed policy options.
	Will it have a specific impact on certain regions, for instance in terms of jobs created or lost?	No
	Is there a single Member State, region or sector which is disproportionately affected (so-called 'outlier' impact)?	No
Third countries and international relations	How does the option affect trade or investment flows between the EU and third countries?	None
	How does it affect EU trade policy and its international obligations, including in the WTO?	None
	Does the option affect specific groups (foreign and domestic businesses and consumers) and if so in what way?	No
	Does the option concern an area in which international standards, common regulatory approaches or international regulatory dialogues exist?	No
	Does it affect EU foreign policy and EU/EC development policy?	No
	What are the impacts on third countries with which the EU has preferential trade arrangements?	No
	Does it affect developing countries at different stages of development (least developed and other low-income and middle income countries) in a different manner?	No
	Does the option impose adjustment costs on developing countries?	No
	Does the option affect goods or services that are produced or consumed by developing countries?	No
Macroeconomic environment	Does it have overall consequences of the option for economic growth and employment?	No
	How does the option contribute to improving the conditions for investment and the proper functioning of markets?	By opening up the availability of in-vehicle data on a non-discriminatory basis.
	Does the option have direct impacts on macro-economic stabilisation?	No

Table 46 Identification of potential social impacts

Area	Key Questions	Expected impacts
Employment & Labour Markets	Does the option facilitate new job creation?	All options should support the emergence of new services and thus job creation.

Area	Key Questions	Expected impacts
	Does it lead directly or indirectly to a loss of jobs?	No
	Does it have specific negative consequences for particular professions, groups of workers, or self-employed persons?	No
	Does it affect particular age groups?	No
	Does it affect the demand for labour?	No
	Does it have an impact on the functioning of the labour market?	No
	Does it have an impact on the reconciliation between private, family and professional life?	No
Standards and rights related to job quality	Does the option impact on job quality?	No
	Does the option affect the access of workers or job-seekers to vocational or continuous training?	No
	Will it affect workers' health, safety and dignity?	No
	Does the option directly or indirectly affect workers' existing rights and obligations, in particular as regards information and consultation within their undertaking and protection against dismissal?	No
	Does it affect the protection of young people at work?	No
	Does it directly or indirectly affect employers' existing rights and obligations?	No
	Does it bring about minimum employment standards across the EU?	No
	Does the option facilitate or restrict restructuring, adaptation to change and the use of technological innovations in the workplace?	No
Social inclusion and protection of particular groups	Does the option affect access to the labour market or transitions into/out of the labour market?	No
	Does it lead directly or indirectly to greater equality or inequality?	No
	Does it affect equal access to services and goods?	No
	Does it affect access to placement services or to services of general economic interest?	No
	Does the option make the public better informed about a particular issue?	No
	Does the option affect specific groups of individuals (for example the most vulnerable or the most at risk of poverty, children, women, elderly, the disabled, unemployed or ethnic, linguistic and religious minorities, asylum seekers), firms or other organisations (for example churches) or localities more than others?	No
	Does the option significantly affect third country nationals?	No
Gender equality, equality treatment and opportunities, non – discrimination	Does the option affect the principle of non-discrimination, equal treatment and equal opportunities for all?	No
	Does the option have a different impact on women and men?	No
	Does the option promote equality between women and men?	N/A
	Does the option entail any different treatment of groups or individuals directly on grounds of sex, racial or ethnic origin, religion or belief, disability, age, and sexual orientation?	No
	Or could it lead to indirect discrimination?	No

Area	Key Questions	Expected impacts
Individuals, private and family life, personal data	Does the option impose additional administrative requirements on individuals or increase administrative complexity?	No
	Does the option affect the privacy, of individuals (including their home and communications)?	No
	Does it affect the right to liberty of individuals?	No
	Does it affect their right to move freely within the EU?	No
	Does it affect family life or the legal, economic or social protection of the family?	No
	Does it affect the rights of the child?	No
	Does the option involve the processing of personal data or the concerned individual's right of access to personal data?	Yes – all options are affected
Governance, participation, good administration, access to justice, media and ethics	Does the option affect the involvement of stakeholders in issues of governance as provided for in the Treaty and the new governance approach?	No
	Are all actors and stakeholders treated on an equal footing, with due respect for their diversity? Does the option impact on cultural and linguistic diversity?	No
	Does it affect the autonomy of the social partners in the areas for which they are competent? Does it, for example, affect the right of collective bargaining at any level or the right to take collective action?	No
	Does the implementation of the proposed measures affect public institutions and administrations, for example in regard to their responsibilities?	No
	Will the option affect the individual's rights and relations with the public administration?	No
	Does it affect the individual's access to justice?	No
	Does it foresee the right to an effective remedy before a tribunal?	No
	Does the option make the public better informed about a particular issue?	No
	Does it affect the public's access to information?	No
	Does the option affect political parties or civic organisations?	No
	Does the option affect the media, media pluralism and freedom of expression?	No
	Does the option raise (bio) ethical issues (cloning, use of human body or its parts for financial gain, genetic research/testing, use of genetic information)?	No
Public health and Safety	Does the option affect the health and safety of individuals/populations, including life expectancy, mortality and morbidity, through impacts on the socio-economic environment (working environment, income, education, occupation, nutrition)?	No
	Does the option increase or decrease the likelihood of health risks due to substances harmful to the natural environment?	No
	Does it affect health due to changes in the amount of noise, air, water or soil quality?	No
	Will it affect health due to changes energy use and/or waste disposal?	No

Area	Key Questions	Expected impacts
	Does the option affect lifestyle-related determinants of health such as diet, physical activity or use of tobacco, alcohol, or drugs?	No
	Are there specific effects on particular risk groups (determined by age, gender, disability, social group, mobility, region, etc.)?	No
Crime, Terrorism and Security	Does the option have an effect on security, crime or terrorism?	No
	Does the option affect the criminal's chances of detection or his/her potential gain from the crime?	No
	Is the option likely to increase the number of criminal acts?	No
	Does it affect law enforcement capacity?	No
	Will it have an impact on security interests?	No
	Will it have an impact on the right to liberty and security, right to fair trial and the right of defence?	No
	Does it affect the rights of victims of crime and witnesses?	No
Access to and effects on social protection, health and educational systems	Does the option have an impact on services in terms of quality/access for all?	No
	Does it have an effect on the education and mobility of workers (health, education, etc.)?	No
	Does the option affect the access of individuals to public/private education or vocational and continuing training?	No
	Does it affect the cross-border provision of services, referrals across borders and co-operation in border regions?	No
	Does the option affect the financing / organisation / access to social, health and care services?	No
	Does it affect universities and academic freedom / self-governance?	No
Culture	Does the proposal have an impact on the preservation of cultural heritage?	No
	Does the proposal have an impact on cultural diversity?	No
	Does the proposal have an impact on citizens' participation in cultural manifestations, or their access to cultural resources?	No
Social impacts in third countries	Does the option have a social impact on third countries that would be relevant for overarching EU policies, such as development policy?	No
	Does it affect international obligations and commitments of the EU arising from e.g. the ACP-EC Partnership Agreement or the Millennium Development Goals?	No
	Does it increase poverty in developing countries or have an impact on income of the poorest populations?	No

Table 47 Identification of potential environmental impacts

Area	Key Questions	Expected impacts
The Climate	Does the option affect the emission of greenhouse gases (e.g. carbon dioxide, methane etc.) into the atmosphere?	No
	Does the option affect the emission of ozone-depleting substances (CFCs, HCFCs)?	No
	Does the option affect our ability to adapt to climate change?	No

Area	Key Questions	Expected impacts
Transport and the use of energy	Will the option increase/decrease energy and fuel needs/consumption?	No
	Does the option affect the energy intensity of the economy?	No
	Does the option affect the fuel mix (between coal, gas, nuclear, renewables etc.) used in energy production?	No
	Will it increase or decrease the demand for transport (passenger or freight), or influence its modal split?	No.
	Does it increase or decrease vehicle emissions?	No
Air Quality	Does the option have an effect on emissions of acidifying, eutrophying, photochemical or harmful air pollutants that might affect human health, damage crops or buildings or lead to deterioration in the environment (soil or rivers etc.)?	No
Biodiversity, flora, fauna and landscapes	Does the option reduce the number of species/varieties/races in any area (i.e. reduce biological diversity) or increase the range of species (e.g. by promoting conservation)?	No
	Does it affect protected or endangered species or their habitats or ecologically sensitive areas?	No
	Does it split the landscape into smaller areas or in other ways affect migration routes, ecological corridors or buffer zones?	No
	Does the option affect the scenic value of protected landscape?	No
Water quality and resources	Does the option decrease or increase the quality or quantity of freshwater and groundwater?	No
	Does it raise or lower the quality of waters in coastal and marine areas (e.g. through discharges of sewage, nutrients, oil, heavy metals, and other pollutants)?	No
	Does it affect drinking water resources?	No
Soil quality or resources	Does the option affect the acidification, contamination or salinity of soil, and soil erosion rates?	No
	Does it lead to loss of available soil (e.g. through building or construction works) or increase the amount of usable soil (e.g. through land decontamination)?	No
Land use	Does the option have the effect of bringing new areas of land (‘green fields’) into use for the first time?	No
	Does it affect land designated as sensitive for ecological reasons?	No
	Does it lead to a change in land use (for example, the divide between rural and urban, or change in type of agriculture)?	No
Renewable of non-renewable resources	Does the option affect the use of renewable resources (fish etc.) and lead to their use being faster than they can regenerate?	No
	Does it reduce or increase use of non-renewable resources (groundwater, minerals etc.)?	No
The environmental consequences of firms and consumers	Does the option lead to more sustainable production and consumption?	No
	Does the option change the relative prices of environmental friendly and unfriendly products?	No
	Does the option promote or restrict environmentally un/friendly goods and services through changes in the rules on capital investments, loans, insurance services etc.?	No

Area	Key Questions	Expected impacts
	Will it lead to businesses becoming more or less polluting through changes in the way in which they operate?	No
Waste production / generation / recycling	Does the option affect waste production (solid, urban, agricultural, industrial, mining, radioactive or toxic waste) or how waste is treated, disposed of or recycled?	No
The likelihood or scale of environmental risks	Does the option affect the likelihood or prevention of fire, explosions, breakdowns, accidents and accidental emissions?	No
	Does it affect the risk of unauthorised or unintentional dissemination of environmentally alien or genetically modified organisms?	No
Animal welfare	Does the option have an impact on health of animals?	No
	Does the option affect animal welfare (i.e. humane treatment of animals)?	No
	Does the option affect the safety of food and feed?	No
International environmental impacts	Does the option have an impact on the environment in third countries that would be relevant for overarching EU policies, such as development policy?	No

Table 48 Assessment against fundamental rights

Fundamental Right	Potential impact
DIGNITY	
1. Human dignity	None
2. Right to life	None
3. Right to the integrity of the person	None
4. Prohibition of torture and inhuman or degrading treatment or punishment	None
5. Prohibition of slavery and forced labour	None
FREEDOMS	
6. Right to liberty and security	None
7. Respect for private and family life	None
8. Protection of personal data	None
9. Right to marry and right to found a family	None
10. Freedom of thought, conscience and religion	None
11. Freedom of expression and information	None
12. Freedom of assembly and of association	None
13. Freedom of the arts and sciences	None
14. Right to education	None
15. Freedom to choose an occupation and right to engage in work	None
16. Freedom to conduct a business	Possible
17. Right to property	Possible
18. Right to asylum	None
19. Protection in the event of removal, expulsion or extradition	None
EQUALITY	

Fundamental Right	Potential impact
20. Equality before the law	None
21. Non-discrimination	None
22. Cultural, religious and linguistic diversity	None
23. Equality between women and men	None
24. The rights of the child	None
25. The rights of the elderly	None
26. Integration of persons with disabilities	None
SOLIDARITY	
27. Workers' right to information and consultation within the undertaking	None
28. Right of collective bargaining and action	None
29. Right of access to placement services	None
30. Protection in the event of unjustified dismissal	None
31. Fair and just working conditions	None
32. Prohibition of child labour and protection of young people at work	None
33. Family and professional life	None
34. Social security and social assistance	None
35. Health care	None
36. Access to services of general economic interest	None
37. Environmental protection	None
38. Consumer protection	None
CITIZENS' RIGHTS	
39. Right to vote and to stand as a candidate at elections to the European Parliament	None
40. Right to vote and to stand as a candidate at municipal elections	None
41. Right to good administration	None
42. Right of access to documents	None
43. European Ombudsman	None
44. Right to petition	None
45. Freedom of movement and of residence	None
46. Diplomatic and consular protection	None
JUSTICE	
47. Right to an effective remedy and to a fair trial	None
48. Presumption of innocence and right of defence	None
49. Principles of legality and proportionality of criminal offences and penalties	None
50. Right not to be tried or punished twice in criminal proceedings for the same criminal offence	None

Appendix F. ESTIMATES OF COMPONENT COSTS OF THE TECHNICAL SOLUTIONS

Using data from the literature review, known sources of data on the costs of ITS components and from stakeholders consulted during this project, the data on the costs of the various components of systems for access to in-vehicle data have been compiled to provide as complete a picture as possible on the costs of the WG6 technical solutions. No information was found that enabled the benefits of gaining data through any of these solutions to be quantified.

In terms of component costs, the solutions which are technically distinct are:

1 On-board application platform

2 In-vehicle interface

3a Data server / extended vehicle

3b Data server / shared server or B2B marketplace

This data is derived from survey responses, recent studies such as the Ricardo report and direct contact with stakeholders to fill in gaps. The data on these components can be summarised diagrammatically in Figure 32.

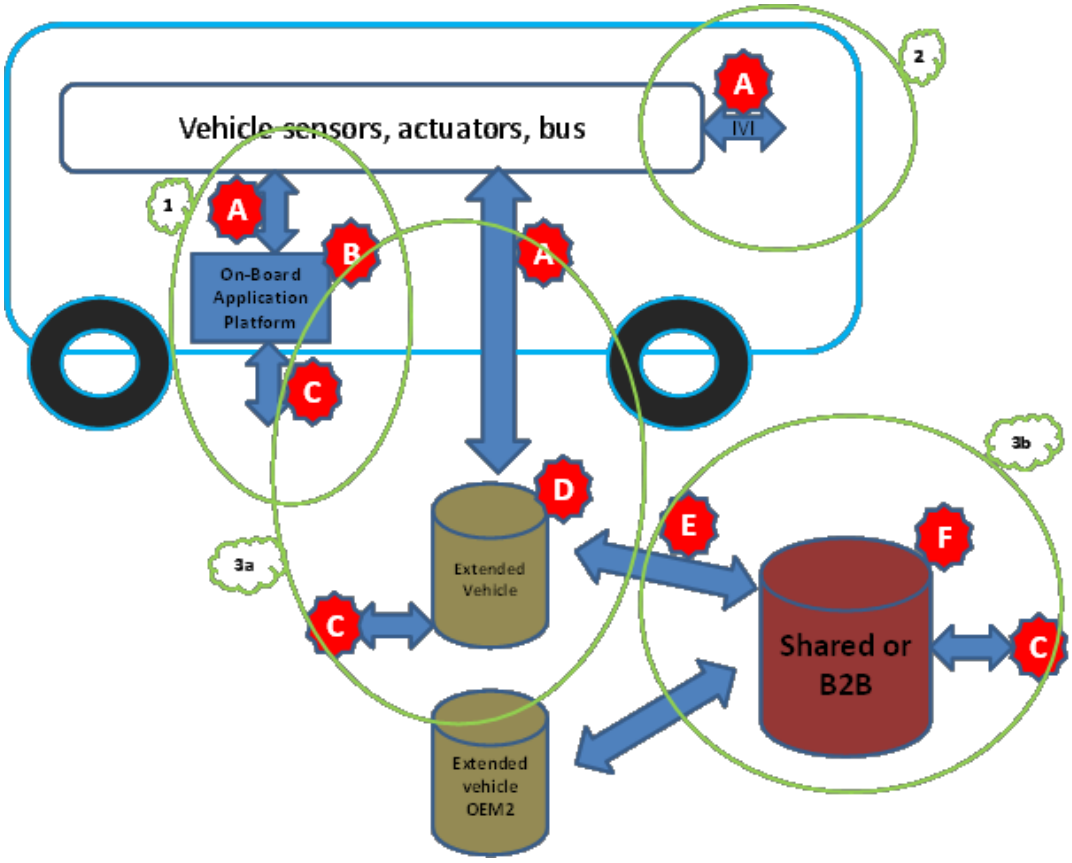


Figure 32: Components of the technical solutions

In Figure 32 the green ovals identify the architectural options and the red stars the costed components. The information available on these costs is summarised in Table 49. The sources of this data are as follows:

- The responses to the stakeholder survey, stakeholder workshop and stakeholder interviews carried out in this project and information from systems currently on the market

- The connected vehicle section of the US Department of Transportation database of ITS costs[40]
- Study on the deployment of C-ITS in Europe for DG MOVE by RICARDO[41]
- Personal communication with the National Data Warehouse in The Netherlands on the costs of setting up and operating a data server for traffic and transport information services
- Expert judgement of the TRL team to fill gaps and derive an overall estimate.

Table 49 shows that the quantitative data available is limited. In order to compare the relative costs of the various technical solutions, the qualitative comparison summarised in Section 4.5 was therefore carried out. The ranked and weighted scores of component costs used to identify the relative costs of technical solutions are shown in Table 51 while the unweighted rankings and the weighting factors used to derive the weighted scores are shown in Table 50.

40 http://www.itsknowledgeresources.its.dot.gov/its/benecost.nsf/SearchCosts?SearchView&Query=%22Connected%20Vehicles%22&Start=1&Count=10&SearchFuzzy=FALSE&SearchWV=TRUE

41 Ricardo Energy and Environment (2015). Study on the Deployment of C-ITS in Europe: input data overview – cost data. Report for DG MOVE MOVE/C.3./No 2014-794

Table 49 Component cost estimates for the technical solutions

Cost Item (Figure 32)	Description	Applies to technical solution				Information from stakeholders, literature review and equivalent components	US-DoT Cost	Ricardo	Summary Cost Estimate
		1	2	3a	3b				
A	Presentation of data from OEM sensors/actuators etc.	✓	✓	✓	✓	€400,000 suggested in questionnaire (seems low?) This would be per vehicle manufacturer So €1m seems likely to cover vehicle software development cost (i.e. ECUs) for presenting the data to the equipment in the vehicle. + €5 per vehicle - hardware for wiring/connectors etc.	Communication Equipment - for vehicle On-Board (VS) - Equipment list adjusted to 2014 dollars Capital Cost : 0.2 - 0.4 $k vehicle manufacturer Cost : 0.004 - 0.008 $k Source: http://www.itscosts.its.dot.gov/ITS/benecost.nsf/SubsystemCostsAdjusted?OpenForm&Subsystem=Vehicle+On-Board+(VS) NB these are based on 1995 estimates	Vehicle software development to vehicle manufacturer €1.51- 2015 NOTE: This is per vehicle cost, based on €1m SW dev cost, 350,000 vehicles per model run, and 50% of SW re-used from previous models	€750k development cost per vehicle manufacturer plus €5 per vehicle for hardware
B	On-board equipment – hardware, design, integration certification	✓				By analogy with eCall. One-off costs are absorbed into unit price €50 per vehicle - maintenance, secure communications and vehicle manufacturer maintenance of in-vehicle software [However eCall has low computing and sensor requirements – a smartphone is a closer analogy] >€70 per vehicle Proprietary solution €2k - €3k per vehicle	Hardware - $175 for 2017 and $75 for 2022. The second round consultation - $148 for 2017 and $73 for 2022. Unit Cost Element - Driver Interface and Schedule Processor i.e. Unit Cost Component - Driver Interface and Vehicle Logic Unit - $3900 Certification - $50/unit Sources http://www.itskrs.its.dot.gov/ITS/benecost.nsf/0/26D0D89DC2F1144185257BB40064D1B6?OpenDocument&Query=Home http://www.itskrs.its.dot.gov/ITS/benecost.nsf/0/CF13FF3616971BE88525796700606C3C?OpenDocument&Query=Home http://www.itskrs.its.dot.gov/ITS/benecost.nsf/0/752FD29FB428F63085257967005E3393?OpenDocument&Query=Home http://www.itskrs.its.dot.gov/ITS/benecost.nsf/0/076B6AC438EFF51485257D6300561C42?OpenDocument&Query=Home	A total upfront cost per vehicle (to the vehicle manufacturer) of €172.92 for ITS-G5 only and €180 for ITS-G5 and cellular. [However the €100 cost of the ITS-G5 receiver is likely to fall dramatically in time. A modern high-end smartphone, excluding display and battery is €50 - €75] Ongoing costs total €13.01- €15.97 per year, per vehicle (€10.57 for maintenance and software updates, plus €2.44 - €5.01 for communications).	€100 per vehicle plus €13-€16/year
C	Standardised interface for data and interface users	✓	✓	✓	✓	In some ways simpler than A as data will be more aggregated and standardised. However, standardisation of interface requires wider agreement so could be more complex & time consuming. Same cost assumed (€1m) Cost per vehicle likely to be lower than estimated for A due to greater level of software re-use from vehicle model to model. Mobivia Xee interface €139 TankTaler app based dongle €10-€150 (price to user, including development, hardware and software but not maintenance) Insurance: €50-€100			€1m development cost per vehicle manufacturer plus €10/vehicle

Cost Item (Figure 32)	Description	Applies to technical solution				Information from stakeholders, literature review and equivalent components	US-DoT Cost	Ricardo	Summary Cost Estimate
		1	2	3a	3b				
D	Database itself			✓		€1m/ year estimated based on equivalent commercial systems Unit Cost Element - Database Server Unit Cost Component - Data Archiving Database Server (High) Unit Cost Component - Design Phase- System and Software Architecture Description - System Requirements Specification - Interface and Database Design Definition- Hardware and Network Architecture - System Test Plan	$2m/year to operate a Traffic Management Centre Source: http://www.itscosts.its.dot.gov/its/benecost.nsf/ID/47A8E1B51CEE50DF852573E9006865D9?OpenDocument&Query=Home		€1.5m/year per manufacturer
E	Interface/integration of single vehicle manufacturer's data into shared server database				✓	€1m (TRL estimate)	Unit Cost Component - Software - Data Archiving (High) - $1,000,000 Source: http://www.itskrs.its.dot.gov/ITS/benecost.nsf/0/E8E6F31BD80340B885257A83007916EF?OpenDocument&Query=Home	Use "cost of developing Traffic Management Centre interface" at €1.5m, though not likely to be as complex	€1m per vehicle manufacturer
F	As D but all participating vehicle manufacturers				✓	€10m/ year (TRL estimate based on equivalent commercial systems – at least 10 times larger than individual server and 10-15 vehicle manufacturers involved) €15m initial cost of central data systems and €2.5m organisation set up, plus €9m/ year data procurement and €7m/year exploitation & innovation - National Data Warehouse www.NDW.nu (NL)			€10m for the 10-15 vehicle manufacturers involved.

In order to estimate the costs of the various technical solutions, TRL used a qualitative method. This was used to provide a high level comparison of the costs and was not designed to determine specific costs, but to broadly categorise the costs relative to each other. The information presented here is to document the method used to estimate the cost category of each technical solution.

Firstly, each cost component (row) in the table was ranked between 0 and 3 (representing zero, low medium and high cost) for each of the technical solutions (columns) considered. This ranking was made in a workshop environment and was based on the stakeholder input, previous research and the quantitative cost information gathered in this project,

Secondly, each component (row) was weighted to take into account how often this cost would be incurred. For example, database component costs would relate to a single (or small number of) hardware units, compared to costs that relate to each vehicle that would be required for millions of units.

These two steps are presented in the following tables and result in the high-level cost assessment for each solution shown in the last row of the second table. This assessment of costs should be repeated in the event that data of better quality becomes available.

Table 50 Ranked scores of component costs used to identify relative costs of technical solutions with weighting factors

Cost element	Weighting	On-Board Application Platform	In-vehicle Interface	Data Server - Extended Vehicle	Data Server - Shared Server	Data Server - B2B Market place	Neutral Server - (ACEA/ CLEPA)
Technical development (including engineering & validation)	10	3	2	1	1	1	1
In-vehicle hardware	100	2	2	1	1	1	1
Maintenance in-vehicle hardware	100	3	3	1	1	1	1
Database development	0.5	0	1	1	1	1	1
Database operation	0.5	0	1	1	1	1	1
Database maintenance	0.5	0	1	1	1	1	1
Server hardware	1	0	1	1	2	2	2
Server operation	1	0	1	1	2	2	2
Server maintenance	1	0	1	1	2	2	2
Administration & contracts	0.1	1	1	1	2	3	3
App service set up	2	1	1	1	1	1	1
App service operation	2	1	1	1	1	1	1
Cellular communication	100	2	2	2	2	2	2
RAN/ LAN/ Wi-Fi comms	0.1	0	0	1	1	2	2

Table 51 Ranked and weighted scores of component costs used to identify relative costs of technical solutions

Cost element	On-Board Application Platform	In-vehicle Interface	Data Server - Extended Vehicle	Data Server - Shared Server	Data Server - B2B Marketplace	Neutral Server - (ACEA/CLEPA)
Technical development (including engineering & validation)	30	20	10	10	10	10
In-vehicle hardware	200	200	100	100	100	100
Maintenance in-vehicle hardware	300	300	100	100	100	100
Database development	0	0.5	0.5	0.5	0.5	0.5
Database operation	0	0.5	0.5	0.5	0.5	0.5
Database maintenance	0	0.5	0.5	0.5	0.5	0.5
Server hardware	0	1	1	2	2	2
Server operation	0	1	1	2	2	2
Server maintenance	0	1	1	2	2	2
Administration & contracts	0.1	0.1	0.1	0.2	0.3	0.3
App service set up	2	2	2	2	2	2
App service operation	2	2	2	2	2	2
Cellular communication	200	200	200	200	200	200
RAN/LAN/Wi-Fi communication	0	0	0.1	0.1	0.2	0.2
Overall weighted score (rounded to nearest 10)	730	730	420	420	420	420
Relative score	High	High	Low	Low	Low	Low