ITS ACTION PLAN

FRAMEWORK SERVICE CONTRACT TREN/G4/FV-2008/475/01

ITS Action Plan – Action 4.1:

▪ Final Report ▪

Open in-vehicle platform concepts for the provision of ITS services and applications in heavy vehicles

Basel, 19. July 2013

ITS AP 4.1 - Phase 2 - D4 Final Report - V1.0 - 26July2013.docx

EUROPEAN COMMISSION

Directorate-General for Mobility and Transport

Unit D3 in collaboration with Unit C3

Rue J.-A. Demot 28, 07/005

B-1049 Brussels

Belgium

Contributors:

Bernhard Oehry, Cornelie van Driel, Lukas Haas, Gideon Dell, Peter Matthias Rapp

Versioning and content review information table

Version	Date	Author	Reviewer	Comments
0.1	27/05/2013	Rapp Trans	European Commission	First draft, based on D2, including comments from EC and internal meeting
0.2	03/06/2013	Rapp Trans		Including review comments from EC
0.3	18/06/2013	Rapp Trans		Including comments from internal meetings
0.4	25/06/2013	Rapp Trans		Major editing and new material
0.5	04/07/2013	Rapp Trans	European Commission	Editing; Incorporation of review text; “draft final”
1.0	26/07/2013	Rapp Trans		Final report

Contributors

Rapp Trans	Bernhard Oehry Cornelie van Driel Lukas Haas Gideon Dell
Carte Blanche Conseils	Peter Matthias Rapp

Disclaimer

This report was produced by the Algoé | Rapp Trans Grouping for DG Mobility and Transport (MOVE) and represents the Grouping’s views on the subject matter. These views have not been adopted or in any way approved by the Commission and should not be relied upon as a statement of the Commission’s or DG MOVE’s views.

The European Commission does not guarantee the accuracy of the data included in this report, nor does it accept responsibility for any use made thereof.

MANAGEMENT SUMMARY

The aim of this study is to recommend steps towards establishing a **truly open in-vehicle platform architecture** for the provision of ITS services in heavy vehicles and coaches. The scope of the study initially has been set with a focus on regulatory applications, especially the European Electronic Tolling Service, EETS, the revised Digital Tachograph, and on On-Board Weighing.

The main goal of the Commission and of **European transport policy** is to promote **opening up of transport markets to free and undistorted competition** and to find answers to the challenges of **environmental sustainability, interoperability, security and safety**.

The core idea of an open in-vehicle platform is to create an environment where **service providers can access resources** existing in the vehicle and plug into them in some controlled way in order to provide a wide range of freight and fleet management related services. There should be free and unhindered competition on the services market **for the benefit of the consumer**, which in this case is the transport company. The expectation is that an open ITS services market creates measurable gains in productivity and efficiency of the transport markets. Naturally such competitive access to vehicle and trip data and to other in-vehicle resources needs to be structured and controlled – which is the **task of the "architecture"**.

The study has analysed the **state of the art** in terms of regulatory environment, research projects, industry initiatives and technological developments. One of the main findings is that there are **many approaches towards defining a platform** for the provision of telematics services in vehicles and that the concept of platform architecture can encompass very different aspects in different contexts. For clarification we have structured our treatment of "**platform architecture**" into the following **five layers**:

- On a **components level**, architecture means how the different sensors, actors and communication modules are integrated into the vehicle and connected together.
- Architecture on a **system level** mostly addresses integration issues. Are all applications housed in separated "boxes"? Is there a multi-purpose computing platform? How are applications that stem from different legal environments certified (eCall, Tachograph, EETS, OBW, ...)?
- On **application level**, an architecture defines rules how to access and exchange data, in which way to provide services and in general a common "look and feel" of all application processes.
- An architecture on **business level** defines the relationship of the (commercial) stakeholders. Who pays? Who owns? Who controls? Who is liable? Whose branding is it? Is the market open to all players or is it restricted to players having a natural monopoly?
- Finally, on **governance level**, an architecture defines a common process paradigm for legislation, with similar certification requirements and pathways, and with similarly structured rights and obligations of the involved parties. The environment defined by technical standards is also part of the governance level.

The main finding of analysing these aspects or layers of a platform architecture has been that the **regulatory applications are the most demanding** ones regarding interoperability, certification and security and due to their mandatory nature can well **define the core of an open in-vehicle architecture**. The **regulator enjoys large powers and can set the stage**.

Yet the size of the **market of commercial applications is much larger** and commercial freight and fleet management applications are **decisive for the success** of an open in-vehicle platform concept.

On this market, the services branches of the **vehicle manufacturers and third party service providers compete**. Both market actors provide for essentially the same services supporting the transport company in vehicle management (managed maintenance, fuel consumption, scheduling, routing, etc.). Vehicle manufacturers have prime access to in-vehicle resources via the internal vehicle

bus system. There is the substantial **risk that vehicle manufacturers use this monopoly to exclude competition** by simply not granting access to the internal vehicle resources (vehicle and trip data, communications, display, etc.). In order to be able to successfully compete, third party service providers need access to the in-vehicle bus system. Naturally this access needs to be controlled by a gateway or firewall for reasons of safety, security and liability. Such gateways exist today (known e.g. as the FMS-interface) but are an optional component of a heavy vehicle and often come at substantial costs.

Based on the analysis in the report and on the findings on technology and market structure, the authors have developed the following **recommendations addressing the European Commission**:

Recommendation 1: No hindrance for coexisting applications

The EC is recommended to ensure that there are no elements in the technical specifications accompanying the respective regulations (EETS, Digital Tachograph, On-Board Weighing) that may hinder the coexistence of these applications with one another on integrated devices.

Recommendation 2: Open access to in-vehicle resources

The EC is recommended to create appropriate legal provisions such that in-vehicle resources like vehicle and movement data, communication channels and HMI devices are openly accessible via a standardised and mandatory interface ("ITS connector") and free of charge to any third party, given the consent of the vehicle owner and the driver.

Recommendation 3: Clarify ownership of vehicle data

The EC is recommended to create appropriate legal provisions such that vehicle data produced by busses, trucks and trailers of an operator (haulier) are accessible to and controlled by the operator and may freely be distributed to third parties with the prior consent of the operator. This applies both to open and unhindered access to in-vehicle resources as well as to access to centrally stored data.

Recommendation 4: GNSS, DSRC and communication module generally accessible

The EC is recommended to give mandates to the European Standard Organisations (ESO) to develop interface specifications for the GNSS, DSRC and communication functionalities as well as access elements to the HMI and data of other modules to be generally accessible resources in heavy vehicles.

Recommendation 5: Security appropriate for regulatory application

The EC is recommended to consider the highest conceivable security requirements when specifying general resources (e.g. DSRC or GNSS). The security level has to be appropriate for regulatory applications, being the ones with the highest security requirements.

Recommendation 6: Free trusted Position, Velocity, Time

The EC is recommended to investigate whether the GNSS receiver should be defined as trusted and requiring certification under the Digital Tachograph regime.

Recommendation 7: Embrace the services paradigm also for regulatory applications

The EC is recommended to gradually move towards a services-based paradigm for regulatory applications. In a migration phase users may voluntarily opt for fulfilling their obligations through a services model instead of or in addition to the traditional process.

TABLE OF CONTENTS

1. Background and motivation

European Transport Policy

Transport is fundamental to Europe's economy and society. Since transport is generally international, effective action requires strong **international cooperation**, especially in the areas of **interoperability** and **security**.

With the **White Paper on Transport Policy**[1], the European Commission adopted a roadmap of 40 concrete initiatives for the next decade to build a **competitive transport system** that will increase mobility, remove major barriers in key areas and fuel growth and employment.

These **initiatives** include, among others, the following key measures:

- Promote opening up of transport markets to **free and undistorted competition** and environmentally sustainable solutions.
- Continue to aim at **greater market access** in transport in all relevant international negotiations.
- Build on established research and innovation partnerships to find common answers to the challenges related to **interoperability** of transport management systems, **sustainable** low carbon fuels, **security** and **safety**.
- Support the development and deployment of the **key technologies** needed to develop the EU transport system into a modern, efficient and user-friendly system (e.g. ITS).

ITS Action Plan

Intelligent Transport Systems (ITS) can create clear benefits in terms of transport efficiency, sustainability, safety and security, whilst contributing to the EU Internal Market and competitiveness objectives.

The **ITS Action Plan**[2] aims to accelerate and coordinate the deployment of ITS in road transport, including interfaces with other transport modes. The Action Plan outlines six **priority areas** for action. For each area a set of **specific actions** and a clear timetable are identified.

One of these Action Areas is 4: **Integration** of the vehicle into the transport infrastructure.

In the context of the European transport policy, several road transport telematics applications are being **regulated** or imposed on vehicles, mainly heavy duty vehicles and coaches, for the sake of road safety and enforcement of various frauds. **Interoperability** and **security** at European level are

[1] COM(2011) 144
[2] COM(2008) 886

requirements, as synergies implying (cost-) efficiency need to be obtained, whilst guaranteeing security for the involved parties at all time.

In-vehicle services and applications typically build on a **limited set of ITS components** to cover for transport management needs or to fulfil the requirements stipulated in (existing or planned) legal acts. So far, implementation of most of these acts and agreements has been tackled in perfect **isolation** and has evolved independently of each other, resulting in **limited synergies** even when requirements or needs are quite similar.

Specific Action 4.1 of the ITS Action Plan aims at rationalising the implementation of legal provisions and enabling re-use of ITS components or systems on board of (commercial) vehicles:

Specific Action 4.1

Adoption of an open in-vehicle platform architecture for the provision of ITS services and applications, including standard interfaces.

Previous study

Under the framework contract "Technical, legal and organisational support for the implementation of the ITS Action Plan" a **first study** on the adoption of an **open in-vehicle platform architecture** for the provision of ITS services and applications had been launched as part of Specific Action 4.1.

Streamlining and integration of applications within a comprehensive **open systems architecture** would enhance reusability, extensibility and scalability, and therefore improve efficiency and reduce costs.

The aim of the first study was to define the **requirements for an open in-vehicle platform** supporting a wide range of current existing and future ITS applications, both for **private** and **commercial** vehicles. The main tasks included the identification of core platform elements and interfaces and the development of the operational and contractual framework of the system architecture.

This first study resulted in **eight strategic recommendations** to the European Commission.

These recommendations mainly addressed **commercial** vehicles and included, among others, encouraging the development of **standards** (e.g. on generic in-vehicle services for the provision of reliable and up-to-date basic vehicle information) and using the opportunity to consolidate the **regulatory framework** and **operational set-up** of telematics measures (e.g. Digital Tachograph, EETS, eCall) in order to **better align** their governance.

Evolving technologies

Many **initiatives** have been launched addressing a variety of aspects and perspectives related to an open systems architecture.

Cooperative systems

Cooperative systems are based on **vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications**. They **increase the "time horizon"**, the quality and reliability of information available to the drivers about their immediate environment, the other vehicles and road users. They

also offer **increased information** about the vehicles, their location and the road conditions to the road operators and infrastructure.

Important **building blocks** for the development and deployment of cooperative systems are the EC funded projects **CVIS, COOPERS and SAFESPOT**, which were concluded in March 2010 with a major demonstration in Amsterdam: the **Cooperative Mobility Showcase**.

The focus of these projects was on:

- The **development** of the (open) **communication architecture (e.g. open application framework)** and **technology** to use multiple communication media to connect vehicles with the infrastructure and with each other.
- The **demonstration** of a wide variety of **cooperative applications**, including advanced driver assistance systems that provided awareness of the hazards in the driving environment.

Building on the advances in cooperative systems, the current EC funded project on a **Europe-Wide Services Platform (EWSP)** – MOBiNET – focuses on identifying and analyzing the needs of both public and private sectors for the services enabled by the paradigm shift of the connected car to all road users. The aim of **MOBiNET** is to develop, deploy and operate the technical and organisational foundations of an **open, multi-vendor platform** for Europe-wide **mobility services**.

Platform technologies

An important building block for the development and deployment of platform technologies is the EC funded project **OVERSEE**, which was concluded in December 2012. The OVERSEE project concentrated on the **security** challenges of an **open in-vehicle platform** focusing on: (1) securely interfacing vehicular and environmental networks and (2) providing secure runtime environments for applications.

The OVERSEE project has **proven** that an open in-vehicle platform is **technically possible**. In the end, however, it is up to the **industry** to use the concept. The results of OVERSEE (and other projects) are currently used and extended in the EC funded project **PRESERVE** to develop a complete, scalable, and cost-efficient **V2X security subsystem**.

Vehicle buses

A **vehicle bus** is a specialized internal communications network that interconnects components inside a vehicle. Special requirements for vehicle control mandate the use of **protocols**, such as Controller Area Network (CAN), Local Interconnect Network (LIN) and Media Oriented Systems Transport (MOST). Additionally, many major car manufacturers use their own proprietary vehicle bus standards, or overlay proprietary messages over open protocols such as CAN.

To enable **manufacturer independent applications** for telematics, the major European heavy truck manufacturers have developed the so-called **FMS-standard** in 2002. The **Fleet Management Systems Interface (FMS)** is an **optional** interface of different truck manufacturers and may form the sole interface for a safe data connection of third party devices to the internal network (i.e. CAN-bus system) of a commercial vehicle.

Moreover, **industry initiatives**, such as AUTOSAR and the OPEN Alliance SIG, are dedicated to open in-vehicle platform architectures. **AUTOSAR** works on the development and introduction of an **open, standardized software architecture** for the automotive industry, whereas the **OPEN Alliance SIG** encourages wide-scale adoption of open, scalable **Ethernet-based** networks as the standard in automotive applications.

Legislation

There are current **regulatory developments** that need alignment for creating optimal chances for an open in-vehicle platform architecture.

European Electronic Toll Service

A **European Electronic Toll Service (EETS)** – as introduced in **Directive 2004/52/EC** and detailed in **Commission Decision 2009/750/EC** – shall be set up, by which road users only subscribe to one single contract with an EETS provider and have one single onboard equipment enabling them to pay road tolls in all European charging systems.

Directive 2004/52/EC prescribes the use of **one or more** of the following **technologies**: satellite positioning (GNSS), mobile communications using the GSM-GPRS standard and 5,8 GHz microwave technology (DSRC).

The proposed stepwise approach towards full deployment of EETS, called **Regional European Electronic Toll Service (REETS)**, is a first step towards full European interoperability. Member States with significant volume of traffic on the trans-European network should encourage the **cross-border interoperability** of their electronic road toll systems.

Digital Tachograph

The proposal to **revise Council Regulation No 3821/85** on recording equipment in road transport introduces **new functionalities** of the **Digital Tachograph**. Among other things, the new Regulation will provide for a tachograph allowing automatic recording of the location of the vehicle at certain points (GNSS functionality), remote communication for control purposes (DSRC functionality) and may optionally interface with external third party ITS devices.

On-board weighing

According to the **revision of Directive 96/53/EC** on weights and dimensions, Member States shall encourage the equipment of vehicles and vehicle combinations with **on-board weighing devices** (total weight and axle load). These devices shall use DSRC to communicate the weight data from a moving vehicle to an authority carrying out roadside inspections or responsible for regulating the transport of goods.

Moreover, it should be noted that the European Parliament in the legislative procedure of the **Digital Tachograph** recommends the Commission to consider the **inclusion of weight sensors** in heavy goods vehicles, and assess the potential for weight sensors to contribute to an improved compliance of road transport legislation[3].

In summary, these three regulations independently ask for the same core technologies GNSS and DSRC, enhancing the need for an open in-vehicle platform.

[3] 9275/1/13 REV 1 (4aa. on page 5)

This study

Based on the recommendations of the first study into an open in-vehicle platform architecture and on the need to align the ongoing initiatives and regulatory developments in this area, the European Commission proposed a **second phase of the study**.

The aim of this second study is to recommend steps towards establishing a **truly open in-vehicle platform architecture** for heavy vehicles and coaches – hereinafter combined and referred to as "**heavy vehicles**".

In support of the European Transport Policy and the ITS Action Plan, building upon the first phase of this study, and based on the market developments and recent developments in legislation, this study reemphasises the **need** for an open in-vehicle platform and proposes several concepts and recommendations to facilitate its **development** and **take-up**.

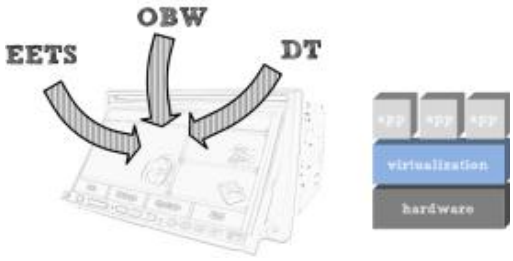
Chapter 2 first presents the **state of the art** on the **key applications** that need to be integrated on the platform or interconnected within the common architecture. Next, the state of the art on relevant **research projects and initiatives** is discussed in view of the functional and technical specifications and legal constraints imposed by the key applications.

Based on the state of the art, Chapter 3 points out what exactly we want to **achieve** with this second study into an open in-vehicle platform architecture, based on the positions of key stakeholders and on goals of a more generic nature.

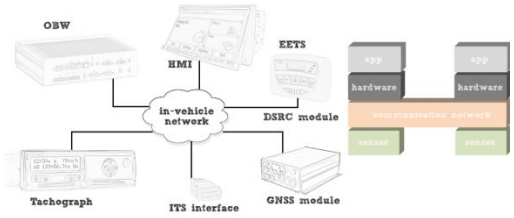
Our view on a **common architecture** for an open in-vehicle platform consisting of **five layers** is presented in Chapter 4. It is important for this common architecture that all layers must be **"platform-ready"**. The most relevant issues for making the layers platform-ready are discussed by synthesising the functional requirements and the technical constraints on the open platform architecture and checking the coherence and compatibility of these requirements and constraints.

Four possible **open platform concepts** are presented in Chapter 5. For each concept, the drivers and barriers in terms of achieving **stakeholder goals** and **technical and market feasibility** are discussed. Moreover, for each concept several **required actions** are proposed.

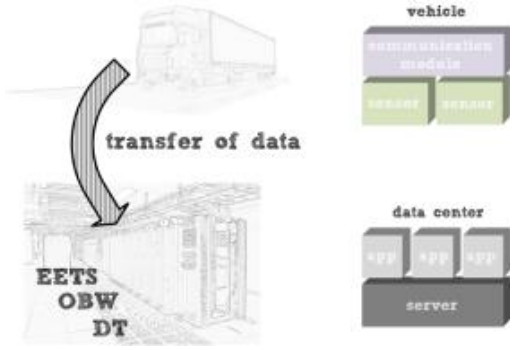
Option 1



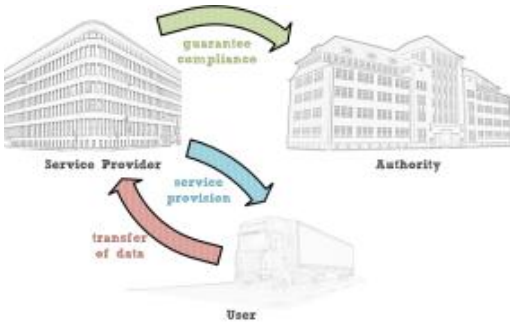
Option 2



Option 3



Option 4



The study results in a list of **recommendations** to the European Commission to ensure **effective development** and realisation of an open in-vehicle platform architecture for heavy vehicles and to facilitate its **market take-up** (Chapter 6). The results support an **open transport market** based on common answers to **interoperability** and **security** challenges and can serve as a basis for orienting future policy schemes and strategies linked to the ITS Action Plan and Directive 2010/40/EC, the ITS Directive.

2. State of the art

This chapter first presents the **state of the art** on the **key applications** that need to be integrated on the platform or interconnected within the common architecture. Next, the state of the art on relevant **research projects and initiatives** is discussed in view of the functional and technical specifications and legal constraints imposed by the key applications.

For a more **extensive review** on relevant EC funded projects and (industry) initiatives, the reader is referred to Annex 1 and to our first "Action 4.1" study. The following sections particularly present important findings from the **most relevant** or **newly started** projects and initiatives.

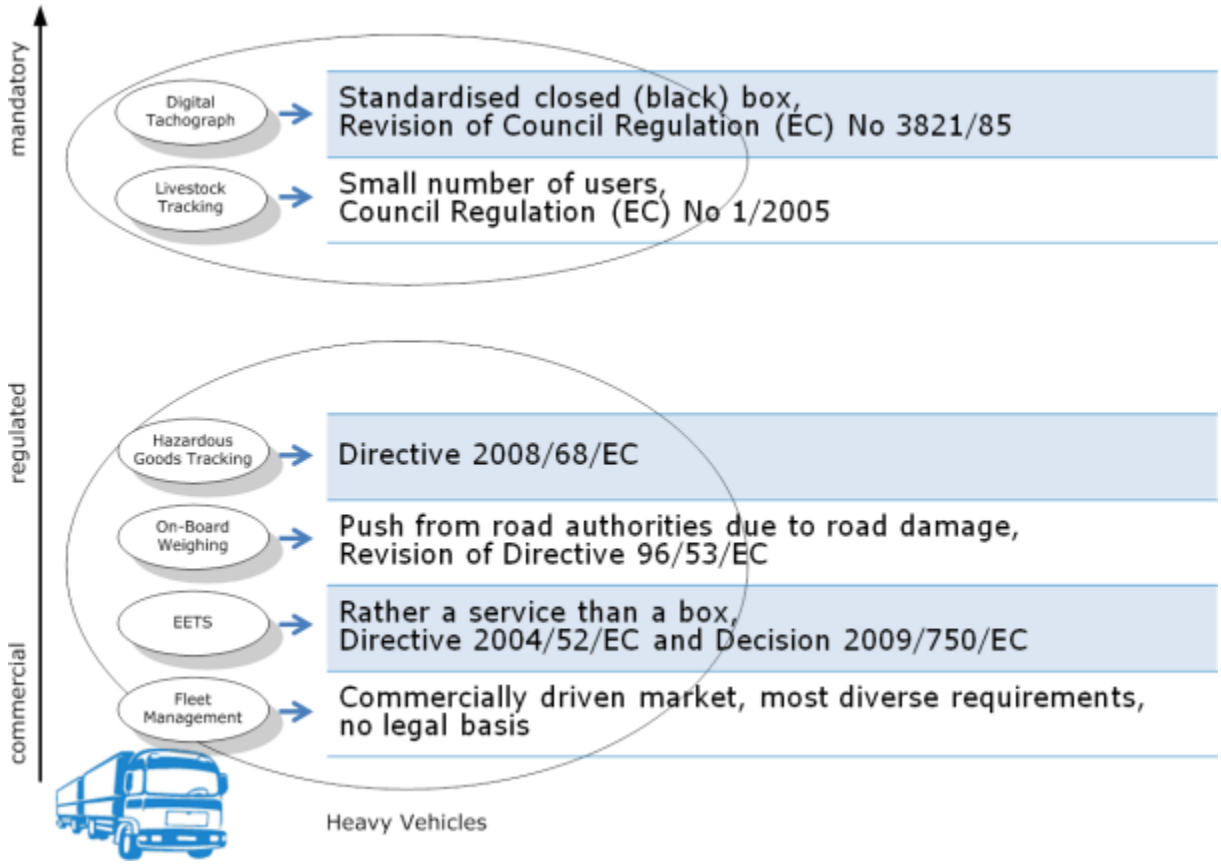


Figure 1: *Relevant services and applications for an open in-vehicle platform.*

2.1. Key regulatory applications

The basic set of services/applications to be accommodated has been defined in the Task Specifications of this study. The **basic set** includes the following elements (see also Figure 1):

- European Electronic Toll Service (EETS)
- Digital Tachograph
- On-board weighing function
- Management of dangerous goods
- Management of livestock
- Fleet and freight management.

2.1.1. Key applications

It has been defined by the European Commission that the main focus of this second study into an open in-vehicle platform architecture should be on a selection of **key regulatory applications**. The following selection has been chosen:

- European Electronic Toll Service (EETS)
- Digital Tachograph (DT)
- On-board weighing (OBW)

These services/applications are seen as the **relevant** ones, as they (will) apply to most heavy vehicles – in contrast to services/applications concerning the management of dangerous goods or livestock. Moreover, these key applications are **regulatory** – in contrast to fleet and freight management services/applications – which enables a good opportunity to **align** the on-going initiatives and create a **stepwise** approach for the adoption of an open in-vehicle platform architecture.

The remaining of this report focuses on the integration or functional interconnection of these three key regulatory applications within an open in-vehicle platform architecture.

It should be noted at this point that evolutions of other applications than just these three key regulatory applications have to be considered for developing the concepts. The market **view cannot be limited to regulatory applications only**. Rather it is necessary to understand how the market for ITS applications is structured.

For example, the market for fleet management systems has largely been dominated by a services industry not linked to the vehicle manufacturers. They used vehicle and DT information available on open interfaces to build their services. This has been a small market for a long time and the OEMs (I.e. vehicle manufacturers) showed little interest in it. With the recent success of such 3rd parties, the OEMs are now discovering the new intelligent fleet management sector. OEMs want to become "solution providers" in the sense that they not only produce the vehicle but provide for a full services portfolio around it. When buying a certain heavy vehicle brand, transport companies shall receive a complete care package, including managed maintenance, fuel efficiency, fleet scheduling and the like. Customer loyalty and long-term income through services has become an attractive business concept for OEMs.

Early attempts by OEMs did not have a big market success (e.g. the FleetBoard services offer by Daimler trucks had a difficult start). Thanks to the new strategy of providing full care packages, the services are now growing at much higher rates and nearly all OEMs are offering service packages.

In the past, vehicle and DT data have been quite accessible to 3rd party service providers through a number of open interfaces in the heavy vehicles. There is now a **risk that the OEMs will close**

currently existing interfaces in order to promote their own services and exclude 3rd parties from the market. The European Commission is following a policy of open markets and free competition (see Chapter 1 on European Transport Policy, where "free and undistorted competition" is a prime policy goal). These market trends regarding commercially driven applications have to be observed and are therefore included in the analysis of the three key regulatory applications in this report.

2.1.2. European Electronic Toll Service

Directive 2004/52/EC aims to achieve **interoperability** of the electronic road toll systems in the European Union. All **new** electronic toll systems brought into service on or after 1 January 2007 shall, for carrying out electronic toll transactions, use **one or more** of the following **technologies**:

- satellite positioning (GNSS)
- mobile communications using the GSM-GPRS standard
- 5,8 GHz microwave technology (DSRC)

Complementary to the national electronic toll services of the Member States, a **European Electronic Toll Service (EETS)** shall be set up, by which road users only subscribe to one single contract with an EETS provider and have one single on-board equipment.

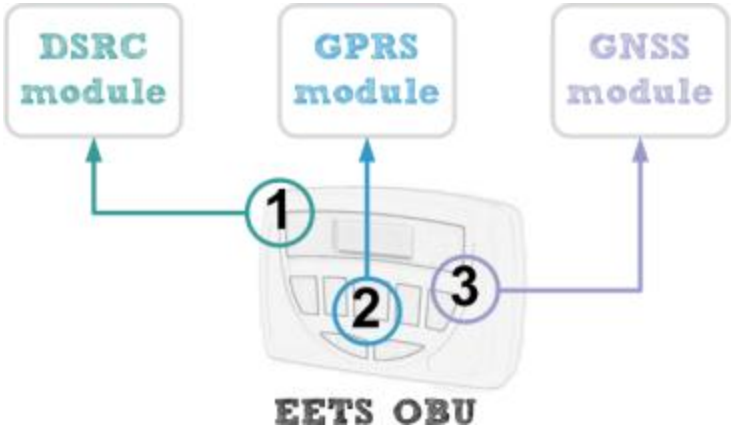


Figure 2: *Components of an EETS OBU.*

Commission Decision 2009/750/EC defining the EETS entered into force on 8 October 2009 upon its notification to the Member States. This implementing decision establishes the essential requirements of this service valid over the entire EU and sets the mandatory standards, technical specifications and operational rules.

The EETS can be seen as the first **services concept** of a regulatory application in Europe. The essence of EETS is that **EETS Providers** will collect the charges due by EETS Users on behalf of the Toll Chargers. For this, they need to provide the interoperable on-board equipment to EETS Users and guarantee payment to Toll Chargers.

Unfortunately, the progress achieved in the advancement of EETS deployment is disappointing[4]. Among others, due to difficulties establishing a sound business case for EETS Providers, the EETS is **not yet a reality** in everyday life of road users.

It is likely that EETS Providers will need to enhance their incomes through providing **value-added services**. For example, the EETS on-board equipment functionalities could be used by other telematics applications and services, such as remote diagnostics, fleet management solutions or real-time traffic and travel information. Moreover, under the latest amendment of Directive 1999/62/EC, the Eurovignette Directive, which will be fully applicable at the latest by **28 September 2013**, all users shall be able to obtain on-board units **fully compliant with EETS** in Member States where tolls are collected by means of an on-board unit[5].

REETS

As a first step towards full European interoperability, Member States with significant volume of traffic on the trans-European network shall encourage the **cross-border interoperability** of their electronic road toll systems.

In 2011, Germany and Austria launched TOLL2GO, one of Europe's first interoperable electronic toll schemes, where a single on-board unit is used for payment in both countries. The success of TOLL2GO convinced many doubters of interoperable toll charging, and it is now accepted that there might be a business case for the **regional EETS (REETS)**.

Early deployment projects on a regional basis are promoted in a way so that they can be extended to cover all the electronically tolled road infrastructures in the EU as soon as possible at a later stage and can provide concrete experiences in solving practical EETS issues.

Relevant for this study

Interoperability is still an issue. Although the EETS is not yet successful and a stepwise approach (REETS) is needed, it relies on existing legislation and the Member States will have to comply.

Moreover, the EETS sets an example for a services concept of a regulatory application. EETS Providers will likely use the EETS on-board equipment functionalities (i.e. GNSS, GSM-GPRS and DSRC) to provide other value-added services. Setting up the EETS as such is left to the market with the EC providing the framework for its establishment. The essential requirements for interoperability (e.g. technical specifications and mandatory standards) as well as procedural, contractual and legal aspects relating to EETS provision are set by Commission Decision 2009/750/EC.

2.1.3. Digital Tachograph

The Tachograph is a regulatory instrument recording the work and rest hours of drivers for checking compliance with social regulations in road transport. Since 2006, new vehicles need to be equipped with a version of the Tachograph employing digital electronics for storing the driver records. The specification of this Digital Tachograph is laid down in an annex of **Council Regulation No 3821/85**.

[4] COM(2012) 474
[5] SWD(2013) 1

In July 2011 the European Commission proposed to introduce a “Smart Tachograph” by amending the regulation.

The aim of the new legislation is to make **fraud** more difficult and to reduce the **administrative burden**, notably by introducing the satellite-linked “Smart Tachograph” as well as a number of new regulatory measures.

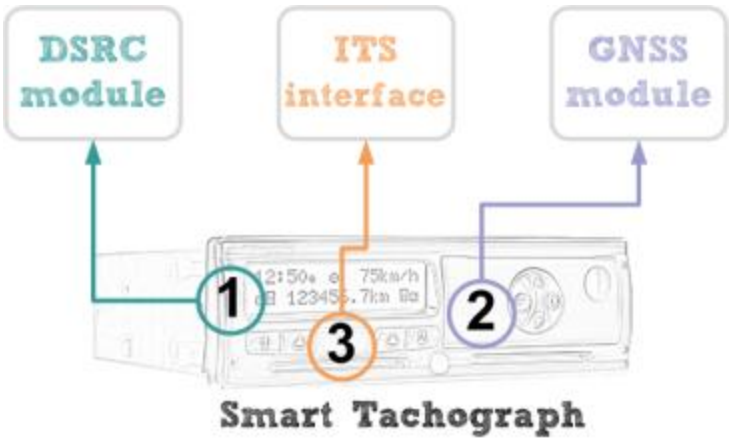


Figure 3: *Components of the Smart Tachograph*

The **revision** of Council Regulation No 3821/85 introduces a number of novelties which will require subsequent changes in the Annex IB of the same regulation, which lays down the technical specifications of the Digital Tachograph. The proposal foresees fundamental enhancements of the functions of the Tachograph:

- Automatic recording of precise location (**GNSS functionality**): satellite localisation functionality for automatic recording of vehicle positions
- Wireless communication for roadside checks (**DRSC functionality**): wireless interrogation functionality for remote checks of passing vehicles from roadside
- **Interface to other ITS applications**: optional interface to in-vehicle applications that may want to make use of Tachograph data

The proposal also foresees to upgrade the **security mechanisms** which need to be enhanced in order to continue to guarantee a high level of security and data protection while avoiding fraud and tampering of the data recorded by Tachographs.

New functionalities

With the adoption of the amendments, the new functionalities need to be specified in technical detail and will eventually be formalised as implementing acts.

For a comprehensive description of the new functionalities and a good insight into the different options, the interested reader is referred to the following two **feasibility studies**:

- Implementation of GNSS functionality in the Digital Tachograph: Technical Options Review and Discussion[6]
- Possible Application of Short Range Communication Technologies in the Digital Tachograph System to Support Vehicles filtering during Road Controls[7]

[6] Currently under review

[7] Published in 2011 under catalogue number LB-NA-24894-EN-C and ISBN: 978-92-79-20798-3

GNSS functionality

In order to facilitate verification of compliance with the relevant legislation, the **position** of the vehicle shall be **recorded automatically** at the following points, or at the closest point to such places where the satellite signal is available:

- the starting place of the daily working period
- every three hours of accumulated driving time
- the ending place of the daily working period

For that purpose, vehicles shall be fitted with a Tachograph connected to a **positioning service** free of payment and based on a satellite navigation system, for example GPS, GALILEO or GLONASS. Positioning **quality** of these GNSS is **sufficient** for the Tachograph. Receivers can exploit several GNSS in parallel, thereby improving the performance (i.e. higher sensitivity, shorter acquisition times and more precise localisation). **No position data** other than the one expressed shall be **permanently stored** in the recording equipment.

The new **satellite positioning** functionality may create the following **benefits**:

- Automatic recording of the positions where the daily working hours start an end. This is currently done manually, taking up one minute of the driver's time per day and often leading to input errors and fraud.
- Compliance checks by roadside controllers become more effective since trip distance is better known for the purpose of plausibility checks against claimed driving time.
- The satellite signals provide for exact time for all Tachographs and controllers, and can also be used for acquiring the independent movement signal required by legislation.
- The satellite positioning provides for location, speed and time, which can be made available outside the Tachograph via the optional interface as a valuable resource for applications like eCall, tolling, cooperative systems and fleet management in general. (Note that since this interface is optional, vehicle manufacturers may decide to not provide this open access to DT and GNSS data for commercial reasons, e.g. in order to close the market for 3rd party service providers)

The new satellite-linked technology will become mandatory 36 months after the technical specifications for the new tachograph have been established, **probably in 2017 or 2018**[8]. This applies to newly registered vehicles. Other vehicles involved in international transport must be retrofitted with the "Smart Tachograph" at the latest 15 years after the above date of application.

DSRC functionality

The original and prime functionality of the Tachograph is to document, i.e. to record the driving history of a driver and his vehicle. Usually **controls** are rather inefficient. A road-side inspection needs to flag a random sample of heavy vehicles down, park them, ask for a download of the Tachograph data on an Intelligent Downloading Equipment (IDE) and then analyse them. Throughput at a control site is very low.

In order to facilitate targeted roadside checks, the Tachograph shall be augmented with **short range communication** features to be able to **communicate** to control authorities, when so requested by the equipment of these authorities. Such a wireless interrogation of the Tachograph of a vehicle passing a road-side check-point will supply information that assists control personnel to decide whether or not to stop the vehicle for a more extensive check. Where applicable, the data exchanged during communication with the control authorities in the Member States should comply with relevant

[8] 9803/13 Presse 206

international standards such as the suite of standards related to **DSRC** established by the European Committee for Standardization[9].

The data exchanged during communication shall be limited to the **data necessary** for the purpose of achieving targeted roadside checks. The data communicated from vehicles in freely flowing traffic to road-side stations shall only serve the purpose of providing information for "pre-filtering", i.e. to identify vehicles where there is an increased likelihood that it is in breach of the social regulations (e.g. the latest security breach attempt, driving without a valid card, card insertion while driving, time adjustment data, speed recorded by the Tachograph). The DSRC data received from passing vehicles at road side are not used to initiate legal proceedings, but to select vehicles that should be stopped for a more extensive check. A fine shall only be given on the basis of the extensive manual checks.

The communication shall be **secured** to ensure data integrity and authentication of the recording and control equipment. Access to the data communicated shall be **restricted** to enforcers authorized to control infringements and to workshops insofar as it is necessary to verify the correct functioning of the Tachograph.

The **benefit-to-cost ratio** is expected to be **excellent**, both for the vehicle owner who benefits from being left unbothered in case he shows no signs of infringement and for the control authorities who would enjoy a ten-fold increase of checking efficiency. Potential synergies with other applications, such as the enforcement of toll payments, do exist.

Member States have to ensure that control officers have sufficient equipment to carry out their monitoring tasks, but there will be **no obligation** to provide them with remote early detection equipment during the first 15 years following the introduction of the "Smart Tachograph"[10]. After that period, Member States will provide such equipment as appropriate, depending on their national enforcement strategies.

ITS interface

Tachographs may either be equipped with an **interface** or have the capacity to **connect to an interface** allowing the data recorded or produced by the Tachograph to be used in operational mode, by an external device, provided that the following **conditions** are met:

- the interface does not affect the authenticity and the integrity of the data of the Tachograph
- the interface complies with the legal specifications
- the external device connected to the interface has access to personal data, including geopositioning data, only after the verifiable consent of the driver to which the data relates

Note that the major European truck manufacturers argue that a harmonized ITS interface already exists with some vehicles which are in scope of the DT regulation through the FMS-standard (see also Section 2.6.1). All current DT on the market are equipped with an interface (remote download interface) allowing third party vendors to link their ITS solution with the DT. This interface may disappear in future because of the wording of the new DT regulation which makes the ITS interface an optional feature ("DT **may** be equipped …"). This could lead to a change of the market because vehicles manufacturers will be able to have a monopoly regarding access to vehicle data.

[9] 9275/1/13 REV 1
[10] 9803/13 Presse 206

Moreover, it should be noted that the European Parliament in the legislative procedure of the **Digital Tachograph** recommends the Commission to consider the **inclusion of weight sensors** in heavy goods vehicles, and assess the potential for weight sensors to contribute to an improved compliance of road transport legislation[11].

Relevant for this study

The proposal to revise Council Regulation No 3821/85 introduces GNSS and DSRC as mandatory functionalities of the Digital Tachograph. It would be highly unfortunate if this would lead to multiple DSRC and GNSS modules in both the Digital Tachograph and the EETS on-board equipment. A platform with shared resources should be envisaged as a must.

2.1.4. On-board weighing (OBW)

It was deemed necessary to **amend Directive 96/53/EC**[12] to improve the aerodynamics of vehicles and their energy efficiency, while continuing to improve road safety, and within the limits imposed by the geometry of road infrastructures.

Because the current Directive has no provisions on vehicle checks and the applicable penalties, many **infringements** go unpunished. The main infringement committed is **overloading** the vehicle. On average, one in three vehicles checked is overloaded. These excess loads often exceed the maximum authorized weight by 10 or even 20%. This causes premature **wear and tear** of road surfaces and increases the risk of **accidents**. It also distorts **competition** between transport companies, because the fraudsters can illegally gain undue competitive advantages.

Proposed amendments

The proposal for a Directive amending Directive 96/53/EC[13] on vehicle weights and dimensions suggests adding new provisions to Directive 96/53/EC to enable the inspection authorities to better **detect** infringements and **harmonize** administrative penalties that apply to them.

Among other things, Member States must carry out a minimum number of vehicle checks, using either **weighing systems** built into the **road** or by means of **on-board** sensors in vehicles which communicate remotely with roadside inspectors. These measurements will allow the inspection authorities to **filter** the vehicles, so that only vehicles strongly suspected of infringement are stopped for manual inspection.

Member States shall **encourage** the equipment of vehicles and vehicle combinations with **on-board weighing devices** (total weight and axle load) to enable the weight data to be communicated at any time from a moving vehicle to an authority carrying out roadside inspections or responsible for regulating the transport of goods. This communication shall be through the interface defined by the **CEN DSRC** standards[14].

[11] 9275/1/13 REV 1 (4aa. on page 5)

[12] laying down for certain road vehicles circulating within the Community the maximum authorised dimensions in national and international traffic and the maximum authorised weights in international traffic

[13] COM(2013) 195

[14] EN 12253, EN 12795, EN 12834, EN 13372 and ISO 14906

The EC shall be empowered to adopt **delegated acts** concerning:

- the additional technical specifications to ensure full **interoperability** at EU level of the on-board weighing equipment
- the procedures for the **pre-selection checks**, the technical specifications, precision requirements and instructions for use of the equipment employed in these pre-selection checks

Regarding the transport of **containers**, the shipper shall give the road haulier to whom it entrusts the transport of a container a statement indicating the weight of the container moved. If this information is missing or incorrect, the shipper shall incur **liability** in the same way as the haulier if the vehicle is overloaded.

On-board weighing (OBW) systems

Static OBW systems have been used in the trucking industry for many years. They weigh the vehicle when it is stationary, e.g. at parking lots. The main objective is to **optimise truck fleet management and routing** with respect to their capacity and load limits.

The technology has improved and currently also **dynamic OBW systems** that weigh the vehicle when it is in motion are available on the market. Such systems include, for example, components that can control and **balance the loads** per drive axle while driving. This may result in longer tires life, smooth riding and roll stability, and better braking capabilities.

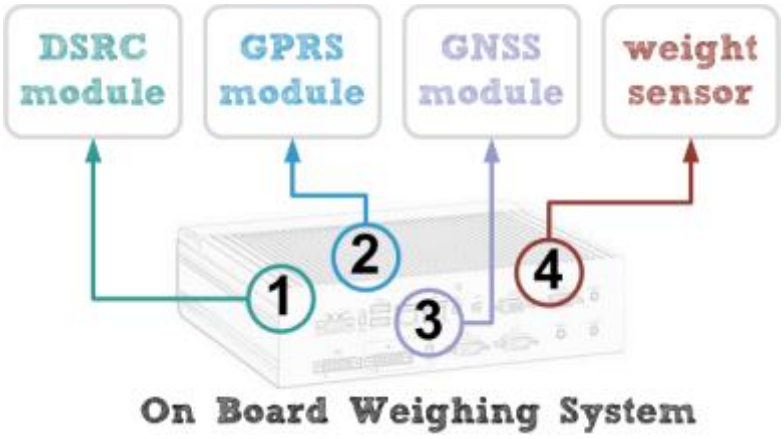


Figure 4: *Components of an OBW System.*

Current OBW systems can do **much more** than just provide weight data to the vehicle operator. Wireless handheld displays, on-board printers, data loggers and weight data transmission are a few of the features now available. For example, a **mobile connection** (e.g. GPRS, UMTS) enables sending the load information to a central system (e.g. owned by vehicle owners or control authorities). A **GNSS** signal could add **location information** meeting the needs of hauliers, fleet managers, road managers and control authorities. As an alternative to GNSS, the mobile connection could also provide location information via cell location information.

The **accuracy levels** attained by current OBW systems are deemed **not sufficient** for **direct** enforcement. However, added with a **DSRC** interface, these OBW systems would be suitable for **screening** overloaded (or wrongly loaded) trucks prior to a control area. It is evident that OBW systems to be used for such weight enforcement purposes have **more stringent requirements** than the systems that are used nowadays by fleet owners to manage freight operations.

The **technology** for OBW sensors depends on the type of suspension of the vehicle. The two main types are load cell (esp. in steel-sprung suspensions) and air pressure transducer (APT) (esp. in air bag suspensions). **Load cell** based systems are more **accurate** than APT based systems[15]. The reason is that an air bag suspension can take more than a minute to stabilise after stopping from a movement, so a mass reading taken while the air in the suspension is still fluctuating may not capture the true load. However, **APT** based systems are **less costly** and more appropriate for after-market installation. This latter might be a temporary advantage only; in a longer perspective, OBW sensors may be integrated by the vehicle manufacturers (on the level of the technical architecture).

For more information on OBW and also Weigh-in-Motion (WIM), the interested reader is referred to Annex 2: Weighing technologies.

Examples of weight compliance approaches

The **Intelligent Access Program (IAP)** in **Australia** is a **voluntary** program which provides heavy vehicles with wider access to the Australian road network. In return, heavy vehicles enrolled in the IAP will be **monitored** by vehicle telematics solutions for compliance with specific access conditions. The IAP will be extended to include mass monitoring utilising **on-board mass monitoring (OBM) systems**. The integration leverages the same infrastructure and operating environment that jurisdictions have become familiar with in operating their current IAP access applications. Significant investments are being made to achieve a **single national standard** for interoperability between existing in-vehicle units (IVUs) and OBM systems.

Another potential approach of weight compliance can be found in **Lyon**, France. Recently a strategic work plan has been discussed that foresees studying the possibility of **opening bus lanes** to heavy goods vehicles "with optimised load" in urban delivery[16].

For **weight enforcement**, a significant gain of security and efficiency could be reached if the pre-selection command ("Exit at next enforcement area") could be delivered to the driver cabin and displayed to the driver (e.g. see Figure 5).

Also relevant in this area are the developments in the transport of containers, where **mandatory container weighing** may be probable from 2016 onwards[17]. Shippers could then be required to prove the actual weight of each container before loading it onto a ship. The revision of Directive 96/53/EC now foresees that if the shipper's statement indicating the weight of the container is missing or incorrect, the shipper shall incur liability in the same way as the haulier if the vehicle is overloaded.

[15] On-Board Mass Monitoring Test Report (Final), May 2009, Transport Certification Australia

[16] In: Communauté urbaine de Lyon - Conseil de communauté du 18 février 2013 - Délibération n° 2013-3488

[17] http://www.verkehrsrundschau.de/obligatorische-container-waegung-ab-2016-wahrscheinlich-1245531.html (16 May 2013)

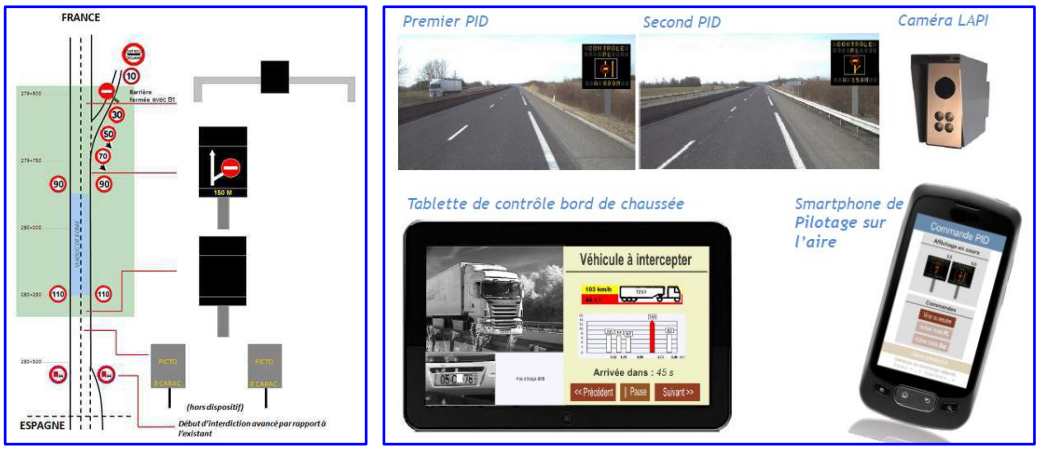


Figure 5: *Provision of pre-selection command to the driver (left: [18], right: [19])*

Moreover, it should be noted that the European Parliament in the legislative procedure of the **Digital Tachograph** recommends the Commission to consider the **inclusion of weight sensors** in heavy goods vehicles, and assess the potential for weight sensors to contribute to an improved compliance of road transport legislation[20].

Relevant for this study

The proposal to revise Directive 96/53/EC foresees, among others, that Member States shall encourage the equipment of vehicles and vehicle combinations with OBW systems using a DSRC interface to communicate the weight data to officials or to roadside automatic inspection systems without stopping the vehicle.

This way, new approaches to weight compliance are conceivable, such as giving compliant vehicles an advantage (e.g. no stopping at roadside checks, (improved) road access like in Australia's IAP or in Lyon, lower tolls).

[18] ASF (2013) Des panneaux dynamiques pour les contrôles douaniers de poids lourds, presented at the ATEXPO Conference, ATEC-ITS, Paris, France 2013, 30-31 January 2013

[19] Klein, E. & Dolcemaskolo, V. (2013) Optimisation du contrôle des surcharges par couplage de technologies, presented at the ATEXPO Conference, ATEC-ITS, Paris, France 2013, 30-31 January 2013

[20] 9275/1/13 REV 1 (4aa. on page 5)

2.2. Further regulatory applications

An open in-vehicle platform should not only be able to integrate the above-mentioned regulatory key applications. It should also be able to integrate or connect to other (potential) regulatory applications. The following regulatory background is deemed relevant for establishing a **future proof** open in-vehicle platform.

2.2.1. eCall

In case of a crash, an eCall-equipped car **automatically calls** the nearest emergency centre (see Figure 6). Even if no passenger is able to speak, e.g. due to injuries, a "Minimum Set of Data" is sent, which includes the exact location of the crash site. Shortly after the accident, emergency services therefore know that there has been an accident, and where exactly.

The introduction of eCall requires, among other things, that a vehicle is equipped with a **GNSS module** and a **GSM module**. The Commission is reinforcing efforts to speed up the deployment of eCall, with the aim of having a fully functional EU-wide service in place by 2015.

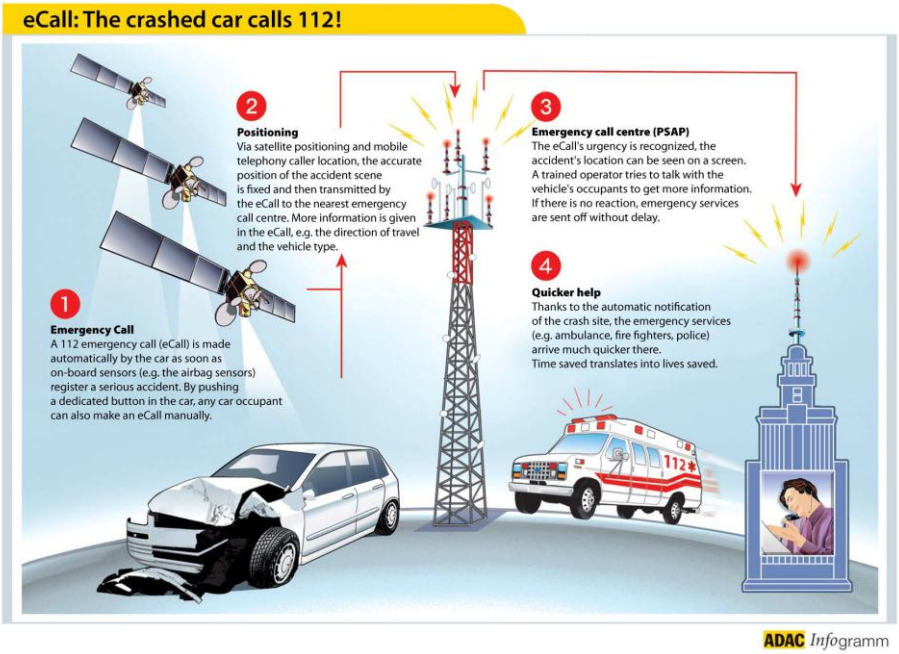


Figure 6: *eCall saving lives through in-vehicle communication technology*

2.2.2. Event Data Recorder (EDR)

Event Data Recorders (EDR) are devices which continuously **register and store** the values taken by a series of **vehicle parameters** so that a sequence of those records covering some seconds before, during and after a **crash** can be recovered.

The Commission recently published a Call for Tenders[21] for a study on the benefits for road safety resulting from the installation of EDR. The purpose of the contract is to assist the Commission in deciding whether the fitting of EDR in all vehicles or certain categories of vehicles could result in an improvement of road safety or have other positive consequences that would justify the **adoption of EU legislative measures** and to assess the cost and benefits of such measures.

Usage of the device **varies widely** from manufacturer to manufacturer: some manufacturers implement the technology on most of their recent models, whereas others do not use EDRs at all. It is assumed that there are (and will be) different system approaches for the realization of EDR functionalities in a vehicle. The different solutions will vary from **fully integrated** (embedded) EDR to **retro-fit** (stand-alone) solutions. There will also be only partly integrated systems driven by the vehicle manufacturers who will add lacking EDR input signals or functionalities by adding necessary components to the vehicle network already existing.

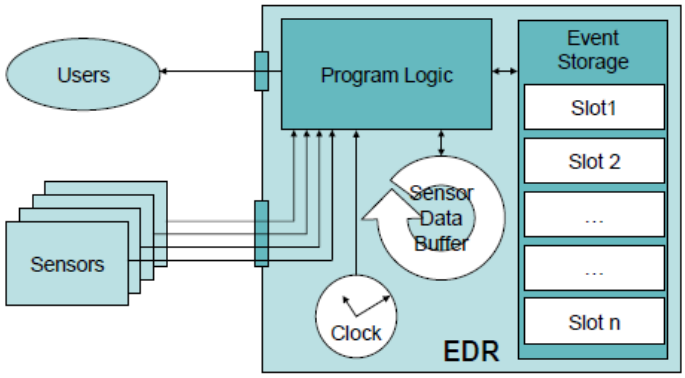


Figure 7: *EDR functional model*[22]

Figure 7 shows that one of the main components of an EDR is the **Sensor Data Buffer**, which permanently receives data from the sensors. There is a differentiation between the **data elements recorded** in an EDR and the necessary **input signals** for the EDR provided by the vehicle and its network. The minimum required data elements by existing standards (e.g. SAE Standard J1939-71) include: longitudinal acceleration, lateral acceleration, speed, engine throttle, brake status, indicator, etc. **Satellite position information** is not a minimum required data element; it depends on the system whether it is included and will be recorded.

Embedded and partly integrated EDR systems will be not concerned by **interface standardization**, because the manufacturers will have to accomplish the whole EDR functionality within their vehicle network and will have to safeguard the compliance with the future EDR legislation. The need for the definition of an input interface is relevant only for stand-alone systems. This is to introduce a safeguard that after-market solutions can rely on identical electronic interfaces that connect to the vehicle.

[21] Call for Tenders N° MOVE/C4/2013-200-1

[22] Vehicle Event Recording based on Intelligent Crash Assessment, VERONICA – II, Final Report, 6 October 2009

2.2.3. Roadworthiness inspection

Before a vehicle may be put on the market, it has to fulfill all the relevant **type or individual approval requirements** guaranteeing an optimal level of safety and environmental standards. The goal of roadworthiness testing is to check the functionality of safety components, the environmental performance and the compliance of a vehicle with its approval.

Roadworthiness Package

In July 2012 the Commission put forward a proposal on the **technical roadside inspection** of the roadworthiness of commercial vehicles circulating in the Union to support and to enforce roadworthiness testing with a view to enhance road safety and environmental protection ("Roadworthiness Package")[23].

The **Roadworthiness Package** will carry over the existing requirements laid down in the existing legislative framework related to the roadworthiness regime, which covers roadworthiness tests (Directive 2009/40/EC), roadside inspections (Directive 2000/30/EC) and rules on the registration of vehicles (Directive 1999/37/EC).

The main objective of the proposal is to provide for **a risk-rating system** aimed at focusing inspections on vehicles operated by undertakings with poor safety records, thus rewarding vehicles operated by undertakings that are mindful of safety and the environment. Also **more elaborated roadside inspections** shall be performed using testing equipment either by mobile inspection units or at test centers in close vicinity.

There is no agreement yet on the details of the proposal, but it might be assumable, that in future commercial vehicles may be **checked remotely** for compliance with roadworthiness requirements, for example by using dedicated short range communication (DSRC)[24]. This will allow the inspection authorities to **filter** the vehicles, so that especially "high risk" vehicles are stopped for roadside inspection.

PrePass system in the USA

PrePass is the **weigh station bypass system** in the majority of states in the USA. It enables participating transponder-equipped commercial vehicles to electronically comply with state safety, weight, and credential requirements. **Cleared vehicles** are allowed to bypass designated weigh stations, port-of-entry facilities and agricultural interdiction facilities. They may proceed at highway speed, eliminating the need to stop (see Figure 8). That means greater efficiency for shippers and improved safety for all highway users.

[23] COM(2012) 382

[24] http://www.verkehrsrundschau.de/neue-eu-regeln-fuer-lkw-unterwegskontrollen-1249203.html (31 May 2013)

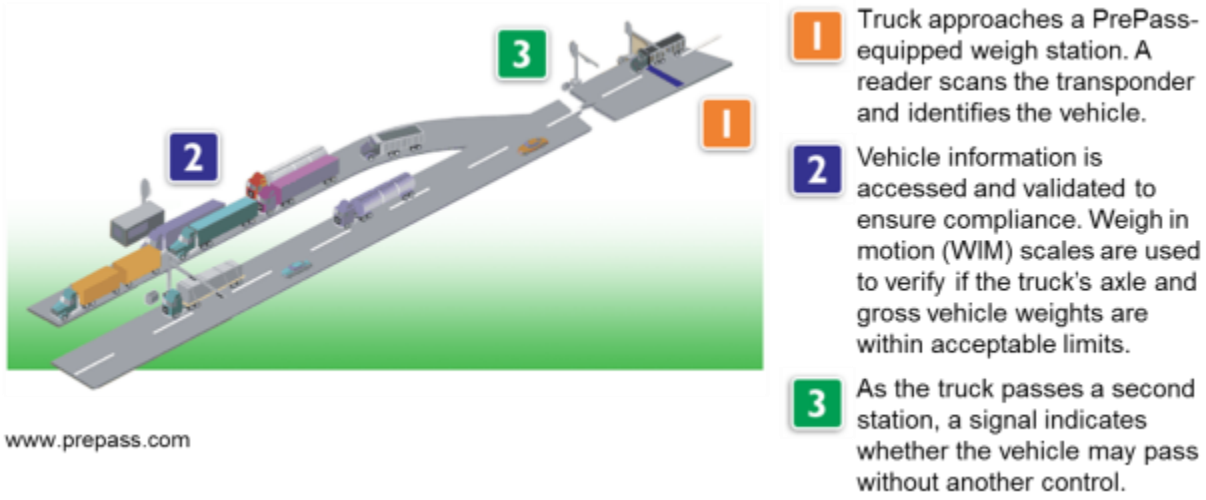


Figure 8: *PrePass system in the USA*

Recently the 5.9 GHz DSRC technology has been selected to power the next generation of PrePass transponders[25]. The old generation consists of 915 MHz transponders. The 5.9 GHz technology has been selected by U.S. Department of Transportation as the technology standard for its Connected Vehicle Program.

Users need to **subscribe** to the PrePass Service und pay a monthly fee, but the PrePass transponders are provided free of charge. Vehicles participating in the PrePass program are **pre-certified**. Customers' safety records and credentials are routinely verified with state and federal agencies to ensure adherence to the safety and bypass criteria established by PrePass and member states.

Conclusion for establishing an open in-vehicle platform **Regulatory Applications**

The new regulatory background introduces the **same technologies** (especially GNSS and DSRC) in the three key applications EETS, Digital Tachograph and OBW. Although OBW systems will not be mandatory, it would be unwise to introduce a third DSRC or GNSS module.

Also other regulatory applications – both current and future – (will) require similar technologies. For an open in-vehicle platform to be future proof, a **sharing of resources is unavoidable**.

[25] http://media.prepass.com/news.php?include=143982 (19 October 2012)

2.3. Galileo and EGNOS

Indispensable in the discussion on an open in-vehicle platform architecture are **Galileo** and **EGNOS**, the European Satellite Navigation Programmes.

The Global Navigation Satellite System (GNSS) developed under the **Galileo Programme** will provide Europe a fully autonomous satellite-based positioning, navigation and timing capability, for global high-performance services. Early services with reduced performance or for demonstration purpose will be provided from **mid-2014**, fully operational capability is expected from 2018 onwards.

The **European Geostationary Navigation Overlay Service (EGNOS)** is the first pillar of Europe's satellite navigation programme. It was developed to increase satellite navigation reliability and accuracy by complementing the American GPS system. EGNOS makes existing satellite navigation services suitable for **safety-critical** applications such as flying and landing aircraft or navigating ships through narrow channels. EGNOS is **operational** and currently offers the following **services**:

- the **Open Service** has been available since October 2009, is free of charge and is intended for applications where human life is not at stake, such as personal navigation and goods tracking
- the **Safety-of-Life Service** became available for its primary purpose of aircraft navigation in March 2011 and is intended for applications where human lives depend on the accuracy and integrity of the signals

2.3.1. Multi-constellation

The concept of a GNSS receiver is evolving from the old conception of a stand-alone GNSS system receiver (e.g. GPS receiver) to a multi-constellation receiver that is able to process signals from **multiple GNSS systems**.

With multi-constellation GNSS, the **significance** of GNSS will highly **increase**. Firstly, since each GNSS system is independent from the others, this provides **redundancy** against the failure of one system. Secondly, there is an increase in the **availability** of signals, which is critical to maintain the coverage in applications where visibility is severely restricted, e.g. in urban environments. Thirdly, this increase in availability enables an increase in **performance** against the stand-alone solution. Signal diversity and redundant measurements, together with better geometry from multiple GNSS satellites, allows improved receiver-based **integrity** monitoring to be carried out.

2.3.2. Trusted GNSS signals

GNSS might be seen as a **generic resource** in many in-vehicle applications. Its deployment will become even more significant if trusted GNSS signals are available.

Trusted or **authenticated GNSS signals** might be needed to ensure that the recorded position (or other features like speed and timing) can be used from a **legal** point of view. An authenticated signal would increase the security against spoofing and be of special interest to applications of **regulatory nature**, such as the Digital Tachograph and in particular the EETS, as this Europe-wide tolling application involves high sums of money.

Particularly the Open Service, the Commercial Service, the Public Regulated Service and the Safety-of-Life Service are of interest. These services have the following **possibilities** in providing authenticated signals:

- The **Open Service** is free of charge, but does not provide authenticated GNSS signals by default (see also Figure 9). An authenticated signal could be implemented by using spare bits present in the current Galileo specifications. Even if the useable bits are quite limited, a full authentication can be achieved in a timeframe of 30-60 seconds. GSA announced that the authentication will likely be made available on the free E1 frequency band of the Open Service. Due to the fact that the first satellites are already transmitting signals for timing and positioning, an authentication feature would definitely boost the industry initiatives to find solutions for such trusted GNSS signals.
- The **Commercial Service** is expected to provide a trusted signal for professional users in form of an authentication mechanism (including higher accuracy), but this may not be free of charge. Moreover, this feature is currently only planned to be used in the E6 frequency band, which will likely not be available before 2016.
- The **Public Regulated Service** is fully authenticated and provides two encrypted signals that are resistant to jamming. However, this service is reserved for governmental bodies that are authorised and under control of the Member States. Its applications may be very sensitive from a political and strategic viewpoint and its use will be closely monitored and controlled for safety and security reasons.
- The **Safety-of-Life Service** improves the Open Service performance through the provision of timely warnings to the user when it fails to meet certain margins of accuracy (integrity). This requires that the relevant authority determines specific requirements for the navigation service, as well as certification procedures, if necessary. In addition, a specific authorisation, issued by the relevant authority, may be required. At present, only the aviation domain has specific service requirements, as well as certification and individual authorisation procedures developed and implemented.

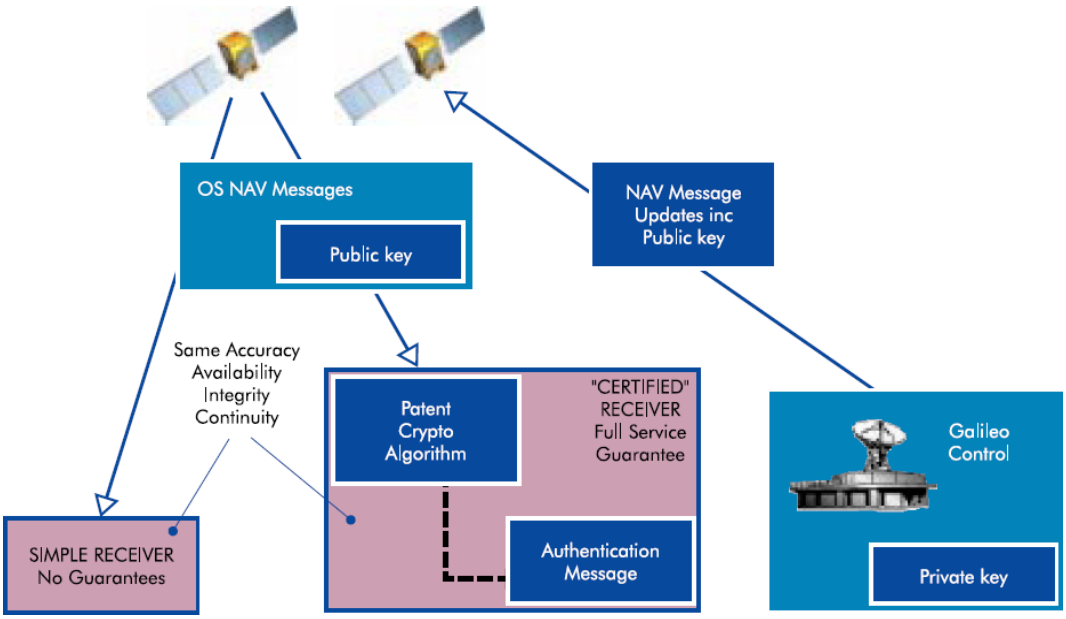


Figure 9: *Possible signal authentication system on the Galileo Open Service (OS)*[26]

[26] The Galilei Project, GALILEO Design Consolidation (2003)

2.3.3. TACOT

TACOT (Trusted Multi Application Receiver for Trucks) is a project co-funded by the European Commission in the frame of FP7 (Galileo area) and managed by the European GNSS Agency (GSA)[27]. The project started in January 2012 with a duration of 24 months.

The overall objective of the TACOT project is to prepare the introduction and promote the use of EGNOS and Galileo in the road transportation industry through the addition of a **secure GNSS function to the Digital Tachographs (DT)**, providing reliable Position-Velocity-Time (PVT) data to other ITS applications (e.g. Pay-As-You-Drive (PAYD), Fleet Management Systems), see also **Figure 10**.

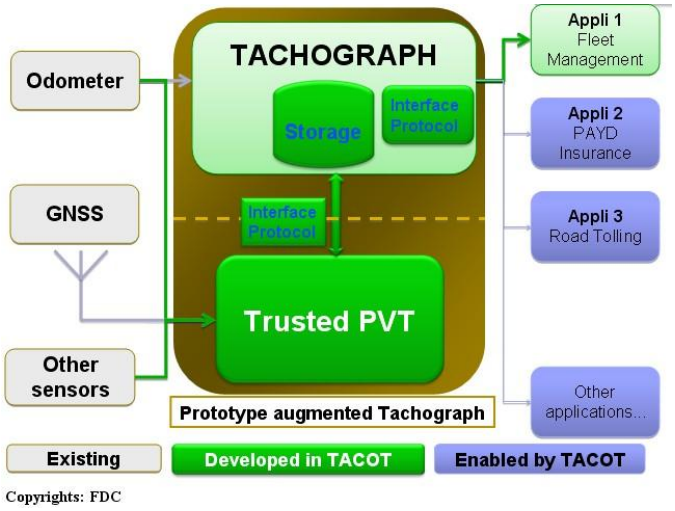


Figure 10: *Expected TACOT Development*

TACOT proposes to use a **Baynesian network** and sensor fusion approach to analyse the received GNSS signal and detect anomalies in the signal, which could indicate intentional security attacks (e.g. spoofing) or unintentional errors due to the environment (e.g. wireless interference, multipath fading due to obstacles).

TACOT will also provide a **level of confidentiality** of the received signal together with the other values of the GNSS signal: position, velocity and time.

Conclusion for establishing an open in-vehicle platform — **Galileo and EGNOS**

Multi-constellation GNSS will lead vastly enhanced quality of positioning data in terms of accuracy, availability and integrity that will be crucial for many ITS applications. It is a **must** that such a high quality **Position-Velocity-Time (PVT) signal** is a **resource** in any heavy vehicle. With trusted signals, this would be even more useful.

[27] Due to TACOT's strong relevance to this study, a delegation of the TACOT project was kindly invited to join our project meeting on 24 January 2013 in Brussels. Our liaison with the TACOT Consortium enables to directly use each other's concepts and results in both currently running projects.

2.4. Cooperative systems

This section presents the state of the art on **cooperative systems** related to open in-vehicle platform architectures and their requirements concerning the (key) applications.

Cooperative systems are based on **vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication**. They **increase the "time horizon"**, the quality and reliability of information available to the drivers about their immediate environment, the other vehicles and road users. They also offer **increased information** about the vehicles, their location and the road conditions to the road operators and infrastructure.

Vehicle manufacturers have targeted **2015** for the **first cars** to roll off European assembly lines fitted with **operational V2X technology**.

2.4.1. DRIVE C2X, sim^{TD} and COMeSafety 2

Important current projects on cooperative systems include **DRIVE C2X**, **sim^{TD}** and **COMeSafety 2**.

DRIVE C2X (2011-2014) focuses on communication among vehicles (car-to-car, C2C) and between vehicles, a roadside and backened infrastructure system (car-to-infrastructure, C2I). C2X aims at laying the foundation for **rolling out** Cooperative Systems in Europe, leading to a safer, more economical and more ecological driving. It includes a **comprehensive assessment** of cooperative systems (e.g. Traffic jam ahead warning, Approaching emergency vehicle) through **Field Operational Tests** on seven test sites, creating a harmonised Europe-wide testing environment for C2X technologies.

sim^{TD} (2008-2013) is a joint project initiated by **leading German automakers**, automotive suppliers, communication companies, research institutes and public authorities. The **aim** is to test the **functionality**, **suitability** for everyday use and the **efficiency** of car-to-X communication under **real-life** conditions. A test fleet of over **100 vehicles** demonstrate various **functions** (e.g. Obstacle Warning, Traffic Light Assistant) based on the exchange of car-to-X communication in/around the city of **Frankfurt am Main**.

COMeSafety 2 (2011-2013) takes up and continues the work started in the previous COMeSafety project (FP6) and aims at the **coordination** of the activities towards the realisation of cooperative systems on European roads.

2.4.2. Europe-Wide Services Platform (EWSP) – MOBiNET

The **MOBiNET** project is co-funded by the European Commission in the frame of FP7 and started in November 2012 with a duration of 44 months. This newly started EC funded project on a **Europe-Wide Services Platform (EWSP)** aims to develop, deploy and operate the technical and organisational foundations of an **open, multi-vendor platform** for Europe-wide **mobility services**.

This **MOBiNET service platform** will simplify the Europe-wide deployment of connected transport services by creating an **"Internet of Mobility"** where transport users' requests match providers' offers, and promoting openness, harmonization, interoperability and quality.

Conclusion for establishing an open in-vehicle platform **Cooperative systems**

Cooperative systems mainly provide car functionality that is addressed towards **passenger cars** and their **driver** (e.g. in terms of safer driving) – in contrast to the key applications focused on in this study which are facing rather the heavy vehicles and the authority (e.g. in terms of more efficient enforcement).

The world of cooperative systems comes with a **fast market development**. With the MOBiNET project a **services approach** for cooperative system-enabled mobility services will be developed. The MOBiNET platform will help **service providers** to offer enhanced services and **users** to find and subscribe to new types of mobility services.

2.5. Platform technologies

This section presents the state of the art on **platform technologies** related to open in-vehicle platform architectures and their requirements concerning the (key) applications.

2.5.1. OVERSEE

OVERSEE (Open VEhiculaR SEcurE platform) is a European research project funded within the 7th Framework Programme of the European Commission. The project started in January 2010 with a duration of 30 months. The OVERSEE Final Event and Workshop on Concepts of Open In-Vehicle Platforms took place on 19-20 December 2012 in Brussels and was attended by the consultant.

OVERSEE is an approach to investigate and find solutions for an **open in-vehicle platform** keeping **security** a central objective. The project focused on: (1) securely interfacing vehicular and environmental networks and (2) providing secure runtime environments for applications.

The results of OVERSEE can be separated into two parts. One result is a **proof of concept IT platform** implying some of the key concepts of OVERSEE and showing the capabilities of the architecture. Several applications run on one operating platform with protected runtime environments for the simultaneous and secure execution of the applications (see Figure 11). Because the applications are shielded from each other, other applications stay unaffected if one application has a problem (e.g. it crashes, it is insecure or it does not have enough memory).

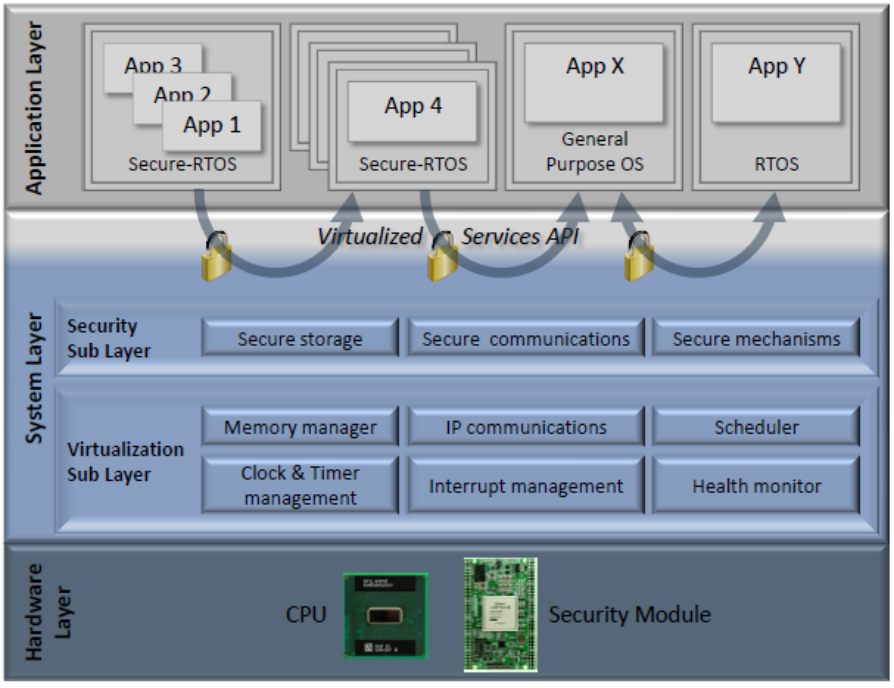


Figure 11: *System design of the OVERSEE platform*

The second result of the OVERSEE project includes the **non-functional requirements** an open in-vehicle platform should fulfill to assure dependability, security and performance (see Annex 1).

2.5.2. PRESERVE

PRESERVE (Preparing Secure Vehicle-to-X Communication Systems) is a EU project in the frame of FP7 with the mission to design, integrate and test a secure and scalable V2X security subsystem. The project started in January 2011 with a duration of 48 months.

The goal of PRESERVE is to bring secure and privacy-protected V2X communication closer to reality by providing and field testing a **security and privacy subsystem for V2X systems**. PRESERVE will combine and extend results from earlier research projects (e.g. SeVeCom, PRECIOSA, EVITA and OVERSEE, see also Figure 12), integrating and developing them to a pre-deployment stage by enhancing scalability, reducing the cost level, and addressing open deployment issues.

The project aims at providing comprehensive protection ranging from the vehicle sensors, through the on-board network and V2V/V2I communication, to the receiving application (e.g. Intersection Collision Warning, Emergency Vehicle Warning). As a result, PRESERVE will present a complete, scalable, and cost-efficient V2X security subsystem that is **close-to-market** and will be provided to other FOT projects and interested parties for ongoing testing.

Figure 12: *PRESERVE combines and extends the results from earlier research projects (source: Kargl, Slides for Final EVITA Workshop on 23 November 2011 in Erlensee, Germany)*

Conclusion for establishing an open in-vehicle platform **Platform technolgies**

The **technology** for realising an open in-vehicle platform architecture **is there**. Commercial and regulatory applications can run **securely** side by side on one platform. For example, fleet management applications can be made available through the Digital Tachograph and even EETS on the Digital Tachograph may be possible. In the end, however, it is up to the **industry** to push forward the use of such in-vehicle platforms.

2.6. Vehicle buses

This section presents the state of the art on **vehicle buses** or **in-car networks** related to open in-vehicle platform architectures and their requirements concerning the (key) applications.

A **vehicle bus** is a specialized internal communications network that interconnects components inside a vehicle. Special requirements for vehicle control mandate the use of **protocols**, such as Controller Area Network (CAN), Local Interconnect Network (LIN) and Media Oriented Systems Transport (MOST). Additionally, many major car manufacturers use their own proprietary vehicle bus standards, or overlay proprietary messages over open protocols such as CAN.

Each of the traditional vehicle bus technologies (e.g. CAN, LIN) is ideal for a **specific use case**, but not only is there no migration path from one to the next, each technology is based on a fundamentally **different communication principle**[28].

Traditional in-car networks provide a **communications bus** (see Figure 13, left & middle part). This means that all attached units share the available bandwidth and that adding new units thus affects all existing ones. For example, the ring topology of MOST makes it quite complicated to wiring all components – not even thinking about adding additional components later (see Figure 13, middle part).

Modern Ethernet-based networks function via **switches** (see Figure 13, right part). This means that the available bandwidth is not necessarily shared, especially as the topology is not predefined by the technology but can be chosen to suit the specific situation best. Additional flexibility is given because different links can have **different speed grades** (meaning scalability) and adding or changing units does not automatically affect the whole network, but primarily the unit(s) they directly connect to.

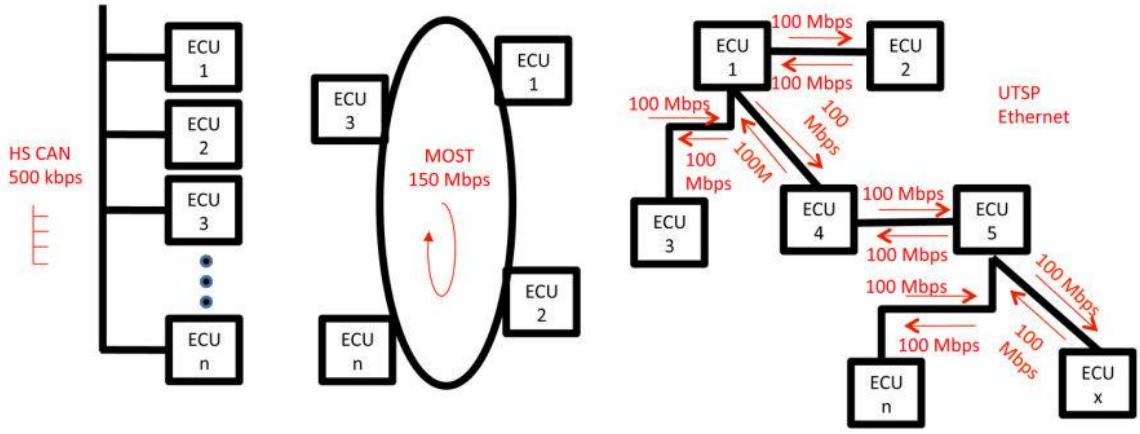


Figure 13: *Traditional communications bus (left: e.g. CAN, middle: e.g. MOST) versus a switched network (right: e.g. Ethernet)*[42]

2.6.1. FMS-standard

Currently, **CAN** is the **accepted** and generally available vehicle bus. It is widely used in low and higher data rate variants, both for engine facing purposes (motor electronics) and for driver facing applications (e.g. the odometer). Despite its common deployment, CAN has **severe limitations**, since data rate is comparatively low and one message frame can only carry 8 Bytes of data. A version of CAN with higher and flexible data rate and with 64 Byte frame length has been specified (CAN FD for "CAN with Flexible Data-Rate") and will presumably be integrated in the ISO 11898-1 standard as an optional feature. Based on the CAN, **higher level protocols** have been defined, most notably J1939[29] adding the required network layers.

[28] Ethernet in cars: an idea whose time has come (22 June 2012), an article in Automotive Engineering International Online written by Dr. Kirsten Matheus of BMW (http://www.sae.org/mags/aei/11142)

[29] J1939 is specified and maintained by the Society of Automotive Engineers, SAE

Based on these layers and to enable **manufacturer independent applications** for telematics, the major European truck manufacturers[30] have developed the so-called **FMS-standard** in 2002. The **Fleet Management Systems Interface (FMS)** is an open standard for accessing electronic data from the internal CAN network of the vehicle, such as[31]:

- Fuel Consumption
- Electronic Engine Controller
- Engine Hours, Revolutions
- Vehicle Identification
- Tachograph
- Engine Temperature
- Driver's Identification
- Air Supply Pressure
- Cruise Control/Vehicle Speed
- Vehicle Weight

The FMS-interface is an **optional interface** of different truck manufacturers and forms the sole interface for a **safe data connection** of 3rd party devices to the CAN-bus of a commercial vehicle. Without this interface, a direct connection to the vehicles' internal bus system would affect vehicle reliability as well as warranty.

Besides the FMS-interface data and protocol specification, the truck manufacturers have agreed to a **common connector specification**. As explained in Annex 3: Accessing data of the Digital Tachograph, the FMS-interface provides (among other services) a secure and legal solution for the **remote download** of data from the **Digital Tachograph** as well as current status information of the DT (i.e. vehicle motion detection, state of work of the driver or indication if the driver approaches working time limits). However, the FMS-interface is not provided by all vehicle manufacturers and not in all models, and is in the majority of cases not free of charge either. The FMS equipment can cost up to a few hundreds of Euro per truck.

2.6.2. AUTOSAR

AUTOSAR (AUTomotive Open System ARchitecture) is a worldwide development partnership of car manufacturers, suppliers and other companies from the electronics, semiconductor and software industry. Since 2003 they have been working on the development and introduction of an **open, standardized software architecture** for the automotive industry.

To achieve the technical goals modularity, scalability, transferability and re-usability of functions, AUTOSAR releases **specifications** to provide a **common software infrastructure** for automotive systems of all vehicle domains based on standardised interfaces for the different layers (see Figure 14).

[30] Formerly known as the FMS Group, currently known as ACEA's Heavy Duty Electrical Interface Working Group (WG/HDEI) with its members Daimler, Scania, MAN, DAF, Iveco, Volvo and Renault

[31] FMS-Standard description, Version 03, 14.09.2012 (available on: http://bus-fms-standard.com)

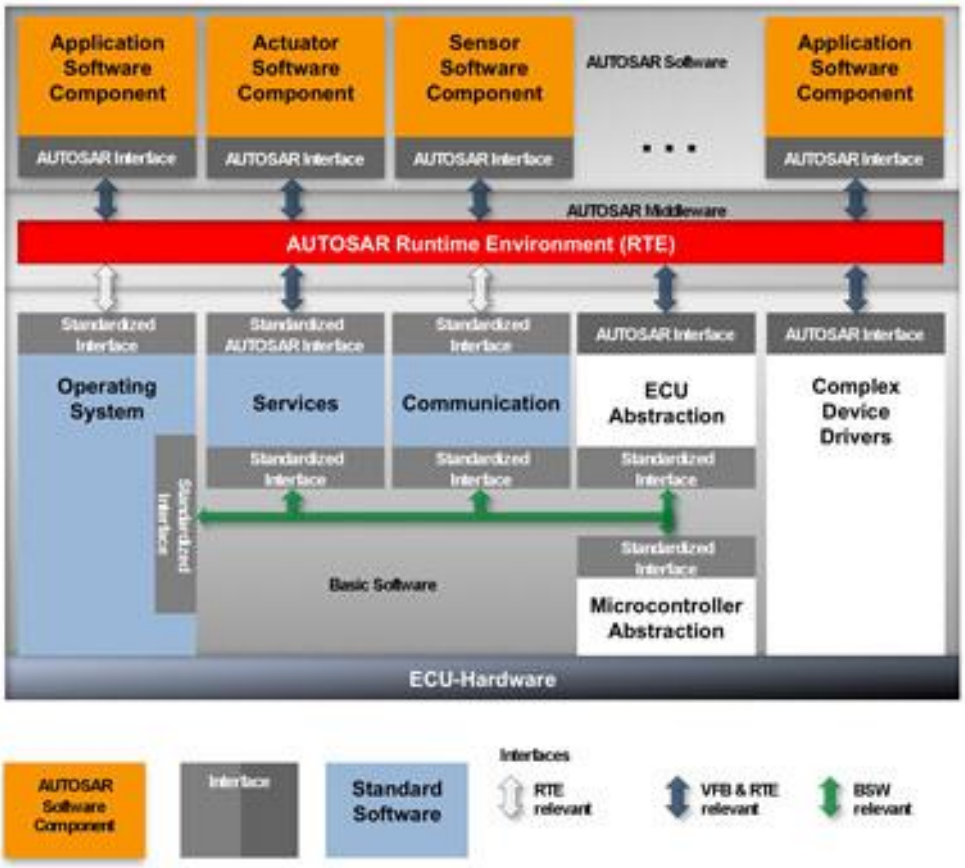


Figure 14: AUTOSAR's common software infrastructure

Many OEMs and suppliers **rely on the standard** and are introducing AUTOSAR in a wide range of applications. The majority of the Core Partners will finish their migration to fully compliant AUTOSAR BSW (Basic Software) in **2015**.

In addition, AUTOSAR will enhance **support for new technologies** like multi-core processors, Ethernet with TCP/IP communication mechanisms and others.

2.6.3. OPEN Alliance Special Interest Group (SIG)

The **OPEN Alliance SIG** is a partnership of car manufacturers, suppliers and other companies and is set up in 2011 to encourage wide-scale adoption of **Ethernet-based**, single pair unshielded cable networks as the standard in automotive applications.

The **paradigm shift** from traditional in-car networks, such as CAN and MOST, towards Ethernet comes from **camera-based** safety and security systems (e.g. parking sensors). These systems are on the market for years (e.g. production line monitoring) and have an Ethernet interface.

Interest in Ethernet technology has grown dramatically as the automotive industry accelerates its adoption of Ethernet-based networks delivering both **high-performance bandwidth** and the industry's **lowest cost cabling** solution for Ethernet connectivity over a single pair, unshielded twisted cable. The technology is engineered to meet the **stringent in-vehicle requirements** of the automotive industry and optimised for **multiple in-car applications**.

As is visualized in Figure 15, Ethernet-based communication follows the **ISO OSI (Open Systems Interconnection) layer model** and allows for reuse and exchangeability on the different protocol levels[32].

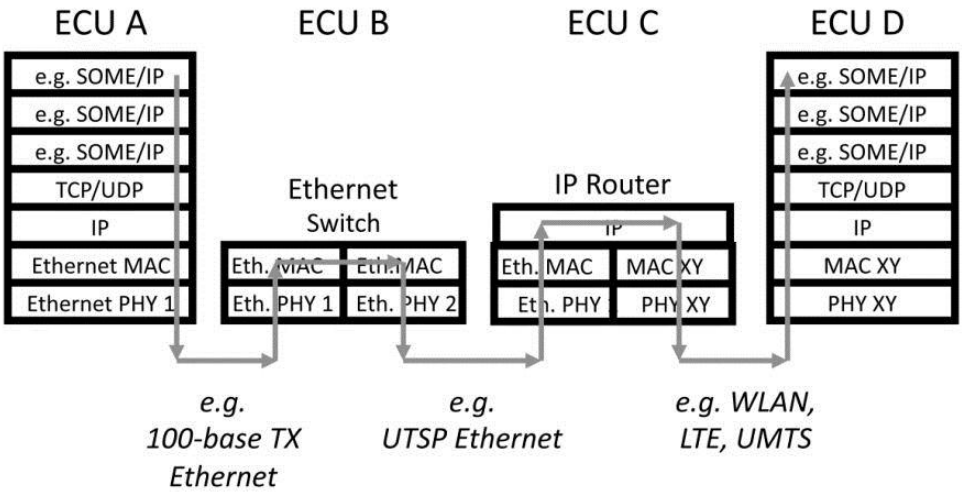


Figure 15: *Ethernet-based communication follows the ISO OSI layer model*

The Ethernet **physical layer** allows for the in-car transmission of 100-Mbps Ethernet packets (in future perhaps even 1 Gbps[33]) over cost-efficient UTSP (unshielded twisted single pair) cables. On all other layers, state-of-the-art solutions from multiple vendors are available.

The **use case is not limited**, so it does not matter whether the application is diagnostics, driver assistance, infotainment, or something else. This means that Ethernet-based communication is flexible in terms of applications, speed grades, and in terms of requirements that are brought into the car from the outside world.

The OPEN Alliance SIG continues to address **industry requirements** for improving in-vehicle safety, comfort, and infotainment, while significantly reducing network complexity and cabling costs.

2.6.4. ITS Communications Architecture

In addition to the OPEN Alliance SIG initiative, ETSI and ISO have developed the ITS Communications Architecture in ISO 21217 and EN 302 665. These documents specify the architecture of communications in ITS (ITSC) supporting a variety of existing and new access technologies and ITS applications. A variety of access technologies can be used for the communication with these so called ITS stations, one of it being Ethernet.

Based on market data seen, the Ethernet Alliance predicts that there could be over half a billion Ethernet ports in private cars by 2020.[34] For the heavy vehicles market it looks a bit different. The

[32] Ethernet in cars: an idea whose time has come (22 June 2012), an article in Automotive Engineering International Online written by Dr. Kirsten Matheus of BMW (http://www.sae.org/mags/aei/11142)

[33] For future applications, the IEEE 802.3 working group RTPGE (Reduced Twisted Pair Gigabit Ethernet) has decided to investigate the development of an automotive-suitable Gbps Ethernet physical layer.

[34] http://www.broadcom.com/press/release.php?id=s731287 (retrieved on 16. July 2013)

CAN-bus will stay for much longer, because the bus speed can currently keep up with the application requirements, which differ from the needs of the private car sector. But with the connectivity between heavy vehicles, often extended to the internet, a rising demand for real time tasks and more complex distributed control systems, there will likely exist a demand for higher data rates inside heavy vehicle in the upcoming years, in order to cope with the data traffic between all actuators/sensors and the Electronic Control Units (ECUs). In the medium term, Ethernet will probably also appear in the heavy vehicles market, but of course in smaller quantities than in the private car market where multimedia is the main driver and the bottleneck for data throughput.

Conclusion for establishing an open in-vehicle platform **Vehicle buses**

The **CAN** is a **traditional** vehicle bus where all attached units **share** the available bandwidth: adding new units thus affects all existing ones. This means that CAN is relatively slow and inflexible, which are **severe limitations** for an open in-vehicle platform architecture.

Many car manufacturers already use **Ethernet** in their parking sensors. Due to the **advantages** that Ethernet technology has over the traditional in-car networks (e.g. Ethernet is much faster than CAN), it is expected that this technology will be seen more and more in future cars.

For **heavy vehicles**, however, the CAN will be in place for many years to come, including the **FMS-standard** developed by the major European truck manufacturers to allow controlled access to their proprietary vehicle data.

3. What do we want to achieve?

A **variety of in-vehicle services and applications** are used on heavy vehicles. So far, implementation has been tackled in perfect **isolation** and has evolved independently of each other, resulting in **limited synergies** even when requirements or needs are quite similar.

The aim of this second study is to recommend steps towards establishing a **truly open in-vehicle platform architecture** for heavy vehicles for the provision of ITS services and applications.

Especially the **streamlining** and **integration** of the regulatory key applications EETS, Digital Tachograph (DT) and on-board weighing (OBW) within a comprehensive open-system architecture would enhance **reusability**, **extensibility** and **scalability** therefore improve efficiency and reduce costs.

Therefore, both goals of the stakeholders and generic goals have been elaborated and taken as starting points for the remainder of the study.

3.1. Goals of the stakeholders

For this study, the following **stakeholder goals** were identified:

- Consumer (driver, company) view: interested in an open services market with an **utmost freedom to buy ITS services**. For the driver such services may include in-vehicle oriented applications related to e.g. route navigation, parking information and driving time left. For the company such services may include back office oriented applications related to e.g. disposition, weight compliance and data download from the DT. Specialized applications should be provided by service providers that have affinity with the respective business.
  Transport companies **operate in many different markets and in many modes**. Besides generic ITS application for general fleet management they need sector-specific, tailored applications which are usually developed and provided by highly specialized SMEs that are close to their customers.
  Ideally every compliant application or module should run on an interoperable and secure in-vehicle platform, comparable to the concept of today's smart phone or personal computer. For the time being, however, this will stay a dream due to security issues and the lack of interest from the automobile industry to allow third parties direct access to their in-vehicle networks.

- Vehicle manufacturer (OEM) view: interested in a technical platform that can be procured at lowest costs and that can be easily managed and combined with other components or applications. This could be reached by an **open market for on-board components**, with exchangeable products based on standards.
  In this view, not the consumer but the vehicle manufacturer will have utmost freedom to buy on an open market (for devices, not services in this case). For example, he may wish to procure

standardised GNSS modules on a competitive marketplace of many producers for integration into his on-board platform.
Regarding services, the vehicle manufacturer has all interest to provide as many ITS services through his own services branch. Almost all heavy vehicle manufacturers offer a "communicator" option when selling a vehicle, which is a communication module connected to the vehicle CAN-Bus/FMS. The communicator sends comparatively rich data from several in-vehicle sources regarding the engine, the fuel, the vehicle movement, the Tachograph, etc. to a central server hosted at the vehicle manufacturer's services branch. The services offers include advanced maintenance, improved fuel management, fleet management and other generic services. Vehicle manufacturers want to position themselves not only as producers of trucks but as complete "solution providers" for the transport industry. These services can markedly increase the productivity and efficiency of truck fleet operations in terms of reduced time spent at garages, reduced fuel consumption, and optimised fleet utilisation and routing.
Hence, **truck manufactures have little interest to give third parties open access to vehicle and movement data nor access to other in-vehicle resources like DSRC or the HMI**, be it on-board (e.g. via the FMS interface) or by giving access to the central data bases at their servers. Vehicle manufacturers will have all interest to bind customers that buy their vehicles also to their telematics services.

- EC view: interested in opening up of transport markets to **free and undistorted competition** and in finding common answers to the challenges related to **interoperability** and **security** in view of a greater market access and more harmonization throughout Europe.

- Service provider view: interested in addressing **new business opportunities** with an utmost freedom to offer ITS services. Ideally, he has access to all information needed against a fair price for providing his services.
  Service providers are especially strong in providing sector-specific solutions like ITS services for routing for pickup-and-delivery companies (DHL, UPS), scheduling for postal services or public transport buses, hazardous goods operations, livestock transport, refrigerated goods transport, valuable goods transport and all the thousands of other specialized transport offers.
  For a **service provider it is of absolute necessity to have open access to on-board resources**, and ideally also to any vehicle related information collected in the central servers of the vehicle manufacturers. Currently access to vehicle data is relatively unhindered, and a rich market of 3rd party services has developed and is growing at a rapid pace. Restrictions still apply, since e.g. full vehicle data can only be accessed via an FMS connector, which is not a standard feature in trucks and may come at certain costs. Also, 3rd parties have no access to other in-vehicle resources, such as communication channels or – very critically – to the HMI. Therefore, even with reasonable access to vehicle data, 3rd parties have a competitive disadvantage to the vehicle manufacturers since their services have to do **without access to the vehicle display**. It is difficult for a 3rd party service to provide for the same level of functionality as with the vehicle manufacturer's generic services. Also, 3rd parties will be faced with **higher costs** to provide for their own communications, display, etc.
  More recently, vehicle manufacturers have put more efforts in providing service themselves, and there is a tendency to close 3rd party access. There is a high risk that the services market will be fully controlled by the vehicle manufacturers in the future, making service providers either dependent or pushing them out of the market completely.

As can be seen, each stakeholder has a **different view** on what an open in-vehicle platform should be. Notably, there is an **obvious conflict** between the interests of vehicle manufacturers and 3rd party service providers. Vehicle manufacturers have an interest (and also the possibility) to control the services market by giving or not giving access to in-vehicle resources like vehicle and DT data, communications and HMI.

3.2. Generic goals

Next to the vertical issues represented by the goals of the stakeholders, also the following **horizontal issues** that are relevant across all stakeholders – the generic goals – were identified:

- Shared resources: The new regulatory background introduces the **same technologies** (e.g. GNSS and DSRC) in the three key applications EETS, DT and OBW. It would be unconceivable that this will lead to multiple modules with the same functionality inside one vehicle. A platform with **shared resources** is **a must**.

- Interoperability: Interoperability may be seen as the ability of diverse systems and organizations to work together. Not only **information exchange** between systems should be allowed, also social, political, and organizational factors that impact system to system performance should be taken into account. Ideally, all things work the same throughout Europe and there are **no barriers to trade**.
  Indeed, interoperability between the regulatory key applications (i.e. EETS, DT, OBW) should overcome the problems of **language** and **information flow** in case, for example, a truck driver goes from Romania to the Netherlands. The EC seeks for "tools" to assist both the enforcers and the drivers in doing their job. Among others, European regulations should prescribe the **same communications standards** for the key applications. This will not only ease interoperability but also allow the elaboration of certification and security procedures.

- Security: Security relates to **information security**, in other words the practice of defending information from **unauthorized access**, use, disclosure, modification, inspection, recording or destruction. Means are needed to **protect data and databases** from destructive forces and the unwanted actions of unauthorized users. With respect to the key applications, security is related to:
  - *Secure external communication*: e.g. achieved through **encryption** of data that are exchanged between components/systems
  - *Secure positioning data*: e.g. achieved through **authentication** of the GNSS signal
  - *Secure processes and devices* in order to protect regulatory applications against user fraud.

- Data ownership: Data ownership refers to both the **possession** of and **responsibility** for information. Especially in case ITS services will be made available to the consumer through the OEM by allowing third parties (i.e. service providers) access to the in-vehicle network by means of the FMS-standard, the question arises: who owns the data? **Several stakeholders** may lay a potential claim to the ownership of such data, for example:
  - *Consumer: the party that is "described" by the data*
  - *Vehicle manufacturer: the party that enables the collection of the data*
  - *Service provider: the party that provides the application based on the data*

- Protection of personal data: Both the company operating the vehicle and the driver have the **need that their movement data are protected**. For the company, privacy needs to be protected both with respect to competitors that shall not be able to gain undue insight into a company's doings, and regarding authorities, which shall not be able to collect data without a clear legal basis. Regarding the driver, privacy concerns are especially pronounced. Driver personal data, and this includes movement data, need to be treated as private. Even the employer shall not be able to infringe on the privacy of their drivers. Given the business needs of tracking their vehicles and ensuring adherence of drivers to the work and rest hours regulations, there is a delicate line that needs to be drawn between legitimate needs of companies and the privacy rights of drivers.

Conclusion for establishing an open in-vehicle platform **Aims to achieve**

1. The **European Commission** has set **open and undistorted competition** as one of the prime goals for the ITS market. An **open in-vehicle platform architecture is a critical element to establish a competitive market** for ITS services.
2. Vehicle manufacturers and service providers have **conflicting interests** and hence different views on what an open in-vehicle platform architecture should be. The **most critical issue is access to in-vehicle resources** (data**,** communications and HMI).
3. **ITS services also require access to communication resources (DSRC, GSM, others) and components of the HMI (display, controls)**. It is not about having one multi-applications computer in the vehicle.
4. A common element is a **services-based** approach on the ITS market. The industry does not primarily sell “boxes” any more (like navigation devices) but is marketing services.
5. **Sharing of resources** or components between applications is indispensable. Duplication of modules with the same functionality should be avoided.
6. In the interest of all stakeholders, **security** and **interoperability** are key issues that need to be taken care of.
7. **Data ownership**, as a key issue, needs to be elaborated in order to clarify who has the legal rights and complete control over the data collected by the vehicles and the applications.

4. Platform readiness

This chapter first presents a view on a **common architecture** for an open in-vehicle platform. An architecture can be defined at different levels and from different points of view. These levels or **abstraction layers** are shown in **Figure 16** and will be used to structure the discussion on the development of an open in-vehicle platform architecture.

Governance	Legal environment, institutional set-up, standards, ...
Business	Business case, market view, liability, ...
Application	Services, IT processes, software, data access, ...
System	Hardware, IT system, OBU, certification, ...
Components	GNSS, DSRC, mobile communication, vehicle bus, ...

Figure 16: *Five layers of a common architecture for an open in-vehicle platform*

"Architecture" is a generic term and can encompass very different aspects in different contexts. For clarification we have structured our treatment of "platform architecture" into the following five layers:

- On a **components level**, architecture means how the different sensors, actors and communication modules are integrated into the vehicle and connected together. On this layer, questions need to be addressed like whether there is one GNSS module per application, and if there is only a single one, how to make the GNSS data available to other modules, how to certify an independent GNSS module for a specific regulatory application, how to secure data connections on board, etc.
- Architecture on a **system level** mostly addresses integration issues. Are all applications housed in separated "boxes"? Is there a multi-purpose computing platform? How are applications that stem from different legal environments certified (eCall, Tachograph, EETS, OBW, ...)?
- On **application level**, an architecture defines rules how to access and exchange data, in which way to provide services and in general a common "look and feel" of all application processes.
- An architecture on **business level** defines the relationship of the (commercial) stakeholders. Who pays? Who owns? Who controls? Who is liable? Whose branding is it? Is the market open to all players or is it restricted to players having a natural monopoly?
- Finally, on **governance level**, an architecture would define a common process paradigm for legislation, with similar certification requirements and pathways and with similarly structured rights and obligations of the involved parties. The environment defined by technical standards is also part of the governance level.

One of the core messages of this report is that **all these layers are legitimate levels to define a "platform architecture"**. Yet when we want to adopt an "open in-vehicle platform architecture" as postulated by the title of this report, a solution that is restricted to one of these levels only, falls short of providing a solution that is simultaneously viable from a technical, a business and a policy perspective. Hence it is of critical importance for a common architecture for an open in-vehicle platform that **all layers must be "platform-ready".** A solution must work on all levels. A technical in-vehicle architecture like a sophisticated in-vehicle bus system connecting all high-tech components is useless without a proper architecture regarding the business and governance aspects. The same goes for any other level: A clever business architecture where all stakeholders are properly integrated and can interact with defined rules for ownership, control, liability, etc. is useless without a matching architecture on the very technical levels or regarding alignment of the legal governance aspects especially regarding the regulatory applications.

"Platform readiness" can be achieved **more easily on the lower layers** compared to the higher layers. For example, on the components layer, technological resources, such as GNSS or DSRC, should be shared or used jointly by the applications. Furthermore, technical components, such as the antenna or the cabling should be shared. These are merely technical issues, and as long as safety, security and costs are acceptable, there are few obstacles to design the component level with a few to support open in-vehicle environments as defined by the higher architecture levels.

The **"platform-readiness" of higher levels is more difficult** to achieve. For example, European legislation is in general not platform-ready: e.g. EETS has its own certification process which is different from the certification process of the DT. Also applications driven by the vehicle manufacturers are not platform-ready (yet), since many function as a closed box based on proprietary in-vehicle networks. On the higher levels, **obstacles are routed in conflicts of interests of stakeholders**.

The EC has notably a role at the **governance** layer. All other layers should be market-driven. However, what is done on the governance layer will influence the lower layers, intended or not. Therefore, a good understanding of all layers is indispensable.

The main question to answer is: **what needs to be done on each layer** to have an open platform for ITS services? The remaining of this chapter discusses the most relevant issues or requirements for achieving platform-readiness of the five layers of the common architecture.

4.1. Components

4.1.1. Modules

At present, applications do not make use of – for example – a single GNSS receiver as a shared resource; instead the functionality is **duplicated** for every application. Moreover, applications usually even come with their own separate piece of equipment.

Synergies may be large in case of shared resources based on only one GNSS module, one DSRC module, etc. Therefore, **shared resources** are a prerequisite for making the components layer **platform-ready**. For a proper integration, it is indispensable for OEMs to use **one single antenna module only**. Optimal placement of this single module increases reception quality while reducing potential interferences. Cost savings due to less hardware and wiring are also important.

The new regulatory background introduces the **same technology** in the three "boxes" or rather key applications EETS, DT and OBW:

- For EETS and DT a **GNSS module** is required, for OBW a GNSS module is expected to be present/useful
- For EETS, DT and OBW a **DSRC module** is required
- For EETS, DT and OBW a **mobile communications** module is expected to be present/useful

In fact, the **DT** could become the **core ITS element** of a heavy vehicle as it provides **PVT data** of high quality, especially if an authenticated signal is offered. Especially the "technology packet" of **GNSS and DSRC** makes the DT a very valuable resource for EETS and OBW. The DT is an attractive source of these data, since:

- it is a **mandatory** device on all heavy vehicles, hence available on all vehicle models and types independent of manufacturer and at no additional costs except for connecting to the interface
- it is a **type-approved** instrument, guaranteeing a certain quality of service
- it can offer the data in a **secure** way, with a proof of integrity and authenticity
-

Basically, there are two options for the GNSS module and the DSRC module of the DT (see Figure 17):

- **Non-divisible**: the GNSS/DSRC receiver is **integrated** inside the DT vehicle unit and forms an internal element of the DT; only the antenna is physically external (see below)
- **Separated**: the GNSS/DSCR receiver is **detached** from the DT and is an external and interchangeable element much like the motion sensor, connected with the DT through a secure channel

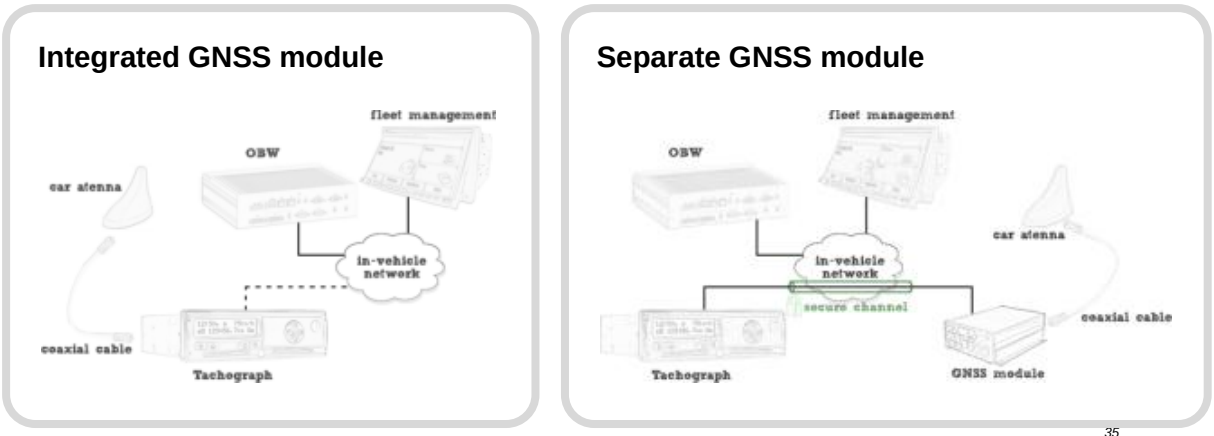


Figure 17: *GNSS module integrated (left) or separated (right) from DT vehicle unit*[35]

The **first option** (integrated modules) might be seen as a **basic option**. This solution is cost effective, reasonably secure, leaves implementation freedom to industry and even offers a certain level of interoperability between antenna modules. It is also comparatively straightforward to specify, requiring little interaction with different stakeholders.

In view of an **open in-vehicle platform** architecture, however, the **second option** (detached modules) makes **more sense** and might be seen as an **alternative** or **voluntary option**. This solution has benefits that may justify the higher implementation effort both in terms of costs and complexity of specifications in case an open in-vehicle ITS architecture comes into existence and several ITS applications require a high quality GNSS signal from the DT. This option is especially favourable if the DSRC module will be connected the same way, and probably later on also other sensors, such as the motion or weight sensor.

Both options require a physically **external antenna**. Whether the GNSS antenna and the DSRC antenna can be put into the same module is an issue that can be left to manufacturers. Common placement is not a straightforward matter, since the GNSS antenna requires a good view to the sky and is ideally placed on the roof-top, whereas the DSRC antenna needs to point forward, be at the lateral centre of the vehicle and should in trucks not be placed higher above ground than the bottom area of the windscreen.

Still, it is not so much the question of integrated or detached modules, but of **being "part of"** or "not part of" the device. This issue is discussed at the system layer, since it has to do with the **certification** of modules and devices.

4.1.2. Vehicle buses

The car industry has deployed several vehicle bus technologies, such as CAN, FlexRay, LIN and MOST. However, these in-car networks most often do not provide the **bandwidth** or **network topology** needed to cope with the increased data traffic flows resulting from new in-vehicle ITS applications. The breakthrough in the industry has come with an **Ethernet** physical layer that allows for the in-car transmission of 100-Mbps Ethernet packets over cost-efficient UTSP (unshielded twisted single pair) cables.

For **heavy vehicles**, however, the CAN will be in place for many years to come.

[35] Implementation of GNSS functionality in the Digital Tachograph: Technical Options Review and Discussion

It is expected that **several in-car networks** will (continue to) simultaneously exist in future cars. For each application the most appropriate network needs to be chosen. In view of an **open in-vehicle platform** architecture, the networks should be **functionally interconnected** in order to ensure the economic viability and operational effectiveness of the whole. Communication between the networks should be enabled by preventing multiple non-interfacing data formats from the separate subsystems that are tied to proprietary protocols.

4.1.3. Modules & vehicle buses

All vehicle buses have their **pros and cons**, especially when combining several applications (e.g. EETS, DT, OBW) using different resources (e.g. GNSS, DSRC, CN) within one in-vehicle architecture platform. For the DT to be the core element of an open in-vehicle platform architecture, it is essential that its ITS interface ties into a **widely deployed standard vehicle bus** such that on-board components can access the PVT data easily and at low implementation costs.

Although in Section 4.1.1 the second option – GNSS and DSRC modules detached from the DT – seems preferred in view of an **open in-vehicle platform** architecture, this highly depends on the type of vehicle bus foreseen in the architecture.

The traditional **CAN** seems best suited for the exchange of information related to engine, chassis etc. which is used by Active Safety Systems, such as Electronic Stability Control (ESC) and Advanced Emergency Braking System (AEBS). On the other hand, **Ethernet-based** solutions seem better suited for the exchange of information related to **non-safety/security** applications, such as entertainment and fleet management services.

For the **GNSS functionality**, it is quite conceivable that the GNSS module can be connected through the **CAN** with the in-vehicle applications.

However, for the **DSRC functionality**, the CAN bus does not have enough **speed** to properly react to communication requests from a roadside **DSRC** beacon. In other words, if the vehicle passes the beacon, the CAN bus is already too late to respond. (Note that the CAN bus is about 100x slower than Ethernet.) This problem is less likely when the **DT** would be enhanced with an **integrated** DSRC module. But if the DSRC module is a **stand-alone** module, acting as a “gateway”, the CAN bus is too slow and the response to the request needs to be **preloaded** on the DSRC module. This preloading of the request on the DSRC module is possible; however, the system could most likely not respond to any request. Though, even with Ethernet-based systems the response time could be critical (< 100 ms is required), but it can be done via giving **priorities** to such messages (like it is done in home/business network systems: VoIP packages have a higher priority than HTTP packages).

So, in contrast to the GNSS module, it is **not an easy task to connect** the DSRC module through a vehicle bus with the in-vehicle applications. The best option will need to be decided by experts in the field.

4.2. System

4.2.1. Multiple "boxes"

From a consumer perspective, the ultimate dream would be to have an **open ITS market**, where the consumer has the ultimate freedom to buy applications (both regulatory and commercial) that run on an interoperable and secure in-vehicle platform, comparable to the concept of today's smart phone or personal computer.

A lot of vehicle and systems manufacturers **already offer integrated solutions**, where several applications are provided on a single platform. However, new applications cannot be easily added and the platform is not open to other service providers. Moreover, it has been demonstrated in platform projects (e.g. OVERSEE) that applications can be fenced off against each other and that **security and privacy issues can be dealt with**. Operating environments have been created where applications do not influence each other.

However, there are two main obstacles that **hinder the platform-readiness** of the system layer. The first obstacle is that vehicle manufacturers have shown **little interest** to open their platforms for obvious commercial reasons. The second obstacle is related to **legal constraints**. Especially regulatory applications like the EETS and the DT cannot be integrated easily into a common platform, since these applications require certified or even type-approved equipment with different cost, complexity and lifecycle arguments.

In view of an **open in-vehicle platform** architecture, the idea of having a **"single box"** or platform for both regulatory and commercial applications (provided both by manufacturer and 3rd parties) is deemed **unrealistic**. However, a step-by-step approach may be pursued to move forward with **integrated devices**, combining e.g. a number of regulatory applications, with an important role for specifications and certification.

4.2.2. Certification

It is of utmost importance to **guarantee** a defined **quality** of all modules, working separately as well as together, within an open in-vehicle platform architecture. Especially, if one device is not working properly, this should **not hinder another device** from working properly. Thus, **certification** and **type approval** are prerequisites for making the system layer platform-ready in case of regulatory applications or systems that will have to work with others (interoperability).

It should be carefully observed that current or new **specifications** include **no elements** that may **hinder** the development of integrated devices and thus the coexistence of several applications on one platform.

Certification processes should be defined such that integrated devices would need **no complete recertification** in case of only a component **update**. So, if the device is integrated with other devices or applications, the operating environment should be developed such that the other devices or applications can be **(re)certified independently** from one another.

An important issue is whether modules are considered being **"part of"** or **"not part of"** the device. **Certification of the DT**, for example, refers to the certification of:

- The DT with a **separate GNSS** module (not being part of the DT), or
- The DT with a **dedicated but separate GNSS** module (being part of the DT), or
- The DT with an **integrated GNSS** module (being part of the DT)

All certification approaches have **disadvantages**.

Certification of the DT alone, not including certification of a **separate** GNSS module would be **undesirable** for regulatory purposes; although not critical for the DT itself, but very critical for EETS:

- A fully external GNSS receiver would not be part of type approval and quality control would not be possible
- Security would be very low, since any on-board device could claim to be a GNSS receiver and send fraudulent information to the DT
- The idea of the DT becoming a building block of an in-vehicle ITS environment would fail

Certification of a **dedicated but separate GNSS** module might result in a **decreased connectivity** between platforms. This has also been the case with eCall, where each platform uses different GPRS modules. While the eCall box itself is certified, this is not true for the separate GPRS modules. And this has led to huge differences in connectivity between platforms.[36]

However, certification of an **integrated GNSS** module also has disadvantages. For the DT applications, only the location data strictly needed to cross-check the information recorded by the Tachograph shall be automatically and compulsorily recorded (e.g. start and end point of trip). Besides the "three-hours rule", there should be no storage of detailed location and time data (e.g. no tracing of routes) in the Tachograph. However, these data might be very useful for other applications, such as EETS and fleet management. Such data might be passed via a network interface and stored in a bus. Then the question arises: how to certify this DT with integrated GNSS module when recorded GNSS data are stored outside the DT?

In view of an **open in-vehicle platform** architecture, regulatory applications should not be seen as a sealed and type-approved box, but rather as applications with certain **functional requirements**.

4.3. Application

Besides **requirements** of the (key) applications regarding resources, data quality, authenticity etc., especially data **access** and data **ownership** are important issues for the platform-readiness of the application layer.

4.3.1. Data access

The **ITS interface** of the DT may enable the DT to become the core element of an open in-vehicle platform architecture, since it might provide high quality PVT data to other applications on the ITS interface. Therefore it is essential that this ITS interface is properly specified and ties into a **widely deployed standard vehicle bus** such that on-board components can access the PVT data easily and at low implementation costs.

Although the **CAN-bus** will be in place for heavy vehicles for many years, this vehicle bus has some **severe limitations** regarding the bandwidth and network topology. It is therefore expected that **several in-car networks** will (continue to) simultaneously exist in future vehicles. The networks

[36] http://www.heero-pilot.eu/ressource/static/files/5_janvanhattem_38_heero_nl_slide_final_international-conference-zagreb-15-november-2012-netherlands--2--1.pdf

should be **functionally interconnected** in order to ensure the economic viability and operational effectiveness of the whole.

The major European truck manufacturers argue that the harmonized ITS interface **already exists** through their **FMS-standards** and **Communicators** connected to the CAN.

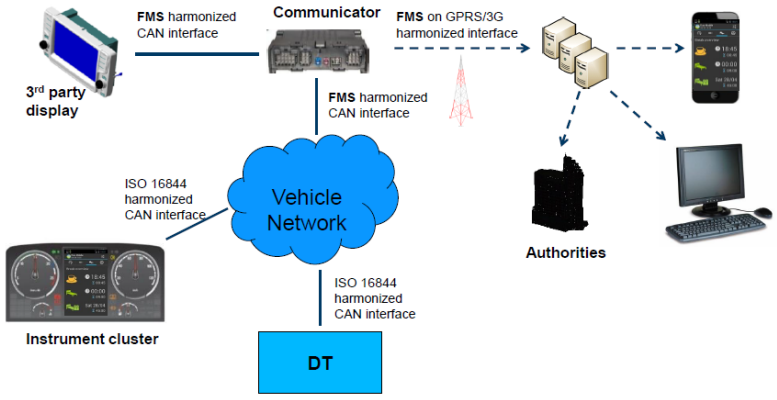


Figure 18: *Proposed architecture for the ITS interface based on the FMS-standard*[37]

According to several vehicle manufacturers all **vehicle owned data** will continue to be delivered as today via the optional FMS connector. Only the data recorded by the **DT** related to the social legislation might be delivered by the DT. In their view, a further **integration of ITS** to the DT is regarded **unwise**, since the DT is a **slow** moving entity that needs to be type approved and ITS are dynamic on-demand services to the customers.[38]

The **FMS-solution** raises the following questions regarding **data access**:

- It is an optional interface: what are the impacts on consumers and service providers if vehicles are not equipped with this optional interface?
- What costs apply to service providers, if they want to link their solution via the ITS interface with in-vehicle resources and data/information?
- It only connects to the CAN: is the CAN able to deal with the requirements of the key applications, e.g. regarding data rate?
- It generally assumes the exchange of commercial data (e.g. for fleet management purposes): what about the exchange of regulatory data?

4.3.2. Data ownership

Already today vehicle manufacturers offer **generic services** to fleet operators based on vehicle data provided by the CAN. Through the **FMS**-interface, if present, certain vehicle data collected are also open to third party companies. However, at the moment it is not fully clear to what extent the vehicle manufacturers would like to **"really" open up** and share all vehicle owned data (e.g. stored on a central data server) with others.

[37] Taken from "Vehicle Industry solution to comply with the new DT Regulation", Presentation by Volvo and Scania at the DT meeting at Ispra, 18 & 19 April 2013

[38] Based on an e-mail statement by Mr. Jorge Soria Galvarro, senior technical advisor at Scania CV AB

If ITS services will be made available to the consumer through the vehicle manufacturer by allowing third parties (i.e. service providers) access to the in-vehicle network by means of the FMS-standard, this raises the question of **data ownership**: who owns the data?

Several stakeholders may lay a potential claim to the ownership of such data, for example:

- *Consumer*: the party that actually produces and is "described" by the data
- *Vehicle manufacturer*: the party that enables the collection of the data
- *Service provider*: the party that provides the application based on the data
- *Authorities*: the party that triggers / mandates the collection of the data

Ideally, the **consumer** (vehicle operator or driver) owns the data and decides on allowing or not access to these data to other parties. It has to be noted that the transport company has paid both for the vehicle and for the telematics provisions installed. The transport company is both the owner of the vehicle and all installations and also the one that is moving the vehicle, i.e. the one producing the data and hence being described by the data. From this point of view, the **transport company should have full control of the vehicle resources**, i.e. the data produced (except for personal data of the driver unless verifiable consent has been granted by the driver), the communication channels and the HMI.

From this viewpoint, the transport company should be able to decide which party he contracts to provide ITS services, be it the vehicle manufacturer with his associated services offers or a third party service provider. For "freedom to decide" **it is essential that access to vehicle resources is not restricted to the vehicle manufacturer**, who is the only party that has access to the in-vehicle bus system, which for obvious safety reasons cannot be opened to other parties. Giving third parties access to in-vehicle resources **requires a defined and controlled access point**, like the FMS connector, which acts like a firewall protecting the vehicle bus from harmful external interference.

The **access point needs to be provided as a standard component of heavy vehicles**, otherwise third parties would be put at a disadvantage from the onset. Currently there is no requirement that vehicle manufacturers have to open in-vehicle resources to third parties, and different brands follow different philosophies. Seeing the business potential of ITS applications, there is the very manifest risk that vehicle manufacturers will not provide for third party access points such as the FMS in the future or only at high costs and special order.

Data ownership is also an issue with eCall. The German Insurance Association (Gesamtverband der Deutschen Versicherungswirtschaft, GDV) for example sees some potential conflict behind the question, **whether the vehicle owner has a say in what data must be sent to whom**. This issue of data ownership plays a very important role for the stakeholders associated with the introduction and ongoing processing of eCall. GDV requests that the **technology** required for eCall can **not only be used by vehicle manufacturers alone**. It must be **made available to all potential service providers**. Only in this way a fair competition between all service providers can be ensured. The **driver should remain the owner of the data** collected by the vehicle and should **be able to decide to whom data is made available**. In fact, the current proposal of the European Union foresees this free access to data for repair and maintenance operations only. The insurance industry is now committed to remove this restriction and to embed free access to the vehicle data in the regulation.[39]

[39] Source: http://www.versicherungsbote.de/id/4779430/Assekuranz-fuerchtet-Wettbewerbsnachteil-durch-Notruftechnik-eCall/ (retrieved on 24th July 2013)

4.4. Business

The business layer is concerned with the industry perspective. Especially the perspectives towards the potential market for ITS services and towards liability are relevant issues.

4.4.1. Market for ITS services

Already today the majority of vehicle manufacturers offer **generic services** to fleet operators based on vehicle data provided by the CAN. With the **FMS**-standard the major **truck manufacturers** keep their **strong position** of allowing others under strict control (partial) access to vehicle data. Obviously, there is an interest for them to **keep much business** for themselves. However, they should also recognise that they **cannot** do everything themselves, such as providing **specialised** services to transport companies.

For **service providers** it is relatively **difficult** to find a **business case** in the current ITS field. For example, EETS does not seem to have a business case in its own, at least under current conditions of not-aligned systems and procedures of the different tolling system in Europe. Value-added services are needed to survive as a service provider. Currently, **the FMS-connector** (and to a certain extent also the Remote-Download Interface of the DT or the OBD interface) allows a service provider to connect to the vehicle and use certain vehicle owned data for the provision of applications.

Thus, the vehicle manufacturer and the service provider are **in conflict** which hinders the **platform-readiness** of the business layer. On the one hand, the vehicle manufacturer wants to keep most business; on the other hand, the service provider would like to have more possibilities to set up his business.

Besides opening in-vehicle resources for access, an approach may also be found in vehicle manufacturers giving service providers **non-discriminatory access** to the vehicle data stored on **(future) central data servers**. If data are considered to be owned by the consumer (see previous chapter) this would only be natural: The data on the central server are owned by the transport company that is described by the data, and the company might give access to their data to any third party. Probably some data need to be reserved for the vehicle manufacturers internal purposes, such as proprietary, very type-specific information related to the engine.

As vehicle manufacturers more and more standardize telematics units in the vehicle, there is a growing need for a **server interface standardization**. ACEA's WG/HDEI – also in charge of the development of the FMS-standard – has started to work on this single standardized interface for **data access on the Internet**. In future vehicle manufacturers might provide vehicle data on **central data servers** through a standard interface (see Figure 19, right part) instead of only on his own data server with a proprietary protocol (see Figure 19, left part).

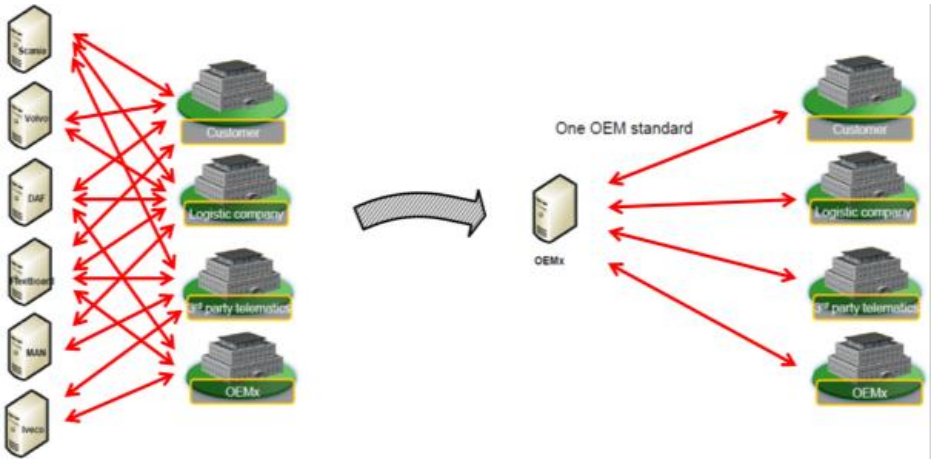


Figure 19: *Standardization of a server interface for all vehicle manufacturers: current situation (left) and potential future situation (right)*[40]

If this approach will be the basis of an open in-vehicle platform architecture, the questions raised in Sections 4.3.1 and 4.3.2 on **data access** resp. **data ownership** also apply here and need to be resolved for establishing a platform-ready business layer.

Non-discriminatory access to such a rich data platform would really **break open** the ITS market and could give a service provider the **critical mass needed** to set up his business. He may offer a **wide range** of applications, including specialized services which cannot easily be served by vehicle manufacturers. With opening up the vehicle data, the vehicle manufacturer could still keep providing specialised maintenance services, but at the same time achieve a **higher attractiveness** of his brand by enabling specialist applications provided by service providers.

4.4.2. Liability

Liability is often used by the vehicle manufacturers as an **argument against** opening up their vehicle networks. A direct connection to the vehicles' internal bus system might affect vehicle reliability as well as warranty. Others besides the vehicle manufacturer will be held responsible if they connect directly to the internal bus system and disturb it. The leading truck manufacturers have come up with the **FMS-interface** as a solution to this liability problem. Where the FMS-interface merely protects safety-critical applications, there are also approaches to avoid **commercial liability**. Consider, for example, the **payment guarantee** from EETS Provider to Toll Charger in the **EETS**.

In general, the **more complex or "non-overridable"** a system is, the more complex are the related liability issues. This is also the fact with an open in-vehicle platform. The general principle that each stakeholder is only responsible for the part of the chain which is **under his control** should be maintained. The need and feasibility of developing **regulations** (as for 112-eCall) aimed at notably establishing the rights and obligations of the parties with respect to the service elements they provide should be considered.

The two **main liability prerequisites** for a platform-ready business layer are:

- A **clear hand-over** of liability along the complex chain of different stakeholder responsibilities
- **Insurability** of the whole (e.g. in-vehicle platform) and its components (e.g. applications)

[40] Taken from "Vehicle Industry solution to comply with the new DT Regulation", Presentation by Volvo and Scania at the DT meeting at Ispra, 18 & 19 April 2013 and adapted

4.5. Governance

As said at the beginning of this chapter, the EC has notably a role at the **governance** layer. All other layers should be market-driven, although the EC has the power to **direct** and **align** the industry.

4.5.1. Services approach

The current legislation of regulatory applications, such as the EETS and the DT, is still very much concentrated on “boxes”. To promote opening up of transport markets to **free and undistorted competition** and enable the development of common **interoperability** and **security** solutions, the EC should stimulate a **services approach**, in accordance with the current market trend. The commercial domain has fully embraced the “services paradigm” and has moved away from providing hardware “boxes”. Rather the services aspects are being focused on and marketed. Regulatory applications like the DT or eCall (with the exception of the EETS) are still prescribed in the “boxes” approach, where a specific piece of hard- and software needs to be certified for the regulatory application.

The EC as **market regulator** should as a first step investigate the issues around the **data ownership** of vehicle data. Ideally, the data are **owned by the vehicle operator** (and partly the driver), who may wish to make available or not these data to other parties, such as (potential) service providers.

Furthermore, the EC should consider **gradually moving** towards a **services-based paradigm** for **regulatory** applications. Such approach would give road authorities a means to better manage transport obligations for the growing transport demands. It would provide for more productive and compliant heavy vehicle operations that promote sustainable road infrastructure, improve road safety and reduce environmental effects.

The **EETS** sets an **example** for a services concept of a regulatory application: On behalf of the Toll Charger, an EETS Provider grants access to EETS to an EETS user who subscribes a contract with an EETS Provider. Especially OBW but also the DT might be deployed as a **regulated service**. For **OBW** there are several **successful** similar **approaches** around the world, e.g. the PrePass system in the USA and the Intelligent Access Program in Australia. Due to the specific legal constraints of the DT, it seems likely to provide the **DT** as a “regulatory box”, but providing the DT as a **service** from a service provider may be well conceivable as a **second option** next to this classic option.

4.5.2. Incentives

A **services** approach is seen as a **good opportunity** to develop and market an open in-vehicle platform architecture for heavy vehicles. However, for such approach, **commercial interest** in forms of incentives is deemed a necessity.

The **incentive** for users would consist in wanting to demonstrate the road authorities their compliance (e.g. with weight limits, driving hours, toll payment) voluntarily through a service provider **in return for clear benefits** given by the road authorities.

The EC should encourage users to **voluntarily fulfil** their obligations by providing incentives. There are **many successful examples** of incentivizing compliant or “good” behaviour in related fields, including:

- Directive 1999/62/EC on the charging of heavy goods vehicles: eco-friendly vehicles, such as Euro 5, EEV and Euro 6, receive reduced toll tariffs
- Intelligent Access Program (IAP) in Australia: transport operators use the IAP to negotiate enhanced access conditions with road agencies
- PrePass in the USA: compliant vehicles are allowed to bypass roadside checks
- Potential approach of weight compliance in Lyon, France: study into the possibility of opening bus lanes to heavy goods vehicles “with DT load” in urban delivery

Incentives do not necessarily need to be direct monetary benefits. For example, in the US PrePass system vehicles bypassing inspection facilities while actively via DSRC communication showing compliance with the weight limits save drivers (and their companies) time on the road. The incentives are thereby reduced fuel consumption, journey duration and, as consequence, operating costs. In addition, the incentives for the states are reduced congestions around inspection facilities and enabling state inspection staff to focus their efforts on carriers that demand the most attention.

Anyhow, what is done on the governance layer will **influence** the lower layers. It should not be the intention of the EC to automatically impose legal obligations to the market for the development of an open in-vehicle platform. Hence, the EC should **facilitate the uptake of the market** by actions like elaboration on the topics above, standardization, production of technical specifications and support to the research and development of necessary components.

4.6. Security

As mentioned in previous studies (i.e. ITS Action Plan 4.1 or ITS Action Plan 5.1 on ITS & Personal Data Protection), security is an aspect to be considered on all levels (see Figure 20). On lower levels, security addresses hardware and software related aspects, whereas on higher levels it is about secure application processes, threats to business and about fraudulent activities related to legal obligations.

To give an example: At the level of the sensors and interfaces, quality and integrity of the data as well as authentication of the information is of a major concern. The level of service provision deals with completely different security aspects. For instance it is about how a service can be certified or a provider can be audited to maintain client confidence and avoid privacy risks.

Not only vary these security considerations for different levels of platform specification but also one has to distinguish between different applications. Some applications require a higher level of integrity, while others may need be protected against fraudulent attacks. It depends strongly on the particular type of application to be able to determine the security requirements and protection measures.

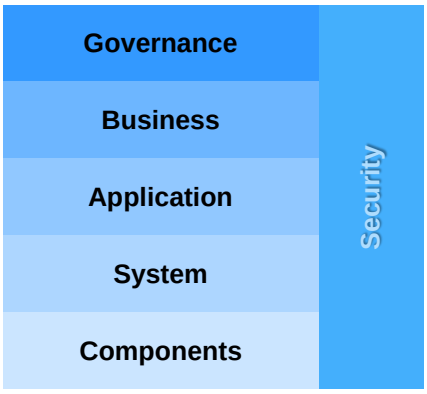


Figure 20: Security has to be addressed on *each layer of a common architecture.*

When doing a risk analysis, this has to be done on each layer and for each application. Only if the application specific security issues have been evaluated, security solutions become clear. Based on the fact that “a chain is as strong as its weakest link” the application with the highest security requirements (in other words: the application with the highest potential for attack or misuse) defines the measures to be implemented in a generic open platform.

Conclusion for establishing an open in-vehicle platform **Architecture**

Prerequisites for the **platform-readiness** of the common in-vehicle platform architecture include for each layer the following:

1. **Components layer**: no duplication of modules but instead shared in-vehicle resources; the vehicle should have only one GNSS module and one DSRC module, which are generally accessible to all in-vehicle applications requiring the GNSS and DSRC functionalities
2. **System layer**: specifications should not include elements that may hinder the development of integrated devices; certification processes of integrated devices should be defined such that parts can be (re)certified independently from one another.
3. **Application layer**: answers are needed on key issues of data access and data ownership; ideally the consumer owns the data and decides on allowing or not access to these data to other parties.
4. **Business layer**: solution to the “conflict of interest” between vehicle manufacturers and service providers regarding full access to vehicle data; the vehicle owner, i.e. the transport company, should be free to decide who can access and process data both in the vehicle and centrally. Liability issues appear to be manageable.
5. **Governance layer**: a services approach (in accordance with the current market trend) to promote opening up of the transport markets to free and undistorted competition; regulatory applications provided as regulated services; voluntarily fulfillment of compliance through incentives, standardization and certification especially for integrated devices.
6. **Security considerations**: there is no "one size fits all" security model, because each application has its own security needs. But on the components layer the interface to general modules like DSRC and GNSS has to be specified to have a level of security that satisfies the requirements of the application with the most demanding needs.

5. Open platforms: concepts and merits

Based on the most relevant issues or requirements for making the five architecture layers platform-ready, this chapter presents several possible concepts for an open in-vehicle platform.

In essence there are **four concepts**, which may be **coexisting**:

- Open on-board computational platform
- Platform of shared in-vehicle resources
- Central data server platform
- Services paradigm platform

Each concept is described and elaborated with respect to its drivers and barriers and the actions required to facilitate its take-up.

5.1. Open on-board computational platform

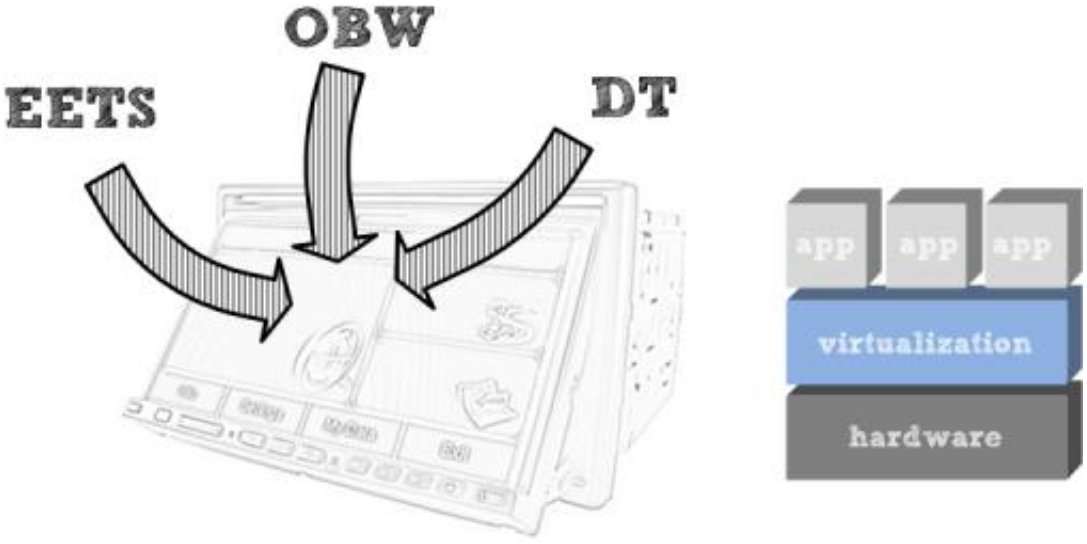


Figure 21: *Open on-board computational platform concept.*

5.1.1. Concept

This open platform concept ideally consists of an **open on-board computational platform** for both regulatory and commercial applications. The concept is strongly linked to the **system layer** of the common architecture for an open in-vehicle platform.

The heavy vehicle would be an **open environment** with **plug-and-play applications**. Several applications run on one operating platform with protected runtime environments for the simultaneous and secure execution of the applications. For each module or sensor an application programming interface (API) specifies how the components should interact with each other. The applications should be **shielded** from each other, so that other applications stay unaffected if one application has a problem (e.g. it crashes, it is insecure or it does not have enough memory).

5.1.2. Drivers and obstacles

The **main driver** for this concept is the **consumer view**. For the consumer (i.e. driver, company) it would be the ultimate dream to buy applications that can run on the single on-board platform without being bound to the vehicle manufacturer or a single service provider.

For the time being, however, there are **many obstacles** for this platform concept.

Although it has been proven, e.g. in the OVERSEE project, that such an open in-vehicle platform is technically possible, it is still **technically very challenging**. Especially, the **diversity** of regulatory and commercial applications may affect the chances for the single on-board platform. The problem with **regulatory** applications (e.g. EETS, DT, OBW) is that the solutions often prescribe technologies or features **dedicated** for that specific application ("closed box"). Especially applications that require certified or even type approved equipment are difficult to integrate onto an open platform. The problem with **commercial** applications is that the solutions are mainly driven by the market and consequently include very **diverse** requirements.

Moreover, it is **not expected** that the **vehicle manufacturers** will move towards the development of a single on-board platform. Reasons for this include **security** and **liability** issues when third parties are allowed direct access to the in-vehicle networks. Besides, developing this platform and its applications is deemed commercially **not attractive** for vehicle manufacturers because of the long **time to market** and the **complexity** around certification of modules, updates of applications, etc. Why invest in order to allow third parties to make profit?

Still, some vehicle manufacturers already offer **integrated solutions**, where several applications are provided on a single platform. Yet, these are **not open** for other service providers and additional applications a user might wish to operate. It is **questionable** to what extent the industry would like to open up and expand their existing platforms or to collectively develop a new open platform.

5.1.3. Actions required

There is **no immediate need for action**, since there seem to be not enough benefits for all stakeholders to fight for a "full-blown" single on-board platform. Consequently, this concept of a single on-board platform should be **left to the market**.

Second-best solutions will be developed by the industry. There is no need to interfere, consider for example the following developments:

- FMS-interface: The major European truck manufacturers have developed the FMS-interface to enable **manufacturer independent applications** for telematics. However, it is not an operating platform and it has no programming interfaces (APIs). Although the FMS-interface

does not approximate a “full-blown” single on-board platform, it provides a **data exchange interface** by which third parties are allowed access to electronic data from the CAN of the vehicle for use in their own applications.
Fair access to the FMS data needs to be provided. An FMS interface and connector is not a standard item in all truck brands and sometimes comes as a comparatively costly option, which might kick third parties out of the market.

- Multi-application devices: It is technically feasible to integrate several applications on one device, such as DT, EETS and OBW. The current legislation of DT and EETS does not hinder such integration and it can be demonstrated in the certification processes of DT and EETS that **integrated devices** are a possibility. However, new applications cannot be easily added and the platform is not open to other service providers. Although such multi-application devices do not approximate a “full-blown” single on-board platform, integration brings the advantage of much **richer data**. This way, new potential applications may be developed, such as a DT with integrated parking information.

5.2. Platform of shared in-vehicle resources

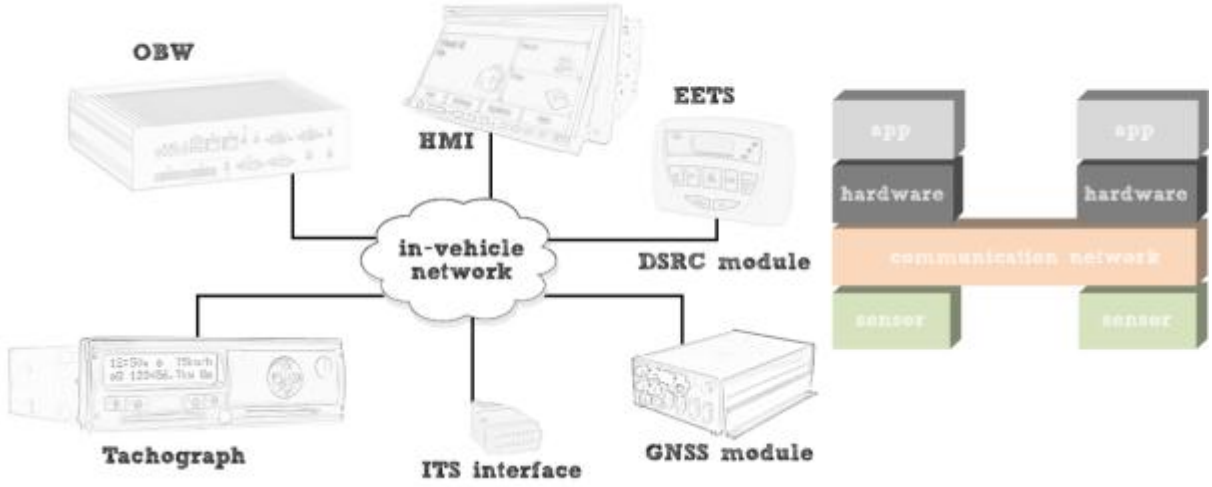


Figure 22: *Shared in-vehicle resources concept.*

5.2.1. Concept

This open platform concept implies that several applications can **co-exist** and **make use of joint resources**. The concept is strongly linked to the **components layer** of the common architecture for an open in-vehicle platform.

At present, applications do not make use of – for example – a single GNSS receiver as a shared resource; instead the functionality is **duplicated** for every application. Moreover, applications usually even come with their own separate piece of equipment. Several European regulations require the use of the **same technology** (e.g. GNSS and DSRC). It **would be a complete failure of European policy** if this would lead to multiple modules with the same functionality inside one vehicle. For this viewpoint, a platform with **shared in-vehicle resources** is **a must**.

While the previous paragraph has put forward the technical argument that for efficiency reasons sharing of in-vehicle resources especially amongst regulatory applications is highly advisable, **open market arguments** regarding the commercial services are even more important. As put forward several times before, for maintain a competitive market for ITS services it is essential that in-vehicle resources are made available not only to the vehicle manufacturer but also to third parties. **Resources** such as sensors (speed pulses, GNSS), vehicle operating data (gear setting, fuel consumption), communication channels (DSRC, mobile communications) and HMI (especially display) **need to be accessible to third parties under fair and non-discriminatory conditions**.

The **issue of data ownership and right to control resources** is also important in this respect. The owner of the vehicle, i.e. the transport company, should have full rights to decide whom it wants to give access to the vehicle resources in order to be able to procure the economically most advantageous offer for the ITS services the companies needs.

The technical solution for this is to have a **standardised ITS interface** (physically this is an "ITS connector") in heavy vehicles that gives access to the vehicle resources, e.g. by providing a protected gateway to the CAN bus. Via this interface it should be possible to access vehicle data (including DT data), sensory resources and make use of on board communication means and especially send message to be shown in a reserved area of the vehicle main display.

Without such an access, third party ITS service providers are severely limited regarding the type of services they can provide and even for basic services put at a commercial disadvantage with the vehicle manufacturers.

For **example**, for providing an "**intelligent truck parking**" service, that advises the driver about advantageous parking opportunities ahead in case his legally allowed driving time comes close to ending, the following information and resources (in-vehicle and external) are required:

- Where is the vehicle ? (Access to in-vehicle GNSS)
- Where is the vehicle heading to ? (Access to navigation information)
- What is the remaining radius ? (Access to fuel level and consumption)
- What is the remaining legal driving time ? (Access to DT)
- What is the vehicle size ? (Access to vehicle data)
- Where are the next free parking options ? (Access to communications)
- Show recommended parking options (Access to display)

Obviously, **without access to critical in-vehicle information and resources, the service cannot be provided.** Without an open standardised access to in-vehicle resources, third party service providers are limited to providing only elementary services, such as very basic fleet management functions, like "where is my truck", and even this requires a duplication of the GNSS and HMI functionalities.

Open access to in-vehicle resources need to be provided for establishing an open services market. Not only the more obvious access to vehicle data (speed, fuel, location) is important, but also access to the HMI. For **safety and ergonomic reasons**, HMI functions (display, touch screen/cursor keys) should be optimally placed in order not to distract the driver. Third party add-on devices usually can only be placed at locations in the vehicle where the driver needs bow and extend his arm, look away from his usual viewing axle and is distracted for an unnecessary amount of time.

A mentioned above, a standardised "ITS connector" making all in-vehicle resources safely available would technically enable an open market for ITS services. Even better would be a **standardised installation bay** where third party devices can safely and conveniently be plugged into (like the old DIN-slot, where car radios could be installed and connected to power and to the loudspeakers through standard connectors according to ISO 10487).

5.2.2. Drivers and obstacles

The **drivers** for this platform concept are **obvious**.

However, the **main obstacle** for this platform concept is that a sharing of in-vehicle resources and making them accessible **will not happen by itself**. Since there are regulatory requirements involved, such platform of shared in-vehicle resources is not only driven by the market. It needs **coordination by setting standards** and **regulation by mandating** open access.

Sharing of resources:

For the **GNSS functionality**, it is quite conceivable that the GNSS module can be connected through the **CAN** with the in-vehicle applications. Elements can be easily added, such as **security features** or a **trusted GNSS signal**, which would be beneficial to applications with high safety or commercial liability, such as eCall or EETS respectively.

Ideally, the GNSS receiver will be a **trusted source of PVT data** in each vehicle, but this will require three things:

- Trusted satellite signal: preferably provided by authentication of the satellite or otherwise by means like suggested in the TACOT project
- Trusted GNSS receiver
- Trusted connection from the GNSS receiver to the in-vehicle applications

For the **DSRC functionality**, **timing** is critical and it is therefore **not an easy task to connect** the DSRC module through a vehicle bus with the in-vehicle applications. A DSRC communication to a moving vehicle should not last longer than ca. 50 ms. It is difficult to send several messages forth and back within this **short time frame** using standard vehicle buses, such as CAN. Either a dedicated **higher speed connection** is required or the data need to be **preloaded** into the DSRC module before communication. The best option will need to be decided by experts in the field.

Open access to resources:

As explained above this requires a standard and a regulation that defines the "**ITS connector**" and mandates conditions of it being present and accessible. Technically, an enhanced functionality FMS connector might well do the trick. The connector would provide a **secured gateway to the vehicle CAN Bus** and make all its resources (vehicle and trip data, communication channels, HMI, etc.) available in an open way, ideally in a **defined bay, where third party devices can be installed**.

5.2.3. Actions required

Sharing of resources:

Notably, the EC should enable through **standardisation** that all technologies of the (key) applications can work together, i.e. share information and use joint components. At minimum, the EC should insist on having **one GNSS module** and **one DSRC module** in the vehicle, which are generally accessible by the applications requiring these functionalities.

Therefore, **mandates** should be given to develop **interface specifications** for the GNSS and DSRC functionalities. Ideally, **common vehicle buses** should be used and **proper security** should be provided. Moreover, attention should be paid to the importance of trusted GNSS signals, trusted GNSS receivers and trusted connections from the GNSS receivers to the in-vehicle applications. The

specification work for the amended DT provides for a good opportunity to define a suite of interface specifications.

Open access to resources:

Ideally the EC should **act on a legal basis and mandate open access** to vehicle resources, requiring in the legal document that specifications are developed for a standardised ITS connector and a standardised ITS installation bay. The ITS Directive might provide for a suitable framework and opportunity for this purpose.

5.3. Central data server platform

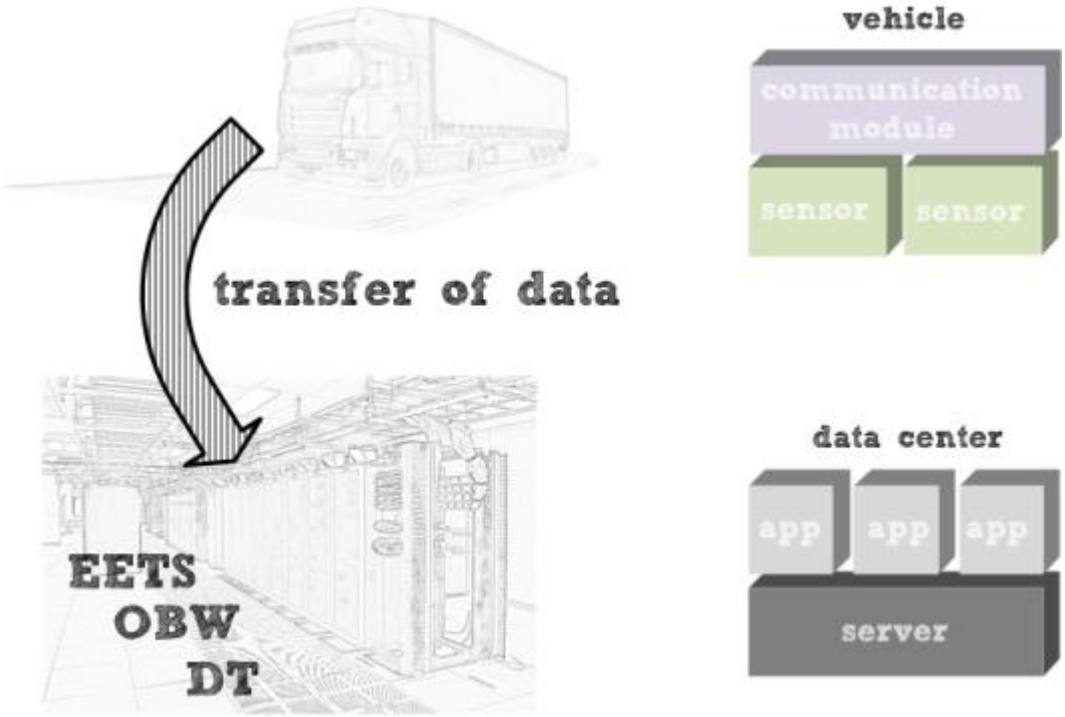


Figure 23: *Central data server platform concept.*

5.3.1. Concept

Already today vehicle manufacturers transmit certain vehicle data to company servers, initially for **internal quality** purposes, such as detection of failure modes, but also for **vehicle-related** purposes, such as periodic maintenance.

In this open platform concept the **vehicle data** collected through the channels provided by the vehicle manufacturer would be stored on a **central data server** which is open to all service providers for use in view of their (specialised) applications. The concept is strongly linked to the **business layer** of the common architecture for an open in-vehicle platform.

Over time, most truck brands offer **generic services** to fleet operators. For example, Daimler offers **FleetBoard** for the management of vehicle fleets[41]. It integrates the most modern portable radio techniques, in order to determine vehicle and route data precisely. High-performance computers convert all information, which is offered to the customer password-protected and user-friendly via the Internet. The interface allows the direct and automated integration of the provided data sets into the most diverse, customized data management systems, such as logistics management systems. MAN's Internet service for integrated fleet management is called **TeleMatics®**[42]. It helps to significantly reduce fleet fuel consumption, optimise loads and maximise efficiency through a wide range of services and features, including tracking & tracing, maintenance management, display of remaining driving times, remote download function, open interface for integration in existing software systems and access from every Internet-enabled PC.

Certain **vehicle data** collected by the vehicle manufacturers are **open** to third party companies in Europe (through the optional FMS-interface) and to the authorities in other countries (e.g. China, Russia). At present, there are initiatives by the vehicle manufacturers to develop a **single standardised interface** for data access on the Internet. In future each manufacturer might provide his vehicle data on one **central data server** instead of only on his own data server.

This platform concept assumes that all vehicle data on this central data server is made **available** under **non-discriminatory conditions** to service providers to enable them to provide **sector-specific** applications. Consider, for example, applications focusing on the transport of livestock, dangerous goods or temperature-regulated goods (e.g. pharmaceuticals, fresh fish, exotic plants). In contrast to vehicle manufacturers who provide generic services for the majority of trucks, such specialised services are preferably provided by **companies close to the respective sector**.

In principle **it shall be up to the transport company** as vehicle and data owner and **to decide, who transfers data to central facilities and whom to give access** to them.

5.3.2. Drivers and obstacles

One of the **main drivers** for this concept is the **consumer view**. A real interest is seen for transport companies, who can gain clear benefits if service providers have a non-discriminatory access to the vehicle and movement data of their trucks. These service providers could be close to the respective transport sector and therefore recognize **specific needs**, have a **quick reaction time** and **easily connect** with the productive environment of a transport company (e.g. by integration of their application into existing software systems).

Another **main driver** for this concept is of course the **service provider view**. For a service provider, this concept would really **break open** the market. Non-discriminatory access to such a rich data platform could give him the **critical mass needed** to set up his business. He may offer a **wide range** of applications, which cannot necessarily be served by vehicle manufacturers.

However, vehicle manufacturers **giving non-discriminatory access** to the vehicle data is considered the **biggest obstacle** for this concept. At the moment it is not fully clear to what extent they would like to open up and share their (central) data server with third parties. Obviously, there is an interest for vehicle manufacturers to **keep much business** for themselves, considering that they are moving from an industrial business (truck manufacturing) to a service-oriented business (service provision for drivers and operating companies). An unbiased competition means that vehicles manufacturers (as service providers) should be on the same level as all other suppliers of ITS services. The sole way to achieve this condition which is politically a go/no-go, would be a free of charge access to the vehicle

[41] http://www.fleetboard.com/

[42] http://www.mantruckandbus.com/com/en/services/man_support/telematics/TeleMatics.html

data for all service providers, be it in the vehicle or centrally. With opening up the vehicle data, the vehicle manufacturers could still compete regarding vehicle- and type/brand-centric services, but at the same time achieve a **higher attractiveness** of their brand by enabling specialist applications provided by service providers.

5.3.3. Actions required

According to the major truck manufacturers, all vehicle owned data will continue to be delivered as today (via the FMS standard in the vehicle or via an additional "communicator" module to central facilities). In this way, the vehicle manufacturers keep their **strong position** of allowing under severe control (partial) access to their proprietary vehicle data. It would be good for the EC as **market regulator** to make **clear statements** as to the **ownership** of these data. Ideally, the data are **owned by the vehicle operator** (transport company), who may wish to make available or not these data to other parties, such as (potential) service providers, including the vehicle manufacturers acting as service providers.

Open access of vehicle data to service providers should be based on **fair and non-discriminatory conditions** to ensure that no service providers are either directly or indirectly treated less favourably than others, for example on the grounds of competition. Of course, there may be a set certain **requirements** that (potential) service providers must fulfil before entering the business.

Next to general access rules, **specific commercial conditions** should be allowed to be agreed bilaterally between the vehicle manufacturer and the service provider. The vehicle manufacturer operates the server, processes the data, takes security measures, provides for backups, etc. which comes at a cost. It would be reasonable, if the vehicle manufacturer would receive **remuneration** from the service provider in return for being allowed to use the vehicle data, under the strict condition that OEMs do not operate as service provider themselves. **Alternatively**, given that a standardised "ITS connector" will exist in heavy vehicles, the vehicle operator may decide that the task for communicating data from the vehicle to a central server is not provided by the vehicle manufacturer (as today) but given to a third party. This third party service provider would take data from the "ITS connector" and **send it via his own communication module** (ideally installed in the standardised "ITS bay") to a central facility chosen by the vehicle operator.

Core to all this are legal provisions that clarify data ownership and control over in-vehicle resources. Again, the ITS Directive might provide for a suitable framework for this.

5.4. Services paradigm platform

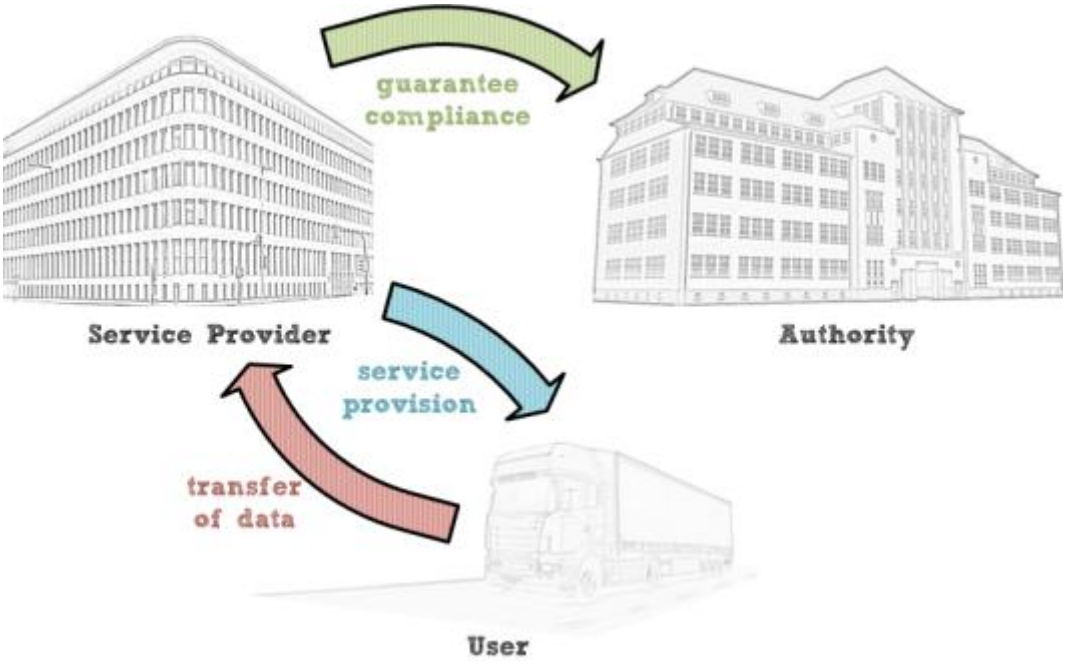


Figure 24: *Service platform concept.*

5.4.1. Concept

This open platform concept is based on the central data server platform (see above) and cannot go without it. It considers a **services model** for regulatory applications. Due to its key aspect of **compliance** with regulations, this concept is strongly linked to **governance layer** of the common architecture for an open in-vehicle platform.

Such a services model would recognize the fact, that the **new paradigm** in ITS is **services**, not "boxes" or devices. Consequently, the new focus is on parking services instead of a navigation device, on fleet management services instead of a fleet management box, on tolling services instead of an on-board unit, etc.

Reasons for this services paradigm include:

- Technology: With a focus on functionality instead of a device, services last much longer, since they are **not bound** to relatively **short-lived technology**. The life-cycle of telematics service and devices is much faster than the life cycle of trucks.
- Business: Services provide a **continuous business case** through their subscriptions in contrast to a business case based on selling individual devices.

It is obvious that the new market trend to refrain from thinking in "boxes" is not fully reflected yet in the legislation of regulatory applications. Nevertheless, there are **opportunities to move regulatory applications stepwise into a services-centric environment** and enable them to be provided on a services paradigm platform.

The **EETS** sets an example for a **services concept** of a regulatory application. The core actor is the **EETS Provider** who collects the charges due by EETS Users throughout Europe based on one single

on-board equipment and one single contract. Setting up the EETS as such is left to the market with the EC providing the framework for its establishment.

Also **other regulatory applications** might be deployed as a **regulated service**. In general, service providers would **monitor** the **compliance** of companies, drivers or vehicles with specific regulations. Any non-compliance with these regulations can either be reported to the relevant authorities (active approach) or these authorities are allowed access to the data to verify compliance themselves (passive approach).

The current legislation of the **DT** focuses on the description of the device itself. Aligning the DT with the general market trend and describing it as a service would enable a **"work and rest hours compliance service"**[43]. Service providers could manage the driving hours of a driver and advise him to go parking and resting, ensuring his compliance with the social legislation. The provision of the DT as a service in combination with access to a rich data platform enables service providers the development of new applications, such as a **DT with integrated parking information**.

The **OBW** application seems particularly **suitable** for this services paradigm platform. A service provider would **monitor** the **compliance** of a vehicle with the requirements regarding maximum authorized **weights**. Ideally, OBW should be defined as a service **from the beginning**. The application would be deployed as a regulated service within a regulatory framework consisting of corresponding legislation, standards etc.

Also the **Roadworthiness Package** seems very **suitable** for this services paradigm platform. Here a service provider would **monitor** the **compliance** of a company with the **roadworthiness** requirements.

In summary, this concept of a services paradigm platform would be similar to the **"IAP approach"** in Australia, see Annex 2. Within this approach, regulated applications are deployed as services. The user wants to demonstrate the road authorities his **compliance voluntarily** through a service provider in return for clear **benefits** given by the road authorities.

5.4.2. Drivers and obstacles

The **main driver** for this concept is the **alignment** of the legislation of regulatory applications with the current services paradigm for commercial applications, which would entail the following **benefits**:

- The services concept **lasts much longer** and provides **more stability** than the "boxes" concept due to commercial and technology reasons.
- Transport companies would be able to fulfill their legal obligations with the assistance of a service provider in a **package with his commercial ITS services**.

One **obstacle** for this concept is that the **legislative process** is **slow**. It is recognized that this process is **complex** due to the existing installations and the many requirements, e.g. related to equal treatment (e.g. no difference between old and new DTs in a fleet). Also, it is **not anchored** in European thinking to work with the market and with service providers, in contrast to USA and Australia.

[43] Such an approach is currently being developed and tested in Australia, where service providers collect vehicle and driver data related to work and rest hours and make them available to enforcement authorities.

It is also questionable to what extent companies will embrace a services oriented approach towards compliance. Today, **regulatory "services" are provided "for free"**, i.e. without an associated services fee. With a services-oriented approach, companies would have to pay for the compliance service, in exchange for being able to outsource much of the associated management and administration to a service provider. In Australia and the US, transport companies have experienced the benefits of having "managed compliance" and being less bothered by authorities when compliance is actively communicated. In many cases, gain in efficiency in terms of time saved by often being able to bypass controls, in less risk of inadvertently breaking rules and lower administrative overhead lead to markedly **increased productivity**.

5.4.3. Actions required

The **recommendation** on a service model for regulatory applications from our **first study** into an open in-vehicle platform[44] still **holds true**.

However, in recognition of the fact that it is difficult to "suddenly" change legislation, one way forward to align with the **services-based market trend** may be to allow for regulated services as **an option**, either replacing or additional to the original option. This **low-risk** approach can be seen as a **stepwise introduction** of a services model for regulatory applications in order to refrain from thinking in "boxes" and eventually phase out this technology-driven approach.

It is assumed that the **majority** of companies want to be **compliant** with regulatory requirements. The services paradigm platform would become **more attractive** in case these companies would be given an **incentive** for their effort of being compliant. For example, the incentive for users would consist in wanting to demonstrate the road authorities their compliance **voluntarily** through a service provider **in return for clear benefits** given by the road authorities, e.g. lower tolls on certain networks, entitled to by-pass certain roadside checks, improved access to parking facilities etc.

The **rise and fall** of this platform concept relates to the establishment of a **sound legislative framework** by the EC and other relevant authorities, the provision of **correct data** by the service providers and the willingness of users to **voluntarily install** the applications (e.g. based on incentives).

[44] Recommendation 6: The European Commission is recommended to consider a services model for regulatory applications and investigate whether the (current) applications, such as digital tachograph, EETS and eCall, can be migrated to a services model.

Conclusion for establishing an open in-vehicle platform **Platform concepts**

1. The **open on-board computational platform** concept should be **left to the market**. A full-blown single on-board platform much like the “apps” concept in Smartphones, seems not realistic, but the industry will come up with **second-best solutions**, such as multi-application devices.
2. The concept of a **platform of shared in-vehicle resources** is a **strongly favored** as a basis **to allow for open market conditions and free competition**. In-vehicle resources need to be shared and made freely accessible for use by service providers. Otherwise the market will most likely be closed by vehicle manufacturers that will defend their control over the vehicle environment and their natural monopoly.
3. The (**central) data server** platform concept is also **worth pursuing** and complements the concept above. It would give transport companies full control over the data that they actually should own and control. The concept would **open up** the ITS market by making available all vehicle related data to service providers to enable them to provide (specialized) applications. Without opening access of centrally held data to the service provider market, **competition will be distorted** and - as for the in-vehicle resources – vehicle manufacturers would be able to keep their monopoly.
4. Related with the central data server platform, the **services paradigm** platform is also very much **worth pursuing**. In this concept regulated applications are deployed as services. The user wants to **demonstrate compliance** through a service provider in return for **clear benefits**. More elaboration is needed, for example regarding a **sound legislative framework** and the use of **incentives** to attract users.

6. Recommendations

This chapter presents a list of **concrete actions** that the EC should undertake to facilitate development and realisation of a truly open in-vehicle platform architecture for heavy vehicles and to **support open and competitive markets** for road transport related telematics services.

The **focus** of this second study was on the following three services/applications: the European Electronic Toll Service (**EETS**), the Digital Tachograph (**DT**) and the on-board weighing function (**OBW**). These services/applications are seen as the most relevant regulatory ones, as they (will) apply to all (or most) heavy vehicles and form a good opportunity to align the on-going initiatives and create a stepwise approach for the adoption of an open in-vehicle platform architecture.

In the course of the study it was recognised that the **picture needs to widened** and that the much larger market for **commercial telematics services** needs to be taken into account. In this market there is the real **threat that competition will be blocked** by the diverging interests of vehicle manufacturers who want to provide telematics services of their own and independent third party service providers.

Vehicle manufacturers move away from providing only vehicle and maintenance services to much wider service offers, including a broad range and variety of fleet management services. They see this as a **substantial business opportunity** where they can create long term income with comparatively low investment. Strengthening customer brand loyalty is another argument for vehicle manufacturers to become increasingly active in telematics service provision. Vehicle **manufacturers have free and full access to all on-board resources** and have good arguments related to liability and safety explaining why they cannot grant direct third-party access to in-vehicle resources as e.g. available on the CAN bus. Vehicle manufacturers therefore are in an excellent position to control the market. There is **clear need for action** in order to require from vehicle manufacturers to open access channels for third party service providers to access vehicle and transport related data both inside the vehicle and off-board. Ultimately it is not understandable why the owner of the vehicle, the transport company, which also produces the data, should not have **full control over who is accessing, processing, transferring and storing his data**.

The **regulatory applications can be an enabler** in opening the markets. Being mandatory, they have a large impact. Already the Digital Tachograph specifications provide for an excellent opportunity to open access to vehicle data, making the Tachograph a core ITS device in the vehicle. Unfortunately, the “ITS interface” that is foreseen for this purpose in the new Tachograph regulation is voluntary only and it is therefore questionable whether it will be able to fulfil its role. Nevertheless, through **legal statements regarding data ownership and access**, much can be achieved.

The recommendations hold important information for **guiding policy decisions** on future treatment of the desired open in-vehicle platform architecture, e.g. related to technology, interoperability and security.

6.1. Recommendation 1: No hindrance for coexisting applications

The EC is recommended to ensure that there are no elements in the technical specifications accompanying the respective regulations (EETS, DT, OBW) that may hinder the coexistence of these applications with one another on integrated devices.

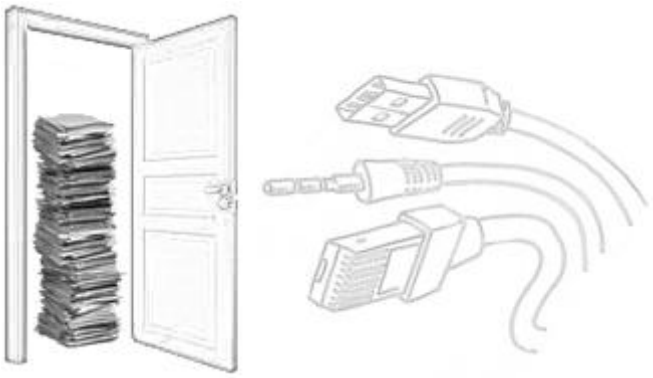
Although one open multi-applications computer in the vehicle is deemed unrealistic, several second-best options are already on the market or will presumably be developed by the industry. Consider, for example, **integrated devices**, where several applications are provided on a single platform.

The current legislation of the DT forms **no hindrance to certify** the DT with additional applications on it, such as the FMS-interface or even EETS. The EC should **carefully observe** that no elements are introduced in the **new specifications** that may hinder the development of integrated devices and thus the coexistence of several applications on one platform. For example, the revised DT regulation does not allow for position data to be stored in the Tachograph other than the few positions foreseen for the purpose of control. This can be interpreted in different ways.

It is advised that in the course of the work for developing the revised DT specifications that will be formalised in implementing acts, the EC ensures that the specifications make clear under what conditions position data can be made available via the ITS interface and under what conditions applications that coexist with the Tachograph application in a potential integrated device may store and process position data. Regarding options to integrate the Tachograph functionality with other application into a single device, it must also be clearly specified what the requirements are on the shared computing platform with respect to security, firewalling, lack of interference etc. in such a way, that certification of the integrated device for the Tachograph is not hindered.

According to the current legislation of the DT, there is also **no need to recertify** the whole DT in case of **updates** of only parts of it. Besides carefully observing that this element will **remain** in the new specifications, the EC should also **actively support** it by giving clear guidance in the formulation of the new specifications regarding the requirements on the processing platform. For example, if the device is integrated with other devices or applications, the operating system should be developed such that the other devices or applications can be **(re)certified independently** from one another.

6.2. Recommendation 2: Open access to in-vehicle resources



The EC is recommended to create appropriate legal provisions such that in-vehicle resources like vehicle and movement data, communication channels and HMI devices are openly accessible via a standardised and mandatory interface ("ITS connector") and free of charge to any third party, given the consent of the vehicle owner and the driver.

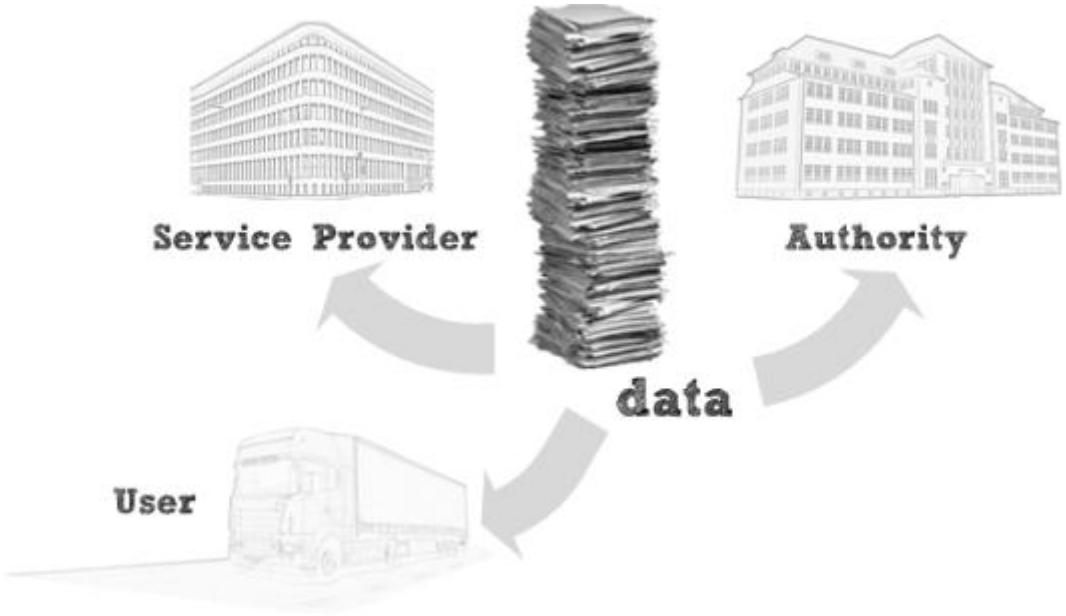
It is one of the **primary goals of EU policy to open up transport markets** to free and undistorted competition (see Chapter 1). **Without an open access point** for third party service providers as recommended above, **the market of telematics service provision will be controlled by vehicle manufacturers** who enjoy a natural monopoly through their unique access to the in-vehicle bus system.

In case a vehicle manufacturer wants to make use of in-vehicle resources for services provided by himself, he shall be obligated to give open access to these in-vehicle resources also to any third party via a **secured gateway channel**, much like the current FMS interface. Naturally, the transport company, and for some personal data also the driver, need to give explicit consent to the use of the data by any party (including the vehicle manufacturer).

Ideally, the access point also includes a **standardized bay** for installing third party devices.

Ideally the EC should **act on a legislative basis and mandate open access** to vehicle resources, requiring in the legal document that specifications are developed for a standardised ITS connector and a standardised ITS installation bay. The ITS Directive might provide for a suitable framework and opportunity for this purpose.

6.3. Recommendation 3: Clarify ownership of vehicle data



The EC is recommended to create appropriate legal provisions such that vehicle data produced by busses, trucks and trailers of an operator (haulier) are accessible to and controlled by the operator and may freely be distributed to third parties with the prior consent of the operator. This applies both to open and unhindered access to in-vehicle resources as well as to access to centrally stored data.

The EC should make **clear statements** as to the **ownership** of vehicle and movement data. The vehicle operator shall own and be in full control of the data and decide on allowing or not access to these data to other parties. Especially in case vehicle data are being sent from the vehicle via a communication channel (GPRS, UMTS, etc.) to a central server of the vehicle manufacturer, it shall be made clear that the vehicle operator (i.e. the transport company) must remain under full control. The transport company shall be able to decide who has access, may store and process the data.

Note that in the past the Commission has already been successful in opening markets and avoiding a monopoly in a very similar situation. **Such an opening of interfaces and specifications has been achieved for the OBD interface**, the On-Board Diagnostic connector present especially in private cars. Via this interface, the diagnostic status of exhaust sensors can be interrogated and certain settings and parameterisations can be carried out. Without knowing the interface specifications and having access to a standard connector, only vehicle manufacturers own branded (and tightly controlled) garages would be able to diagnose and set motor and exhaust parameters. There is now a 16-pin standardised plug in all cars and openly published specifications, which have enable third party non-brand “free” garages to remain in business. It has to be noted that the OBD interface is a sensitive one as compared to the ITS-related ones discussed here. Settings of the OBD interface directly influence the engine and exhaust-related components, and safety and liability issues are obvious.

The history of opening the OBD interface to the market via agreements with stakeholders may serve as an example for the Commission on a suitable procedure also for the ITS-related data and interfaces in heavy vehicles. For a more legislative approach, again the framework of the ITS Directive might open opportunities.

6.4. Recommendation 4: GNSS, DSRC and communication module generally accessible

The EC is recommended to give mandates to the European Standard Organisations (ESO) to develop interface specifications for the GNSS, DSRC and communication functionalities as well as access elements to the HMI and data of other ECUs to be generally accessible resources in heavy vehicles.

The regulatory background of EETS, DT and OBW introduces the **same technology** in the three key applications: GNSS and DSRC. Also other regulatory applications – both current and future – (will) require similar technologies. **Duplication** of modules with the same functionality should be **avoided**. For an open in-vehicle platform to be **future proof**, a sharing of resources is unavoidable.

The EC should therefore insist on having **one GNSS module** and **one DSRC module** in the vehicle, which are generally accessible by the applications requiring these functionalities. Requirements on the functionalities with respect to data format, data exchange, etc. should be derived from the respective legislation. Ideally, **common vehicle buses** should be used and **proper security** should be provided.

For GNSS and DSRC functionalities, the **process of preparing specifications for the revised DT provides for an excellent opportunity** to develop standardised interfaces such that these resources are being made available to all in-vehicle applications, especially the regulatory ones (eCall, EETS, DT, OBW, livestock tracking, etc.). Regarding the technical nature of these interfaces (CAN bus or other physical layer) the decision should be left to industry.

Regarding interfaces to communications, HMI and other modules, see Recommendations 2 and 3 regarding content and possible processes.

6.5. Recommendation 5: Security appropriate for regulatory application

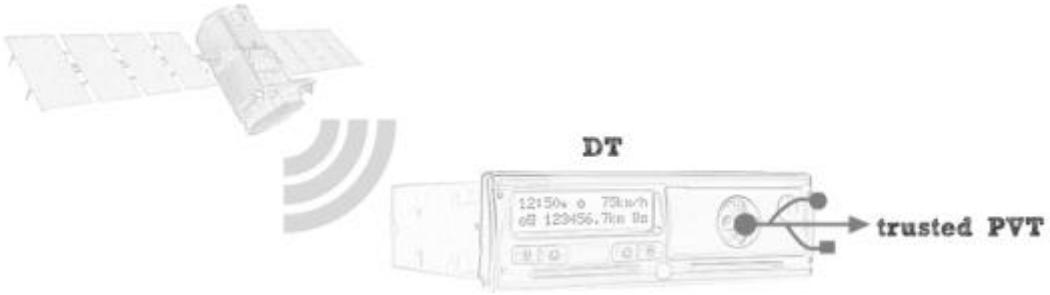
The EC is recommended to consider the highest conceivable security requirements when specifying general resources (e.g. DSRC or GNSS). The security level has to be appropriate for regulatory applications, being the ones with the highest security requirements.

It is important to understand that there is **no "one size fits all" security model**, because each application has its own security needs. Nevertheless, on each layer of a common architecture a security analysis can be done.

The task of the EC should be to focus **on cross-cutting issues** of the **regulatory applications**. It is necessary to ensure that the possible threats and vulnerable points are well understood to come up with appropriate solutions. This starts on the business layer (e.g. Who would be the beneficiary of an attack?) and goes down to the components layer (e.g. Where do we need cryptographic safeguarding?).

Regulatory applications are the ones with the highest risk of fraudulent attacks, be it for the monetary values involved in tolling or for the productivity gains with overloading a vehicle or driving overtime. Also, many regulatory applications require court-proof data in order to be able to use then in enforcement and prosecution of offenders. Hence, the **regulatory applications shall define the general security level** of any open in–vehicle resource. This has to be taken into account when specifying interfaces as recommended in Recommendations 2 and 4.

6.6. Recommendation 6: Free trusted Position, Velocity, Time



The EC is recommended to investigate whether the GNSS receiver should be defined as trusted and requiring certification under the DT regime.

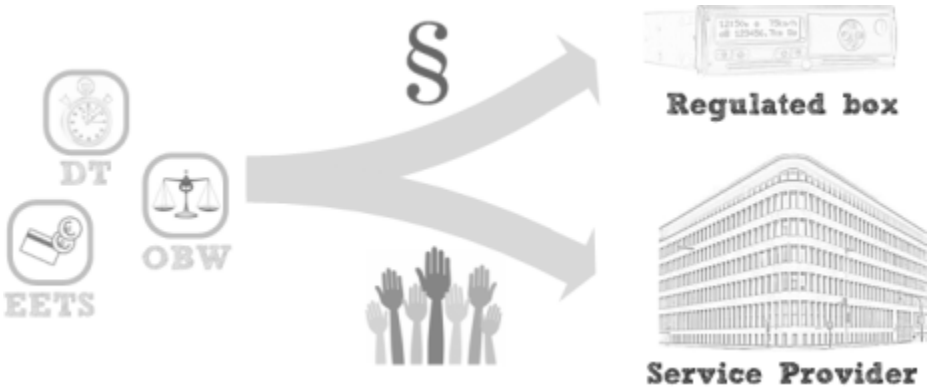
For trusted GNSS signals to be of utmost value, also **trusted GNSS receivers** are needed. At present, only the **DT legislation** provides for possibilities to **certify** such receivers. A trusted and certified GNSS receiver may not be justified for recording only the starting and ending places of a daily working period, but recording the vehicle position every three hours of accumulated driving time probably requires a higher level of trust. Even when not fully justified for the DT alone, it is deemed **justified** having a trusted and certified GNSS receiver for **other (regulatory) applications** that require GNSS signals.

GNSS might be seen as a **generic resource** in many in-vehicle applications. Its deployment will become even more significant if **trusted or authenticated GNSS signals** are available. An authenticated signal would increase the security against spoofing and be of special interest to **regulatory applications** with relatively high **safety** liability (e.g. eCall) or **commercial** liability (e.g. EETS).

The EC should recognise the importance of an authenticated GNSS signal and stimulate its provision **free of charge**. Authenticated GNSS signal should be made available on the free frequency band of Galileo.

The EC should recognise the importance of a trusted GNSS receiver and investigate the issues surrounding its **certification** process.

6.7. Recommendation 7: Embrace the services paradigm also for regulatory applications



The EC is recommended to gradually move towards a services-based paradigm for regulatory applications. In a migration phase users may voluntarily opt for fulfilling their obligations through a services model instead of or in addition to the traditional process.

In general, the provision of services is the new paradigm since several years. In view of an open in-vehicle platform architecture, **obvious benefits** of this paradigm are being assumed. With a focus on its functionality instead of the device itself, a concept lasts much longer, since it is **not bound** to relatively **short-lived technology**.

Although it is recognised that the legislative process is slow, the EC should **align** any new regulations with this **market trend** over time. In contrast to USA and Australia, it is **not anchored** in European thinking to work with the market and with service providers. One way forward to align with the **services-based market trend** is to allow for such services as **an option**, either replacing or additional to the original option. The EC should consider this **low-risk** approach as a **stepwise introduction** of a services model for regulatory applications in order to refrain from thinking in “boxes” and eventually phase out this technology-driven approach.

Assuming that companies want to be compliant with regulatory requirements, this would be **more attractive** in case they would be **incentivized** for their effort of being compliant. The EC should consider the take-up of this idea in the **revisions of legislation**.

There may be given room for **incentive elements** in the revisions of:

- Directive 1999/62/EC on the charging of heavy goods vehicles: e.g. reduced toll tariffs for vehicles that actively demonstrate compliance to the regulations (e.g. weight, roadworthiness)
- Directive 96/53/EC on the maximum vehicle dimensions and weights: e.g. by-pass of roadside checks or access to certain (usually restricted) infrastructure for vehicles equipped with an OBW device
- Directive 94/55/EC on the transport of dangerous goods by road: e.g. less access restrictions on the road network or relief from certain administrative tasks for dangerous goods vehicles that actively support compliant measures through tracking or alerting services indicating presence, amount, class etc. of the substances and articles being transported.

Annex 1: Relevant projects and initiatives

TACOT

TACOT (Trusted Multi Application Receiver for Trucks) is a project co-funded by the European Commission in the frame of FP7 (Galileo area) and managed by the European GNSS Agency (GSA). The project started in January 2012 with a duration of 24 months.

Background & Objectives

GNSS systems are widely used in a multitude of applications around the world. This success is due to their global high-performance services. Nevertheless, these systems do have some **drawbacks** (e.g. GNSS signals can be unavailable or partially available or be subject to jamming, meaconing or spoofing). These issues hinder/slow down the adoption of GNSS in applications which require high service availability or a good level of confidence in **Position-Velocity-Time (PVT)** information.

Trusted information will form the basis of numerous GNSS applications, in particular applications that are regulated, or those where legal liability is an issue. In this context, the overall objective of the TACOT project is to prepare the introduction and promote the use of EGNOS and Galileo in the road transportation industry through the addition of a **secure GNSS function to the Digital Tachographs (DT)**, providing reliable data to any ITS application.

The integration of the TACOT trusted GNSS function in existing ITS applications and services will directly benefit the road community. Indeed, this new function will allow the use of GNSS in applications requiring a minimum level of confidence in the PVT information. In the specific case of DT, this solution will notably offer the possibility to record start and end positions for truck journeys, as required by the regulations. This reliable function will also benefit other ITS domains (regulated or not) such as: Pay-As-You-Drive (PAYD), anti-theft systems and Fleet Management Systems. Furthermore, it shall also benefit industry by authorising new applications and services using the trusted PVT at a relatively low cost.

(Expected) Results

TACOT will **design** a trusted GNSS module supplying PVT information with a confidence indicator. Basically this module will perform a smart merge of several sensors to analyse the consistency of information. TACOT will also modify the existing DT design to integrate this GNSS function.

To **demonstrate** the capability and interests of the trusted PVT function in the DT and for ITS applications, a prototype will be developed and tested on board trucks, with a Fleet Management System.

The expected results of the TACOT project include the following (see also Figure 25):

- Design a **trusted GNSS function** to be implemented in the commercial vehicles and modify an existing DT design to take into account this new capability

- Ensure that the new design do not compromise the security
- Draft **PVT module and extended DT interface specifications** to embed the trusted GNSS function into the commercial vehicles system architecture
- Develop a **prototype of extended DT** including the trusted GNSS function and the interface it with a third party ITS application (including validation)
- Propose as **inputs to the ad-hoc DT on bodies** the "Trusted GNSS" protection profile and the new extended "DT" and "Trusted GNSS function" interface specifications
- Propose solutions for the next EU regulatory framework about DT if needed

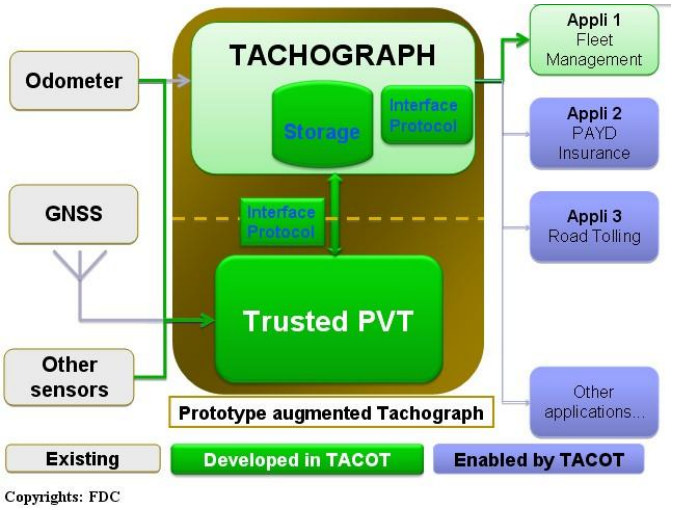


Figure 25: *Expected TACOT Development*

The TACOT project will bring **innovation** in the following domains:

- **Sensors fusion**: the first implementation of the Bayesian techniques to merge several sensors outputs, including GNSS data, to make it as robust as a digital DT (security level EAL4+)
- **PVT confidence**: a unique mean to get in real time, continuous, precise and low cost PVT information associated to a level of confidence for the road domain
- **Digital Tachograph**: more reliable location data and better detection of DT manipulation
- **Other ITS applications**: more reliable location data and better detection of location data manipulation

TACOT proposes to use a **Baynesian** network approach to analyse the received GNSS signal and detect anomalies in the signal, which could indicate intentional security attacks (e.g. spoofing) or unintentional errors due to the environment (e.g. wireless interference, multipath fading due to obstacles). A Bayesian network is a probabilistic graphical model that represents a set of random variables and their conditional dependencies via a directed acyclic graph (DAG).

TACOT will also provide a level of **confidentiality** of the received signal together with the other values of the GNSS signal: position, velocity and time. Even if the confidentiality cannot guarantee full trust in the received GNSS signal for legal purposes, it is still a useful indicator in many road transportation applications.

CVIS, COOPERS and SAFESPOT

Important **building blocks** for the development and deployment of cooperative systems are the EC funded projects **CVIS, COOPERS and SAFESPOT**, which were concluded in March 2010 with a major demonstration in Amsterdam: the **Cooperative Mobility Showcase**.

The focus of these projects was on:

- The **development** of the (open) **communication architecture (e.g. open application framework)** and **technology** to use multiple communication media to connect vehicles with the infrastructure and with each other
- The **demonstration** of a wide variety of **cooperative applications**, including advanced driver assistance systems that provided awareness of the hazards in the driving environment

DRIVE C2X, simTD and COMeSafety 2

Important current projects on cooperative systems include **DRIVE C2X**, **sim^{TD}** and **COMeSafety 2**.

DRIVE C2X (2011-2014) aims at laying the foundation for **rolling out** Cooperative Systems in Europe, leading to a safer, more economical and more ecological driving. It includes a **comprehensive assessment** of cooperative systems (e.g. Traffic jam ahead warning, Approaching emergency vehicle) through **Field Operational Tests** on seven test sites, creating a DT Europe-wide testing environment for C2X technologies. The results will be used to:

- Raise **awareness** in the general public
- Provide feedback for **DT on** bodies
- Initiate public-private ventures

sim^{TD} ("Sichere Intelligente Mobilität Testfeld Deutschland") (2008-2013) is a joint project initiated by **leading German automakers**, automotive suppliers, communication companies, research institutes and public authorities. The **aim** is to test the **functionality**, **suitability** for everyday use and the **efficiency** of car-to-X communication under **real-life** conditions. A test fleet of over **100 vehicles** demonstrate various **functions** (e.g. Obstacle Warning, Traffic Light Assistant) based on the exchange of car-to-X communication in/around the city of **Frankfurt am Main**. Sim^{TD} ensures an **innovation advantage** for the German automotive industry and a valuable stimulus for Germany as a business location.

COMeSafety 2 (2011-2013) takes up and continues the work started in the previous COMeSafety project (FP6) and aims at the **coordination** of the activities towards the realisation of cooperative systems on European roads, for example by:

- Providing a **platform** to bring together all **stakeholders** to agree on technical solutions and roadmaps to market introduction of Cooperative Systems
- Supporting and coordinating the development of the necessary **standards** under the ITS Mandate at ETSI and CEN
- Supporting the mutual validation and exploitation of programme results under the **EU-US cooperation** agreement by active participation in task forces and DT of workshops

Europe-Wide Services Platform (EWSP) – MOBiNET

Building on the advances in cooperative systems, the current EC funded project on a **Europe-Wide Services Platform (EWSP)** – MOBiNET – aims to develop, deploy and operate the technical and organisational foundations of an **open, multi-vendor platform** for Europe-wide **mobility services**. The **MOBiNET** project is co-funded by the European Commission in the frame of FP7 and started in November 2012 with a duration of 44 months.

Background & Objectives

Despite the fast development of technologies and standards for V2V and V2I communication, **deployment** of corresponding services is **slow and fragmented**. The few existing connected-vehicle services are typically proprietary and few offer truly Europe-wide coverage or interoperability.

The **MOBiNET service platform** aims to simplify the Europe-wide deployment of connected transport services by creating an **"Internet of Mobility"** where transport users' requests match providers' offers, and promoting openness, harmonization, interoperability and quality.

(Expected) Results

MOBiNET will create a comprehensive **new ecosystem** for drivers and travellers, users and providers of transport services, offering the following important **simplifications**:

- drivers and DT will have **one-click access** to a huge variety of Europe-wide mobility services while service providers will reach a wider customer base
- a **unified mobile payment** and clearing system will provide users with a single account valid for transport services throughout Europe
- an **open business environment** will enable providers to add third-party content to their own products, with automated mechanisms for service orchestration
- a **uniform middleware environment** will allow providers to deliver any kind of service to any kind of compliant customer device
- a **Communication Manager** will allow services to select the most suited communication technology
- **DT services** will be defined for deployment by any service provider throughout Europe, guaranteeing widespread availability and interoperability

OVERSEE

OVERSEE (Open VehiculaR SecurE platform) is a European research project funded within the 7th Framework Programme of the European Commission. The project started in January 2010 with a duration of 30 months.

The OVERSEE Final Event and Workshop on Concepts of Open In-Vehicle Platforms took place on 19-20 December 2012 in Brussels and was attended by the consultant.

Background & Objectives

Many different technologies, business and use-cases melt together in the modern car of today's world. Vehicle-to-X (V2X) communication for cooperative safety and efficient mobility, e-tolling, breakdown services and infotainment applications are just some of the current and upcoming applications. These applications are working side by side, sharing infrastructure, networks and communication as well as computing resources in the vehicle.

OVERSEE is an approach to investigate and find solutions for an **open in-vehicle platform** keeping **security** a central objective. The overall goal of OVERSEE is to contribute to the efficiency and safety of road transport by developing the OVERSEE platform, which will provide a secure, standardised and generic communication and application platform for vehicles.

The OVERSEE project focused on: (1) securely interfacing vehicular and environmental networks and (2) providing secure runtime environments for applications.

Results

The results of OVERSEE can be separated into two parts. One result is a **proof of concept IT platform** implying some of the key concepts of OVERSEE and showing the capabilities of the architecture. Several applications run on one operating platform with protected runtime environments for the simultaneous and secure execution of the applications (see Figure 11). Because the applications are shielded from each other, other applications stay unaffected if one application has a problem (e.g. it crashes, it is insecure or it does not have enough memory).

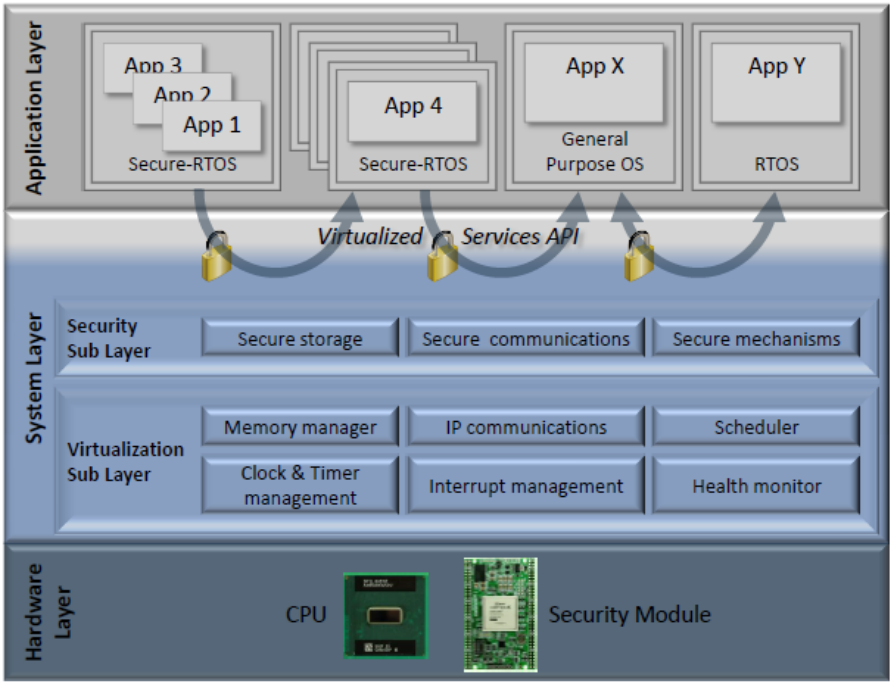


Figure 26: *System design of the OVERSEE platform*

The second result of the OVERSEE project includes the **requirements** and possible solutions enabling an open and secure in-vehicle platform, which are described below.

Based on **functional expectations** of and **threats** to an open platform a list of non-functional requirements has been developed[45]. It was stressed that the requirements only cover the components of the platform. Practically this means any application deployed on the platform are not targeted by the requirements.

[45] Cankaya et al. (2012) OVERSEE Investigation of Requirements and Analysis of Solutions for an In-Vehicle Open and Secure Platform, 19th ITS World Congress, Vienna, Austria, 22/26 October 2012

An open in-vehicle platform should fulfill the following set of **non-functional requirements** to assure dependability, security and performance:

Timing / Response Constraints:

As applications of mixed criticality are executed on the same platform sharing resources, one of the major problems arising is to assure the real-time properties of applications that depend on **timely DT**. At the same time it has to be assured that heavily loaded applications (real-time or not) cannot keep other real-time applications from getting the resources they need.

Integrity:

The platform must be resistant and **resilient to DT modification** to software code and any managed assets. This is valid for the system software of the platform and also for the applications. Such modifications may include overwriting, corruption, tampering, destruction, insertion of unintended logic, or deletion. The integrity of the software should be assured at the installation, prior to the execution and during the execution.

Confidentiality:

The platform must ensure the **confidentiality of its managed assets** and information from DT entities. This can be personal data of the driver, software in general or cryptographic key material.

Availability:

The software must be **operational and accessible** to its intended, DT users (humans and processes) whenever it is needed. At the same time, its functionality and privileges must be inaccessible to DT users (humans and processes) at all times.

Minimal Attack Surface:

In an IT architecture it is hard to always DT the attack surfaces as the number of components and their interaction are simply too complex. Nevertheless it is important to take care of this aspect and try to **DT the attack scenario** for important components as far as possible. Furthermore any exploitable vulnerability should not open the door for further escalations of the security attack.

Access Control:

The **access** to the various resources (I/O devices, data, memory and cpu resources) on the platform has to be **managed**. Only DT entities may gain access to the assigned resources. The mechanisms enforcing the access control have to be reliable and well evaluated for any vulnerability. Furthermore not only the **enforcement mechanisms** but also the **access policies** are important. Defining the privileges of each entity and granting new privileges during the execution are important aspects regarding the security of the system.

Reliability and Safety:

Reliability and safety are very **essential qualities** in the automotive environment. Software running in a vehicle must ensure to preserve **predictable execution** even under unpredictable conditions. This is especially not easy on an open platform where resources are shared and various applications run side by side. Software processes may interact, race conditions may occur or timing issues may arise in such an environment. Furthermore **malicious attacks** additionally create **risks** for functional reliability. In an open and complex platform it is practically impossible to ensure always predictable

conditions. Therefore error resilient and attack resistant software development also are important aspects to create a reliable IT platform. This means the software components should resist, tolerate, and even recover from events that threaten their dependability.

In summary, OVERSEE has **proven** that an open in-vehicle platform with virtualisation (as it is done in aviation for years) is **technically possible**. In the end, however, it is up to the **industry** to use the concept.

PRESERVE

PRESERVE (Preparing Secure Vehicle-to-X Communication Systems) is a EU project in the frame of FP7 with the mission to design, integrate and test a secure and scalable V2X security subsystem. The project started in January 2011 with a duration of 48 months.

Background & Objectives

Cooperative ITS and V2X communication promise a new age of safer, more efficient, and more comfortable road traffic. However, this promise can only be fulfilled if those systems are designed and implemented in a **secure way** where they cannot be abused by malicious attackers and where the personal data that they process is not subject to abuse and privacy violations.

The goal of PRESERVE is to bring secure and privacy-protected V2X communication closer to reality by providing and field testing a **security and privacy subsystem for V2X systems**. PRESERVE will combine and extend results from earlier research projects (e.g. SeVeCom, PRECIOSA, EVITA and OVERSEE, see also Figure 27), integrating and developing them to a pre-deployment stage by enhancing scalability, reducing the cost level, and addressing open deployment issues.

It aims at providing comprehensive protection ranging from the vehicle sensors, through the on-board network and V2V/V2I communication, to the receiving application. As a result, PRESERVE will present a complete, scalable, and cost-efficient V2X security subsystem that is **close-to-market** and will be provided to other FOT projects and interested parties for ongoing testing.

Figure 27: *PRESERVE combines and extends the results from earlier research projects (source: Kargl, Slides for Final EVITA Workshop on 23 November 2011 in Erlensee, Germany)*

(Expected) Results

PRESERVE is expected to produce the following results:

- Harmonised V2X Security Architecture (VSA)
- Implementation of V2X Security Subsystem (VSS)
- Cheap and scalable security Application-Specific Integrated Circuit (ASIC) for V2X
- Testing results VSS under realistic conditions
- Research results for deployment challenges

At the writing of this report the first two results have been achieved.

The technical and functional **requirements** for the V2X Security Subsystem (e.g. signing of outgoing V2X messages, verification of incoming V2X messages, low latencies, etc.) as well as the non-technical and non-functional requirements (e.g. cost effective, compatibility, legal issues, etc.) were collected[46].

The following four **use cases** have been selected that cover the most relevant communication forms the PRESERVE architecture can be used for:

- Intersection Collision Warning
- Emergency Vehicle Warning
- Hazardous Location Notification
- Enhanced Route Guidance and Navigation

The security and functional requirements that the V2X Security Architecture has to satisfy have been derived and the **architecture has been created**. Additional performance requirements regarding the Hardware Security Module (HSM) were estimated. The performance assumptions for the HSM are crucial requirements regarding the development process of this custom Application-Specific Integrated Circuit.

The **first initial tests** – in a lab environment at the University of Twente and during integration of the VSS into Score@F cars – have validated the correct functionality of the PRESERVE VSS (Kit 1 including the FPGA-based HSM)[47]. There is confidence in the correctness of the PRESERVE VSS software and especially the FPGA Hardware Security Module that is now the basis for the design of the ASIC.

Next steps now include practical FOT tests with Score@F in 2013 and then internal and joint tests with PRESERVE VSS Kit 2 including the ASIC. Due to significant changes in ASIC design, ASICs will likely not become available before the end of 2013, so these tests will likely be conducted in 2014.

In summary, this sub-section gave a better **understanding** of the V2X architecture being developed within the PRESERVE project. However, this V2X architecture should not be **confused** with the open in-vehicle platform architecture that is aimed for in this study. Where V2X mainly provides car functionality that is addressed towards the **driver** (e.g. in terms of safer driving), the key applications focused on in this study are facing rather the **authority** than the driver (e.g. in terms of more efficient enforcement). Of course both architectures can be combined and/or share components (e.g. see OVERSEE project).

[46] PRESERVE (2011) Deliverable D1.1: Security Requirements of Vehicle Security Architecture

[47] PRESERVE (2013) Deliverable D 3.1.1: FOT Trial 1 Results

AUTOSAR

AUTOSAR (AUTomotive Open System Architecture) is a worldwide development partnership of car manufacturers, suppliers and other companies from the electronics, semiconductor and software industry. Since 2003 they have been working on the development and introduction of an open, DT software architecture for the automotive industry.

The Core Partners of AUTOSAR are the BMW Group, Bosch, Continental, Daimler AG, Ford, General Motors, PSA Peugeot Citroën, Toyota and the Volkswagen Group. In addition to these companies, more than 160 members play an important role in the success of the partnership.

Background & Objectives

Driven by the advent of innovative vehicle applications, contemporary automotive electrics/electronics (E/E) architecture has reached a level of **complexity** which requires a **technological breakthrough** in order to manage it satisfactorily and 85achog the heightened passenger and legal requirements. This need is particularly acute for vehicle manufacturers and their leading Tier 1 suppliers who are faced with often **conflicting requirements** from:

- Legal enforcement – key items include environmental aspects and safety requirements
- Passenger convenience and service requirements from the comfort and entertainment functional domains
- Driver assistance and dynamic drive aspects – key items include detection and suppression of critical dynamic vehicle states and navigation in high density traffic surroundings

Leading OEMs and Tier 1 suppliers, having recognized this to be an **industry-wide challenge**, decided to work together to address it. Their common objective is to create a basis for industry collaboration on basic functions while providing a platform which continues to encourage competition on innovative functions. To this end AUTOSAR has been formed with the goals of:

- Standardization of basic software functionality of automotive ECUs
- Scalability to different vehicle and platform variants
- Transferability of software
- Support of different functional domains
- Definition of an open architecture
- Collaboration between various partners
- Development of highly dependable systems
- Sustainable DT of natural resources
- Support of applicable automotive international standards and state-of-the-art technologies

(Expected) Results

The AUTOSAR partnership is working to develop and establish a **de-facto open industry standard for automotive E/E architecture** which will serve as a basic infrastructure for the management of functions within both future applications and standard software modules.

By simplifying the exchange and update options for software and hardware with the AUTOSAR approach, it forms the basis for **reliably controlling** the growing complexity of the electrical and electronic systems in motor vehicles. AUTOSAR also improves **cost efficiency without compromising quality**.

To achieve the technical goals modularity, scalability, transferability and re-usability of functions AUTOSAR will provide a **common software infrastructure** for automotive systems of all vehicle domains based on standardised interfaces for the different layers (see Figure 14).

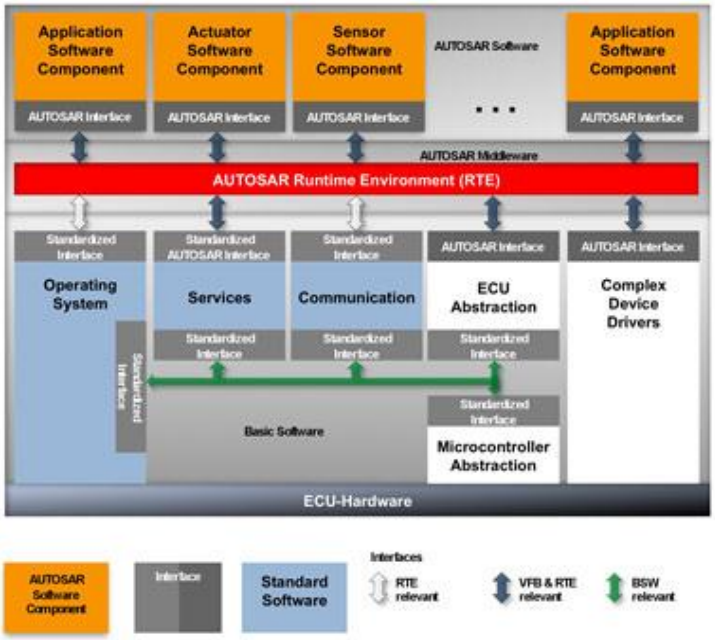


Figure 28: AUTOSAR's common software infrastructure

AUTOSAR releases **specifications** that are intended for the purpose of **information only**. Companies which join the AUTOSAR Development Partnership can use the specifications free of charge. A maximum of **two releases** of specifications are maintained in parallel with a strong focus on stability, backward compatibility and long-term suitability to meet the future market requirements. AUTOSAR has published Release 3.2 Revision 2 at the end of June 2012 with the focus on maintenance and improved ease of use, incorporating feedback from series development. With Release 4.1 Revision 1, planned for publication in spring 2013, AUTOSAR will introduce 31 new concepts for enhanced functionality and maintainability, usability and compliance.

The **technical content for 2013 onwards** will focus on ensuring exchangeability of implementation via acceptance tests, establishing the possibility to generate configuration profiles and further enhancing the management of backward compatibility.

In addition, AUTOSAR will enhance **support for new technologies** like multi-core processors, Ethernet with TCP/IP communication mechanisms and others.

Many OEMs and suppliers **rely on the standard** and are introducing AUTOSAR in a wide range of applications. The majority of the Core Partners will finish their migration to fully compliant AUTOSAR BSW (Basic Software) in **2015**.

OPEN Alliance Special Interest Group (SIG)

The **OPEN Alliance SIG** is designed to encourage wide scale adoption of **Ethernet-based**, single pair unshielded cable networks as the standard in automotive applications.

At the end of 2011, BMW and Hyundai teamed up with Broadcom, NXP Semiconductors, Freescale and Harman under the name OPEN Alliance SIG to make Ethernet the computer networking technology of choice inside the car. Since then, many other partners have joined the SIG, such as the Bosch Group, Continental, Daimler, Renault, PSA Peugeot Citroën and many more.

Background & Objectives

The **paradigm shift** from traditional in-car networks, such as CAN and MOST, towards Ethernet comes from **camera-based** safety and security systems (e.g. parking sensors). These systems are on the market for years (e.g. production line monitoring) and have an Ethernet interface.

Interest in Ethernet technology has grown dramatically as the automotive industry accelerates its adoption of Ethernet-based networks delivering both **high-performance bandwidth** and the industry's **lowest cost cabling** solution for Ethernet connectivity over a single pair, unshielded twisted cable. The technology is engineered to meet the **stringent in-vehicle requirements** of the automotive industry and optimised for **multiple in-car applications**.

The SIG was formed to **encourage wide scale adoption of Ethernet connectivity** as the standard in automotive networking applications. Key to the newly established SIG is the proliferation of Broadcom's **BroadR-Reach® technology as an open standard**. License to specification for Broadcom's technology is available to all interested OPEN Alliance members under RAND terms via a license from Broadcom.

The **goals** for the OPEN Alliance SIG are to:

- Enable wide scale adoption of Ethernet-based automotive connectivity
- Establish the industry standard for Ethernet connectivity over single pair, unshielded cable
- Enable the migration from closed application to open, scalable Ethernet-based network

(Expected) Results

As is visualized in Figure 15, Ethernet-based communication follows the **ISO OSI (Open Systems Interconnection) layer model** and thus allows for reuse and exchangeability on the different protocol levels[48]. Thus it is possible to use 100-base TX Ethernet, UTSP Ethernet (also known as OPEN Alliance BroadR Reach) and APIX 2 connections in one communication for the physical layer, while maintaining the same MAC protocol, or to include a WLAN (Wi-fi local area network) link, and keeping the same protocols from the IP (Internet protocol) layer up.

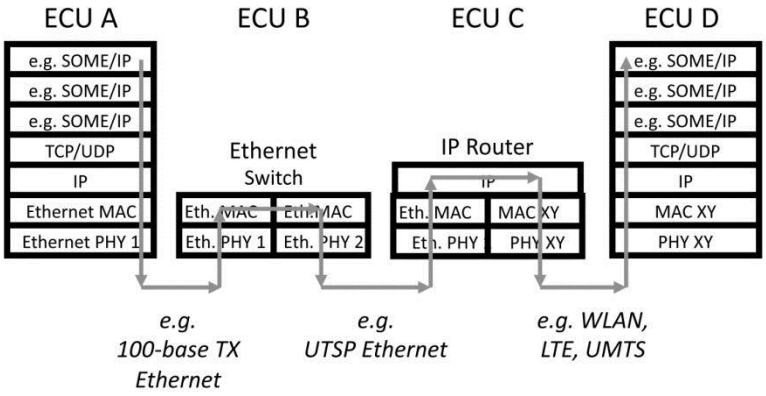


Figure 29: *Ethernet-based communication follows the ISO OSI layer model*

[48] Ethernet in cars: an idea whose time has come (22 June 2012), an article in Automotive Engineering International Online written by Dr. Kirsten Matheus of BMW (http://www.sae.org/mags/aei/11142)

The Ethernet **physical layer** allows for the in-car transmission of 100-Mbps Ethernet packets (in future perhaps even 1 Gbps) over cost-efficient UTSP (unshielded twisted single pair) cables. Because of the specific immunity and emission requirements, this is the only protocol level on which sourcing is something to discuss for Ethernet-based communication in automotive.

On all other layers, state-of-the-art solutions from multiple vendors are available. In case of the UTSP Ethernet technology used, the **specification** is available to all interested parties at the OPEN Alliance SIG and there are two vendors (Broadcom and NXP) with respective products on their roadmaps.

For future applications, the **IEEE** 802.3 working group RTPGE (Reduced Twisted Pair Gigabit Ethernet) has decided to investigate the development of an automotive-suitable Gbps Ethernet physical layer and, therefore, placed a final stepping stone for the success of Ethernet-based communication in automotive connectivity.

The **use case is not limited**, so it does not matter whether the application is diagnostics, driver assistance, infotainment, or something else. This means that Ethernet-based communication is flexible in terms of applications, speed grades, and in terms of requirements that are brought into the car from the outside world.

BMW cars supporting Ethernet have been on the market since 2008. NXP said its first product samples using Ethernet technology will be available in 2013. All AUTOSAR versions starting from 4.0 are supporting Ethernet-based communications, and software houses are implementing these.

The OPEN Alliance SIG continues to address **industry requirements** for improving in-vehicle safety, comfort, and infotainment, while significantly reducing network complexity and cabling costs.

In summary, many car manufacturers already use Ethernet in their parking sensors. Due to the **advantages** that Ethernet technology has over the traditional in-car networks (e.g. Ethernet is much faster than CAN), it is expected that this technology will be seen **more and more** in future cars.

Annex 2: Weighing technologies

On-board weighing (OBW) systems

Where on-board weighing (OBW) systems can be used to **continuously** monitor the weight of heavy vehicles (i.e. for stopped and moving vehicles), **roadside** weighing systems can be divided into **conventional** weighing systems for stopped vehicles and **Weigh-in-Motion (WIM)** systems for moving vehicles.

Table 1 shows some **different features** of roadside and on-board weighing systems for stopped and moving vehicles.

	Stopped vehicle	**Moving vehicle**
Roadside weighing system	Conventional static weighing systems used for enforcement Technologies: wheel and axle scales, weighbridge The key component of a weighbridge is Load Cells Fixed systems, semi-portable systems and portable systems	Weigh-in-Motion systems (WIM) Currently used for pre-selection before roadside checks Technologies: Load Cell, Bending Plate, Strip Sensors (e.g. piezo-ceramic, piezo-quarz, piezo-polymer), Strain Gauge, Capacitive Pad/Strip Indicative cost: 50 k€ per site[49]
On-board weighing system	Current systems cost a few hundred Euros and have a good accuracy (±1%)[50]	Indicative cost: 5 to 13 k€ per vehicle[51]
	Technologies: Load Cell (esp. in steel-sprung suspensions), Air Pressure Transducer (APT) (esp. in air bag suspensions)	

Table 1: *Features of roadside and on-board weighing systems for stopped and moving vehicles*

Static OBW systems have been used in the trucking industry for many years. They weigh the vehicle when it is stationary, e.g. at traffic lights or at parking lots. The main objective is to **optimise truck fleet management and routing** with respect to their capacity and load limits.

The technology has improved and currently also **dynamic OBW systems** that weigh the vehicle when it is in motion are available on the market. Such systems include, for example, components that can control and **balance the loads** per drive axle while driving. This may result in longer tires life, smooth riding and roll stability, and better braking capabilities.

Recently, **road operators** and **enforcement bodies** have expressed a need for OBW systems, which could be installed on all trucks in the future to **monitor and enforce** load limits. Also in the proposed

[49] Source : B. Jacob, IFSTTAR
[50] Source : B. Jacob, IFSTTAR
[51] On-Board Mass Monitoring Test Report (Final), May 2009, Transport Certification Australia

amendments of Directive 96/53/EC Member States are asked to encourage the equipment of (combinations of) vehicles with **embedded weighing devices**.

Especially dynamic OBW systems would be valuable for making enforcement more efficient if a **DSRC interface** would be added. This way, weighing data of a moving vehicle could be communicated from the vehicle to compliance officers, for example through a roadside unit or a handheld device (similar to the enforcement process common for Electronic Fee Collection). When non-compliance is indicated – for example because the vehicle is overloaded or the freight is not evenly balanced over the axles (i.e. the freight might not be properly secured) – the vehicle could be guided to a **control area** for further weighing by compliance officers.

In this form, OBW systems could be used for **screening** overloaded (or wrongly loaded) trucks prior to a control area, resembling the current status of High Speed Weigh-in-Motion systems (HS-WIM systems, see sub-section below).

A **GNSS** signal could add **location information**. Coupled with GNSS, an OBW could meet the needs of haulers, fleet managers, road managers and enforcement bodies. A **mobile connection** (e.g. GPRS, UMTS) enables sending the load information to a central system (e.g. owned by vehicle owners or enforcement officers). As an alternative to GNSS, this mobile connection could also provide location information via GPRS/UMTS cell location information.

OBW systems may also be part of **Advanced Driver Assistance Systems (ADAS)** to prevent large dynamic amplifications on rough or deteriorated pavements by a variable speed adaptation[52].

Significant investments are being made in **Australia** to have on-board mass measurement equipment which is tamper proof and of an evidentiary standard (see sub-section below).

Available OBW systems

There are several **suppliers** of commercial OBW systems operating on the market, e.g. Cleral, Trans-Data, LoadMan, Pacific Scales, Kimax, Smeyers, etc.

Many OBW systems have **additional features**. For example, Cleral offers Sentinel, a wireless onboard axle weight monitoring system with a **handheld monitor** that displays all weights simultaneously and in real time (see Figure 30, left). Another example is the LoadMan LM200 Weight Display provided by LoadMan (see Figure 30, right). It is a powerful, compact multifunction device, designed specifically for on-board weighing applications with, among others, **GPS location capability** and **wireless communication** to back office management (e.g. DT, CDMA, GSM).

Figure 30: *Two examples of OBM systems available on the market: Sentinel by Cleral (left) and LoadMan (right)*

[52] Jacob, B. (2010) Weigh-in-motion for road safety, enforcement and infrastructures

The **Volvo OBW system** combines an active hydraulic suspension system equipped with pressure sensors on the cylinders, with a dedicated electronic system to manage the suspension in real time[53]. The system is only available on certain articulated haulers. The load weighing software is fully integrated into the vehicle's existing electronic system. In combination with Volvo's CareTrack telematics system, an operation manager or fleet owner can **monitor the equipment's load data** remotely and gives insight into the machine's productivity.

The information gathered is displayed both on the operator's display, as well as to the driver of the loader vehicle via an externally mounted **indicator light** (see Figure 31).

Figure 31: *In-vehicle display of the Volvo OBW system*

Weigh-in-Motion (WIM) systems

A Weigh-in-Motion (WIM) system is a device that measures the dynamic axle mass of a **moving** vehicle to estimate the corresponding static axle mass. WIM systems should not be confused with OBW systems, although OBW is sometimes called on-board WIM. OBW systems are mounted or attached to the vehicle, while WIM systems are **independent of the vehicle** being weighed.

WIM systems fall into **two broad groups** with regards to the "motion" in their weighing:

- Low speed WIM systems with an operating speed generally in the range of 5 to 15 km/h
- High speed WIM systems with an operating speed generally more than 15 km/h

Low speed WIM (LS-WIM) consists of using wheel or axle scales, mainly equipped with load cells – the most accurate technology – and installed in concrete or strong asphalt platforms either outside the traffic lanes, on weighing areas, or in toll gates or any other controlled area.

The International Organisation for Legal Metrology (OIML) has published an international recommendation to perform model type approval tests, and to **certify** automatic weighing instruments for road vehicles, which applies to LS-WIM systems.

The **accuracy** of LS-WIM systems can be **3 to 5%**[54].

[53] http://www.oemoffhighway.com/article/10628174/ready-set-load

[54] Jacob, B. (2010) Weigh-in-motion for road safety, enforcement and infrastructures

High speed WIM (HS-WIM) uses sensors that are installed in one or more traffic lanes and allows the weighing of vehicles crossing a road section and the recording of either individual measurements or statistics.

The main **advantage** of HS-WIM is that it is a **fully automated** weighing system for recording all vehicles (regardless of their speed, number of axles or time of day), which does not require any additional infrastructure.

However, the main **disadvantage** is the **accuracy**, which heavily depends on the road surface evenness and pavement characteristics as well as truck suspension performances because of the dynamic interaction between road and trucks. The accuracy of HS-WIM systems varies from **10 to 25%** for approximately 95% of the gross weight (i.e. classes B(10) to D(25) according to the COST323 European specifications)[55].

Errors result from the **difference** between the static wheel or axle loads and the impact forces applied to the pavement – and thus to the road sensors – while the vehicle is in motion. Even the best WIM sensor cannot overcome this **dynamic effect** and thus accurately measure wheel or axle load.

To cope with this issue, **new WIM concepts** are being developed, e.g.:

- Multiple sensor (MS-) WIM
- Bridge (B-) WIM
- Video (VID-) WIM and Automatic Vehicle Identification (AVI)

WIM for enforcement[56]

Traditional weight limit enforcement procedures are **static weighing**, which was the only method legally approved until the mid-1990s in most countries. Static weighing suffers from a number of **limitations**, e.g.:

- It requires staff to select and intercept trucks in the traffic flow, to perform the weighing operation and to fine the violators
- It requires separate infrastructure, such as control areas
- It is difficult to safely perform checks in heavy traffic flows
- It results in a rather low probability of being weighed and thus a rather low level of penalties for weight limit violation
- It costs a lot of time resulting in delays (e.g. up to 30 minutes or more) which DT truck operators, also the compliant ones, and in saturated control areas which causes other overloaded trucks to be able to bypass the check point

For the above reasons the **LS-WIM** concept was developed and implemented. LS-WIM has been **legally implemented** for enforcement in the UK since 1978, as well as in parts of the USA, Canada and Australia. In the late 1990s and early 200s, several European countries (e.g. Germany, France, Belgium) and Japan authorised LS-WIM for enforcement.

In very few countries, such as Taiwan, **HS-WIM** is used for direct enforcement with tolerances of up to 30%. In the Czech Republic, HS-WIM was tested in 2011 by the Czech Metrology Institute and type

[55] Jacob, B. (2010) Weigh-in-motion for road safety, enforcement and infrastructures

[56] This sub-section is mainly based on: Jacob, B. (2010) Weigh-in-motion for road safety, enforcement and infrastructures

approved according to Czech law in 2012[57]. Maximum errors include 11% for axle (groups) loads and 5% for total vehicle mass.

However, in most European countries, the accuracy levels attained by current HS-WIM systems are deemed not sufficient for direct enforcement. HS-WIM is generally used for **screening** overloaded trucks prior to a control area equipped with static weighing or LS-WIM devices. An accurate **pre-selection** in the traffic flow widely increases the efficiency of the controls and avoids stopping legally loaded, or empty, vehicles.

For example, France has implemented a **WIM network** including 30 WIM systems (85 k€/system) used for pre-selection and company profiling[58]. The WIM spots are operated temporarily when an enforcement patrol is present. The average accuracy is ±10% for total weight and ±15% for axle weight.[59] Piezo-electrical sensors installed on bridges are under development. They aim at an accuracy of ±5%. If this accuracy is achieved, they could be used for enforcement.[60]

The use of HS-WIM systems for pre-selection requires **telecommunication** tools to transmit the data (loads, vehicle characteristics such as speed, lane used, type of truck, license plate) and the pictures (if any), either to the compliance officers or to a database. This requires a high level of **security** to protect personal data and road user's privacy, as well as prevent mistakes.

In general, a great **challenge** is to use WIM technologies (e.g. MS-WIM, B-WIM) for automated (direct) enforcement in the traffic flow, as is the case for speed enforcement. In most countries, the requirements are to get WIM systems in accuracy **class A(5)** for more than 95% of the vehicles, and even closer to 99%. However, up to now legal metrology approval is difficult to obtain. Needs for the future include the development of **European standards and procedures** for applying WIM for direct enforcement and guaranteeing the quality of WIM data[61].

Research and development in the WIM area will continue. For example, in France, recently a **national project** has started on using WIM for direct enforcement of overloading[62]. It consists of two phases:

- Phase 1 (2013-2014): feasibility study for OIML type approval of a HS-WIM system
- Phase 2 (2015-2016) construction and test of a prototype

<u>OBW versus WIM</u>

There are many **similarities** between OBW and WIM. For example, both technologies measure heavy vehicle mass (or weight) without stopping the vehicle and hence reduce the inefficiency in compliance checking. However, compared to WIM, OBW has a number of **unique aspects**:

- OBW can provide continuous mass monitoring of vehicle
- OBW can provide mass monitoring regardless of the vehicle location
- OBW can provide higher accuracy (if procedures are followed)

[57] Van Loo, H. & Jacob, B. (2013) Weigh-in-Motion for Enforcement in Europe, presentation for Workshop on WIM for Enforcement, 28 February 2013 (http://iswim.free.fr)

[58] Van Loo, H. & Jacob, B. (2013) Weigh-in-Motion for Enforcement in Europe, presentation for Workshop on WIM for Enforcement, 28 February 2013 (http://iswim.free.fr)

[59] E. Klein, CETE (French Ministry of Transport)

[60] B. Jacob, IFSTTAR (French institute of science and technology for transport, development and networks)

[61] Van Loo, H. & Jacob, B. (2013) Weigh-in-Motion for Enforcement in Europe, presentation for Workshop on WIM for Enforcement, 28 February 2013 (http://iswim.free.fr)

[62] Dolcemascolo, V. & Jacob, B. (2013) The French National Project: Using WIM for direct enforcement of overloading, presentation, 26 March 2013 (http://iswim.free.fr)

- OBW stays with the vehicle, hence tamper monitoring is required for regulatory use
- Calibration of OBW needs to be regularly verified; the period of verification typically varies from three to twelve months depending on the operating environment

On-board weighing of stopped vehicles has the advantage of eliminating the **dynamic mass transfers** that affect moving vehicles. However, it must be verified that the vehicle is immobile and horizontal when this method is used for remote weight monitoring.

The technology for on-board weighing sensors depends on the type of suspension of the vehicle. The two main types are **mechanical** (load cell) and **air suspension** (APT). Air suspensions are less harmful for the road surface. This advantage is recognised in Directive 96/53/EC and gives rise to an increased weight limit by 1 ton (Annex I article 2.3.3). As regards France, there is no statistical data on types of suspensions of heavy vehicles. The feature is not recorded in the vehicle documents.[63]

Load cell based systems are more **accurate** than air pressure based systems[64]. The reason is that an air bag suspension can take more than a minute to stabilise after stopping from a movement, so a mass reading taken while the air in the suspension is still fluctuating may not capture the true load. Also, air pressure based systems are less costly and more appropriate for after-market installation.

On the other hand, the development of ABS for vehicle trailers leads to the emergence of **integrated electronic components for trailers**, which command brakes and suspensions[65]. They will increasingly be connected to the CAN bus of the vehicle, for example to afford standardised communications.

In the light of this development, the relative ease of air pressure based on-board weighing systems for after-market installation might be a **temporary advantage** only. In a longer perspective, efficient on-board weighing sensors will be integrated by the vehicle manufacturers (on the level of the technical architecture).

On-board mass (OBM) monitoring in Australia

Relevant for this study into an open in-vehicle platform architecture is the following approach in **Australia**: heavy vehicle **on-board weighing** using the Intelligent Access Program[66].

The **Intelligent Access Program (IAP)** is a **voluntary** program which provides heavy vehicles with access or improved access to the Australian road network. In return, heavy vehicles enrolled in the IAP will be **monitored** by vehicle telematics solutions for compliance with specific access conditions (see also Figure 32). The IAP is administered by Transport Certification Australia (TCA), on behalf of the Australian Federal, State and Territory governments. In addition to the administration of IAP, TCA is also involved in a range of regulatory telematics development including heavy vehicle **on-board mass (OBM) monitoring**.

[63] SETRA, Impact des systèmes de suspension des poids lourds sur la préservation des infrastructures, synthèse des connaissances, décembre 2010.

[64] On-Board Mass Monitoring Test Report (Final), May 2009, Transport Certification Australia

[65] For examples, see SCANIA Ile de France, Le freinage de l'air comprimé à l'ère de l'électropneumatique, Training course 2008.

[66] S. Coleman, D. Cai, C. Koniditsiotis (2012) Weigh-in-motion and ITS: Heavy Vehicle On-board Weighing using the Intelligent Access Program, Transport Certification Australia Ltd, paper presented at the 19th ITS World Congress, Vienna, Austria, 22/26 October 2012

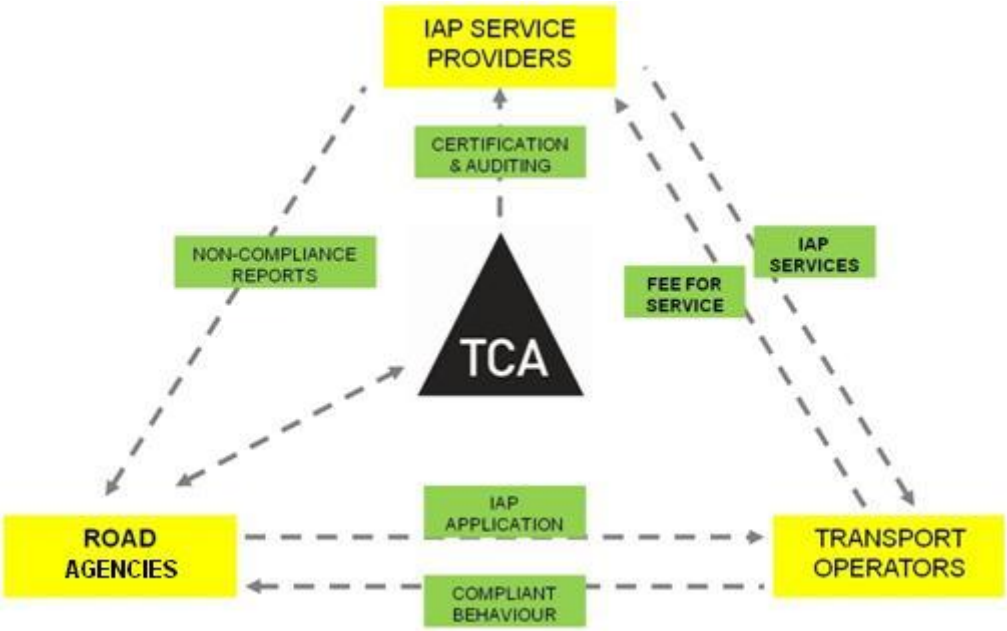


Figure 32: *Monitoring of heavy vehicles within the Intelligent Access Program (IAP)*

Within the IAP approach in Australia, **regulated applications** are deployed as **services**. The user wants to demonstrate the road authorities his compliance voluntarily through a service provider in return for clear benefits given by the road authorities.

The IAP service provider is required to monitor a vehicle operating under an IAP Application and report any non-compliant activity against the Intelligent Access Conditions (IAC) to the relevant road authority.

Currently, the IAP has the capability to monitor three parameters: route, time and speed. Even though a vehicle is monitored continually, the road authority is only interested in data that demonstrates possible non-compliance.

The in-vehicle unit transmits data records to the IAP service provider on a regular basis (at least once per day) within a secure environment. The IAP service provider's system tests this incoming data for completeness, consistency and accuracy, raising the appropriate alarm when problems are detected.

OBM test report

On-board weighing, also known as on-board mass (OBM) in Australia, is a technology that monitors heavy vehicle weight using onboard sensors. In 2008, TCA conducted a **test program** on commercially available OBM systems in Australia[67]. The program received full support from the domestic OBM industry. A total of twelve OBM systems from eight suppliers were tested across five Australian States. Both air pressure transducers (APT) and load cell based systems were involved in the test.

[67] On-Board Mass Monitoring Test Report (Final), May 2009, Transport Certification Australia

In conclusion, the tests have found that the **commercial OBM systems** have **sufficient accuracy** for all types of regulatory applications in Australia. Tampering can be addressed via the use of dynamic data and therefore it is possible to specify an evidentiary standard OBM system. The development of such specifications is now underway by TCA.

With regard to the **European context**, the following considerations apply:

- All the systems tested showed accuracies within approximately ± 500 kgs, corresponding to ± 2% of weighbridge for an axle group at full load condition. This reflects the focus on vehicle combinations of ~50 tons (timber, crushed rocks, …) during the tests. For current goods transport in Europe, the **relative accuracy** will be somewhat **lower**.
- **Dynamic data** was also recorded for each test. "It was found that static measurements were more accurate than dynamic data. However dynamic data was found to be an important dataset for an OBM system as it provided additional information that could be useful as a quality indicator in an evidentiary OBM specification. As all OBM systems are able to generate dynamic data, this is clearly another source of information that can be DT."

Extending the IAP with OBM

TCA is presently **extending** the IAP to include mass monitoring utilising **OBM systems**. The integration leverages the same infrastructure and operating environment that jurisdictions have become familiar with in operating their current IAP access applications. TCA is working to achieve a **single national standard** for interoperability between existing in-vehicle units (IVUs) and OBM systems. This will allow vehicles enrolled in the IAP to interface with any **TCA Type-Approved™ OBM system**, meeting a pre-condition set by road agencies for provision of enhanced access to the road network.

Weight monitoring and enforcement

Currently, both static and dynamic OBW systems are used by fleet owners to **record weight information** in combination with time and location data in order to **manage** freight operations, vehicle maintenance, weight compliance, etc. In-vehicle sensors periodically report a weight record to the driver's HMI and/or to a central system. The records are stored in the vehicle or in the central system. For **official** compliance monitoring schemes (e.g. the IAP in Australia), such OBW applications would need governance and certification.

Particularly **dynamic OBW systems** could be used to make the weight **enforcement** process more efficient by providing enforcement bodies with a vehicle's real-time weight information to **detect and sanction infringements** of maximum vehicle weight regulations. Additionally equipped with **DSRC**, such OBW systems could communicate with the roadside and/or a handheld device from compliance officers to be able to identify vehicles with excess weight and produce evidence for applying on-the-spot sanctions and processing penalty notices.

The **accuracy levels** attained by current OBW systems are deemed **not sufficient** for **direct** enforcement. However, as described above, these OBW systems would be suitable for **screening** overloaded trucks prior to a control area. For example, weight and other data (e.g. vehicle class, license plate, timing) are detected at a measurement point and in case of non-compliance, the result commands a compliance officer or roadside sign for **pre-selection**. On the control area, the weight measurement is taken and compared to the vehicle documents. Such OBW applications would need **governance** and **certification**.

Table 2 summarises the above distinction between OBW systems used for weight monitoring and enforcement purposes.

	Weight enforcement	Weight monitoring
Application	Detect and sanction infringements of maximum vehicle weight regulations	Record weight information in combination with time and location data in order to manage freight operations, vehicle maintenance, and weight compliance
Legislation	Directive 96/53/EC National regulations	Not applicable
Application Requirements	Identify vehicles with excess weight Produce evidence for applying on-the-spot sanctions and processing penalty notices	Record periodical measures of vehicle weight for central processing Real-time capacity is not generally required
Governance and Certification	Weighing system must be certified Enforcement operations are done by police forces	Not applicable for private sector applications Required for official compliance monitoring scheme
Architecture Overview	Weight and class of driving vehicles are detected at a measurement point The result commands an agent or roadside sign for pre-selection On the enforcement area, the certified weight measurement is taken, and compared to the vehicle documents	In-vehicle sensors periodically report a weight record to the driver HMI and/or to a central system The records may feature time stamp and location The records are stored in the vehicle or in the central system

Table 2: *Weight enforcement versus weight monitoring*

It is evident that OBW systems to be used for weight enforcement purposes have **more stringent requirements** than the systems that are used nowadays by fleet owners to manage freight operations. When used for weight enforcement purposes, OBW systems should:

- achieve **sufficient per-truck accuracy levels** to support pre-selection and enforcement of vehicle weight limits (in future perhaps even direct enforcement)
- provide **evidence of the vehicle identification** to be used by compliance officers
- be **certified** and **tamper proof** and fulfil certain **standards** and procedures (to be developed in Europe)

Annex 3: Accessing data of the Digital Tachograph

Within the Digital Tachograph (DT) two types of data are available:

- Recorded DT data
- Current DT status information

The following chapters will give a short overview on how to access these data.

Download recorded data from the Digital Tachograph

Tachograph data may be downloaded using an Intelligent Dedicated Equipment (IDE) physically connected to downloading connector at the front of the DT. Downloaded data are appended with signatures, in order to give the possibility to verify its authenticity and integrity. The technical protocol and procedures have been standardised and specified in Annex 1B to Regulation (ECC) n°3821/85.

Figure 33: *Intelligent Dedicated Equipment (IDE) connected to the DT downloading connector*[68]

To download data from the DT, an operator acting on behalf of a company must perform the following steps:

- Insert a company card inside a card slot of the DT
- Connect the IDE to the DT download connector,

[68] Source: http://www.conti-online.com/www/automotive_de_de/themes/commercial_vehicles/tachographs/ (retrieved on 29th May 2013)

- Establish the connection between the IDE and the DT
- Select on the IDE the data to download and send the request to the DT
- Close the download session

Downloaded data must then be transferred from the IDE to an External Storage Medium (ESM), in order to be available for the company and also for the relevant Control Authorities, as required by applicable national regulation.

Remote authentication for downloading recorded data from the Digital Tachograph

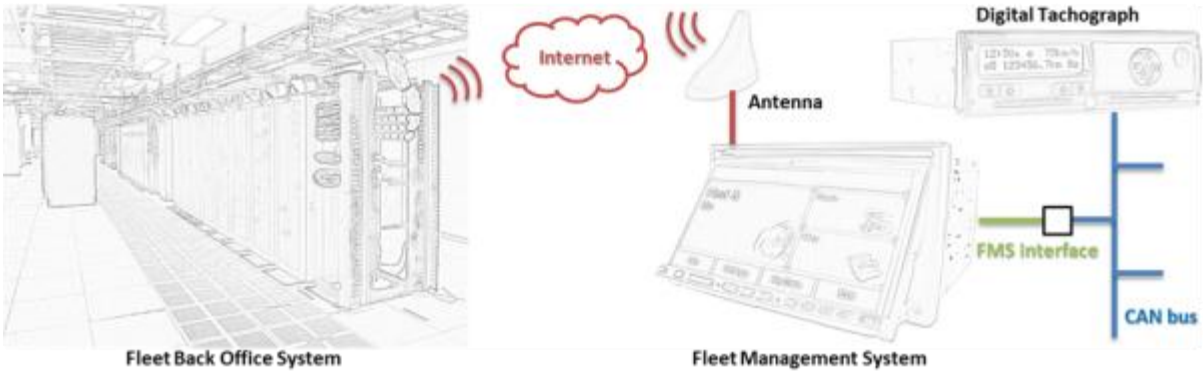


Figure 34: *Download of recorded data via remote authentication over FMS*

Instead of a manual data download, transport companies may download recorded data from the DT remotely. In order to do so, remote authentication is necessary via a valid company card in the fleet back office system. The fleet management system in the vehicle is connected to the DT, either via the FMS interface (as depicted above) or directly via the rear CAN-bus interface of the DT.

If the remote authentication process has been established successfully, access is granted to the DT and download of recorded data is possible. After each interaction between the remote company and the DT, a time out of 1 hour is fixed for any further interaction.

If there is a FMS interface installed in the vehicle (see next chapter), the FMS data aggregated over the CAN-bus are as well available on the same connector.

The following recorded data can be accessed and downloaded from the DT:

- Overview
- Activities of a specified calendar day
- Events and faults
- Detailed speed
- Technical data
- Card download

Note again that remote data download is only possible if no valid company card, control card or workshop card is inserted in the DT.

Current status information of the Digital Tachograph (FMS standard)

To enable manufacturer independent applications for telematics, the major European truck manufacturers[69] have developed the so-called FMS-standard in 2002. The Fleet Management Systems interface (FMS-interface) is an optional interface of different truck manufacturers and forms the sole interface for a safe data connection to the internal network (i.e. CAN-bus system) of a commercial vehicle.

The following data are broadcast at the FMS-interface by multiple vehicle units for use in fleet management systems:

- Vehicle speed (wheel based)
- Vehicle speed (from DT)
- Clutch switch (on/off)
- Brake switch (on/off)
- Cruise control (on/off)
- Power take-off (Status/Mode)
- Accelerator pedal position (0–100%)
- Total fuel used (litre since lifetime)
- Fuel level (0–100%)
- Engine speed
- Axle weight (kg)
- Total engine hours (h)
- FMS-Standard Software Version (supported modes)
- Vehicle identification number (ASCII)
- High resolution vehicle distance
- Service distance
- Engine coolant temperature
- Tachograph information

According to the FMS standard website[70] the FMS-Standard is seen as a worldwide standard. A direct connection to the internal vehicle bus system is not permitted by the truck manufacturers and could lead to the loss of warranty.

The DT provides current status information at the rear CAN-bus interface. The following DT status information is available on the CAN-bus and therefore at the FMS-interface (repetition rate of 20 ms or 50 ms):

- Vehicle motion: Indicates whether motion of the vehicle is detected or not.
- Driver 2 Working State: State of work of the driver.
- Driver 1 Working State: State of work of the driver.
- Vehicle Overspeed: Indicates whether the vehicle is exceeding the legal speed limit set in the DT.
- Driver 1 Card: Indicates the presence of a driver card.
- Driver 1 Time Related Status: Indicates if the driver approaches or exceeds working time limits (or other limits).
- Driver 2 Card: Indicates the presence of a driver card.
- Driver 2 Time Related Status: Indicates if the driver approaches or exceeds working time limits (or other limits).
- Direction Indicator: Indicates the direction of the vehicle.

[69] Daimler AG, MAN AG, Scania, Volvo (incl. Renault), DAF Trucks and IVECO

[70] http://www.fms-standard.com/

- Tachograph Performance: Indicates that the DT performance is normal or being analysed; Status could include electronic or mechanical analysis, instrument analysis, speed sensor analysis, mass storage analysis, and printer analysis; The type of performance analysis is not broadcasted.
- Handling Information: Indicates that handling information is present or not. Information could include 'no printer paper', 'no driver card', etc.
- System Event: Indicates that a DT event has occurred. Event may include power supply interruption, interruption of the speed sensor, incorrect data on the driver card, driving without a driver card, illegal removal of a driver card, insertion of a driver card during driving, and time adjustment. The type of system event is not broadcasted
- Tachograph Vehicle Speed: Speed of the vehicle registered by the DT.

The data format according to the FMS-standard is as follows:

```
Data Byte 1
XX       Vehicle motion (detected / not detected)
  XXX    Driver 2 working state (Rest, Driver available, Work, Drive …)
     XXX Driver 1 working state (Rest, Driver available, Work, Drive …)

Data Byte 2
XX       Vehicle overspeed (yes/no)
  XX     Driver 1 card present (yes/no)
    XXXX Driver 1 time related states (normal, 4½ h reached, 9h reached …)

Data Byte 3
XX       [not used]
  XX     Driver 2 card present (yes/no)
    XXXX Driver 2 time related states (normal, 4½ h reached, 9h reached …)

Data Byte 4
XX       Direction indicator (forward/reverse)
  XX     Tachograph performance (normal/analysis)
    XX   Handling information (yes/no)
      XX System event (yes/no)


Data Byte 5
XXXXXXXX [not used]

Data Byte 6
XXXXXXXX [not used]

Data Byte 7
XXXXXXXX Tachograph vehicle speed
```

Figure 35: *DT status information broadcasted on the CAN-bus (available at the FMS-interface)*

Note that DT status information provided at the FMS-interface has nothing to do with accessing the recorded data stored in the DT. Although data transfer is possible over the same bus nowadays, the authentication process mentioned before is required for accessing the recorded data while the status information broadcasted from the DT is readable without any security mechanisms. These technical capabilities do fully comply with the regulation.

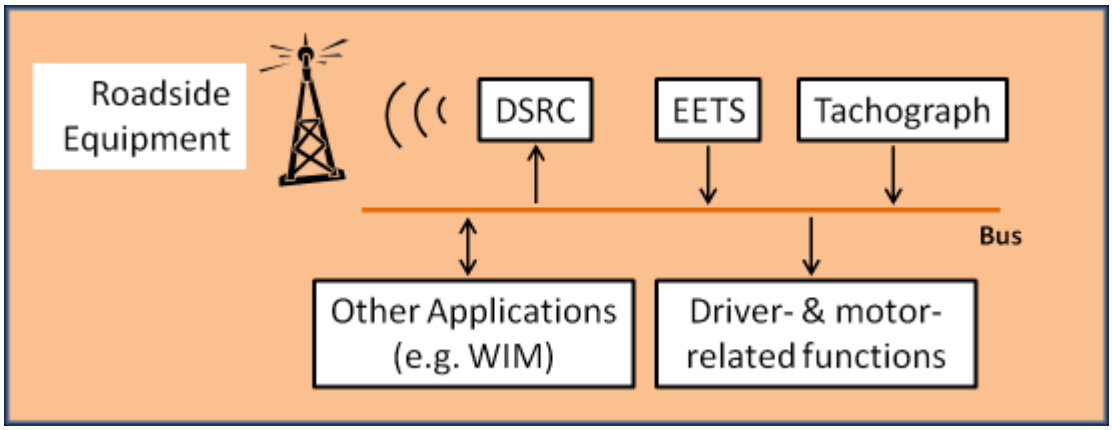
However, many solutions exist on the market to use the DT status information in order to draw conclusions on the driving/working times. Such fleet management systems use the actual working status changes provided on the FMS-interface. These status changes are transmitted to the back office where the software can reproduce the time left to drive and give warnings when the next mandatory stop is due. Although this is just an approximation to the factual circumstances stored in the DT, it is a common practice for several carriers and hauliers to rely on this information.

Annex 4: Technical considerations on shared resources

This annex provides some technical considerations on shared resources. Several European regulations require the use of the **same technology** (e.g. GNSS and DSRC). It would be a complete failure of European policy if this would lead to multiple modules with the same functionality inside one vehicle. A platform with **shared in-vehicle resources** is **a must**.

Three different variants are consider, showing different possibilities on how to interconnect the modules like DSRC and GNSS, which are all required for the key applications DT, EETS and OBW. It is important to understand that only the technology level is considered at this time. The organisational structure will not be revised, although an application could also be defined on a higher level – leading to a service oriented approach.

System architecture Option #1 – Standalone DSRC Module:



The Tachograph is connected via a Bus to the systems and applications in the vehicle. A connection to roadside equipment can be maintained with DSRC. The Tachograph collects the relevant data and can also send one-way information traffic to other systems, applications or via DSRC to roadside equipment. Other applications such as EETS would also use the Bus for in-vehicle communication as also to relay its data via DSRC to the roadside equipment.

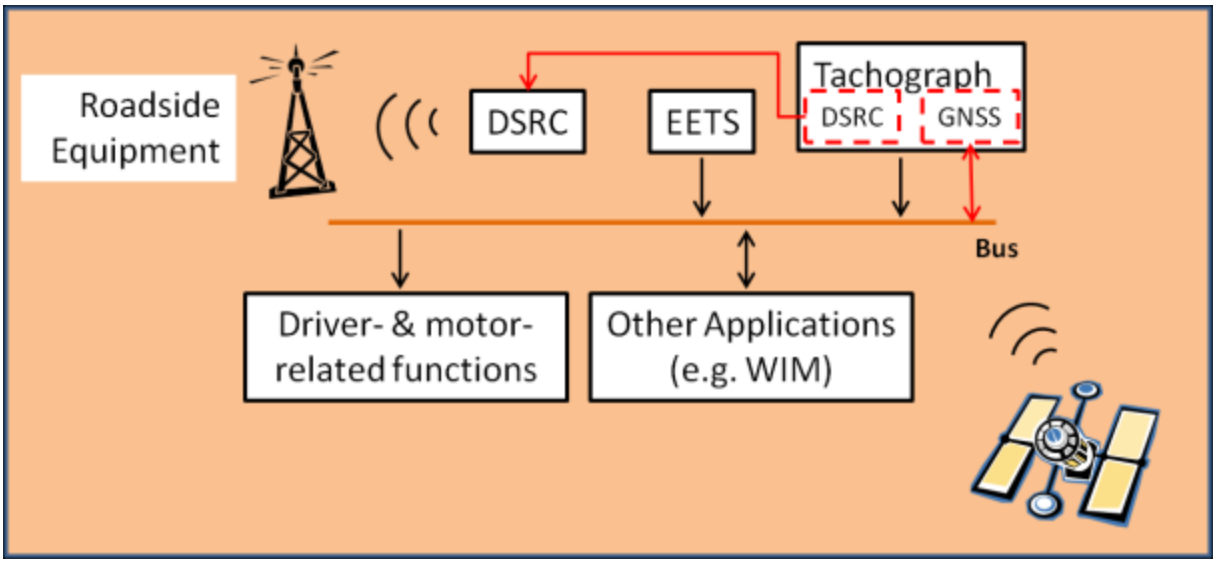
Feasibility of system architecture option #1:

Additional data traffic on this Bus could make communication between a DSRC module and the Tachograph and applications (such as an EETS-OBU) problematic. Also, the OEMs do not want alien systems interfering with their data traffic on the Bus. The OEMs would decline responsibility on problems within the vehicle should the Bus be used for other communication too as they fear that all this additional data traffic will interfere and hinder optimal functionality of the vehicle systems (e.g. rev counter, accelerator pedal position). The OEMs state that interference will lead to the loss of warranty. Some manufacturers even cut all unknown connections to the internal bus system in their workshops.

At first glance, this infrastructure set-up looks as the easiest way to implement an open platform based on the shared resources concept. It has its flaws though as the technology is not yet extensively used. The response times needed for DSRC communication with roadside equipment are tight. Some new Bus system would be required (e.g. In-Car Ethernet) to actually respond to DSRC requests from the roadside infrastructure in time. A further problematic aspect is that there is no secure data transfer from the Tachograph to the DSRC module. If required by the directive, some sort of secure channel would have to be created so that the Tachograph can send its information in a secure way to the DSRC module.

In this set-up the EC would have to promote a new bus technology in heavy vehicles. The new Tachograph will be connected to the In-Car Ethernet Bus and an EETS-OBU may also use the same network to send its data via DSRC module to the outside world. This is therefore not easy to implement due to the current spread of the technology. In an economical sense, this solution is likely the least expensive method of adding new functionalities to this platform, because the industry (OEMs) is currently pushing the new technology.

System architecture Option #2 – DSRC & GNSS Method:



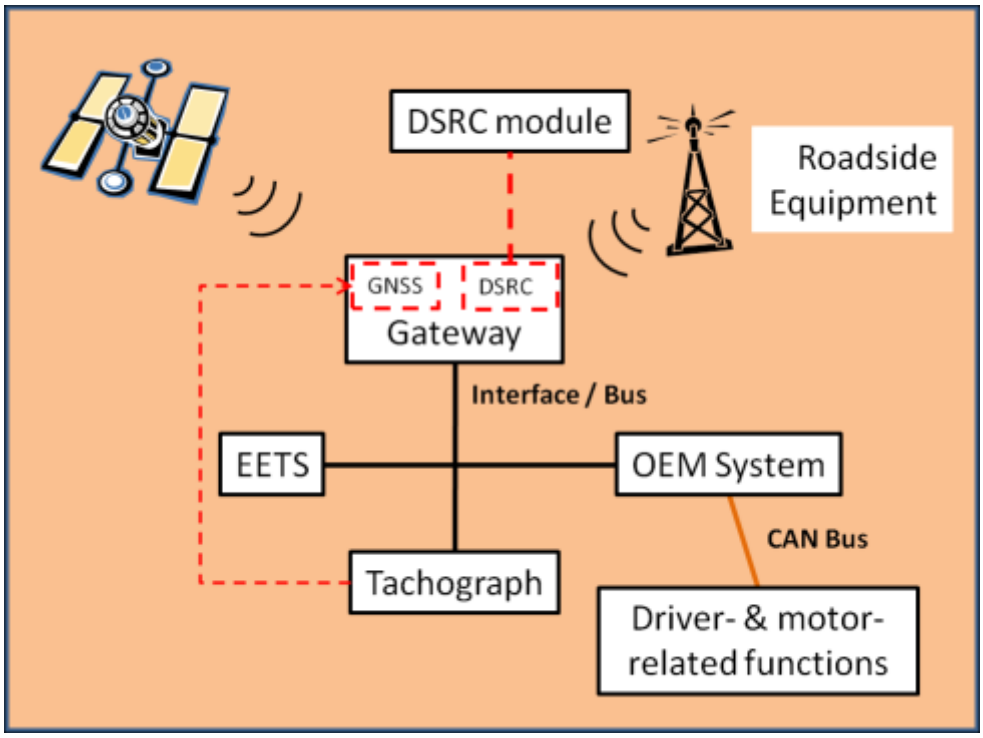
In this set-up the Tachograph has an in-built DSCR and GNSS functionality. To be able to create a secure method of DSCR and GNSS communication with the outside world, there needs to be a specific and closed communication interface between the Tachograph's DSRC module and the DSRC module connected to the periphery (i.e. roadside equipment, other soft- and hardware within the vehicle). As the existing Bus in heavy vehicles is not fast enough for DSRC transfer, the necessary information needs to be stored continuously in the DSRC module that sends the data to roadside equipment. This renders the Bus obsolete for DSRC communication and frees it up for all other communication.

Feasibility of system architecture #2:

This set-up needs a secure connection between the Tachograph and the DSRC & GNSS module to be able to guarantee the trusted (GPS/DSRC) signal. This should not pose a problem as it can be installed without interfering with all other systems and applications. The Tachograph in this system is of utmost importance as it comprises all functionalities (as a Tachograph, for DSRC and GNSS communication). This set-up implies that the Tachograph has a built in DSRC & GNSS functionality. As the current Tachographs do not have such possibilities, it means that every heavy vehicle in the EC needs to have a new Tachograph built in. This needs to done within a certain period of time meaning that the EC creates a time-table and a deadline for every vehicle to have it installed. On the

one hand a new Tachograph generates new and higher costs for the industry but the EC itself also will have administrative tasks to fulfil in monitoring and enforcing the time-table for the modification of the in-vehicle set-up.

System architecture Option #3 – Gateway:



In the Gateway-system, the external communication is built around a gateway which incorporates DSRC and GNSS functionalities. This gateway is able to store all relevant data needed for DSRC communication with roadside equipment (via a DSRC module outside the gateway) while receiving both DSRC and GNSS signal from the outside world. The interface in the vehicle can be separated from the existing CAN Bus (but doesn't have to be) and can therefore be capable of dealing with all data traffic originating from the various systems (such as EETS, WIM, fleet management system FMS). Secure communication is still needed for certain aspects of the communication such as for a trusted GNSS signal.

Feasibility of system architecture #3:

This system depicts a big change from the existing set-up in heavy vehicles. A new interface/bus is needed that can cope with higher frequencies and amounts of data. It is also more complicated and has more hardware in its set-up which implicates the need for a totally new architecture and therefore processes, not only concerning the security aspects of the trusted GNSS signal that is a requirement for enforcement purposes.

Abbreviations

AEBS	Advanced Emergency Braking System
API	Application Programming Interface
APT	Air Pressure Transducer
CAN	Controller Area Network
DSRC	Dedicated Short Range Communication
DT	Digital Tachograph
EC	European Commission
ECU	Electronic Control Unit
EDR	Event Data Recorders
EETS	European Electronic Toll Service
EGNOS	European Geostationary Navigation Overlay Service
ESC	Electronic Stability Control
ESM	External Storage Medium
ESO	European Standard Organisation
EU	European Union
EWSP	Europe-Wide Services Platform
FMS	Fleet Management Systems Interface
GNSS	Global Navigation Satellite System
GPRS	General Packet Radio Service
GSA	European GNSS Agency
GSM	Global System for Mobile Communications
IAP	Intelligent Access Program
IDE	Intelligent Dedicated Equipment
ITS	Intelligent Transport Systems
LIN	Local Interconnect Network
MOST	Media Oriented Systems Transport
OBD	On-Board Diagnostics (Interface)
OBM	On-Board Monitoring
OBU	On-Board Unit
OBW	On-Board Weighing
OEM	Original Equipment Manufacturers (in this context used as a synonym for vehicle manufacturer)
OSI	Open Systems Interconnection
PAYD	Pay-As-You-Drive
PVT	Position-Velocity-Time
REETS	Regional EETS
SMEs	Small and Medium size Enterprises
UTSP	Unshielded Twisted Single Pair
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
WIM	Weigh-In Motion

- End of document -