AFCAR
Alliance for the Freedom of CAR Repair in the EU

C-ITS WG 6 Task Force 1 – AFCAR[i] alternative proposal V.01

In-vehicle interoperable, standardized, secure and open-access platform of shared in-vehicle resources

16th June 2016

Background

The purpose of the C-ITS forum is to reach a common vision on fair and equal access to in-vehicle resources and data. Independently of the model/solution retained to give access to in-vehicle data and resources, the main objective should be to allow customers the freedom to choose which service they desire, that meets their specific needs. This goes through an open and undistorted competition for the provision of these services.

This objective is backed by the recent adoption of the eCall type-approval Regulation ((EU) 2015/758), with the provision that the Commission shall assess the need of requirements for an interoperable, standardised, secure and open-access platform no later than two years after the entry into force of this eCall Regulation.

Goals:

a) Define in-vehicle platform functional requirements
b) Define standardized API requirements
c) Define standardized minimum set of security measures

Steps (proposed by DG Move):

d) Building blocks of the solution (e.g. security, physical mounting and organisational issues etc.)
e) Impact of the type of access (only access to data, access to data + other resources e.g. HMI or communication channels) on these building blocks
f) Elements of the solution already available
g) Gaps to be fulfilled (e.g. standardisation)
h) Timeline to make the solution feasible

Prepared by:

Neil Pattemore – AFCAR Secretariat

Alternative proposal

The existing C-ITS WG6 TF1 proposal describes the building blocks and requirements from the vehicle manufacturers' perspective of the roadmap for implementing an in-vehicle interoperable, open-access platform, but this proposes a timeline of approximately 25 years.

This seems unjustifiably long and does not sufficiently consider what elements already exist, or could be developed in a shorter timescale (i.e. in parallel) to reduce the timeframe of the roadmap.

Therefore, this document describes an alternative to the current TF1 document based on existing telematics system designs, technologies and security requirements, together with the additional interim solution requirements until a final in-vehicle interoperable, standardised, secure and open-access platform can be fully implemented. This is considered both possible and desirable for the benefit of all stakeholders.

Existing C-ITS WG6 TF1 document

The existing TF1 document proposes a 'bottom up' development strategy, with the subsequent long development period.

The existing C-ITS WG6 TF1 has depicted the open platform as being the natural, but unfortunately very long term development consisting of a long series of standardization steps that have be taken sequentially. As a result, the appearance of a fully-fledged open in-vehicle platform is not foreseen earlier than some 25 years from now. The prior steps that are seen as starting points in the sequence of standardization efforts by this existing TF1 document are:

- **OBD+:**
  A secured and enhanced OBD port with a new supervising gatekeeper software. The OBD+ is a mandated port (connector) to the vehicle, or an in-vehicle standardised hardware interface. Alternative service providers would be able to physically connect devices to the connector for the exchange of in-vehicle data. Rational behind it: 3rd party service providers would have access to real-time in-vehicle data, functionalities & ECUs, and so be able to develop custom/telematics based services. This 'OBD+' standardised connector would allow diagnostic/telematics hardware to be plugged into the vehicle, allowing retrofit solutions. A unified/standardised hardware interface would allow the same access to real-time in-vehicle data and ECUs. Safety is ensured by the VM implemented Unified Port Security Layer as well as tests of the application prior to release. An expanded OBD (OBD+) is needed for reasons of latency and data volume. Applications could be able to function independently of the vehicle's wireless connection, as they would use their own communication systems connected to the standardised OBD+ connector.

- **OBD+ and a communication control unit (CCU)**
  To be able to deploy software to the vehicle through the functionality of the CCU.

- **OBD+, CCU with an Application Programming Interface (API)**
  To be able to host applications in the car, although a display to the driver as well as a method of safe & secure handling via in-car controls are not explicitly mentioned.

Overall, this does not appear to be the right way to develop an in-vehicle open-access platform, because with the current TF1 proposal, the standardization starts from an access point (OBD+) that was never designed to handle the current amount of data requests in the field of telematics and lacks even the very basic security features: i.e. the physical OBD-port from the 1980s

However, the existing TF1 proposal states that only after all of this, the final, full solution of an in-vehicle open-access platform is deemed to be feasible. Overall, this approach can rightfully be classified as a bottom-up-approach from an IT-architecture perspective.

……

Alternative proposal - details

A best practice as well as a state-of-the-art approach would be to start 'top down'.
This means, as the development of this in-vehicle open-access platform is the key objective, the focus should be on how this can be developed and implemented in the shortest timescale to provide the widest benefits to all stakeholders.

To start the development at least the following key elements shall be answered to define the overall functionality of an open in-vehicle platform:

1. Define the services/operations that need to be supported for the car/driver/owner.
2. Define the communication requirements. (e. g. which computing capacity needs to be installed inside the car to allow a client-side computation in the case of an absent server, which bandwidth is needed to transfer the data to and from the car via future mobile networks)
3. Define the access conditions for the different applications or actors.
4. Ensure that the service is presented to the car driver in a safe and secure way to avoid any driver distraction.
5. Ensure the integrity of the in-vehicle as well as the vehicle/server communication.
6. Ensure non-monitoring of the data exchange of in-vehicle data/information with 3rd party service providers.
7. Ensure that the vehicle owner/driver has the ability to review and select any service providers via the in-vehicle HMI.

Existing VM and other technical solutions

Some of the VM existing telematics systems are already designed in such a way that new applications can be uploaded and implemented without compromising security and safety requirements.

This is achieved through the fundamental design of the in-vehicle telematics platform which is designed in a way that it isolates applications into 'silos' and then verifies the application before it is run, whilst continuing to monitor the application while it is running and if required, is capable of blocking the application if it is deemed to be malicious. This is achieved through a combination of design criteria which includes a 'hypervisor' to control the verification, security credentials, run-time scheduling and implementation of the applications, as well as the control to all external interfaces. It is also possible to go a stage further and quarantine or even delete the rogue application, or re-set the telematics platform if it is ever compromised.

Current manufacturers support such functionalities:

Mercedes ME or BMW ConnectedDrive:

Control of applications via in-car-displays and controls, applications coded especially for this architecture (e.g. facebook connectivity for BMW with limited functionality). In depth monitoring of in-vehicle data, exclusive transfer to OEM-server

PSA:

The PSA-platform that allows the coding of applications for third parties as long as they conform to the API and SDK-guidelines of the PSA-Operating System and Operating Model. (This Android based solution had only a small target base and thus attracted very few applications)

Google Android Auto and/or Apple car play:

Some OEMS have already opted to install one of the two mobile operating systems in their car, GM has scheduled (and others are developing this too) a solution where the user can switch between the Apple and the Google solution, so that in fact at least three Sandboxes are residing within the car's head unit: the OEM's operating system and the solutions for the mobile platforms. Customers can choose which applications to download, which may include the vehicle manufacturer's permission to provide access to in-vehicle controls like speakers or climate controls. The technical details and security of each of these "Smartphone on wheels" solutions have successfully been demonstrated and depicted within the European Oversee-project, with a special focus of the so called Hypervisor-layer, where communication and access to the in-car ECUs by the Telematics control unit within the headunit is supervised and controlled to ensure a safe and secure operation of the moving vehicle.

Oversee Project:

The OVERSEE project report clearly demonstrates that it is possible to implement such an in-vehicle design and that by using this concept, the objectives of the C-ITS forum can be achieved.

This project showed that many of the technical requirements of an in-vehicle 'interoperable, standardised, secure and open-access platform' already exist and that a long development period is not necessary.

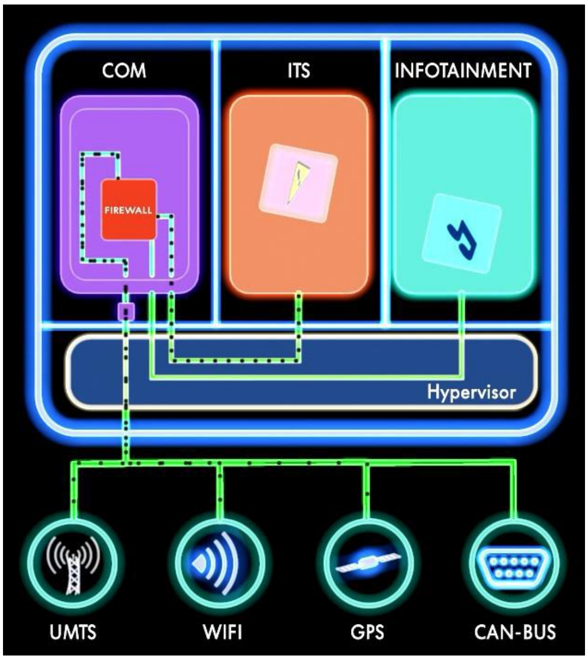


Figure 1: OVERSEE project design proposal

The OVERSEE project used an 'XtratuM' hypervisor:
XtratuM is a hypervisor specially designed for real-time embedded systems.

It is important to note that a hypervisor is an "enabling" technology, rather than a technology to solve problems. The hypervisor provides a framework to run several operating systems (or real-time executives) in a robust partitioned environment - the XtratuM hypervisor can be used to build partitioned systems.

Building blocks and requirements for an in-vehicle open-access platform

Therefore the in-vehicle OBD+ port should be developed as part of a bi-lateral development for the in-vehicle open-access platform:

Element 1: Enhanced OBD+-Port:
Can be used in the future for high speed reprogramming/flashing in the workshops of OEMS as well as Aftermarket workshops. See TF2 proposal for further details.
Timeframe: Start now

Element 2: Data (shared) server platform:
Will be used as an interim solution to provide access to in-vehicle data/information/resources and allow the vehicle owner/driver to review and select any service providers via the in-vehicle HMI.
See AFCAR TF3 proposal (16th March 2015) for further details.
Timeframe: Start now

Element 3: In-vehicle open-access platform:
Will be used in the future to install applications in the car from 3rd party service providers as well as OEM Apps.
Timeframe: Start now

Element 4: Security strategy:
Parrallel development of the security requirements for both the OBD+ port and in-vehicle open-access platform.
See also the security proposal from TF2.
Timeframe: Start now

Interim solution

However, as the development and implementation of the in-vehicle open-access platform will still take some time, an interim solution is needed to maintain equal access to in-vehicle data, information and resources. This interim solution is based on the combined in-vehicle connector (WG6 TF2 proposal) as well as equal access of the in-vehicle data via a server (WG6 TF3 – AFCAR proposal 16th March 2015). These interim solutions shall not unnecessarily delay the development of the in-vehicle open-access platform, but should be developed in parallel.

Independently and directly in parallel of any plug-in device solution (WG6 TF2), the data access must also be equally available on a server:

Shared server

A 'shared server' model is where the vehicle data and information is sent wirelessly to a server using the vehicle manufacturer's existing communication procedures. This server is controlled by a stakeholder consortium, including the vehicle manufacturer and independent operators, but is run by a mutually acceptable and independent third party (e.g. IBM or SAP). Equal access to in-vehicle data is ensured for both the vehicle manufacturer and 3rd party service providers.

……………………………………

In-vehicle open-access platform:

Operational aspects

The downloading and implementation of 3rd party applications would only be possible via an agreed 'App Store' and could only be implemented in a vehicle if they had met the acceptance and access conditions.
These 3rd party applications would be selected by the driver using the in-vehicle HMI before being implemented in the vehicle and would support the ability to directly exchange in-vehicle data with an independently operated remote server, without this being monitored by the vehicle manufacturer and independently of any agreement that the driver may have with the VM for telematics services.

Security

Consultation should be encouraged between the automotive industry stakeholders for which automotive cyber security* is an issue, together with those professional bodies and associations in non-automotive sectors that are already engaged in cyber security awareness building.

A ‘working party’ or ‘consultative committee’ should be established to explore the feasibility of initiating briefings between a range of parties with a declared interest in automotive cyber security. Specifically, it should discuss the development of code-of-practice guidelines/reference model that address the systems engineering, accessibility, security, privacy, legal and ethical issues associated with the increasing autonomy of vehicles.

The communication between the vehicle and the CCU (in-vehicle communication control unit) respectively and the backend must be secured in terms of confidentiality, integrity and authenticity.

**Cyber security includes ‘cyber physical’ that relates to capabilities such as automated braking, steering or parking sensors that could be controlled using wireless commands.*
A car's wireless 'attack surface' includes the range of features that could be hacked, including Bluetooth, Wi-Fi, mobile network connections, key fobs, or tyre pressure monitoring systems.
The ‘network architecture’ includes how much access these features give to the vehicle’s critical systems, such as the steering or brakes.

Conclusion and Roadmap

All these existing VM and other technical solutions share some characteristics:

1. Safe selection and implementation of applications using in-vehicle controls and displays.
2. One or more parallel operating systems (e.g. Google, Apple, Linux..) alongside the OEM specific system
3. Applications for the car have to follow certain design and technical guidelines to avoid driver distraction and to ensure the integrity of the in-vehicle and vehicle-server communication
4. A supervising layer (e.g. Hypervisor) shields the in-car ECUs from potential attacks (e.g. a denial of service attack that consumes too much Can-bus-bandwith)
5. Security solutions are developed either in parallel or as a single solution to protect all communication to and from the vehicle.
6. Apps are deployed via an App store and have to pass acceptance tests prior to their installation into the vehicle
7. There is no way foreseen to install Apps directly into the vehicle and therefore circumventing the App store access controls.

Summary:

In all these approaches the design and configuration of the in-vehicle-networks, as well as the surrounding infrastructure, are designed to ensure safe and secure access to real-time in-vehicle data on an equal basis for 3rd party service providers.

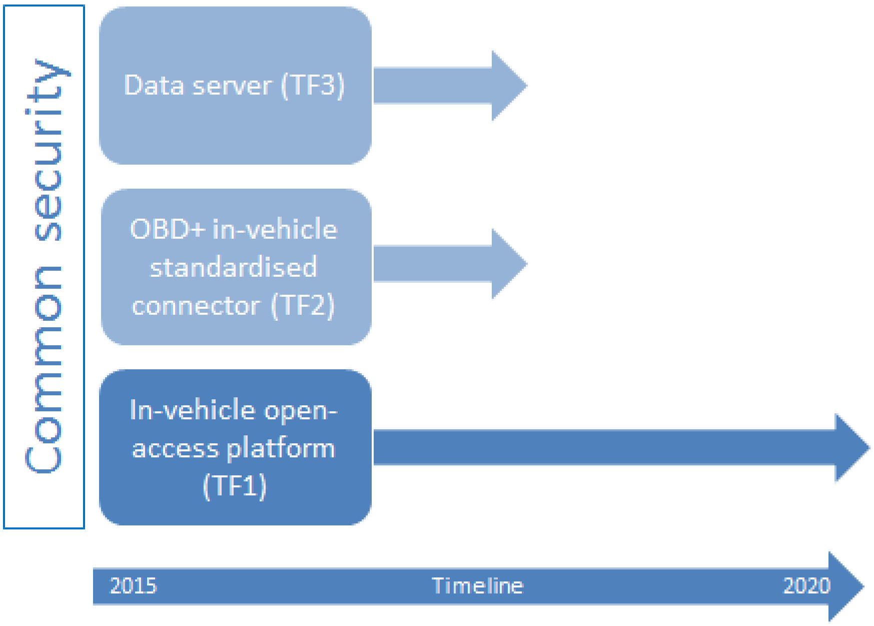
This can be achieved more quickly and effectively by utilizing existing telematics system designs and working with the wider field of security experts to develop both the in-vehicle open-access platform and the standardized OBD connector to provide access to real time in-vehicle data/information or the V2V/V2X communication exchange. This security solution should be developed either in parallel or as a single solution to protect all communication to and from the vehicle

This is a much more natural approach to developing an in-vehicle open-access platform than trying to retrofit and enhance telematics functionality through the (already too narrow and too open) OBD-port. This alternative proposal will support a double communication line:

- Exchanging in-vehicle data/information through the embedded telematics route, controlled via the in-vehicle controls and displays.
- A standardized OBD-port supporting plug-in devices to access in-vehicle data.

The revised timeline therefore reflects the development of the interim solutions, together with the in-vehicle, interoperable, standardized, secure and open-access platform as parallel developments using existing or more easily developed solutions, thereby reducing the total time needed to a more realistic 5 to 10 years.

Roadmap:


Common security
Data server (TF3)
OBD+ in-vehicle standardised connector (TF2)
In-vehicle open-access platform (TF1)
2015
Timeline
2020

---

[i] **A**lliance for the **F**reedom of **Car** Repair in the EU**.** Created in 1997, AFCAR is an alliance of the independent European associations with the **aim** is to promote fair competition in the market for vehicle servicing and repair to ensure the freedom of choice for 260 million motoring consumers in the EU. **Members of AFCAR are**: AIRC (Association International Réparateurs en Carrosserie), CECRA (European Council for Motor Trades and Repair), EGEA (European Garage Equipment Association), FIA (Fédération Internationale de l'Automobile) and FIGIEFA (International Federation of Automotive Aftermarket Distributors).