EGEA Report on WG 2 Activities

EGEA General Assembly, 17th October 2012, Amsterdam



Content



Vehicle Telematics

Technical findings and common way forward

- Access to OBD, Repair and Maintenance Information for Electric Vehicles & Hybrid Electric Vehicles Presentation of key points of interest
- Impact of the MVEG meeting on 17th September 2012 organised by the European Commission where vehicle manufacturers proposed a 'round-up' solution (for SCR additive monitoring, odometer fraudulent manipulation and vehicle theft) via an electronic certificate for tool manufacturers.



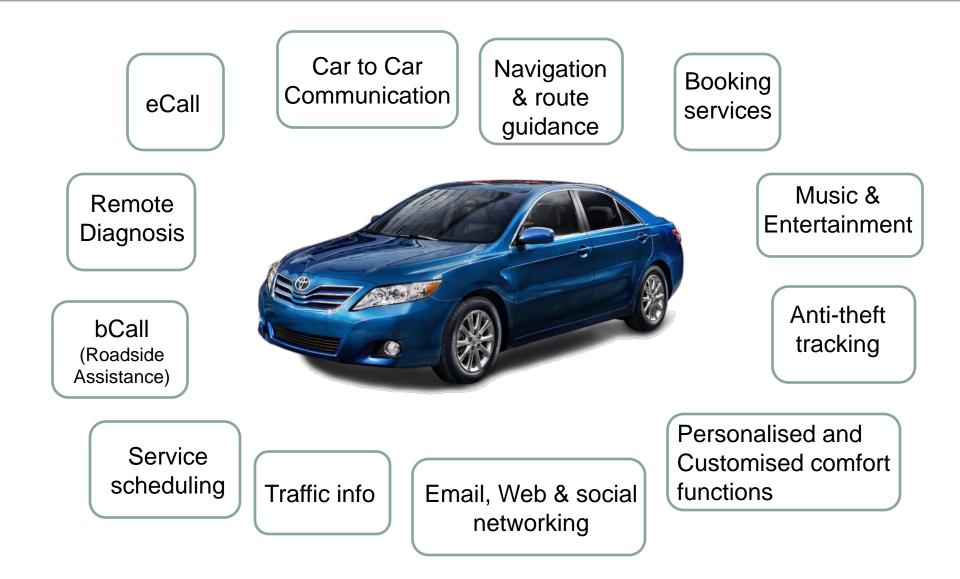
VEHICLE TELEMATICS TECHNOLOGY

Technical findings and the way forward





Vehicle Telematics Functions





Wireless communication will replace traditional methods



Traditional transfer of information via a cable will be used less and less as wireless communication becomes more prevalent.

Therefore Independent Operators must be able to receive information wirelessly in a similar way to the vehicle manufacturers.



Vehicle Telematics

What is the threat posed by telematics to the European aftermarket?

Vehicle Telematics could threaten the continued effectiveness of existing EU Regulations (Euro 5/6 and Euro VI) which currently grant rights of access to vehicle OBD and technical information to independent operators.

Vehicle telematics technologies could become a new barrier to this access.



What is needed?

Independent Operators need:

- equal access to the same information and the same functionalities
- same timescale as vehicle manufacturers to allow Independents to offer competitive services
- a standardised vehicle API that allows Independent Operators to upload their own applications into the vehicle, enabling the vehicle owner to connect his telematics system to a service provider of his own choice.



The future of Diagnostic tools manufacturers with telematics

TODAY



- The diagnostic software is on a computer/tool in the workshop.
- The diagnostic software starts the communication and request data from the car via the OBD-communication.
- The in-car-software is answering these external requests via the 16-pin connector.



- The in-car-software detects problems or conducts regular health checks and sends the results to a designated server (owned by VMs).
- > The car **starts** the communication.
- Multibrand tool companies have to access the car's telematics system via the TCU and then use their own app to access the specific vehicle data they need.



Several possible scenarios:

- 1. Each multibrand tools manufacturer writes its own application that has to be installed on the telematics platform and send the data to a designated MBTC server.
- 2. Multibrand tools manufacturers form a consortium, they write one "App" to a standardised API that collects every interesting data from inside the car and sends it to a consortium-server (gateway). Every member of the consortium can now write software that communicates via the Gateway and the App with the car's telematics system.
- 3. If required by EU legislation, a selected pool of in-car-data has to be made available to any company with a legitimate interest at a non-discriminatory fee. This would force the VMs to write the related app for each of their future cars and set up a gateway inhouse, accessible to every independent company.

ELECTRIC VEHICLES AND HYBRID ELECTRIC VEHICLES

Access to Repair and Maintenance Information





Type-approval framework for EVs:

- UN Regulation No 100 (functional safety at vehicle level)
- Adaptation of UN Regulations No 94 and 95 (crash safety).
- Specific battery requirements under development (RESS)

Access to RMI for EVs:

The EU Commission confirmed that EVs and HEVs are in principle covered under the scope of Euro 5 Regulations.



EVs & HEVs: State of Affairs

At AFCAR/EGEA level?

Our aim:

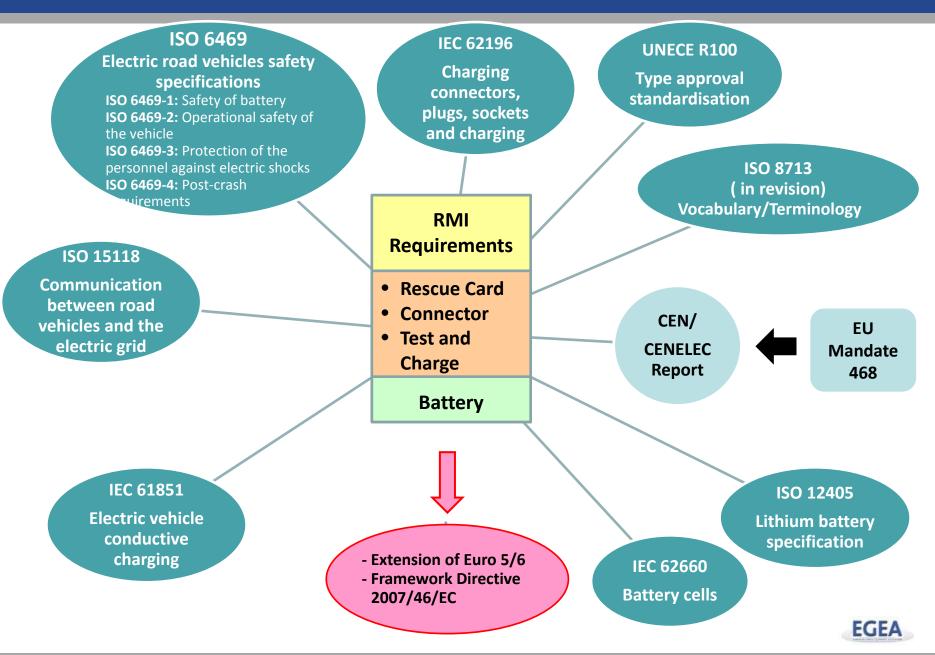
Adapt the existing Euro 5 aftermarket provisions to Electric Vehicles

Several Experts meetings:

- 'AFCAR Technical Experts Workshop' (3rd August 2011) to adapt, where technically necessary, Euro 5/6 RMI provisions
- 'EGEA Electric Vehicle Workshop' (31st January 2012) to discuss with our members how these new types of vehicle technologies could generate changes in the design of our tools and test equipment, as well for PTI.
- Several internal meetings with experts on the standardisation of EVs to cross-check whether any technical features might already sufficiently be covered (or not) by existing ISO/SAE/UN-ECE standards and legislation.



EVs: Existing EU & International standards



Access to RMI for EVs & HEVs: Our findings

Technical adaptation of EU legislation to EVs <u>where</u> <u>current international standards are not sufficient</u>:

Vehicle design requirements:

- > Cable colour coding and protection against electrical shock
- > Rescue Card
- > Service Disconnect Switch (High voltage battery isolation switch)

RMI:

- > Abbreviations (terminology)
- Info for EGEA (Diagnostic connector & communication protocols/ Power train DTCs/ connector design & communication protocol)
- > Battery Management System + Test Criteria
- Battery handling and transportation information
- Vehicle Communication Controller + Charging grid
- Remote vehicle communication (cf. Telematics)
- Strong magnetic characteristics
- PTI testing



EVs & HEVs: Next Steps

- > Our position has been sent to the European Commission
- A meeting to be organised with the EC (DG Enterprise) to discuss further in details
- > A letter has been sent to Nissler to ask about PTI and Evs.
- Next steps will be discussed and defined at the next AFCAR meeting (tbd)





IMPACT OF THE **MVEG** MEETING ON 17.09.2012

Vehicle Manufacturers proposing a round-up solution (for SCR additive monitoring, odometer fraudulent manipulation and vehicle theft) via an electronic certificate for tool manufacturers





Background

UK transport and Thatcham investigated about rising theft of 'prestige' vehicles by breaking into the vehicle and programming a key that then allowed the vehicle to be started and driven away.

This was initially being blamed on the introduction of the Euro 5 legislation and the corresponding access to security information for independent operators and diagnostic tool manufacturers allowing the information necessary to create such a tool to be accessed.

NOT a Euro 5 problem, but rather poor vehicle security system design!



MVEG meeting on 17th September 2012

- During the MVEG meeting on 17th September, an item on the agenda was the problem of truck operators electronically falsifying the 'Ad-Blue' monitoring system to avoid having to buy (expensive) additive.
- VMs proposed that the additional issues of vehicle theft through reprogramming keys and the problems of falsifying vehicle odometer readings should also be included in a 'round-up' solution.

> Solution proposed by ACEA :

to use the SERMI scheme (that provides accreditation for access to vehicle anti-theft information through the use of an electronic certificate) to become more widespread and be applied to 'certifying' equipment as well as the users.



Threat

From the original claim that this was a Euro 5 based issue, it is now developing into an alternative method for VM's to pressurise the European Commission into amending legislation and to subsequently create further burdens for IO's and equipment manufacturers.

Their objective has not changed, just the way to achieve it.



EGEA members would need therefore to be accredited



Next Steps

The European Commission will organise a Working Group to deal with

vehicle theft through re-programming keys issues, problems of falsifying vehicle odometer readings and the 'ad-Blue' monitoring system issue involving stakeholders at EU level.

- EGEA WG2 to schedule soon a meeting to review the response to the EC and prepare for the proposed EC technical working groups.
- The WG2 members/experts will need to create an objective technical response to these issues of vehicle theft, manipulation of the SCR additive or of the vehicle's odometer for discussion in the proposed EC Technical Working Group.





Thank you!

