

Comments on informal document GRSG-108-38 on Regulation No. 39 (Speedometer)

The text reproduced below was prepared by the expert from the Fédération Internationale de l'Automobile (FIA), to express their comments to the discussion on item 3 of the agenda of the 108th meeting of the GRSG on 4-8 May 2015 and to answer to the questions and concerns raised at the meeting with regard to its proposal for the protection of odometer data.

Further, as a next step, the FIA proposes to set up an informal working group in UNECE/GRSG to work with all relevant stakeholders a common protection profile for odometer data and the type approval process.

I) Scope of the proposal

The FIA proposes to include all vehicles that can be tampered via any electronic vehicle interface like OBD.

The proposed IT solution does not apply to mechanical odometer systems. The proposal aims to include odometer systems of all vehicle categories that may be frauded e.g. via the 16 PIN OBD port or any other electronic vehicle interface.

If the manipulation via the electronic interface like the OBD port is hindered, all other means to tamper the odometer are more costly (time, skills, equipment) for the fraudsters.

L-Category vehicles with mechanical odometers are excluded and N-Category vehicles can be excluded, if deemed appropriate by the Contracting Parties.

II) Technological diversity

Regarding concerns about technological diversity, the FIA underlines that most vehicles currently can be frauded via the OBD port, following the same method and using, in general, the same tools. There is currently no significant diversity in terms of security between technical solutions of different vehicle manufacturers.

III) Reparability

Regarding concerns about odometer reparability, the FIA proposes that provisions allowing repair or replacement of a defective odometer should be defined together with relevant stakeholders. Odometer repairs are, however, very rare. The data are stored in the ECU and not in the dashboard itself. Changing the dashboard does not change the stored mileage in the ECU. If the ECU, which stores the mileage, is changed, an authorised access (as described in SERMI) can be developed.

IV) Competence of UNECE GRSG

Regarding concerns about the competence of the UNECE GRSG to protect the odometer, considering the lack of relevance of the odometer to vehicle/traffic safety, the FIA underlines that:

1. The odometer will be part of the type approval from 2017 on proposal of the GRSG and therefore will soon be within its competence.
2. Anti-theft systems have been protected, although they are not purely relevant for safety, and have been part of the type-approval in GRSG for years.

V) Methodology

Regarding concerns about the proposed methodology, the FIA proposes to use the methodology of common criteria according to an ISO standard. This would ease the drafting of a unique protection profile. Although the ISO standard is not legally binding, it is accepted by 27 countries and used in several sectors, such as in the military sector and the automotive sector (e.g. in electronic tachographs). FIA refers to the "List of certified products" including electrical tachographs here: <http://www.commoncriteriaportal.org>.

Odometer protection by common criteria is an application of this methodology. The FIA sees further relevant use cases for common criteria in the sector of vehicle telematics and autonomous driving. Currently vehicle manufacturers develop the extended vehicle under ISO, to remotely enter in-vehicle-data.

ISO 15408 is already common in the automotive industry and contains a methodology to develop a protection profile. Once it is developed, the type approval authorities do not need to know the details of the ISO standard. The type approval authorities only need to check if the manufacturers have met the established common criteria. For the development of UNECE regulations, the standards are available free of charge. The methodology of common criteria saves cost and development time.

The protection proposed by the FIA will minimize the financial benefits of fraudsters and make odometer tampering unattractive. This is an essential difference to other IT safety requirements where requirements are much tougher and more costly. The methodology of common criteria is cost effective, technically smart and technology neutral. Each manufacturer can keep its individual solution. There is one protection profile, similar to a threshold and individual ways on how to reach this security target.

VI) Ongoing security improvements

The security target of each vehicle manufacturer has to be constantly checked and, where needed, upgraded to fulfill the requirements for new vehicles in order to guarantee a level of security that is as high as possible. Examples are Anti-Theft Systems or the security gaps in connected vehicles, which several manufacturers had to close in 2015. But even if the technology is moving forward, the standard of the protection profile can be kept and the regulation can remain unchanged. It is sufficient to keep the security target up to date.

VII) Databases

The European Commission has addressed odometer tampering within the European Union in the Roadworthiness Package. Car odometers are most often tampered before the first roadworthiness check (PTI). The PTI then registers and officialises incorrect values. This does not mean that the mileage cannot be frauded anew in between inspections by lowering the value significantly, to just above the last registered value.

The FIA welcomes the provisions on mileage fraud in the EU Roadworthiness Package. However, this will not address the vehicles that are most frequently frauded, i.e. new vehicles of less than four years of age, as the incentive to tamper with a vehicle constantly decreases with the vehicle's age. In addition, the FIA proposes the protection of the odometer to safeguard the rest of the fleet.

The FIA proposes the most effective solution that is attainable at the lowest cost.

VIII) Justification

Odometer fraud is a rising problem in the automotive aftermarket. It is based on the unprotected odometer data of vehicles. The FIA figures are taken from an EU impact assessment documents for PTI. The FIA believes that an average €3000 in damages per frauded vehicle as a critical loss to consumers.

The European Commission regards these figures as sufficiently robust to write and pass European legislation (PTI directive). Further research confirms the findings of the European Commission, while in many instances concluding with higher figures, e.g. from the German police and from the Belgian police, which highlighted the cross-border cases.

The European vehicle manufacturers Association (ACEA) called upon the European Commission to address mileage fraud as a rising problem in the automotive aftermarket and proposed in 2012 to put protection against mileage fraud under the umbrella of EU regulation 692/2008 (SERMI) The problem has, in the meantime, grown significantly more pressing due to the increased ease of odometer tampering and its decreasing cost.
