31 Oktober 2018
Submitted by FIA

FIA Comments on
Draft Recommendation on Software Updates of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA

Informal document GRVA-01-18 1st GRVA session

FIA contributed actively in the Task Force on Cyber Security and Over The Air Updates. As a Consumer Organisation, we addressed relevant issues for consumers throughout the working period of the task Force.

In principle the FIA welcomes this initiative to tackle Cyber Attacks, Over the Air Updates and Data Protection issues for Automated Vehicles.

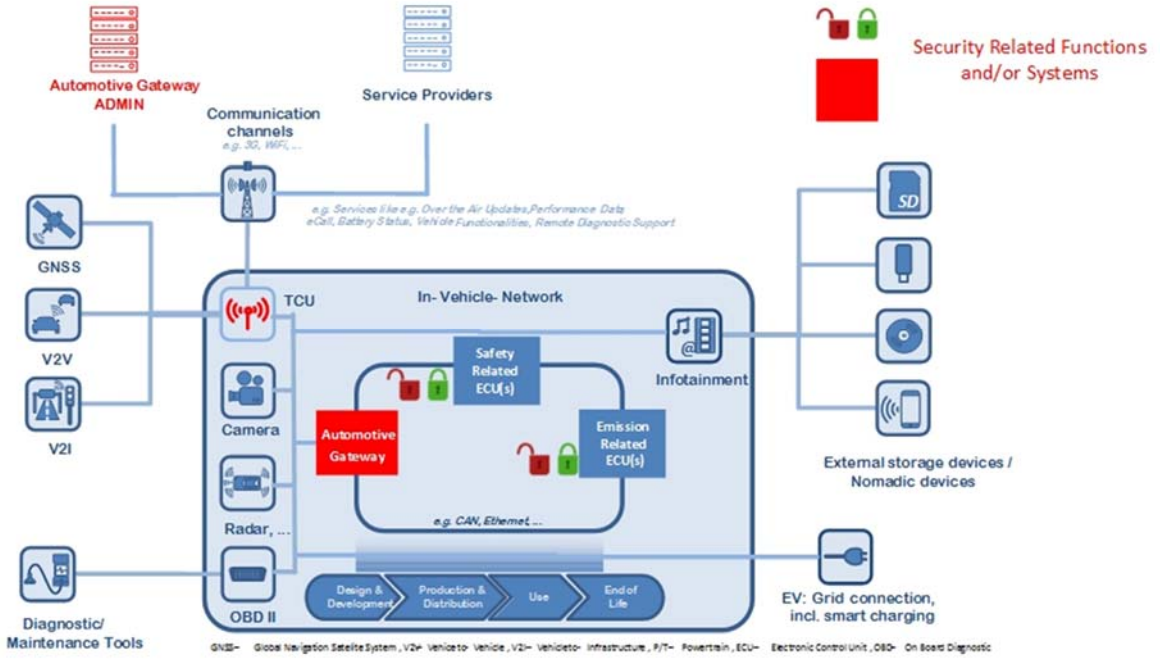
We comment hereby on the report on software updates, GRVA-01-18.

In chapter "7 Conclusion and Recommendations for further Proceedings", we would like the following points to be amended:

1) Automated Vehicles need not only soft- but also hardware updates. The parent group (GRVA) should decide about an extension of the mandate to include hardware updates too.
   Justification:
   FIA club ADAC showed, that the Keyless Entry systems are unsecure. By simply extending the range of the signals the vehicles can be opened and driven away. Only a change of soft- and hardware could solve the problem for the existing fleet. VW, Fiat, Honda, Kia and Volvo had vulnerabilities in key codes of millions of vehicles. Replacing the keys (hardware), affected by the vulnerability was too costly for the vehicle manufacturer.

2) The vehicle manufacturer shall provide soft- and hardware updates over the lifetime of the vehicle. If the vehicle manufacturer ceases to update the vehicle software and hardware before the end of the vehicle lifetime after this period, all relevant documentation for the production of software and hardware shall be handed over to interested third parties.
   Justification:
   In the current document there is no information on how long the vehicle manufacturer intends to keep the automated vehicle secure. The average duration of a vehicle in operation is 10 years after first registration. 40% of the car fleet in Germany is older than 10 years. A lot of cars older than 10 years are used on a daily basis but when the vehicles get older than 20 years a lot of people use such cars as collector cars and use them only for leisure purposes. Vehicles between 20 and 30 years are defined as Youngtimer. Vehicles older than 30 years are defined as Oldtimer which are not used on a daily basis.

3) It is appropriate to introduce an enhanced reference model which represents the 'objective' of a cyber secured conceptual model. The intent is that it would show a functional architecture – and not imply what a physical solution must look like.



Justification:

The reference models shows all security related components as well as the environmental and safety relevant components that should be accessible for authorised user groups. These systems are covered by UNECE regulations and therefore their IT security is type approval relevant.

Munich
31 October 2018
Gerd Preuss