15 November 2018

German comments on the Draft Recommendations on Cyber Security and Software Updates of the Task Force on Cyber Security and Over-the-air issues of UNECE/WP.29/GRVA – Revised Version

In the following, Germany provides a revised version of the comments it sent on 31 October 2018 regarding the proposals made by the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA on cyber security and software updates for automated and connected vehicles.

Germany welcomes the development of appropriate recommendations for the spheres of cyber security and software updates in automated and connected driving and thanks the experts for their efforts.

Germany would like to start by making the following general comments:

Fundamentals of risk analysis

A systematic threat analysis of the vehicle systems and their environment should definitely be conducted. To conduct a complete threat analysis, it is first necessary to define objects of protection (assets worthy of protection) and identify the security objective with regard to which they have to be protected. In a second step, threats, vulnerabilities and potential harm to these objects as well as the probability of them occurring can be named. On the basis of these data, risks can be identified analysed and evaluated. The risks will serve as a basis for the formulation of security objectives and eventually of requirements to be met by security functions and mitigations to eliminate unacceptable risks.

Further definitions should be made on the basis of already established and internationally recognized cyber security standards. The threats and mitigations should be fleshed out in more specific terms and there should be a clear link to vulnerabilities. Care should also be taken to ensure a more consistent description. In addition, when formulating the mitigations, a clearer distinction should be made between mitigations for the (connected) vehicle itself and mitigations that also relate to back-end systems. Nevertheless, care should be taken to ensure a formulation that does not favour a specific technology and does not stipulate any architecture requirements.

In addition, Germany would like to make the following remarks on the Cyber Security Management System and technical testing requirements, software updates and a standardized communication gateway.

Cyber Security Management System

The present recommendation of the CS/OTA Task Force calls for the implementation of a Cyber Security Management System by the manufacturer, covering the whole lifecycle of the vehicle. Manufacturers must provide evidence about the implementation of their Security Management System. Likewise, they "shall demonstrate that the processes used within their Cyber Security Management System ensure security is adequately considered". This is welcomed, but binding auditing criteria, testing processes and standards need to be defined for this. Documentation obligations are mentioned, but no technical requirements. It is absolutely essential that requirements to be met by the evidence/documentation and specific requirements to be met by technical tests of components to ensure comparable and legally secure assessment/approval be defined. (In the current version, a number of mandatory mitigations are listed in Chapter 5. These, in particular, would have to be checked for correct implementation within the scope of approval). This is to be done within the framework of WP.29 and to be based on internationally established cyber security standards in order to prevent individual states from going it alone. Technical measures must be based on the state of the art, both at the time of placing into service and over the vehicle's service life, in order to guarantee the safe operation of the vehicle. For this purpose, suitable test criteria that do not favour a specific technology have to be defined and prescribed.

Software updates

Safe operation is to be guaranteed over the entire service life of the vehicle.

Standardized communication gateway

To ensure adequate cyber security of connected vehicles in public road traffic, there is a fundamental requirement for a secure communication channel into/out of the vehicle, both at the time of placing into service and over the vehicle's entire service life. The external communication interfaces in the vehicle should be provided by a physical or logical communication gateway with standardized security functionality and with connection to the in-vehicle networks.