30 October 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

Germany provides the following comments on the respective proposals made by the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA for automated and connected vehicles.

First of all 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.

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

Fundamentals of threat 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 vulnerabilities (assets worthy of protection). In a second step, threats and potential harm to these vulnerabilities can be named. Risks can be identified on the basis of these data. The risks will serve as basis for the formulation of security objectives and eventually of requirements to be met by security functions and mitigations to eliminate unacceptable risks.

This method is also identified by the new ISO 21434. Further definitions should be made on the basis of a sufficiently stable status of ISO 21434 and other already established cybersecurity 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 relating 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 TF-CS/OTA calls for the implementation of Cyber Security Management System by the manufacturer, covering the whole life cycle of the vehicle. Here, there is no clear definition of what exactly the CSMS is to cover. Coverage of the vehicle itself and the back-end systems would be advisable. 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, technical services and standards need to be defined for this. Some 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 type-approval). This is to be done within the framework of WP.29 and to be based on ISO 21434 and other internationally established cyber security standards in order to prevent individual states from going it alone. Technical measures should be based on the state of the art at the time of placing into service. The implementation of a Cyber Security Management System with regard solely to type-approval is not sufficient. The correct implementation of the security processes in the vehicle must also take place at the technical level. Corresponding evidence is to be provided to the approval authorities. Suitable test criteria should be defined for this purpose.

Specific technical solutions stipulated and tested by the approval authority are not considered appropriate.

Software updates

The issue of software support for vehicles should be resolved. This includes the question as to how long a manufacturer is obliged to supply software updates for the vehicle and what is to be done if support is discontinued.

The basis for deciding whether an update is safety-critical and thus has to be reported must be clearly defined. Even updates to remedy minor bugs can have an impact on the safety of a vehicle. Otherwise, it might not be possible to determine compliance at all.

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, based on the state of the art at the time of placing into service. It should be clarified whether communication interfaces in the vehicle should be provided by means of single, standardized physical or logic gateway connected to the vehicle's on-board networks.

From a security perspective, incidents have confirmed that limiting the number of communication partners is essential for security that is effective in the long term (and, in particular, is kept up to date). A large number of communication partners to be authorized is highly questionable.