No. 03 - 24

Type-Approval Procedure

Information System of the German Type-Approval Authority

UN Regulations No. 155 (Cybersecurity)
- The CSMS within the context of the EU multi-stage type approval process

Issue/Statement of the problem:

The common multi-stage approval process in Europe in accordance with Annex IX of Regulation (EU) 2018/858 and the associated obligations on the manufacturers involved are neither specifically regulated by UN Regulation No. 155 nor generally by the UNECE legal system. This raises the question of under what conditions a stage-2 manufacturer must have its own CSMS in accordance with UN Regulation No. 155, which is audited by a type approval authority and on the basis of this a system approval and ultimately the entire vehicle approval can be granted in the further approval process.

Result:

Even if the multi-stage approval process is not covered by the UNECE legal system, this issue was discussed among the type approval authorities as part of the UNECE/GRVA workshop on UN Regulation No. 155 and the following recommendation was made (see GRVA-18-37):

Reference: GRVA-18-37
How to assess Stage-2-OEM?

Depending on the impact of the changes made by the Stage-2-OEM. The Stage-2-OEM must explain the changes made and why they are not CSMS relevant.
Three categories have been defined:

- ***Cat. A - UN R155 CSMS for the Stage-2- OEM not required:*** *Changes which are not cyber relevant and do not relate to the E/E Architecture of the Stage-1-OEM (e.g. by adding pure hardware or devices which are not connected to the E/E Architecture of the Stage-1-OEM).*

- ***Cat. B - UN R155 CSMS might (not) be required:*** *Changes are cyber relevant or related to the E/E Architecture but only with "read-access". Stage-2-OEM has to explain based on a risk assessment why the changes are not relevant.*

- ***Cat. C - UN R155 CSMS required:*** *Changes are cyber relevant or related to the E/E Architecture with "read/write" access to the E/E Architecture. For cyber relevant modifications, elements given to the type approval authority/technical service should include information regarding interface between manufactures at each stage.*

Note: Type approval for multi stage vehicles regarding UN R155 needs to be further explored.

Due to the non-binding nature of this recommendation, an exchange on the implementation of the recommendation took place at the Type Approval Authority Meeting (TAAM) in February 2023. The member states agreed to follow the recommendation from the UNECE/GRVA workshop on UN Regulation No. 155 in the operational type approval process.

The following clarification serves to further detail this recommendation.

1) The body manufacturer must provide evidence to a technical service designated for UN Regulation No. 155 and by the KBA to what extent the changes to the base vehicle that they have made themselves have an impact on cybersecurity in accordance with UN Regulation No. 155 and which ones of the above categories is applied.

2) The technical service has assured itself of the completeness of the risk analysis and the classification in Cat. A (not cyber-relevant) or Cat. B (cyber-relevant, but only with "read access").. If the technical service comes to a different conclusion when evaluating the body manufacturer's risk analysis, the type approval authority must be informed. The type approval authority then decides on a case-by-case basis whether the body manufacturer must have its own CSMS in accordance with UN Regulation No. 155.

3) Proof of points 1) and 2) must be documented within the multi-stage type approval by the technical service within the main test report in accordance with Regulation (EU) 2018/858 or previous framework directives by means of a corresponding comment.

Flensburg, 13.02.2024
400-347/001#050
Kai Tams Petersen