

Proposal for amendments to ECE/TRANS/WP.29/GRVA/2019/4

I. Proposal

Paragraph 3.4.4., amend to read:

"3.4.4. The documentation shall be supported, by an analysis which shows, in overall terms, how the system will behave on the occurrence of any of those hazards or faults which will have a bearing on vehicle control performance or safety.

The chosen analytical approach(es) shall be established and maintained by the Manufacturer and shall be made open for inspection by the Technical Service at the time of the type approval.

The Technical Service shall perform an assessment of the application of the analytical approach(es). The assessment shall include:

- (a) Inspection of the safety approach at the concept (vehicle) level with confirmation that it includes consideration of:
- interactions with other vehicle systems;
 - ~~[Safety critical risks that arise from malfunctions of the electronic control system within the scope of this UN Regulation;~~
 - ~~Safety critical risks due to inadequate or incorrect responses of the system under non-fault conditions.]~~
 - **Malfunctions of the electronic control system, within the scope of this UN Regulation;**
 - **Situations when a system free from faults may create safety critical risks (e.g. due to a lack of or wrong comprehension of the vehicle environment);**
 - **Potential misuse or simple unauthorised modification of the system.**

This approach shall be based on a Hazard / Risk analysis appropriate to system safety.

- (b) Inspection of the safety approach at the system level. This may be based on a Failure Mode and Effect Analysis (FMEA), a Fault Tree Analysis (FTA) or any similar process appropriate to system safety.
- (c) Inspection of the validation plans and results. This shall include validation testing appropriate for validation, for example, Hardware in the Loop (HIL) testing, vehicle on-road operational testing, or any other testing appropriate for validation.

The assessment shall consist of spot checks of selected hazards and faults to establish that argumentation supporting the safety concept is understandable and logical and validation plans are suitable and have been completed.

The Technical Service may perform or may require to perform tests as specified in paragraph 4. to verify the safety concept."

II. Justification

1. The proposed amendment is to ensure that the safety approach includes considerations for malfunctions, non-fault errors, and misuse.
-