Proposal for amendments to ECE/TRANS/WP.29/GRRF/2017/8

I. Proposal

*Annex 6*

*Paragraph 1.,* amend to read (insert a last subparagraph):

"1. General

 …

This information shall show that "The System" respects, under normal and fault conditions, all the appropriate performance requirements specified elsewhere in this Regulation **and that it operates in such a way that it does not induce any safety critical situations**".

[Paragraph 2.3., amend to read:

2.3. "Complex electronic vehicle control systems" are those electronic control systems which ~~are subject to a hierarchy of control in which~~ **may override** a controlled function ~~may be over-ridden by a higher level electronic control system/function~~. A function which is over-ridden becomes part of the complex system.]

*Paragraph 3.2.,* amend to read:

"3.2. Description of the **design process methodology and** functions of "The System"

**A description shall be provided of the methodology applied for the design of “The System”, which includes the processes and standards followed within the design and development life cycle[, for example for the automotive industry these may include ISO 26262, MISRA C and Automotive SPICE]. The application of the methodology shall be demonstrated by an assessment report made by a [competent authority] [Technical Service [/ third party]]. [This may include a certificate of accreditation issued by an accreditation body.]**"

*Paragraph 3.4.1.,* amend to read:

"3.4.1. The manufacturer shall provide a statement which affirms that the strategy chosen to achieve "The System" objectives will not, under **fault and** non-fault conditions, prejudice the safe operation of systems which are subject to the prescriptions of this Regulation."

*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 ~~specified~~ **hazards or** faults which will have a bearing on vehicle control performance or safety.

~~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 considerations.~~

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 audit of the application of the analytical approach(es). The audit shall include:**

* **Inspection of the safety approach at the concept (vehicle) level with confirmation that it includes consideration of interactions with other vehicle systems. This may be based on a Hazard and Operability analysis (HAZOP) or any similar process appropriate to system safety.**
* **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.**
* **Inspection of the validation plans. This may include Hardware in the Loop (HIL) testing and vehicle on–road operational testing with expert and/or non-expert drivers or any similar testing appropriate for validation.**

**The audit 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 performtests as specified in paragraph 4. to verify [/ be satisfied with] the safety concept.]**"

*Insert new paragraph 3.4.4.2.*, to read:

["**3.4.4.2. This documentation shall describe the resistance of "The System" to environmental influences, e.g. climate, mechanical resistance and electromagnetic compatibility.**"] (Here or in the core of the Regulation?)

*Paragraph 4.1.2.*, amend to read:

"4.1.2. Verification of the safety concept of paragraph 3.4.

The reaction of "The System" shall, at the discretion of the type approval authority, be checked under the influence of a failure in any individual unit by applying corresponding output signals to electrical units or mechanical elements in order to simulate the effects of internal faults within the unit.

**[The Technical Service shall verify ] that these tests include aspects that impact on vehicle controllability and user information (HMI aspects).**"

*Paragraph 5.,* amend to read:

**5. Reporting by technical service**

**Reporting of the audit by technical service shall be performed in such a manner that allows traceability, e.g. versions of documents inspected are coded and listed in the records of the technical service.**

**An example of a possible layout for the report from the technical service to the type approval authority is given in the template in Part II of this document.**

 II. Example of Report Layout







