Submitted by the expert from The Netherlands

Informal document **GRRF-83-24**
83rd GRRF, 23-27 January 2017
Agenda item 9(a)

Comments to EC-proposal ECE/TRANS/WP.29/GRRF/2017/8

Comments in **bold blue** between the original text of the EC-proposal

General comment:

*** Terminology with regard "technical service" (par. 1, 3.1.1 and 3.4.4), "technical authorities" (par. 3.4.3), type approval authority (par. 4.1.2) and "competent authority" and "accreditation body" (EC-doc. …/2017/8) should be used consequently, one term for one application.**

*** Annex 6 deals with the documentation, fault strategy and verification in fact as declared by the manufacturer. There is no requirement saying something like "the system shall be fail safe and cause no unsafe situation with or without failures". Real requirements are missing. There is too much vagueness in the text. Therefor technical services are understanding and applying the Annex in a different way. What is expected of them?**

I. Proposal

Annex 6

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

"1. General

…

Involvement of the technical service at an early stage in the design process is recommended for an effective assessment of "The System" to the requirements of this annex."

This text is in fact useless because it is not a requirement. There is no incentive, just wishful thinking. Better to delete this paragraph from the proposal since it only adds more vagueness to the Annex.

Annex 6 misses is a general requirement that the system shall not cause dangerous situations. Currently there is only a reference to the performance requirements specified in the regulation.

To address that Annex 6 par.1 could be supplemented (bold red text) as follows:

Current Annex 6- Special requirements to be applied to the safety aspects of complex electronic vehicle control systems:

1. GENERAL

This annex defines the special requirements for documentation, fault strategy and verification with respect to the safety aspects of Complex Electronic Vehicle Control Systems (paragraph 2.3. below) as far as this Regulation is concerned.
This annex may also be called, by special paragraphs in this Regulation, for safety related functions which are controlled by electronic system(s).
This annex does not specify the performance criteria for "The System" but covers the methodology applied to the design process and the information which must be disclosed to the technical service, for type approval purposes.
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.**

The current definition 2.3 "complex electronic vehicle control systems" should be clarified. The proposed text below could be used as a starting point:

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.

This text would cause that systems like ABS become complex electronic systems.

In addition par. 3.4.1. should be supplemented with a requirement that also in fault condition the safe operation is guaranteed, as proposed below:

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 3.2., amend to read:

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

A description should 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 established by a competent authority. This may include a certificate of accreditation issued by an accreditation body."

*** It is said that the assessment report shall be established by a competent authority. What does that mean, shall the authority or technical service be accredited? And if yes, by whom?**
By putting "may" this requirement is reduced to a non-requirement. We should strive to mention at least a minimum level, may be ISO 26262 is too expensive when "simple" complex electronic systems have to be assessed.
If anyhow possible, we should try to make a kind of extract from ISO 26262 and put that in the regulation.

*** This requirement belongs more to par. 3.1 which sais:**

"… Documentation shall be brief, yet provide evidence that the design and development has had the benefit of expertise from all the system fields which are involved …."

*** Moreover, the whole paragraph 3 is a bit inconveniently arranged. This could be improved by putting the requirements with regard the**

documentation clearly specified one below the other, only one item per paragraph.

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 one of those ~~specified~~ **identified 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.

Recommendations may be made for tests to be performed in paragraph 4. to verify the safety concept."

*** First paragraph: may be better to delete "identified" (as well as "specified") because all hazards should be addressed. There should be no room to say: "I did not identify this …".**

*** Annex 6 par. 3 is dedicated to "documentation", par. 4 is dedicated to "verification and tests". The proposed requirements should be part of par. 4.**

*** Last sentence, "Recommendations may be made for tests….", has no effect with "may", should be "shall" or the complete sentence can be deleted from the proposal since everyone can at all time make some recommendations.**

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.**"

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.

It is recommended 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.