Submitted by the experts from OICA

Informal document **GRVA-04-29**
4th GRVA, 24-27 September 2019
Agenda item 6(b)

Proposal for amendments to ECE/TRANS/WP.29/GRVA/2019/20

Proposed changes and justifications by OICA are shown with red text.

General comments

1. The task of upgrading the Annex 6 to UN R79 ("CEL annex") was given by GRRF-86 (February 2018) to the expert from UK, when the development of ACSF-B2 was discussed in the frame of UN R79.
2. When it was decided to construct the requirements for ACSF B2 as a Level 3-4 system, and to rename it as "ALKS" in a separate regulation the amendments were erroneously left in the format of UN R79.
3. OICA believe that the requirements as proposed by the CEL task-force (document GRVA/2019/20) should be applicable to ALKS rather than to systems covered in UN R79.
4. Should GRVA at its 4th session nevertheless decide to apply the amended CEL annex to UN R79, then the changes proposed in red below are considered as a necessary adjustment by OICA.

I. Proposal

Title of the document, amend to read:

"Proposal for a Supplement to the 03 series of amendments to UN Regulation No. 79"

Annex 6

Paragraph 1., amend to read:

"1. General

This annex defines the special requirements for documentation, fault strategy and verification with respect to the safety aspects of **Electronic System(s) (paragraph 2.3.) and** Complex Electronic Vehicle Control System**(s)** (paragraph 2.4. below) as far as this **UN** Regulation is concerned.

~~This annex shall also apply to safety related functions identified in this UN Regulation which are controlled by electronic system(s) (paragraph 2.3.) as far as this UN Regulation is concerned.~~

[…]"

Paragraph 2.3., amend to read:

"2.3. "*Electronic control system*" means a combination of units, designed to co-operate in the production of the stated vehicle control function by electronic data processing. Such systems, ~~often~~ **commonly** controlled by software, are built from discrete functional components such as sensors, electronic control units and actuators and connected by transmission links. They may include mechanical, electro-pneumatic or electro-hydraulic elements."

Paragraph 2.10., amend to read:

"2.10. "*Safety Related Function*" means a function of "The System" that is capable of changing the dynamic behaviour of the vehicle. "The System" may be capable of performing more than one safety related function."

Insert new paragraph 2.11., to read:

"2.11. **"*Control strategy*" means a strategy to ensure robust and safe operation of the function(s) of "The System" in response to a specific set of ambient**

and/or operating conditions (such as road surface condition, traffic intensity and other road users, adverse weather conditions, etc.). This may include the automatic deactivation of a function or temporary performance restrictions (e.g. a reduction in the maximum operating speed, etc.)."

Paragraph 3.1., amend to read:

"3.1. Requirements

The manufacturer shall provide a documentation package which gives access to the basic design of "The System" and the means by which it is linked to other vehicle systems or by which it directly controls output variables. The function(s) of "The System"**, including the control strategies,** and the safety concept, as laid down by the manufacturer, shall be explained. 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. For periodic technical inspections, the documentation shall describe how the current operational status of "The System" can be checked.

The Technical Service shall assess the documentation package to show that "The System":

(a) Is designed to operate, under non-fault and fault conditions, in such a way that it does not induce safety critical risks;

(b) Respects, under non-fault and fault conditions, all the appropriate performance requirements specified elsewhere in this UN Regulation; and

(c) Was developed according to the development process/method declared by the manufacturer **and that this includes at least the steps listed in paragraph 3.4.4**."

Paragraph 3.2., amend to read:

"3.2. Description of the functions of "The System" **including control strategies**

A description shall be provided which gives a simple explanation of all the ~~control~~ functions **including control strategies** of "The System" and the methods employed to achieve the objectives, including a statement of the mechanism(s) by which control is exercised.

Any described function that can be over-ridden shall be identified and a further description of the changed rationale of the function's operation provided.

Any enabled or disabled safety related functions~~, including both those~~ providing assistance to the driver as defined in paragraph 2.3.4. of this UN Regulation~~ and those where the driver is not necessarily in primary control of the vehicle~~, when the hardware and software are present in the vehicle at the time of production, shall be declared and are subject to the requirements of this annex, prior to their use in the vehicle."

Paragraph 3.2.1., amend to read:

"3.2.1. A list of all input and sensed variables shall be provided and the working range of these defined**, along with a description of how each variable affects system behaviour**."

Paragraph 3.3.4., amend to read:

"3.3.4. There shall be a clear correspondence between ~~these~~ transmission links and the signals carried between Units. Priorities of signals on multiplexed data paths shall be stated wherever priority may be an issue affecting performance or safety."

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 ~~audit~~ **assessment** shall include:

(a) Inspection of the safety approach at the concept (vehicle) level with confirmation that it includes consideration of:

(i) interactions with other vehicle systems**;**

(ii) **Malfunctions of the system, within the scope of this UN Regulation;**

(iii) **For functions defined in paragraph 2.3.4. 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);**
- **Reasonably foreseeable misuse by the driver;**
- **Intentional 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."

Paragraph 4.1.1., amend to read:

"4.1.1. Verification of the function of "The System"

The Technical Service shall verify "The System" under non-fault conditions by testing a number of selected functions from those ~~declared~~ **described** by the manufacturer in paragraph 3.2. above.

For complex electronic systems, these tests shall include scenarios whereby a declared function is overridden."

Insert new paragraph 4.1.1.1., to read:

"4.1.1.1. **The verification results shall correspond with the description, including the control strategies, provided by the manufacturer in paragraph 3.2.**"

Appendix 1, amend to read:

Annex 6 - Appendix 1

Model assessment form for electronic systems

Test report No: .....

1. Identification

1.1. Vehicle make: .....

1.2. Type: .....

1.3. Means of identification of type if marked on the vehicle: .....

1.4. Location of that marking:.....

1.5. Manufacturer's name and address:.....

1.6. If applicable, name and address of manufacturer's representative:.....

1.7. Manufacturer's formal documentation package:

Documentation reference No: .....
Date of original issue: .....
Date of latest update: .....

2. Test vehicle(s)/system(s) description

2.1. General description: .....

2.2. Description of all the control functions of "The System", and methods of operation: ..

2.3. Description of the components and diagrams of the interconnections within "The System":

2.4. General description: .....

2.5. Description of all the control functions of "The System", and methods of operation: .

2.6. Description of the components and diagrams of the interconnections within "The System":.....

3. Manufacturer's safety concept

3.1. Description of signal flow and operating data and their priorities: .....

3.2. Manufacturer's declaration:

The manufacturer(s) ..... affirm(s) that the strategy chosen to achieve "The System", objectives will not, under non-fault conditions, prejudice the safe operation of the vehicle.

3.3. Software outline architecture and the design methods and tools used: .....

3.4. Explanation of design provisions built into "The System" under fault conditions: .....

3.5. Documented analyses of the behaviour of "The System" under individual hazard or fault conditions: .....

3.6. Description of the measures in place for environmental conditions: .....

3.7. Provisions for the periodic technical inspection of "The System": .....

3.8. Results of "The System" verification test, as per para. 4.1.1. of Annex 6 to UN Regulation No. 79: .....

3.9. Results of safety concept verification test, as per para. 4.1.2. of Annex 6 to UN Regulation No. 79: .....

3.10. Date of test: .....

3.11. This test has been carried out and the results reported in accordance with ….. to UN Regulation No. 79 as last amended by the ..... series of amendments.

Technical Service[+] carrying out the test
Signed: ..... Date: .....

~~3.12. Type Approval Authority[1]~~
~~Signed: ..... Date: .....~~

3.1~~3~~2. Comments: ....."

II. Justification

1. The proposed amendments clarify the assessment to be conducted by a technical service for electronic systems. An in-depth assessment is particularly important for steering systems providing driver assistance. As such, the proposal includes a new definition to ensure the assessment includes system response to changes in the ambient and/or operating conditions.

2. The proposed amendments also seek to ensure that any disabled functions intended for use on a production vehicle are declared and assessed.

3. The Type Approval Authority signature is removed from the model assessment form as this could falsely give the impression that it is possible to grant an approval to the Annex alone.

Justification of OICA proposals

1. Clarification that this supplement applies to 03 series only, and not to previous series which do not include the changes introduced by the 03 series (defined during the "CEL step 1" task force led by the UK). The application of the new requirements on existing systems will require extra-work, which justifies the need for transition provisions. The transitional provisions proposed in the 03 series are really a minimum for industry to update their production.
2. The change in paragraph 3.2 prevents the risk that the UN R79 regulation is understood as a regulation covering automated functions like e.g. ALKS, via the use of the CEL Annex. Since this is obviously not the intention of the amendment, it is proposed to delete the part of the sentence referring to those functions "where the driver is not necessarily in primary control of the vehicle".
   Additionally this also prevents the risk that this would be understood as a request to cover (e.g.) ALKS both in the CEL Annex of the future regulation on ALKS and in the CEL Annex of UN R79, which is not the intention either.

---

[1] ~~To be signed by different persons even when the Technical Service and Type Approval Authority are the same or alternatively, a separate Type Approval Authority authorization is issued with the report.~~