Submitted by Industry

Informal Document - ACSF-23-04

CEL Annex for ALKS new regulation
Industry draft proposal

The black text below is based on R79 series 03, as amended by proposal to amend UN R79 CEL Annex which will be submitted at GRVA-04 by the task force on "CEL step 2".

The purple text adapts the proposal to the context of ALKS new UN regulation.

Proposal

Annex ~~6~~x

Special requirements to be applied to the safety aspects of electronic control systems

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.~~

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 non-fault and fault conditions, all the appropriate performance requirements specified elsewhere in this UN Regulation and that it is designed to operate in such a way that it does not induce safety critical risks.

~~The applicant (e.g. the manufacturer) may provide evidence that an Auxiliary Steering Equipment (ASE) (if fitted) has previously been assessed as part of an approval in accordance with the requirements of Annex 4 of this UN Regulation (as required under the original version of this UN Regulation, its 01 or its 02 series of amendments). In this case, the requirements of this Annex shall not be applied to that ASE for the purposes of an approval in accordance with the 03 series of amendments.~~[TP1]

2. Definitions

For the purposes of this annex,

2.1. "*The System*" means an electronic control system or complex electronic control system that provides or forms part of the control transmission of a function to which this UN Regulation applies. This also includes any other system covered in the scope of this UN Regulation, as

well as transmission links to or from other systems that are outside the scope of this UN Regulation [(e.g. braking, steering)][TP2], that acts on a function to which this UN Regulation applies.

2.2. "*Safety concept*" is a description of the measures designed into the system, for example within the electronic units, so as to address system integrity and thereby ensure safe operation under fault and non-fault conditions, including in the event of an electrical failure. The possibility of a fall-back to partial operation or even to a back-up system for vital vehicle functions may be a part of the safety concept.

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.

2.4. "*Complex Electronic Vehicle Control Systems*" are those electronic control systems in which a function controlled by an electronic system or the driver may be over-ridden by a higher level electronic control system/function. A function which is over-ridden becomes part of the complex system, as well as any overriding system/function within the scope of this UN Regulation. The transmission links to and from overriding systems/function outside of the scope of this UN Regulation shall also be included.

2.5. "*Higher-Level Electronic Control*" systems/functions are those which employ additional processing and/or sensing provisions to modify vehicle behaviour by commanding variations in the function(s) of the vehicle control system. This allows complex systems to automatically change their objectives with a priority which depends on the sensed circumstances.

2.6. "*Units*" are the smallest divisions of system components which will be considered in this annex, since these combinations of components will be treated as single entities for purposes of identification, analysis or replacement.

2.7. "*Transmission links*" are the means used for inter-connecting distributed units for the purpose of conveying signals, operating data or an energy supply. This equipment is generally electrical but may, in some part, be mechanical, pneumatic or hydraulic.

2.8. "*Range of control*" refers to an output variable and defines the range over which the system is likely to exercise control.

2.9. "*Boundary of functional operation*" defines the boundaries of the external physical limits within which the system is able to maintain control.

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.

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.).**

3. Documentation

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**.

3.1.1. Documentation shall be made available in two parts:

(a) The formal documentation package for the approval, containing the material listed in paragraph 3. (with the exception of that of paragraph 3.4.4.) which shall be supplied to the Technical Service at the time of submission of the type approval application. This documentation package shall be used by the Technical Service as the basic reference for the verification process set out in paragraph 4. of this annex. The Technical Service shall ensure that this documentation package remains available for a period determined in agreement with the Approval Authority. This period shall be at least 10 years counted from the time when production of the vehicle is definitely discontinued.

(b) Additional material and analysis data of paragraph 3.4.4. which shall be retained by the manufacturer, but made open for inspection at the time of type approval. The manufacturer shall ensure that this material and analysis data remains available for a period of 10 years counted from the time when production of the vehicle is definitely discontinued.

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 No 79 ~~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~~ the relevant annex of UN Regulation No 79, prior to their use in the vehicle.

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**.

3.2.2. A list of all output variables which are controlled by "The System" shall be provided and an indication given, in each case, of whether the control is direct or via another vehicle system. The range of control (paragraph 2.7.) exercised on each such variable shall be defined.

3.2.3. Limits defining the boundaries of functional operation (paragraph 2.8.) shall be stated where appropriate to system performance.

3.3. System layout and schematics

3.3.1. Inventory of components.

A list shall be provided, collating all the units of "The System" and mentioning the other vehicle systems which are needed to achieve the control function in question.

An outline schematic showing these units in combination, shall be provided with both the equipment distribution and the interconnections made clear.

3.3.2. Functions of the units

The function of each unit of "The System" shall be outlined and the signals linking it with other units or with other vehicle systems shall be shown. This may be provided by a labelled block diagram or other schematic, or by a description aided by such a diagram.

3.3.3. Interconnections

Interconnections within "The System" shall be shown by a circuit diagram for the electric transmission links, by a piping diagram for pneumatic or hydraulic transmission equipment and by a simplified diagrammatic layout for mechanical linkages. The transmission links both to and from other systems shall also be shown.

3.3.4. Signal flow, operating data and priorities

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.

3.3.5. Identification of units

Each unit shall be clearly and unambiguously identifiable (e.g. by marking for hardware and marking or software output for software content) to provide corresponding hardware and documentation association.

Where functions are combined within a single unit or indeed within a single computer, but shown in multiple blocks in the block diagram for clarity and ease of explanation, only a single hardware identification marking shall be used. The manufacturer shall, by the use of this identification, affirm that the equipment supplied conforms to the corresponding document.

3.3.5.1. The identification defines the hardware and software version and, where the latter changes such as to alter the function of the Unit as far as this Regulation is concerned, this identification shall also be changed.

3.4. Safety concept of the manufacturer

3.4.1. The Manufacturer shall provide a statement which affirms that the strategy chosen to achieve "The System" objectives will not, under non-fault conditions, prejudice the safe operation of the vehicle.

3.4.2. In respect of software employed in "The System", the outline architecture shall be explained and the design methods and tools used shall be identified. The manufacturer shall show evidence of the means by which they determined the realisation of the system logic, during the design and development process.

3.4.3. The Manufacturer shall provide the Technical Service with an explanation of the design provisions built into "The System" so as to generate safe operation under fault conditions. Possible design provisions for failure in "The System" are for example:

(a) Fall-back to operation using a partial system.

(b) Change-over to a separate back-up system.

(c) Removal of the high level function.

In case of a failure, the driver shall be warned for example by warning signal or message display. When the system is not deactivated by the driver, e.g. by turning the ignition (run) switch to "off", or by switching off that particular function if a special switch is provided for that purpose, the warning shall be present as long as the fault condition persists.

3.4.3.1. If the chosen provision selects a partial performance mode of operation under certain fault conditions, then these conditions shall be stated and the resulting limits of effectiveness defined.

3.4.3.2. If the chosen provision selects a second (back-up) means to realise the vehicle control system objective, the principles of the change-over mechanism, the logic and level of redundancy and any built in back-up checking features shall be explained and the resulting limits of back-up effectiveness defined.

3.4.3.3. If the chosen provision selects the removal of the Higher Level Function, all the corresponding output control signals associated with this function shall be inhibited, and in such a manner as to limit the transition disturbance.

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 individual hazard or fault 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:

- interactions with other vehicle systems**[(e.g. braking, steering)];**
- **Malfunctions of the system, within the scope of this UN Regulation;**
- ~~**For functions defined in paragraph 2.3.4. of this UN Regulation:**~~[TP3]
  - **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.**[TP4]

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 approach shall 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 validation shall use, for example, Hardware in the Loop (HIL) testing, vehicle on–road operational testing, or any means appropriate for validation.

The assessment shall consist of checks of hazards and faults chosen by the Technical Service to establish that the manufacturer's explanation of the safety concept is understandable, logical and that the 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.

3.4.4.1. This documentation shall itemize the parameters being monitored and shall set out, for each fault condition of the type defined in paragraph 3.4.4. of this annex, the warning signal to be given to the driver and/or to service/technical inspection personnel.

3.4.4.2. This documentation shall describe the measures in place to ensure the "The System" does not prejudice the safe operation of the vehicle when the performance of "The System" is affected by environmental conditions e.g. climatic, temperature, dust ingress, water ingress, ice packing.

4. Verification and tests

4.1. The functional operation of "The System", as laid out in the documents required in paragraph 3., shall be tested as follows:

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.

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

4.1.2. Verification of the safety concept of paragraph 3.4.

The reaction of "The System" shall 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 conduct this check for at least one individual unit, but shall not check the reaction of "The System" to multiple simultaneous failures of individual units.

The Technical Service shall verify that these tests include aspects that may have an impact on vehicle controllability and user information (HMI aspects).

4.1.2.1. The verification results shall correspond with the documented summary of the failure analysis, to a level of overall effect such that the safety concept and execution are confirmed as being adequate.

5. Reporting by Technical Service

Reporting of the assessment by the 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 assessment form from the Technical Service to the Type Approval Authority is given in Appendix 1 to this Annex.

Submitted by Industry

Informal Document - ACSF-23-04

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":

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[1] carrying out the test
Signed: ..... Date: .....

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

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

~~[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.~~