Submitted by the expert from the United Kingdom
of Great Britain and Northern Ireland

Informal document **GRVA-15-08**
15th GRVA, 23-27 January 2023
Provisional agenda item 8(b)

Proposal for amendments to UN Regulation No. 13

Contents, Annex 18 title, amend to read:

"18. Special requirements to be applied to the safety aspects of ~~**complex**~~ electronic ~~vehicle~~ control systems"

Contents, after Annex 18 title, insert:

Appendix - Model Annex 18 assessment report.

At the end of paragraph 12, insert new paragraphs:

Paragraph 12. Transitional Provisions, add:

12.X.1. As from the official date of entry into force of the XX series of amendments, no Contracting Party applying this Regulation shall refuse to grant or refuse to accept type approvals under this Regulation as amended by the XX series of amendments.

12.X.2. As from the official date of entry into force of the XX series of amendments, Contracting Parties applying this ~~UN~~ Regulation shall grant type approvals *for a vehicle equipped with an electro-mechanical braking system* only if the vehicle type to be approved meets the requirements of this Regulation as amended by the XX series of amendments.

12.X.3. As from 1 September 2027, Contracting Parties applying this Regulation shall not be obliged to accept type approvals to the preceding series of amendments, for a vehicle type having a braking system equipped with an electronic control system, first issued after 1 September 2027.

12.X.4. As from 1 September 2029, Contracting Parties applying this Regulation shall not be obliged to accept type approvals issued to the preceding series of amendments to this Regulation [, for a vehicle having a braking system equipped with an electronic control system].

12.X.5. Notwithstanding paragraph 12.X.4., Contracting Parties applying this Regulation shall continue to accept type approvals issued according to the preceding series of amendments to this Regulation, for the vehicles which are not affected by the changes introduced by the XX series of amendments [(i.e. for vehicles not having a braking system equipped with an electronic control system).]

12.X.6. Notwithstanding the transitional provisions above, Contracting Parties whose application of this Regulation comes into force after the date of entry into force of the most recent series of amendments are not obliged to accept type approvals which were granted in accordance with any of the preceding series of amendments to this Regulation/ are only obliged to accept type approval granted in accordance with the XX series of amendments.

12.Y. General transitional provisions:

12.Y.1. Contracting Parties applying this Regulation may grant type approvals according to any preceding series of amendments to this Regulation.

12.Y.2. Contracting Parties applying this Regulation shall continue to grant extensions of existing approvals to any preceding series of amendments to this Regulation

Replace Annex 18 with the following:

Annex 18

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 **Electronic System(s) (paragraph 2.3.) and** 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 shall be disclosed to the Technical Service, for type approval purposes.

This information shall show that "the system" respects, under ~~**normal**~~ **non-fault** and fault conditions, all the appropriate performance requirements specified elsewhere in this Regulation.

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 Regulation applies. This also includes any other system covered in the scope of this Regulation, as well as transmission links to or from other systems that are outside the scope of this Regulation, that acts on a function to which this 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** ~~**even**~~ 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-mechanical,** electro-pneumatic or electro-hydraulic elements.

"*The system*", referred to herein**,** is the one for which type approval is being sought.

2.4. "*Complex electronic* ~~***vehicle***~~ *control systems*" are those electronic control systems **in** which ~~**are subject to a hierarchy of control in which a controlled**~~ **a** function may be over-ridden by a higher-level electronic control system/function.

A function which is over-ridden becomes part of the complex **electronic control** system**, as well as any overriding system/function within the**

scope of this Regulation. The transmission links to and from overriding systems/function outside of the scope of this Regulation shall also be included.

2.5. "*Higher-level control*" systems/functions are those which employ additional processing and/or sensing provisions to modify vehicle behaviour by commanding variations in the normal 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 optical, pneumatic, hydraulic or mechanical.

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. **"Control strategy" means a strategy to ensure robust and safe operation of the function(s) of "The System" in response to the input from the vehicle or the driver.**

This may include the automatic deactivation of a function or temporary performance restrictions.

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, as specified in paragraph 3.4., to show that "The System":

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

(b) implements strategies which do not, under non-fault conditions, prejudice the safe operation of systems which are subject to the prescriptions of this Regulation; and,

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

(d) Was developed according to the development process/method ~~declared~~ chosen by the manufacturer according to 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. below) which shall be supplied to the Technical Service at the time of submission of the type-approval application. ~~**This will be taken**~~ **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 **confidential** material and analysis data (**intellectual property**) of paragraph 3.4.4., which shall be retained by the manufacturer, but made open for inspection **(e.g., on-site in the engineering facilities of the manufacturer)** 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.

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**~~ **explanation** 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. above) 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 electrical transmission links, by an optical-fibre diagram for optical 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 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 as far as this Regulation is concerned.

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 systems which are subject to the prescriptions of this Regulation.

The vehicle manufacturer shall supplement this statement by an explanation showing in overall terms how the chosen strategy ensures that "The System" objectives does not prejudice the safe operation of the systems referred above, and by a description of the part of the validation plan supporting the statement.

The Technical Service shall perform an assessment to establish that the vehicle manufacturer's explanation of the chosen strategy is understandable, logical and that the validation plan is suitable and have been completed.

The Technical Service may perform tests, or may require tests to be performed, as specified in paragraph 4. below, to verify that "the system" operates as per the chosen strategy.

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 ~~**be prepared, if required,**~~ to show ~~**some**~~ 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 authorities 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 ~~**one of those specified faults which will have a bearing on vehicle control performance or safety**~~ **fault identified by the procedure below 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)**, chosen by the manufacturer,** 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. This approach may be based on a Hazard / Risk analysis appropriate to system safety.

(b) Inspection of the safety approach at the system level. This approach 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 validation may 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 plan is suitable and ~~have~~ has been completed.

The Technical Service may perform tests, or may require tests to be performed, as specified in paragraph 4. below, 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. above, the warning signal to be given to the driver and/or to service/technical inspection personnel.

3.4.4.2. Where this Regulation contains particular requirements for the operation of "The System" under different environmental conditions, this documentation shall describe the measures in place to ensure compliance with those requirements.

4**.** Verification and test

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

4.1.1. Verification of the function of "the system"

~~**As the means of establishing the normal operational levels, verification of the performance of the vehicle system under non-fault conditions shall be conducted against the manufacturer's basic benchmark specification unless this is subject to a specified performance test as part of the approval procedure of this or another Regulation.**~~

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.

The verification of the performance of those selected functions shall be conducted following the manufacturer's test procedures unless a test procedure is specified in this Regulation.

For cases where the braking system is subject to input signal(s) from systems outside the scope of this Regulation, the test shall be conducted using the test procedure of the relevant UN regulation, or by another means that generates the relevant input signal(s), (e.g. simulation).

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. above

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 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.

4.2. Simulation tool and mathematical models for verification of the safety concept may be used in accordance with Schedule 8 of Revision 3 of the 1958 Agreement, in particular for scenarios that are difficult on a test track or in real driving conditions. Manufacturers shall demonstrate the scope of the simulation tool, its validity for the scenario concerned as well as the validation performed for the simulation tool chain (correlation of the outcome with physical tests).

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.

Insert new Annex 18, Appendix

Title: Annex 18 – Appendix. Model assessment form for electronic, and/or complex electronic, control systems

Test Report: UN Regulation 13, Annex 18

Test report No:

Identification

Vehicle make:

Type:

Means of identification of type if marked on the vehicle:

Location of that marking:

Manufacturer's name and address:

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

Manufacturer's formal documentation package:

Documentation reference No:

Date of original issue:

Date of latest update:

Test vehicle(s)/system(s) description:

2.1. General description:

2.2. Description of the functions of "The System", including control strategies (Annex 18, paragraph 3.2.):

2.2.1. List of input and sensed variables and their working range including a description the effect of the variable on system behaviour (Annex 18, paragraph 3.2.1.):

2.2.2. List of output variables and their range of control (Annex 18, paragraph 3.2.2.):

2.2.2.1. Directly controlled:

2.2.2.2. Controlled via another vehicle system:

2.2.3. Boundaries of functional operation (Annex 18, paragraph 3.2.3.):

2.3. Description System layout and schematics (Annex 18, Paragraph 3.3.):

2.3.1 Inventory of components (Annex 18, Paragraph 3.3.1.):

2.3.2 Functions of the units (Annex 18, Paragraph 3.3.2.):

2.3.3 Interconnections (Annex 18, Paragraph 3.3.3.):

2.3.4 Signal flow and priorities (Annex 18, Paragraph 3.3.4.):

2.3.5 Identification of units (hardware & software) (Annex 18, Paragraph 3.3.5.):

3. Manufacturer's safety concept.

3.1. Manufacturer's declaration (Annex 18, Paragraph 3.4.1.):

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.

3.2. Software (outline architecture, software design methods and tools used) (Annex 18, Paragraph 3.4.2.):

3.3. Explanation of design provisions built into "The System" under fault conditions (Annex 18, Paragraph 3.4.3.):

3.4. Documented analyses of the behaviour of "The System" under individual fault conditions (Annex 18, Paragraph 3.4.4.1.):

3.4.1. Parameters monitored:

3.4.2. Warning signals generated:

3.5. Description of the measures in place for environmental conditions (Annex 18, Paragraph 3.4.4.2.):

3.6. Provisions for the periodic technical inspection of "The System" (Annex 18, Paragraph 3.1.).

Description of the method by which the operational status of the system can be checked:

4. Verification and test

4.1. Verification of the function of "The System" (Annex 18, Paragraph 4.1.1.):

4.1.1. List of the selected functions and a description of the test procedures used:

4.1.2. Test results verified according to Annex 18, paragraph 4.1.1.1. Yes/No

4.2. Verification of the system safety concept (Annex 18, Paragraph 4.1.2.):

4.2.1. Unit(s) tested and their function:

4.2.2. Simulated fault(s):

4.2.3. Test results verified according to Annex 18, paragraph 4.1.2. Yes/No.

4.3. Date of test:

4.4. This test has been carried out and the results reported in accordance with Annex 18 to UN Regulation No. 13 as last amended by the …… series of amendments.

Technical Service carrying out the test:

Signed: ..... **Date: .....**

4.5. Comments:

_____