Transmitted by the Expert from the United Kingdom

Informal document **GRVA-13-19**
13th GRVA, 23-27 May 2022
Provisional agenda item 8(b)

Proposal for amendments to UN Regulation No. 13

The text reproduced below was prepared by the Expert from the United Kingdom. The proposal seeks to align the requirements of UN Regulation 13 concerning the assessment of electronic control systems with the latest developments adopted by WP.29 for UN Regulations No. 79 and No. 157. It is intended that this amendment is introduced in parallel to the requirements being developed for electromechanical braking systems (ECE/TRANS/WP.29/GRVA/2022/8). The proposed changes are marked in strikethrough characters for deleted text and in bold characters for added text.

I. Proposal

Contents, Annex 18 title, amend to read:

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

Annex 18, amend to read:

Annex 18

SPECIAL REQUIREMENTS TO BE APPLIED TO THE SAFETY ASPECTS OF ~~**COMPLEX**~~ ELECTRONIC VEHICLE CONTROL SYSTEMS

1. GENERAL

This annex is intended to ensure that an acceptable thorough consideration of functional and operational safety for the system(s) that provides the function(s) regulated by this UN Regulation has been performed by the manufacturer during the design and development processes and will continue to be done throughout the vehicle type lifecycle (design, development, production, field operation, decommissioning).

It covers the documentation which must be disclosed by the manufacturer to the type-approval authority or the technical Service acting on its behalf (hereafter referred as type-approval authority), for type approval purposes.

This documentation shall demonstrate that the systems meet the performance requirements specified in this UN Regulation, that they are designed and developed to operate in such a way that they are free of unreasonable safety risks to the driver, passengers and other road users.

~~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 2.4.**. below) as far as this Regulation is concerned.~~

This annex shall also apply to safety related functions identified in this Regulation which are controlled by electronic system(s) (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 and that it is designed to operate in such a way that it does not induce safety critical risks.**

The type-approval authority granting the approval shall verify the reasoning provided by the documentation is strong enough and that the design and processes described in documentation are actually implemented by the manufacturer.

While based on the provided documentation, evidence and process audits/product assessments carried out to the satisfaction of the type-approval authority concerning this UN Regulation, the residual level of risk of the assessed system(s) is deemed to be acceptable for the entry into service of the vehicle type, the overall vehicle safety during system lifetime in accordance with the requirements of this regulation remains the responsibility of the manufacturer requesting the type-approval.

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.~~1.~~2. "Safety concept" is a description of the measures designed into the system, for example within the electronic units, **so that the vehicle operates in such a way that it is free of unreasonable safety risks to the driver, passengers and other road users 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.~~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 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, **electro-mechanical** or electro-hydraulic elements.

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

2.~~3.~~4. "Complex electronic vehicle control systems" are those electronic control systems **in which a function controlled by an electronic system or the driver ~~which are subject to a hierarchy of control in which 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**, 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.**

2.4.~~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 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.~~5.~~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.~~6.~~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.~~7.~~8. "Range of control" refers to an output variable and defines the range over which the system is likely to exercise control.

2.~~8.~~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 operating conditions.**

2.12. ***"Functional safety":*** **absence of unreasonable risks under the occurrence of hazards caused by a malfunctioning behaviour of electric/electronic systems (safety hazards resulting from system faults).**

2.13. ***"Fault":*** **abnormal condition that can cause an element (system, component, software) or an item (system or combination of systems that implement a function of a vehicles) to fail.**

2.1.4. ***"Failure"*** **means the termination of an intended behaviour of an element or an item.**

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 Type Approval Authority 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 risks for the driver, passengers or other road users.,

(b) Respects, under non-fault and fault conditions, all the appropriate performance requirements specified elsewhere in this 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**~~ **Type Approval Authority** at the time of submission of the type approval application. **This documentation package shall be used by the Type Approval Authority** ~~**This will be taken**~~ as the basic reference for the verification process set out in paragraph 4. of this annex**. The Type Approval Authority 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. 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"

A description shall be provided which gives a simple explanation of all the ~~**control**~~ functions**, including the 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.) 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 **and/or operating data** carried between units.

Priorities of signals **and/or operating data** 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 software version can be changed without requiring replacement of the marking or component, the software identification must be by software output only.**

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, **to** 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.

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 (See Paragraph 3.5.1.). 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**~~ **Type Approval Authority** with an explanation of the design provisions built into "The System " ~~so as to generate safe operation~~ **ensure functional and operational safety** 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** ~~**of those specified faults**~~ which will have a bearing on vehicle control performance or **the** safety **of the driver, passengers or other road users**.

~~**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**~~ **Type Approval Authority** at the time of the type approval.

The Type Approval Authority shall perform an assessment of the application of the analytical approach(es):

(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 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), a System-Theoretic Process or any similar process appropriate to system functional and operational safety.

(c) Inspection of the validation plans and results, including appropriate acceptance criteria. 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 Type Approval Authority shall perform or shall require confirmatory tests to be performed 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. ~~**above 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 free from unreasonable risks for the driver, vehicle occupants, and other road users when the performance of "The System" is affected by environmental conditions e.g., climatic, temperature, dust ingress, water ingress, ice packing.

3.5. Safety management system (Process Audit)

3.5.1. In respect of software and hardware employed in "The System", the manufacturer shall demonstrate to the Type Approval Authority in terms of a safety management system that effective processes, methodologies and tools are in place, up to date and being followed within the organization to manage the safety and continued compliance throughout the product lifecycle (design, development, production, operation including respect of traffic rules, and decommissioning).

3.5.2. The design and development process shall be established including safety management system, requirements management, requirements' implementation, testing, failure tracking, remedy and release

3.5.3. The manufacturer shall institute and maintain effective communication channels between manufacturer departments responsible for functional/operational safety, cybersecurity and any other relevant disciplines related to the achievement of vehicle safety.

3.5.4. The manufacturer shall demonstrate that periodic independent internal process audits are carried out to ensure that the processes established in accordance with paragraphs 3.5.1 to 3.5.4. are implemented consistently.

3.5.5. Manufacturers shall put in place suitable arrangements (e.g., contractual arrangements, clear interfaces, quality management system) with suppliers to ensure that the supplier safety management system comply with the requirements of paragraphs 3.5.1. (except for vehicle related aspects like "operation" and "decommissioning"), 3.5.2, 3.5.3 and 3.5.5.

4. VERIFICATION AND TEST

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 Type Approval Authority shall verify "The System" under non-fault / non-failure conditions by testing a number of selected functions from those declared by the manufacturer in paragraph 3.2. above.

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

~~**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.**~~

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 Type Approval Authority 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.**

4.1.2.1. The verification results shall correspond with the documented summary of the ~~**failure**~~ **hazard** analysis, to a level of overall effect such that the safety concept and execution are confirmed as being adequate **and in compliance with the requirements of this Regulation**.

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.

6. COMPETENCE OF THE AUDITORS/ASSESSORS

The assessments under this Annex shall only be conducted by auditors/assessors with the technical and administrative knowledge necessary for such purposes. They shall in particular be competent as auditor/assessor for ISO 26262-2018 (Functional Safety - Road Vehicles), and ISO/PAS 21448 (Safety of the Intended Functionality of road vehicles); and shall be able to make the necessary link with cybersecurity aspects in accordance with UN Regulation No 155 and ISO/SAE 21434). This competence should be demonstrated by appropriate qualifications or other equivalent training records.

Annex 18 - Appendix 1

Model assessment form for electronic systems

Test report No: .....

1. Identification

1.1. Vehicle make: .....

1.2. Vehicle Type: .....

1.3. Means of system identification 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 "The System" is free from unreasonable risks for the driver, vehicle occupants and other road users.

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 18 to UN Regulation No. 13:.....

3.9. Results of safety concept verification test, as per para. 4.1.2. of Annex 18 to UN Regulation No. 13:.....

3.10. Date of test:.....

3.11. This test has been carried out and the results reported in accordance with UN Regulation No. 13 as last amended by Supplement […] to the 11 series of amendments.

Technical Service[1] carrying out the test

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

3.12. Type Approval Authority[1]

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

Comments:

Footnote [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.**

II. Justification

1. During the development of UN Regulation No. 79 the informal working group identified the necessity to review the content of Annex 6 which is concerned with the safety of electronic systems. The group identified that there was an inconsistent understanding of the requirements of Annex 6 by all parties. It also identified areas of improvement that could be made to reflect the design and production of modern electronic systems and to ensure more consistent application during the type-approval process. Significant amendments were proposed to this annex; these were agreed by GRRF and then adopted by WP.29. The revised Annex can be found in document ECE/TRANS/505/Rev.1/Add.78/Rev.4. which entered into force on 18 October 2018.

2. Developments with regard to new Regulations concerning cyber security (R.155) and software management (R.156) were recognised during the development of UN Regulation No. 157 (Automated Lane Keeping Systems - ECE/TRANS/505/Rev.3/Add.156). These were addressed in Annex 4 to this regulation together with some further refinements to the provisions for electronic control system safety.

3. This proposal to amend Annex 18 of UN Regulation 13 and align it with the most recent developments of electronic system assessment. The proposed amendments replicate the requirements adopted by WP.29 on the recommendations pf GRRF/GRVA in recent times and the methodology is completely compatible and in line with those that are likely to be employed during the approval of other advanced systems on the vehicle.