Submitted by the United Kingdom on behalf of the
GRRF Group of Interested Experts

Informal document **GRRF-85-01-Rev.1**
85th GRRF, 11 December 2017
Agenda item 2

Regulation 79: Proposals for changes to Annex 6

This document represents the progress made by an informal group of experts in reviewing the content of Annex 6 since the 84th session of GRRF. The proposal has the purpose of clarifying the purpose of Annex 6 and ensuring its suitability when used in the assessment of steering systems featuring advances in automation.

I. Proposal

Insert new paragraph 12.7., to read:

[12.7. **As a derogation, Annex 6 to this Regulation, as amended by [Supp.1 to the O2 series of amendments], shall not be applicable when granting extensions to approvals for Auxiliary Steering Equipment approved to earlier versions of this Regulation and when assessed in accordance with Annex 4 to this Regulation.]**

Annex 6

Title amend to read:

SPECIAL REQUIREMENTS TO BE APPLIED TO THE SAFETY ASPECTS OF ~~COMPLEX~~

ELECTRONIC ~~VEHICLE~~ CONTROL SYSTEMS

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

"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~~**4**. below) as far as this Regulation is concerned.

This annex ~~may~~ **shall** also **apply** ~~be called, by special paragraphs in this Regulation, for~~ **to** safety related functions identified in this Regulation which are controlled by electronic system(s) **(paragraph 2.3.) as far as this Regulation is concerned**.

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**.

Insert new paragraph 2.1., discussion on new definition to read:

"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.

Paragraph 2.1. (former), amend to read and renumber:

"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.

Paragraph 2.2. (former), amend to read and renumber:

"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 or electro-hydraulic elements. ~~"The System", referred to herein, is the one for which type approval is being sought.~~

Paragraph 2.3. (former), discussion on amending and renumber:

"2.4. "Complex electronic vehicle control systems" are those electronic control systems ~~which are subject to a hierarchy of control~~ in which a ~~controlled~~ 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 ~~function~~ become~~s~~ 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**.**]**

Paragraph 2.4. (former), discussion on amending and renumber:

"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 ~~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.

Paragraphs 2.5. to 2.8. (former), no changes and renumber to 2.6. to 2.9.

Insert new Paragraph 2.10. 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.

Paragraph 3.1., amend to read:

"3.1. …

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

- **is designed to operate, under non-fault and fault conditions, in such a way that it does not induce safety critical risks**

- **Respects, under non-fault and fault conditions, all the appropriate performance requirements specified elsewhere in this Regulation, and**
- **Was developed according to the development process/method declared by the manufacturer**

Paragraph 3.1.1., amend to read:

"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** ~~will be taken~~ 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 [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.]** "

Paragraph 3.2., discussion on amending:

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

[These declarations shall include any functions that are present but not enabled at the time of type approval. However, functions that cannot be performed with the hardware combination presented for approval are exempt.]

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

Paragraph 3.3.3., amend to read:

"3.3.3. 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.**

Paragraph 3.3.4., discussion on amending to read:

"3.3.4. Signal flow **and operating data** 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~~.

Paragraph 3.4.1., discussion on amending:

"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** ~~systems which are subject to the prescriptions of this Regulation~~.

Paragraph 3.4.2., amend to read:

"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.

Paragraph 3.4.3., amend to read:

"3.4.3. The Manufacturer shall provide the ~~technical authorities~~ **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:

…

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~~ **individual** ~~of those specified~~ **hazard or** fault~~s~~ 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 assessment 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 approach shall be based on a Hazard / Risk analysis appropriate to system safety.**
- **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.**
- **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 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.

Insert new paragraph 3.4.4.2., to read:

"**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.**

Paragraph 4.1.1., amend to read:

"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 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 at least [10%] of the functions declared by the manufacturer in paragraph 3.2.

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

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 an~~y~~ 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).

Insert new Paragraph 5., to read:

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 Appendix 1, 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:.....

1.3.1. Location of that marking:.....

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

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

1.6. 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 4.1.1. of this Annex: .....

3.9. Results of safety concept verification test, as per 4.1.2. of this Annex:.....
.....

3.10. Date of test: .....

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

Technical Service 1/ carrying out the test
Signed: ..... Date: .....

3.12. Approval Authority 1/
Signed: ..... Date: .....

3.13. 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.**]**