Submitted by the chair of GRRF on behalf of the
Informal Group concerning Complex Electronic Systems

Informal document **GRRF-84-14**
84th GRRF, 19-22 September 2017
Agenda item 9

Working Document: Revision of Annex 6 to UN ECE Regulation 79

This document represents the progress made by an informal group of experts in reviewing the content of Annex 6. The review 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.

It is provided to GRRF for information. A revision to paper, based upon a further meeting of the informal group, will be provided to GRRF 84.

I. Proposal

Amend paragraph 5.1.10., to read:

[5.1.11. **…**

Manual steering equipment and power-assisted steering equipment are exempted from the application of Annex 6 to this Regulation, provided they are not part of a complex system as defined in paragraph 2.4 of Annex 6 to this Regulation.]

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

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

"1. General

…

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).

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.

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 in such a way that it does not induce a response that negatively affects the safety**
- **is designed so that it in fault condition does not induce a risk or can be permanently switched off without affecting the performance of other systems.**

- **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.

…

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.**]**

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. 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~~**]**.

Insert new paragraph 3.3.4.1., discussion on new requirement to read:

["3.3.4.1. Any function which can affect the fulfilment of the requirements of this [Annex / Regulation], shall be declared by the manufacturer. The declaration shall include a description of the rationale of the function's operation.

In addition, 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.

These declarations shall include any functions that are present but not enabled at the time of type approval.]

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 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~~ of those ~~specified~~ **hazards or** faults 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 may be based on a Hazard and Operability analysis (HAZOP) or any similar process appropriate to system safety.**
- **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.**
- **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 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.]

Insert new paragraph 3.4.4.2., to read:

["3.4.4.2. This documentation shall describe the resistance of "The System" to environmental influences, e.g. climate and mechanical resistance.]

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~~ **The Technical Service shall verify "The System"** under non-fault conditions **by randomly testing at least [10%] of the instances where a function to which this Regulation applies can be over-ridden, as declared by the manufacturer in 3.3.4.1. The requirements of this Regulation shall not be comprised when any function to which this Regulation applies is overridden.** ~~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.~~**]**

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 vehicle manufacturer may propose to the Technical Service when is the most relevant time during the development process to perform the test, provided the system is at a sufficient technical level reflecting the final production of the system to be approved.]**

[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 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 report from the technical service to the type approval authority is given in the template in Part II of this document.]

[II. Example of Report Layout

Nr. 01-05

Type-Approval Procedure

Information System of the German Type-Approval Authority

0. **General data**

0.1 Vehicle make:

0.2 Type:

0.3 Idenfication mark: (if applicable)

0.4 Name and address of the manufacturer:

0.4.1 Name and address of the appointee:

0.5 Information folder or documentation

No.:

Date of issue:

Date of last update:

Type-Approval Procedure
Information System of the German Type-Approval Authority

1. Test vehicle(s) / object(s)

1.1 General description: *N.B.: Information to be provided either here or as an attachment*

General description of the complex electronic system with its main components and functions, as well as brief explanation of the safety concept and of the possibility of testing the operating condition of the system as part of the periodic technical inspections *(see, for instance, ECE Regulation 13, Annex 18, paragraph 3.1)*

1.2 Description of the control function: *N.B.: Information to be provided either here or as an attachment*

Specific description of all control functions and
- list of all input and measurement variables,
- list of all output variables,
- boundaries within which the system functions *(see, for instance, ECE Regulation 13, Annex 18, paragraph 3.2)*

1.3 Description of the components: *N.B.: Information to be provided either here or as an attachment*

Specification (in list form) of the discrete functional units
with their respective
- combinations of assembly in the system,
- linkages and signal flow priorities,
- information regarding the identifiability of hard- and software *(see, for instance, ECE Regulation 13, Annex 18, paragraph 3.3)*

2. Manufacturer's safety concept *N.B.: Information to be provided either here or as an attachment*

2.1 Manufacturer's declaration:

The manufacturer(s) XXX has/have confirmed that the strategy chosen for the achievement of the objectives of the "system", assuming flawless conditions, does not interfere with the safe operation of parts of the equipment required under this regulation *(e.g. braking device)* (see appendix).

2.2 Hard and Software development:

Specification of the documents in which the software development process is described. Description/diagram of the software development process including the software design factors

2.3 Function in case of errors in the system:

General description of the fallback, change or shut-off functions and any possible partial operation functions, including their conditions and boundaries of their effectiveness in the event of
any failures in the "system"

Description of the simulated malfunction

2.4 Analysis of the behavior of the "system" in case of errors:

Description of the results and confirmation by the Technical Service that the corresponding documentation *(for instance in accordance with ECE Regulation 13, Annex 18, paragraph 3.4.4)* can be accessed by the approval authority through the manufacturer under its reference number XXXX.

Specification of the documents evidencing the verification of the fault-free performance of the vehicle system in operation.

2.5 Resistance against environmental influences:

E.g. type and scope of tests on climate and mechanical resistance and electromagnetic compatibility

2.6 Testability of the system:

Description of the possibility of testing the operating condition of the system as part of the periodic technical inspections

2.7 General information:

Test location:

Test date:

2.8 Comments:

3. Appendices:

Appendix 1: *e.g. list of changes*

Appendix 2: *e.g. general description regarding 1.1*

Appendix 3: *e.g. manufacturer's declaration regarding 2.1*

...

4. Final certificate
Statement of conformity

The information folder referred to under item 0.5. and the type described therein – do conform – to the above-mentioned test specification.

This test report consists of pages 1 to 5.

TEST LABORATORY

accredited by the Accreditation Office of the Federal Motor Vehicle Department,
Federal Republic of Germany

City Date

Order number

E-mail: firstname.lastname@td.de

Phone: XXX
Fax: YYY

Signature

Chartered Engineer

Name (please print):

]