Note by the secretariat

Informal document **GRRF-83-29**
83rd GRRF, 23-27 January 2017
Agenda item 9(b)

Proposal for amendments to ECE/TRANS/WP.29/GRRF/2017/8

I. Proposal

Annex 6

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

"1. General

…

~~**Involvement of the technical service at an early stage in the design process is recommended for an effective assessment of "The System" to the requirements of this annex.**~~"

This information shall show that "The System" respects, under normal and fault conditions, all the appropriate performance requirements specified elsewhere in this Regulation **and that it operates in such a way that it does not induce any safety critical situations**".

[Paragraph 2.3., amend to read:

2.3. "Complex electronic vehicle control systems" are those electronic control systems which ~~are subject to a hierarchy of control in which~~ **may override** 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.]

Paragraph 3.2., amend to read:

"3.2. Description of the **design process methodology and** functions of "The System"

A description ~~should~~ shall be provided of the methodology applied for the design of "The System", which includes the processes and standards followed within the design and development life cycle[, for example for the automotive industry these may include ISO 26262, MISRA C and Automotive SPICE]. The application of the methodology shall be demonstrated by an assessment report ~~established~~ made by a [competent authority] [Technical Service [/ third party]]. [This may include a certificate of accreditation issued by an accreditation body.]"

Paragraph 3.4.1., amend to read:

"3.4.1. The manufacturer shall provide a statement which affirms that the strategy chosen to achieve "The System" objectives will not, under **fault and** non-fault conditions, prejudice the safe operation of systems which are subject to the prescriptions of this Regulation."

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~~ ~~identified~~ **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 audit 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. This may include Hardware in the Loop (HIL) testing and vehicle on–road operational testing with expert and/or non-expert drivers or any similar testing appropriate for validation.**

The audit 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 ~~Recommendations~~ may ~~be made for~~perform or may require to perform ~~—~~tests as specified ~~to be performed~~ in paragraph 4. to verify [/ be satisfied with] 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, mechanical resistance and electromagnetic compatibility.**"] (Here or in the core of the 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 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 verify ~~It is recommended ~~] that these tests include aspects that impact on vehicle controllability and user information (HMI aspects)."

Paragraph 5., amend to read:

5. Reporting by technical service

Reporting of the audit 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. <u>Test vehicle(s) / object(s)</u>

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 – d o con-f o r m – to the above-mentioned test specification.

This test report consists of pages 1 to 5.

This test report may be reproduced and distributed only by the client and only in its entirety. Any partial reproduction and publication of the test report is permissible only with the prior written approval of the test laboratory.

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):