Transmitted by the Russian Federation

Informal document **GRVA-05-51**
5th GRVA session, 10-14 February 2020
Agenda item 5(a)

Proposal for amendments to GRVA-05-05

Note: This document reflects on the discussion around GRVA-05-05 with regards to the proposals introduced verbally by the expert from the Russian Federation.

I. Proposal

A. Amendments to para. 5 to introduce the use of DETA

5.3. Approval Authorities shall not grant any type approval without verifying that the manufacturer has put in place satisfactory arrangements and procedures to manage properly the cyber security aspects as covered by this Regulation.

~~[~~5.3.1. ~~Each Approval Authority shall actively inform and seek guidance from other Approval Authorities before making the decision grant a type approval under this Regulation. To this effect, the Approval Authority concerned shall notify the Approval Authorities applying this Regulation of the draft approval decision, together with the description of the method and criteria of assessment employed by the Approval Authority. The documents referred to in paragraph 3.3 and the results of the tests performed pursuant to paragraph 5.1.2. shall be open for inspection by the Approval Authorities applying this Regulation, except where the manufacturer notifies, with the notifying Approval Authority, opposition to the inspection of designated part of the documentation, no later than at the moment of notification.~~

~~5.3.2. Each Approval Authority applying this Regulation may notify the other Parties, within 30 calendar days, its reasoned reservations with regard to the whole or the part of the decision notified. Subsequently, the Approval Authority shall notify to the Approval Authorities applying this Regulation the draft decision revised taking into account the reservations received.~~

~~5.3.3. If at least two Parties notify, within 30 calendar days, reasoned reservations to this draft decision, the Approval Authority shall not adopt a type approval decision. In this case, the draft type approval decision, together with the description of the method and criteria of assessment employed by the Approval Authority, and the reservations notified pursuant to this section shall be referred to the Chair of the World Forum for Harmonization of Vehicle Regulations (WP.29) and to the Chair of the subsidiary Working Party as diverging interpretations within the meaning of Schedule 6 to the [1958 Agreement]. The procedure provided for in paragraph 3 of Schedule 6 shall apply. The documents referred to in paragraph 3.3.of this Regulation and the results of the tests performed pursuant to paragraph 5.1.2. shall be open for inspection by the Chair of WP.29 and the Chair of the subsidiary Working Party on the same conditions as those set out in paragraph 5.3.1. above.~~

~~5.3.4. The interpretation agreed in the Working Party shall be implemented and the approval authority shall issue UN type approval accordingly.]~~

5.4. **The type approvals together with the supplemented documentation shall be uploaded by the Approval Authority to the the secure internet database established by the United Nations Economic Commission for Europe (DETA).**

5.5. **The type approvals together with the supplemented documentation shall be subject to review by the Oversight Committee consisting of the representatives of the Approval Authorities of the Contracting Parties (the Commitee). The Committee shall assess the relevance of the uploaded type approvals with the criteria stipulated in this UN Regulation. If the Committee decides by consensus that a type approval is not fully relevant with the said criteria, the Committee shall, if necessary, propose corrections to this UN Regulation in order to avoid the discovered discrepancies in future. The Committee may also recommend the Approval Authority issued the type approval to withdraw it.**

~~5.4.~~ **5.6**. For the purpose of paragraph 7.2. of this Regulation, the manufacturer shall ensure that the cyber security aspects covered by this Regulation are implemented.

B. Extract from ISO 17021 :2011 plus GRVA-05-29

Note : The text reproduced below is an extract from ISO 17021 :2011 (not the latest version). The paragraph numbers from ISO 17021 :2011 are kept for the reasons of traceability. The paragraphs considered as not relevant are deleted. The blue text requires alignment with the provisions of the draft UN Regulation on Cybersecurity. The green text incorporates the requirements to the Technical Services as proposed by France in GRVA-05-29 picked up with paragraph numbers.

7.5. Requirements for audit process

9.1 General requirements

X.X. Technical Services performing the audit

5.3.1 To conduct assessments the technical services shall be designated by the Approval Authority which will issue the Certificate of Compliance for the Cyber Security Management System and the approval of the vehicle type with regard to Cyber Security.

5.3.2. Technical Services shall demonstrate appropriate cyber security skills and specific automotive risk assessments knowledge and proven associated experience. In addition, technical services shall comply with the relevant applicable standards for cyber security.

5.3.4. The Technical Service shall have competent personnel and implemented procedures for the uniform evaluation according to the current regulation. These procedures shall be made available for the manufacturer and the Type Approval Authority.

5.3.4. The Technical Service shall operate independently of external influences.

9.1.1 Audit programme

9.1.1.1 An audit programme shall be developed to clearly identify the audit activity(ies) required to demonstrate that the client's Cyber Security Management System fulfils the requirements stipulated in paragraphs 7.2. and 7.3. of this Regulation.

9.1.1.2 The audit programme shall consider the size of the client organization, the scope and complexity of its management system, products and processes as well as demonstrated level of management system effectiveness.

NOTE 1

Annex E is a flowchart of a typical third-party audit and certification process.

NOTE 2

Annex F lists additional items that can be considered when developing or revising an audit programme.

9.1.2 Audit plan

9.1.2.1 General

The Technical Service shall ensure that an audit plan is established for each audit identified in the audit programme to provide the basis for agreement regarding the conduct and scheduling of the audit activities. This audit plan shall be based on documented requirements of the Technical Service.

9.1.2.2 Determining audit objectives, scope and criteria

9.1.2.2.1 The audit objectives shall be determined by the Technical Service. The audit scope and criteria, including any changes, shall be established by the Technical Service after discussion with the manufacturer.

9.1.2.2.2 The audit objectives shall describe what is to be accomplished by the audit and shall include the following:

a) determination of the conformity of the manufacturer's cybersecurity management system, or parts of it, with audit criteria;

b) evaluation of the ability of the cybersecurity management system to ensure the manufacturer meets applicable requirements of this UN Regulation;

c) evaluation of the effectiveness of the cybersecurity management system to ensure the manufacturer organization is continually meeting its specified objectives;

d) as applicable, identification of areas for potential improvement of the cybersecurity management system.

9.1.2.2.3 The audit scope shall describe the extent and boundaries of the audit, such as activities and processes to be audited.

NOTE Annex F lists additional items that can be considered when preparing or revising the audit scope.

9.1.2.2.4 The audit criteria shall be used as a reference against which conformity is determined, and shall include:

a) the requirements of a defined manufacturer’s normative document on cybersecurity management systems;

b) the defined processes and documentation of the cybersecurity management system developed by the manufacturer.

9.1.2.3 Preparing the audit plan

The audit plan shall be appropriate to the objectives and the scope of the audit. The audit plan shall at least include or refer to the following:

a) the audit objectives;

b) the audit criteria;

c) the audit scope, including identification of the vehicle types and processes to be audited;

d) the dates and sites where the on-site audit activities are to be conducted, including visits to temporary sites, as appropriate;

e) the expected time and duration of on-site audit activities;

f) the roles and responsibilities of the audit team members and accompanying persons.

NOTE 1 The audit plan information can be contained in more than one document.

NOTE 2 Annex F lists additional items that can be considered when preparing or revising the audit plan.

9.1.3 Audit team selection and assignments

9.1.3.1 The Technical Service shall have a process for selecting and appointing the audit team, including the audit team leader, taking into account the competence needed to achieve the objectives of the audit. If there is only one auditor, the auditor shall have the competence to perform the duties of an audit team leader applicable for that audit.

9.1.3.2 In deciding the size and composition of the audit team, consideration shall be given to the following:

a) audit objectives, scope, criteria and estimated time of the audit;

c) the overall competence of the audit team needed to achieve the objectives of the audit;

f) whether the members of the audit team have previously audited the cybersecurity management systems.

9.1.3.3 The necessary knowledge and skills of the audit team leader and auditors may be supplemented by technical experts, translators and interpreters who shall operate under the direction of an auditor. Where translators or interpreters are used, they are to be selected such that they do not unduly influence the audit.

NOTE The criteria for the selection of technical experts are determined on a case-by-case basis by the needs of the audit team and the scope of the audit.

9.1.3.4 Auditors-in-training may be included in the audit team as participants, provided an auditor is appointed as an evaluator. The evaluator shall be competent to take over the duties and have final responsibility for the activities and findings of the auditor-in-training.

9.1.3.5 The audit team leader, in consultation with the audit team, shall assign to each team member responsibility for auditing specific processes, functions, sites, areas or activities. Such assignments shall take into account the need for competence, and the effective and efficient use of the audit team, as well as different roles and responsibilities of auditors, auditors-in-training and

technical experts. Changes to the work assignments may be made as the audit progresses to ensure achievement of the audit objectives.

9.1.4 Determining audit time

9.1.4.1 The Technical Service shall have documented procedures for determining audit time, and for each manufacturer the Technical Service shall determine the time needed to plan and accomplish a complete and effective audit of the manufacturer's cybersecurity management system. The audit time determined by the Technical Service, and the justification for the determination, shall be recorded. In determining the audit time, the Technical Service shall consider, among other things, the following aspects:

a) the requirements of the relevant cybersecurity management system standard;

b) size and complexity;

c) technological and regulatory context;

d) any outsourcing of any activities included in the scope of the cybersecurity management system;

e) the results of any prior audits of the same manufacturer;

g) the risks associated with the products, processes or activities of the manufacturer/

9.1.4.2 The time spent by any team member that is not assigned as an auditor (i.e. technical experts, translators, interpreters, observers and auditors-in-training) shall not count in the above established audit time.

NOTE The use of translators, interpreters can necessitate additional audit time.

9.1.6 Communication of audit team tasks

The tasks given to the audit team shall be defined and shall be made known to the manufacturer, and shall require the audit team to

a) examine and verify the structure, policies, processes, procedures, records and related documents of the manufacturer organization relevant to the cybersecurity management system,

b) determine that these meet all the requirements relevant to the intended scope of type approval,

c) determine that the processes and procedures are established, implemented and maintained effectively, to provide a basis for confidence in the manufacturer's cybersecurity management system, and

d) communicate to the manufacturer, for its action, any inconsistencies between the client's policy, objectives and targets (consistent with the expectations in the relevant management system standard or other normative document) and the results.

9.1.7 Communication concerning audit team members

The Technical Service shall provide the name of and, when requested, make available background information on each member of the audit team, with sufficient time for the manufacturer’s organization to object to the appointment of any particular auditor or technical expert and for the Technical Service to reconstitute the team in response to any valid objection.

9.1.8 Communication of audit plan

The audit plan shall be communicated and the dates of the audit shall be agreed upon, in advance, with the manufacturer.

9.1.9 Conducting on-site audits

9.1.9.1 General

The Technical Service shall have a process for conducting on-site audits. This process shall include an opening meeting at the start of the audit and a closing meeting at the conclusion of the audit.

NOTE In addition to visiting physical location(s) (e.g. factory), “on-site” can include remote access to electronic site(s) that contain(s) information that is relevant to the audit of the cybersecurity management system.

9.1.9.2 Conducting the opening meeting

A formal opening meeting, where attendance shall be recorded, shall be held with the manufacturers's management and, where appropriate, those responsible for the functions or processes to be audited. The purpose of the opening meeting, which shall usually be conducted by the audit team leader, is to provide a short explanation of how the audit activities will be undertaken and shall include the following elements. The degree of detail shall be consistent with the familiarity of the manufacturer with the audit process:

a) introduction of the participants, including an outline of their roles;

b) confirmation of the scope of type approval;

c) confirmation of the audit plan (including type and scope of audit, objectives and criteria), any changes, and other relevant arrangements with the manufacturer, such as the date and time for the closing meeting, interim meetings between the audit team and the manufacturer's management;

d) confirmation of formal communication channels between the audit team and the manufacturer;

e) confirmation that the resources and facilities needed by the audit team are available;

f) confirmation of matters relating to confidentiality;

g) confirmation of relevant work safety, emergency and security procedures for the audit team;

h) confirmation of the availability, roles and identities of any guides and observers;

i) the method of reporting, including any grading of audit findings;

j) information about the conditions under which the audit may be prematurely terminated;

k) confirmation that the audit team leader and audit team representing the Technical Service is responsible for the audit and shall be in control of executing the audit plan including audit activities and audit trails;

l) confirmation of the status of findings of the previous review or audit, if applicable;

n) confirmation of the language to be used during the audit;

o) confirmation that, during the audit, the manufacturer will be kept informed of audit progress and any concerns;

p) opportunity for the manufacturer to ask questions.

9.1.9.3 Communication during the audit

9.1.9.3.1 During the audit, the audit team shall periodically assess audit progress and exchange information. The audit team leader shall reassign work as needed between the audit team members and periodically communicate the progress of the audit and any concerns to the client.

9.1.9.3.2 Where the available audit evidence indicates that the audit objectives are unattainable or suggests the presence of an immediate and significant risk (e.g. safety), the audit team leader shall report this to the manufacturer and, if possible, to the Technical Service to determine appropriate action. Such action may include reconfirmation or modification of the audit plan, changes to the audit objectives or audit scope, or termination of the audit. The audit team leader shall report the outcome of the action taken to the certification body.

9.1.9.3.3 The audit team leader shall review with the manufacturer any need for changes to the audit scope which becomes apparent as on-site auditing activities progress and report this to the Technical Service.

9.1.9.4 Observers and guides

9.1.9.4.1 Observers

The presence and justification of observers during an audit activity shall be agreed to by Technical Service and client prior to the conduct of the audit. The audit team shall ensure that observers do not influence or interfere in the audit process or outcome of the audit.

NOTE Observers can be members of the manufacturer's organization, consultants, witnessing accreditation body personnel, regulators or other justified persons.

9.1.9.4.2 Guides

Each auditor shall be accompanied by a guide, unless otherwise agreed to by the audit team leader and the manufacturer. Guide(s) are assigned to the audit team to facilitate the audit. The audit team shall ensure that guides do not influence or interfere in the audit process or outcome of the audit.

NOTE The responsibilities of a guide can include:

a) establishing contacts and timing for interviews;

b) arranging visits to specific parts of the site or organization;

c) ensuring that rules concerning site safety and security procedures are known and respected by the audit team members;

d) witnessing the audit on behalf of the manufacturer;

e) providing clarification or information as requested by an auditor.

9.1.9.5 Collecting and verifying information

9.1.9.5.1 During the audit, information relevant to the audit objectives, scope and criteria (including information relating to interfaces between functions, activities and processes) shall be collected and verified to become audit evidence.

9.1.9.5.2 Methods to collect information shall include, but are not limited to:

a) interviews;

b) observation of processes and activities;

c) review of documentation and records.

9.1.9.6 Identifying and recording audit findings

9.1.9.6.1 Audit findings summarizing conformity and detailing nonconformity and its supporting audit evidence shall be recorded and reported to enable an informed certification decision to be made or the certification to be maintained.

9.1.9.6.2 Opportunities for improvement may be identified and recorded, unless prohibited by the requirements of a management system certification scheme. Audit findings, however, which are nonconformities in accordance with 9.1.15 b) and c) shall not be recorded as opportunities for improvement.

9.1.9.6.3 A finding of nonconformity shall be recorded against a specific requirement of the audit criteria, contain a clear statement of the nonconformity and identify in detail the objective evidence on which the nonconformity is based. Nonconformities shall be discussed with the client to ensure that the evidence is accurate and that the nonconformities are understood. The auditor however shall refrain from suggesting the cause of nonconformities or their solution.

NOTE Nonconformities, consistent with the requirements of 9.1.15 b), can be classified as major, whereas other nonconformities [9.1.15 c)] can be classified as minor nonconformities.

9.1.9.6.4 The audit team leader shall attempt to resolve any diverging opinions between the audit team and the client concerning audit evidence or findings, and unresolved points shall be recorded.

9.1.9.7 Preparing audit conclusions

Prior to the closing meeting, the audit team shall:

a) review the audit findings, and any other appropriate information collected during the audit, against the audit objectives;

b) agree upon the audit conclusions, taking into account the uncertainty inherent in the audit process;

c) identify any necessary follow-up actions;

d) confirm the appropriateness of the audit programme or identify any modification required (e.g. scope, audit time or dates, surveillance frequency, competence).

9.1.9.8 Conducting the closing meeting

9.1.9.8.1 A formal closing meeting, where attendance shall be recorded, shall be held with the manufacturer's management and, where appropriate, those responsible for the functions or processes audited. The purpose of the closing meeting, which shall normally be conducted by the audit team leader, is to present the audit conclusions, including the recommendation regarding type approval. Any nonconformities shall be presented in such a manner that they are understood, and the timeframe for responding shall be agreed.

NOTE “Understood” does not necessarily mean that the nonconformities have been accepted by the client.

9.1.9.8.2 The closing meeting shall also include the following elements. The degree of detail shall be consistent with the familiarity of the manufacturer with the audit process:

a) advising the manufacturer that the audit evidence collected was based on a sample of the information; thereby introducing an element of uncertainty;

b) the method and timeframe of reporting, including any grading of audit findings;

c) the Technical Service's process for handling nonconformities including any consequences relating to the status of the manufacturer's certification;

d) the timeframe for the manufacturer to present a plan for correction and corrective action for any nonconformities identified during the audit;

e) the Technical Service’s post audit activities;

f) information about the complaint handling and appeal processes.

9.1.9.8.3 The manufacturer shall be given opportunity for questions. Any diverging opinions regarding the audit findings or conclusions between the audit team and the manufacturer shall be discussed and resolved where possible. Any diverging opinions that are not resolved shall be recorded and referred to the Technical Service.

9.1.10 Audit report

9.1.10.1 The Technical Service shall provide a written report for each audit. The audit team may identify opportunities for improvement but shall not recommend specific solutions. Ownership of the audit report shall be maintained by the Technical Service.

9.1.10.2 The audit team leader shall ensure that the audit report is prepared and shall be responsible for its content. The audit report shall provide an accurate, concise and clear record of the audit to enable an informed decision on type approval to be made and shall include or refer to the following:

a) identification of the Technical Service;

b) the name and address of the manufacturer and the manufacturer's management representative;

d) the audit criteria;

e) the audit objectives;

f) the audit scope, particularly identification of the organizational or functional units or processes audited and the time of the audit;

g) identification of the audit team leader, audit team members and any accompanying persons;

h) the dates and places where the audit activities (on site or offsite) were conducted;

i) audit findings, evidence and conclusions, consistent with the requirements of the type of audit;

j) any unresolved issues, if identified.

9.1.11 Cause analysis of nonconformities

The Technical Service shall require the manufacturer to analyse the cause and describe the specific correction and corrective actions taken, or planned to be taken, to eliminate detected nonconformities, within a defined time.

9.1.12 Effectiveness of corrections and corrective actions

The Technical Service shall review the corrections, identified causes and corrective actions submitted by the manufacturer to determine if these are acceptable. The Technical Service shall verify the effectiveness of any correction and corrective actions taken. The evidence obtained to support the resolution of nonconformities shall be recorded. The manufacturer shall be informed of the result of the review and verification.

NOTE Verification of effectiveness of correction and corrective action can be carried out based on a review of documentation provided by the manufacturer, or where necessary, through verification on-site.

9.1.13 Additional audits

The manufacturer shall be informed if an additional audit or documented evidence will be needed to verify effective correction and corrective actions.

9.1.14 Type approval decision

The Technical Service shall ensure that the persons or committees that make the decisions on type approval are different from those who carried out the audits.

9.1.15 Actions prior to making a decision

The Technical Service shall confirm, prior to making a decision, that

a) the information provided by the audit team is sufficient with respect to the type approval requirements;

b) it has reviewed, accepted and verified the effectiveness of correction and corrective actions, for all nonconformities that represent :

1) failure to fulfil one or more requirements of the cybersecuriey management system standard, or

2) a situation that raises significant doubt about the ability of the manufacturer's cybersecurity management system to achieve its intended outputs;

c) it has reviewed and accepted the manufacturer's planned correction and corrective action for any other nonconformities.

C. Extract from GRVA-05-18 (Draft Annex 4 on audit/CEL to the new UN Regulation on Automated Lane Keeping Systems (ALKS) submitted by the EC)

Note : The text reproduced below is an extract from GRVA-05-18. Due to the lack of time, the alignment with the provisions of the draft Cybersecurity UN Regulation was not made.

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" within the declared ODD:

(a) Is designed and was developed to operate in such a way that it is free from unreasonable risks for the driver, passengers and other road users;

(b) Respects, under the performance requirements specified elsewhere in this UN Regulation;

(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.

(d) Is designed to recognize its ODD limits

(e) Does not operate outside of the declared ODD and any attempt to activate the System outside of the ODD will not lead to activation

3.1.1. Documentation shall be made available in 3 parts:

(a) Application for type approval: The information document which is submitted to the type approval authority at the time of type approval application shall contain brief information on the items listed in Appendix 2. It will become part of the approval.

(b) The formal documentation package for the approval, containing the material listed in this section 3. (with the exception of that of paragraph 3.4.4.) which shall be supplied to the Type Approval Authority for the purpose of conducting the product assessment / process audit. This documentation package shall be used by the Type Approval Authority 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 of at least 10 years counted from the time when production of the vehicle type is definitely discontinued.

(c) 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 the product assessment / process audit. 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 functions including control strategies of "The System" and the methods employed to perform the dynamic driving tasks within the boundaries under which the automated driving system is designed to operate, including a statement of the mechanism(s) by which control is exercised. The manufacturer shall describe the interactions expected between the system with the driver, vehicle occupants and other road users.

Any enabled or disabled automated driving functions providing when the hardware and software are present in the vehicle at the time of production, shall be declared and are subject to the requirements of this annex, prior to their use in the vehicle. The manufacturer shall also document the data processing in case of continuous learning implemented.

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 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 including ODD-limits shall be stated where appropriate to system performance.

3.2.4 Interaction concept with the driver when ODD limits are reached shall be explained including an overview of types of situations in which the system will generate a transition demand to the driver.

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.

This outline shall include:

- Perception and objects detection including mapping and positioning

- Characterization of Decision-making

- Remote supervision and remote monitoring by a remote supervision (if applicable).

- Perception and objects detection including mapping and positioning

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 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.

3.3.4. There shall be a clear correspondence between 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.”

3.3.5. Identification of units

Each unit shall be clearly and unambiguously identifiable (e.g. by marking for hardware, and by 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 “The System” is free from unreasonable risks for the driver, passengers and other road users.

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 3.5.1). The manufacturer shall show evidence of the means by which they determined the realization of the system logic, during the design and development process.

3.4.3. The Manufacturer shall provide the Type Approval Authority with an explanation of the design provisions built into "The System" so as to ensure functional and operational safety. Possible design provisions in "The System" are for example:

(a) Fall-back to operation using a partial system.

(b) Redundancy with a separate system.

(c) Removal of the automated driving function(s).

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 performance of the dynamic driving tasks, 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, this shall be done in compliance with the relevant provisions of this regulation (e.g. on minimum risk manoeuver and transition demand). 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 to mitigate or avoid hazards which can have a bearing on the safety of the driver, passengers and other road users.

The chosen analytical approach(es) shall be established and maintained by the Manufacturer and shall be made open for inspection by the 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.

This approach shall be based on a Hazard / Risk analysis appropriate to system safety.

(b) Inspection of the safety approach at the system level including a top down (from possible hazard to design) and bottom up approach (from design to possible hazards). The safety approach may be based on a Failure Mode and Effect Analysis (FMEA), a Fault Tree Analysis (FTA) and a system-theoretic process analysis (STPA) or any similar process appropriate to system functional and operational safety.

(c) Inspection of the validation/verification plans and results including appropriate acceptance criteria. This shall include validation testing appropriate for validation, for example, Hardware in the Loop (HIL) testing, vehicle on-road operational testing, or any other testing appropriate for validation/verification.

The inspection shall confirm that each of the following items is covered where applicable under (a)-(c):

(i) Interactions with other vehicle systems (e.g. braking, steering);

(ii) Failures of the automated driving system and system risk mitigation reactions;

(iii) Situations within the ODD when a system may create unreasonable safety risks for the driver, passengers and other road users due to operational disturbances (e.g. lack of or wrong comprehension of the vehicle environment, inadequate control, challenging scenarios)

(iv) Identification of the relevant scenarios within the ODD and management method used to select scenarios and validation tool chosen

(v) Decision making resulting in performance of the dynamic driving tasks (including e.g. emergency manoeuvres) and

interaction with other road users and in compliance with traffic rules

(vi) Reasonably foreseeable misuse by the driver driver (including e.g. driver availability recognition system and an explanation on how the availability criteria were established) and intentional tampering of the system.

(viii) Cyber-attacks having an impact on the safety of the vehicle (can be done through the analysis done under the cyber regulation).

The assessment by the approval authority shall consist of spot checks of selected hazards (or cyber threats) to establish that argumentation supporting the safety concept is understandable and logical and implemented in the different functions of the systems. The assessment shall also check that validation plans are robust enough to demonstrate safety and have been completed.

It shall demonstrate that the vehicle is free from unreasonable risks for the driver; vehicle occupants and other road users in the operational design domain:

- The safety demonstration shall include a quantitative pre-validation target (e.g., using validation acceptance criteria), documented by the manufacturer, demonstrating that the introduction of the ADS will overall not increase the level of risk for the driver, passengers and other road users compared to a manually driven vehicles; and

- A qualitative approach showing that the overall level of risks have been minimized during development to a acceptable level for the driver, vehicle occupants and other road users.

The Type Approval Authority shall perform or shall require to perform tests 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 failure condition of the type defined in paragraph 3.4.4. of this annex, the warning signal to be given to the driver/passengers/other road users and/or to service/technical inspection personnel.

3.4.4.2. This documentation shall also describe the measures in place to ensure the "The System" is free from unreasonable risks for the driver, passengers 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/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, decommissioning).

3.5.2. The design/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 functional/operational safety, cybersecurity and any other relevant disciplines related to the achievement of vehicle safety.

3.5.4. The manufacturer shall have processes to monitor safety-relevant incident/accidents caused by the engaged automated driving systems and a process to manage potential safety-relevant gaps post-registration (closed loop of field monitoring). They shall [have a process to] report critical incidents (e.g. collision with another road users) to the type-approval authorities when they occur.

3.5.5. 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

3.5.6. 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 paragraph 3.5.1. to 3.5.5.