Submitted by the experts from France

Informal document **GRVA-05-29**
5th GRVA, 10-14 February 2020
Agenda items 5 (a)

Proposal for amendments to GRVA-05-05

Paragraph 5.3

I. Proposal

Paragraph 5.3., amend to read:

"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 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.

~~[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.~~]"

II. Justification

Recognizing the objective of full, robust and harmonized application of the requirements of the cybersecurity regulation, the French authorities nevertheless consider this proposal inappropriate.

Even if this approach targets to secure cyber security approval process, current paragraphs 5.3.1. to 5.3.4. seems to not be adapted to the current approval process, especially in terms of time schedule. This “cross check” between TAA would require a longer period, which is not compatible with the approval constraints. In addition, this approach could bring some misunderstanding regarding the mutual recognition between TAA under the 1958 agreements terms.

France is more in favour to continue the activity of the TF CS/OTA on this topic, more oriented under the required skills and experience for a technical service to be designated by a TAA. As a basis for discussion, the wording of paragraphs 5.3.1 to 5.3.4. of the current proposal could be used.

Paragraph 7.4

I. Proposal

Paragraph 7.4.1., amend to read:

“7.4.1. The vehicle manufacturer shall report **when relevant or** at least once **a year** ~~in a quarter~~ to the Approval Authority or the Technical Service the outcome of their monitoring activities, as defined in 7.2.2.2. sub-clause g), this shall include relevant information on ~~new cyber threats, vulnerabilities and~~ **detected** cyber-attacks **focused on vehicle safety functions.** The vehicle manufacturer shall also report and confirm to the Approval Authority or the Technical Service that the cyber security mitigations implemented for their vehicle types are still effective and any additional actions taken.”

II. Justification

France support this approach but with a lower periodicity and only dedicated to cyber attacks or new threats. Such reporting seems to not be relevant for vulnerabilities, already covered by the approval evaluation. In addition, in order to rationalize the volume of data to be reported, we suggest as a basis for discussion, the wording of § 7.4.1. of the current proposal which aims to only focus on safety relative threats or attacks.

ANNEX 5

I. Proposal

France proposes to keep tables A, B and C in the resolutions as a guide used by the Technical Services to conduct the audits.

II. Justification

Parts A, B and C are lists of examples by definition non-exhaustive and shall not be understood as restrictive.

The part A must be considered as a repository of threats and could be a common reference but needs to stay opened. It should be relevant only if it is updated, which is not applicable under the approval process.

The part B (mitigations) seems to be system dependent, specific to each car manufacturer and shall be considered as guidelines.

The part C (mitigations of threats outside the vehicle) is not directly in the scope of the Type Approval and we propose to remove it. Cybersecurity of back-end servers (which are not always under the car manufacturer's control) should be considered in a global framework and is not specific to vehicle type design.

Furthermore, in a context where technological developments are very fast, where attack operating modes are constantly evolving, where the state of threat is not frozen, we think that it is not appropriate to keep Annex 5 in the regulation.