Informal document **GRVA-05-33**
5th GRVA, 10-14 February 2020
Agenda item 5 (a)

CLEPA
European Association of Automotive Suppliers

Draft UN Regulation on Cyber Security (CS)

Comments to document GRVA-05-05 from the experts of OICA and CLEPA

Status after 17th session of UN TF CS & SU

- Extensive and fundamental changes to the **applicability, testing, reporting** and **type approval provisions** of the Draft-CS-Regulation have been introduced and adopted during the 17th session of TFCS & SU on 21-23 January 2020 in Washington DC.
- The experts from OICA and CLEPA have **serious concerns** regarding the **maturity** and **applicability** of those new provisions of the Draft CS-Regulation (document GRVA-05-05).

Concerns regarding the maturity and applicability of the Draft-CS-Regulation

CLEPA
European Association of Automotive Suppliers

- **Context**
  - Document TFCS-17-14rev1 has been introduced **on short notice**: shared on January 17th and adopted by TFCS on January 22nd
  - **Testphase‘s general outcome** was the **confirmation of the applicability** of the former Draft-CS-Regulation by all participating CPs (ECE/TRANS/WP.29/GRVA/2020/6)

- **Major concerns**

1. Changes to the **type approval procedure** (5.3.1 - 5.3.4)
2. New requirements for **vehicle type approval** with insufficient considerations on the needs for existing architectures (7.3.)
   - 2.1 Transition time to be clarified and considered (7.3.1, 7.3.3, 7.3.4)
   - 2.2 Technical vehicle type requirements, mandatory application of Annex 5 Part B on existing architectures (7.3.3. – 7.3.4)
   - 2.3 New provisions for the vehicle type (7.3.7)
3. Excessive **reporting provisions** (7.4.1, 7.4.2)

- **Request to consider those concerns and to resolve them on a consensual basis.**

1. Changes to the type approval procedure

Proposal

Delete paragraphs 5.3.1 to 5.3.4

Justification

- Limitation of the sovereignty of approval authorities.
- The 1958 Agreement already allows the consultation amongst Authorities in cases of doubt or uncertainty.
- By making this provision for exceptional situations a general procedure, the proposal undermines the principle of **mutual recognition**.
- The proposed procedure implies **mistrust** amongst **approval authorities**. If such exists, the qualification of approval authorities and technical services should be addressed on a higher level, not within a singular type approval regulation.
- The Netherlands have already started defining requirements for the accreditation of technical services (minimum qualification).
- Confidential sharing of information and protection of intellectual property (sharing of full information package required since sharing of information document will be insufficient for evaluation)
- Legal uncertainty regarding market access and timing for manufacturers.
- Excessive Workload for Approval Authorities and Manufactures.
- The procedure could be misused for economic interests to cause market distortion and limit free competition.

=> OICA and CLEPA fully support GRVA-05-13 from Japan

2.1 Transition time for existing architectures

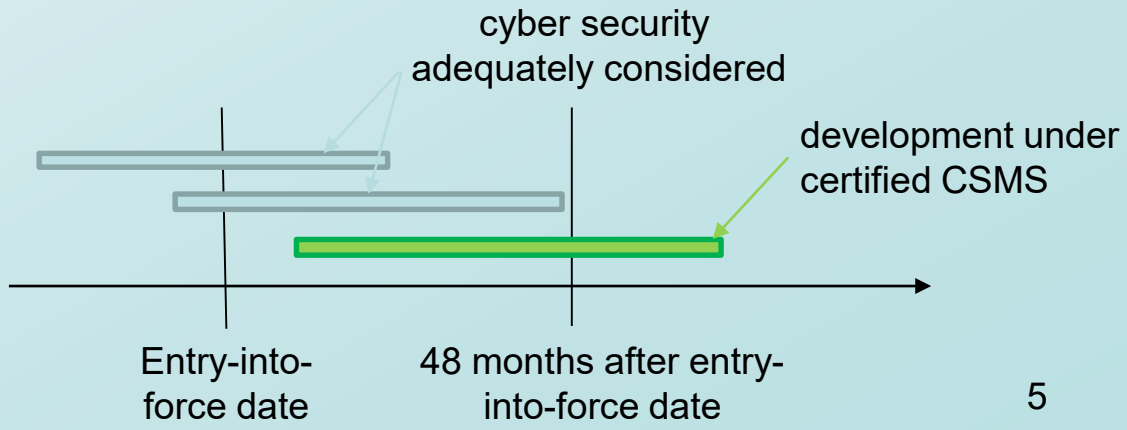
Proposed amendments (in bold):

7.3.1. The manufacturer shall have a valid Certificate of Compliance for the Cyber Security Management System relevant to the vehicle type being approved.

However, if the vehicle manufacturer can demonstrate that the vehicle type could not be developed in compliance with the CSMS, because it was ~~**partly or**~~ fully developed ~~**before**~~ **latest until [48 months]** after entry into force of this Regulation, then the vehicle manufacturer shall demonstrate that cyber security was adequately considered during the development phase.

Justification

- Transitional provision required for **existing vehicle architectures** and for such which are already under development **cannot be retrospectively brought into compliance** with the requirements of the new regulation (**formally and technically**).
- Deletion of “partly or” and “before” and the introduction of “latest until” to clarify that the **development has to be finished 48 months after the entry into force of the regulation**.
- The **development** of automotive **architectures** takes **typically 4-6 years**.
- Architecture will be used across various carlines.
- Transition time required for **manufacturers** and **suppliers** to **adopt their technology** and roll-out plans accordingly.



2.2 Use of Annex 5

Proposed amendments (in bold):

7.3.4. The vehicle manufacturer shall protect critical elements of the vehicle type against risks identified in the vehicle manufacturer's risk assessment. Proportionate mitigations shall be implemented to protect such elements. ~~**The mitigations implemented shall include all mitigations referred to in Annex 5, Part B and C which are relevant for the risks identified. However, if a mitigation referred to in Annex 5, Part B or C, is not relevant or not sufficient , the vehicle manufacturer shall ensure that another appropriate mitigation is implemented.**~~

Justification

- Annex 5 represents a state-of-the-art, which is not necessarily required to ensure cyber security. **Existing architectures can be secure** even though **not all of the mitigations of Annex 5 Part B are implemented**.

- The vehicle manufacturer will have to **prove that proportionate mitigations** to **protect critical elements** are implemented according to the **functionality of the vehicles**. Implementing all of the mitigations of Annex 5 Part B will be excessive.

- Annex 5 can be **transferred in the resolution**

2.3 New provisions for the vehicle type

Current paragraph 7.3.7.

7.3.7.The vehicle manufacturer shall implement measures for the vehicle type to:

(a) detect and prevent cyber-attacks against vehicles of the vehicle type;

(b) support the monitoring capability of the vehicle manufacturer with regards to detecting threats, vulnerabilities and cyber-attacks relevant to the vehicle type;

(c) provide data forensic capability to enable analysis of attempted or successful cyber-attacks.

Proposed Changes:

- Delete Paragraph 7.3.7. (a) and (b)
- Transfer paragraph 7.3.7. (c) to paragraph 7.2.2.2. (CSMS)

Justification

- 7.3.7 are requirements for the CSMS not for the vehicle type. (a) and (b) are already covered under 7.2.2.2.
- Forensic data to be specified.
- Such technologies are not state of the art within the automotive industry.
- Such technologies cannot be implemented on existing architectures.
- This approach has been discussed and rejected by the TF; see TFCS 17-02rev2 (Chair) Minutes of TFCS 16.docx
- Regulation should be technology neutral (on-board or off-board) and not mandating a specific technical solution

3. Excessive reporting provisions

Proposed Changes

Delete 7.4. (Reporting provisions)

Justification

- According to 6.8, audits are possible at any time in order to cover the aspects mentioned under 7.4.
- Systematic reporting especially on vulnerabilities is very sensitive and becomes a target for hackers.
- Volume of such a reporting would be excessive