Evaluation of ACSF during periodic technical inspection

Informal group ACSF #2

2015-06-16 / 17 in Tokyo

OICA

3. Possible discussion items on Automated Driving Technologies

The narrative definitions below have been taken from the SAE and can be used as a starting point to understand the level of assistance/automation:

[…] [Partial automation systems shall be so designed as to provide a continuous integrity check, recording any faults, failures, implausible messages etc., and shall record such events in a non-volatile memory. These data shall be accessible for the purposes of roadworthiness and maintenance inspection through a standardised scan tool. […]

3-2. Others

Discussion concerning electronic security, cybersecurity, roadworthiness inspection provisions (OBD), EDR, etc. could also be made in the IG-AD but should not preclude consideration by the appropriate GRs.

4. Guidance to GRRF (provisional draft)

Possible points to note

5) Adequate safety measure provision should be considered so as not to inhibit current development of such systems. These shall include, but not be limited to, HMI, system integrity monitoring, status recording.

OICA input:
- The guidance opens up a number of items for possible discussions.
- Recorded data are directly connected to roadworthiness and maintenance inspection.
- OBD is only mentioned in the context of roadworthiness inspection provisions (PTI)

ACSF IG Terms of Reference

➢ The terms of reference were endorsed at 79th session of GRRF

➢ Extracts from GRRF-79 report (same as in ACSF-01-02)

2.The informal group shall address the following issues:

  a) Review the current speed limitation (10 km/h) with the purpose of permitting ACSF functionality during [urban] and [interurban] journeys.
  b) Define requirements for communicating to the driver a malfunction of ACSF.
  c) Define requirements to enable the evaluation of ACSF during periodic technical inspection.

➢ The focus of the ACSF group is on periodic technical inspection, which is quite aligned with the ITS / AD guidance

OICA input:
1. Based on the TOR of the ACSF group, OICA has prepared proposals to fulfil the need for ACSF evaluation during PTI.
2. OICA proposal also covers the "real time" driver information of detected malfunctions.
3. OICA proposal does not consider Maintenance aspects, since not in the TOR of the group, and covered in other regulations (RMI)
4. Yet OICA is open to discussions on other items mentioned in the ITS/AD guidance, for further considerations in other relevant UNECE groups

Clarifications

➤ OBD does not mean an "electronic interface to diagnose a vehicle with a scan tool"…

➤ Below is reminded the definition of OBD in GTR 5:

> 3.12. "On-board diagnostic system (OBD)" **means a system on board of a vehicle or engine which has the capability of detecting malfunctions, and, if applicable**, of indicating their occurrence by means of an alert system, of identifying the likely area of the malfunctions by means of information stored in computer memory, and/or communicating that information off-board.

➤ Based on this definition, **UN safety regs (R13, R79, R131…) already includes OBD requirements**:
  - Capability of detecting malfunctions:
    - Failure detection
    - Failure classification (e.g. brake failures classified acc. to their impact on performance)
  - Warning signals are an alert system
  - Coarse identification of the area of the malfunctions: at least one warning per system/function, e.g.
    - Braking yellow and red, tractor and trailers, ESC…
    - Steering, LDWS, AEBS, TPMS etc.

OICA summary:
Current requirements in UN regulations ensures safety in fault condition, based on failure detection and warning indication to driver in real time.

OICA Proposals for PTI - 1

➢ Existing "OBD" requirements in safety UN regs ensure safety in fault condition, based on failure detection and warning indication to driver in real time.

  - They can easily be used for an efficient PTI

  - Up-to-date AEBS & LDWS regulations are suggested as a solid base for a starting point

➢ CEL Annex guarantees performance of the steering system under fault and non fault conditions of the complex electronic system, including ACSF:

  - This is done via e.g. a description and a verification of the safety concept.

  - Extract: "In case of a failure, the driver shall be warned … by warning signal or message display"

➢ In addition to the above, OICA is ready to consider the following extra-requirements, should they be judged necessary and justified by the CPs:

  - Request an electronic interface to confirm the "operational status of the ACSF system" (e.g. by reading the warning signal status or a system "roadworthiness" status…)

  - Such a requirement would permit the implementation of an efficient "fitment test" at PTI, to determine if the original system fitted from factory is still fitted to the vehicle and operational

This OICA proposal…
1. Ensures safety and driver information 24/7 and fulfils the need for an efficient PTI
2. Is perfectly matching with…   New EU directive on PTI (applicable 2018)
                                                German PTI regulation (deployment on-going by FSD)
3. Can be implemented within a reasonable time frame compatible with industry targets

OICA Proposals for PTI - 2

Cornerstones:

➢ **The interface must be "read only"**, to avoid safety and security issues (system damage, over-writing of calibration data, hacking…), leading to liability potential disputes:

- ⬡ Vehicle manufacturers cannot validate all PTI electronic tools → tool vendors must take the responsibility of the above mentioned risks.

- ⬡ The only way is to keep safety OBD simple, to be safe and efficient

➢ There must be no further design requirement on:

- ⬡ The connector type of the interface, other than those already included in the EURO VI / Euro6 OBD emission regulation.

- ⬡ Furthermore, the connector must remain open to other standards used e.g. in Japan.

- ⬡ The communication protocol of the interface other than those already applicable for diagnostic in ISO or SAE standards, e.g. SAE J1587, SAE J1939, ISO27145 etc.

➢ The new PTI requirements on the electronic interface **should apply only to new ACSF systems** (above 10km/h), in order to avoid burdening existing / simpler technologies like e.g. LKAS or electronically controlled auxiliary axles, which are anyway our of the scope of this group

➢ **No Diagnostic Trouble Codes (DTC) list should be defined or required for PTI**. DTCs are for repair, only the effect of DTC on performance is important for safety and roadworthiness of the vehicle.

- **These are the conditions to keep PTI requirements compatible with industry and CPs targets on lead-time for ACSF implementation, while still ensuring safety and efficient PTI.**
- **They avoid adding a burden on systems not related to new ACSF functions**

Proposal for draft amendment

5.5.2.   It ~~must~~ **shall** be possible to verify in a simple way the correct operational status of those **Complex** Electronic Systems, which have control over steering. If special information is needed, this shall be made freely available. It ~~must~~ **shall** be possible to verify the correct operational status of those Electronic Systems by a visible observation of the failure warning signal status, following a "power-ON" and any bulb check.

In the case of the failure warning signal being in a common space, the common space must be observed to be functional prior to the failure warning signal status check.

[In the case of an ACSF system able to operate at higher speed than 10km/h, it shall be possible to confirm ~~the correct operational status given by~~ **the failure warning signal status via the use of an electronic communication interface** ~~(i.e. the correct operational status shall be readable by an external electronic device)~~**.]**

5.5.2.1.   At the time of Type Approval the means implemented to protect against simple unauthorized modification to the operation of the verification means chosen by the manufacturer (e.g. warning signal) shall be confidentially outlined.

Alternatively this protection requirement is fulfilled when a secondary means of checking the correct operational status is available, **e.g. by using an electronic communication interface.**