EC study on Assessment and certification of automated vehicles – Main findings

Follow us on:

facebook.com/EU.Growth
facebook.com/MrSmeForEurope

@EU_Growth

YouTube youtube.com/c/EUGrowth

Web sites:
ec.europa.eu/growth
ec.europa.eu/bienkowska

Internal market, Industry, Entrepreneurship and SMEs

Introduction

- TRL’s study was performed in the context of ACSF updates to UN Regulation No 79.
- Focus: Ensure safe system function in all real-world driving situations.
- The study identified five safety-relevant areas that might need attention:
    1. **Interpretation of the existing assessment procedure for the safety of complex electronic systems (“CEL annex”).**
    2. **Operational safety of ACSF under all real-world driving conditions.**
    3. **Driver monitoring to prevent foreseeable misuse.**
    4. **Real-world safety performance after approval (“In-service safety performance”).**
    5. **Over-the-air (OTA) software updates.**
- The main findings are summarised on the following slides as *identified issues* and *proposed solutions* for each of these five areas.

CEL Annex - Issues

- Annex 6 of UN Regulation No. 79 regulates the safety of complex electronic systems. This “CEL annex” is also included in other regulations.
- It prescribes an analysis of the development life cycle or design methodology = effectively an audit by the technical service.
- Aim is to show safety of the design (with verification) and in particular that ‘the system’ does not adversely affect the function of the main steering system in non-fault (i.e. normal) and fault operating conditions.
- It does *not* enforce any specific performance requirements.

- Issue identified by TRL’s analysis: **The CEL Annex assessment is not applied in a consistent manner across technical services.**

CEL Annex - Solutions

- TRL identified the current ‘best practice’ application and developed a proposal for amendments to Annex 6.
- Main items proposed:
  - **Involve technical service (TS) early-on in the development process.**
  - **Ensure traceability of the work of the TS.**
  - **TS to perform a document ‘audit’ of the safety approach at both concept (e.g. HAZOP) and system level (e.g. FMEA, FTA): Check existence of documents, their history and (to a certain extent) their content.**
  - **TS to assess resistance to environmental influence: Inspect type and scope of tests on climate, mechanical resistance and electromagnetic compatibility.**
  - **Possibly include report template in CEL Annex to ensure all aspects are addressed.**

Operational safety - Issues

- Aim: Ensure safety under all real-world scenarios.
- ‘Hands-off’ systems (such as, category B2 and E) will allow the driver to be ‘out of the loop’ for significant periods of time - up to about 3 minutes according to an ACSF IWG proposal.
- The system must be capable of controlling the vehicle entirely for this period of time.

- Issue: The currently proposed requirements are based on the assumption of an SAE level 2 system (driver supervising driving environment). **TRL think that requirements similar to those appropriate for an SAE Level 3 system should be imposed (driver is only supervising the system)**.

Operational safety - Solutions

- TRL propose to require a comprehensive assessment to assure safe operation in the full range of real-world conditions which may occur in the operational design domain (ODD).
- A list of areas to be considered for assessment has been developed:
  - **Roadway types, geographic area, speed range, environmental conditions (weather, daytime / nighttime, etc.)**
  - **Driver complacency and misuse (and effective countermeasures).**
  - **Object and event detection and response (e.g. stopped or rapidly slowing vehicle , roadworks, emergency vehicles, animals/pedestrians in road, ...).**
  - **Minimal risk manoeuvre (MRM).**
- These areas could be assessed based on:
  - **Submission of documentation (describing OEM process for the assessment, testing and validation of 'operational safety'); and**
  - **Signed declaration by an authorised company official.**
- These requirements could be implemented within Regulation 79 or more logically in a new **horizontal regulation for automated vehicles**.

Driver monitoring - Issues

- The proposed requirements for driver monitoring in ACSF regulation draft are:
  - **For Category B1 systems: ‘Hands-on detection’.**
  - **For Category B2 systems: ‘Driver activity detection’.**

- The main issues identified by TRL’s analysis:
  1. **Hands-on detection leaves room for potential misuse of Category B1 systems. (For example, phone-related activities using one hand which would draw attention away from the driving environment.)**
  2. **Draft requirements for ‘driver activity detection’ are considered too unspecific and underdeveloped to ensure safe operation.**

Driver monitoring - Solutions

- TRL performed a technology review to determine current state of the art of driver monitoring systems.

- Proposed regulatory solution for the short term:
  - **Potential driver misuse should be evaluated and addressed by manufacturers during system development (HAZOP to cover foreseeable misuse).**
  - **This step should be checked by the technical service during the CEL Annex assessment (if TRL's proposed changes to the Annex are implemented).**

- In the longer term:
  - **Include specific driver monitoring requirements to ensure a similar standard of misuse prevention between different systems.**
  - **This will require additional regulatory work to develop appropriate requirements (don't exist at the moment).**
  - **Should ideally be placed into a horizontal regulation on driver monitoring that can be called upon by different regulations and can be updated and developed further independently.**

In-service safety performance - Issues

- For ‘hands-off systems’ (such as B2 and E) it is impossible to test at the time of type-approval all real-world scenarios that may be encountered.
- Therefore, the approach currently being developed for type-approval is:
  - **To check a limited number of scenarios; and**
  - **to audit aspects of the system development process, in particular the safety concept.**

- **Issue: This leaves a potential for safety-relevant issues which are not detected during type-approval in the future.**

In-service safety performance - Solutions

- Solution could be to not only add more scrutiny up-front, but also ensure that safety issues in real-world use are detected and resolved early.
- **In-service safety performance monitoring coupled with recall action to address any safety issues identified could be implemented**.
- Measures could be put in place in UN Regulation to enable the use of the three approaches:
  - **Enhanced requirements for operational safety checked by authorities at type-approval level,**
  - **Self-declaration by the manufacturer on some design aspects, and**
  - **Proactive in-use safety monitoring.**
- A first step would be a requirement for the collection of "*event, incident, and crash data, for the purposes of recording the occurrence of malfunctions, degradations, or failures in a way that can be used to establish the cause of any such issues*".
- **DSSA requirements could be expanded** to include collection of data for events, incidents and road accidents sufficient for use to establish the cause of any such issues and any related system defects.

OTA updates - Issues

- Over-the-air (OTA) software updates can offer large benefits to the automotive industry and the consumers.

- However, OTA software updates can also:
  - **Cause safety or emissions problems; and**
  - **make a vehicle non-compliant with its initial type-approval and registration certificate.**
- Particularly relevant if OTA updates provide new functions subject to type-approval which were not initially type-approved.

OTA updates – Solutions (1/2)

- For pre-registration/production vehicles, OTA updates could follow the current practice for a type-approval update:
  - **OEM to inform type-approval authorities.**
  - **Authorities to decide if this should be considered as revision/extension or as new type-approval.**

- For post-registration software updates, the situation is more complex:
  - **Modifications to registered vehicles are covered by *national* legislation.**
  - **EU type-approval framework could be extended to updates affecting approved systems. (Similar to UN regulations on retrofitting of LPG/CNG vehicles or for replacement parts.)**
  - **Updates could be validated by type-approval authorities.**
  - **Updates could then be deployed by OEMs under their responsibility.**
  - **Potentially in combination with an individual approval/periodic technical inspection (depending on the scope of the update).**

OTA updates – Solutions (2/2)

- Main considerations for implementation:
  - **Responsibility should be clarified: Today under most of national rules, it is the vehicle owner (not manufacturer) who is responsible for maintaining the vehicle in compliance with legislation.**
  - **OTA updates could be limited to non-critical functions. For critical functions a physical inspection (by the manufacturer, authorities) could be required. Updates not impacting type-approved functions could be left out from the type-approval framework.**

- Software / firmware versions could also be checked at PTI:
  - **Potential introduction via Implementing Act for Directive 2014/45/EU.**
  - **But: First PTI only occurs after a number of years (4 years in many member states).**

- Cyber-security is still a major issue and much work is being performed on it at present, (e.g. WP.29 ITS/AD working group).

Thank you for you attention

For further information please contact:

Study available publicly here:

https://circabc.europa.eu/sd/a/b6f6de76-184e-4967-93dd-9d7f1e1e3984/item%204-2017-01%20Commission%20study%20on%20vehicle%20certification.pdf

Contacts:

- Commission: Antony Lagrange (antony.lagrange@ec.europa.eu)
- TRL: Meryn Edwards (medwards@trl.co.uk) and Matthias Seidl (mseidl@trl.co.uk)