Data Storage Requirements for Draft ALKS Regulation

Contributions by Germany in blue.

NOTE: Text in brackets will be discussed at IWG's January 2020 meeting in Tokyo. Terms in yellow will need to be defined by the group.

NOTE: Current draft regulatory text for ALKS (ACSF-25-03) foresees requirement that for ALKS activation "DSSAD is operational"; requirement in the sense of "vehicle equipped with ALKS shall comprise of DSSAD" may be included to ALKS draft regulatory text.

Specifications for DSSAD:

~~Each vehicle with a DSSAD shall meet the requirements specified below:~~

2.2. Data elements

Upon the occurrence of the following triggers the respective trigger and the specified data elements shall be stored:

- Trigger: Activation and deactivation of the ALKS together with:
  - Time stamp,
  - GNSS position (highly accurate position data),
  - [Vehicle identification number],
  - List of error codes [with harmonized descriptions], if any.

- Trigger: Start and end of Transition Phase by the ALKS together with:
  - Time stamp
  - GNSS position (highly accurate position data),
  - [Vehicle identification number,]
  - Its causing factor,
  - List of error codes [with harmonized descriptions], if any.

- Trigger: Start and end of Minimum Risk Maneuver by the ALKS together with:
  - Time stamp
  - GNSS position (highly accurate position data),
  - [Vehicle identification number.]

- Trigger: Start and end of Emergency Maneuver by the ALKS together with:
  - Time stamp,
  - GNSS position (highly accurate position data).
  - [Vehicle identification number.]

- ✧ Trigger: Override together with:
  - ✧ Time stamp,
  - ✧ GNSS position (highly accurate position data),
  - ✧ [Vehicle identification number,]
  - ✧ The mode/causing factor of the override (steering, accelerating or braking).

- ✧ Trigger: [Start and end] of driver availability recognition system together with:
  - ✧ Time stamp,
  - ✧ GNSS position (highly accurate position data),
  - ✧ [Vehicle identification number,]
  - ✧ mode/status of (selected) criteria for deeming driver availability.

- ✧ Trigger: Failures (ALKS failure, severe ALKS failure and severe vehicle failure) together with:
  - ✧ Time stamp,
  - ✧ GNSS position (highly accurate position data),
  - ✧ [Vehicle identification number]
  - ✧ The mode of the failure [including the detection of an accident, e.g. by EDR triggering].

[GNSS = Global Navigation Satellite System, e.g. GPS, Galileo, Glonass,…]
Additional elements may be required at the national level.

2.3. Data format

Each data element listed in paragraph 2.2 shall be recognized without any possible confusion by the [standardised format **China**: chosen by the manufacturer]. Each timestamp (including the date) attached to this data shall enable to determine when the interaction (any change of the system status) occurred with [specified time stamp accuracy requirements: e.g. 10 ms derived from the same time source].

2.4. Data storage

2.4.1 DSSAD shall be able to store [minimum number OR minimum] time stamped interactions or [minimum number OR minimum] period of use, whichever is achieved first.

The recorded data must not be deleted automatically within a period of 180 days.

~~Once these storage limits of DSSAD are achieved, additional data storage may erase the previous data.~~

If storage limits of DSSAD are reached and the aforementioned period not undercut, data storage may be created by erasing data, following a first in first out procedure.

2.4.2 Notwithstanding paragraph 2.4.1. data storage is subject to national or regional law.

2.4.3 The DSSAD ~~[shall/~~may~~]~~ be fitted with an embedded hardware, allowing authentication and secured access to the over the air (OTA) interface.

2.5. Data retrievability

The data shall be retrievable for authorities by commercially available] tools or electronic communication interface. If the main on-board vehicle power supply is not available, it shall be possible to retrieve all stored data from the DSSAD.

Even after an impact [UN R94, UN R95], it shall be possible to retrieve ~~timestamped~~ all data stored from the DSSAD.

2.6 System diagnosis

The DSSAD shall store the following information together with their time stamps:

- Malfunctions / fault diagnosis:
  - Any kind of DSSAD malfunction [harmonized categories] and its cancellation
- Successful data transmission:
  - Extent of data transmission (according to all mandatory [and optional] data elements)
  - Target location of data transmission [e.g., uploaded in garage to national authorized server or OTA transfer]
- [Harmonized] Reasons for unsuccessful data transmissions

~~[~~2.6. Protection against manipulation

It shall be ensured that there is adequate protection against manipulation of stored data such as anti-tampering design.~~]~~

2.7. Information to the driver

Information provided to the ~~[~~driver ~~OR vehicle owner]~~will be an issue of national law.

2.x Definitions:

2.x.1. "*Data Storage System for Automated Drving (DSSAD"* enables the determination of interactions between the ALKS and the human driver and respective boundary conditions.

2.x.2. *"DSSAD operational"* means the DSSAD is without failure and has sufficient storage capability to store the required data elements.