Data Storage Requirements for Draft ALKS Regulation

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.

2.1 Specifications:

[Each vehicle equipped with an ALKS shall be fitted with a DSSAD that meets the requirements specified below: This section is provided as an introductory remark to the ALKS drafters]

2.2. Data elements

Each vehicle equipped with a DSSAD shall store the data elements listed below:

1. Activation of the ALKS (timestamp)
2. Deactivation of the ALKS (timestamp)
    a. [Main ALKS system control
    b. override on steering control
    c. override on braking or accelerator control while holding steering control]
3. Transition Demand by the ALKS, (timestamp) [including the source of the transition demand identification whether the transition demand is requested by:
    a. Planned event
    b. unplanned event
    c. driver unavailability
    d. ALKS failure
    e. Other system or vehicle failure
    f. System override by braking input
    g. System override by accelerator input]
4. Suppression of driver input (timestamp)
5. Emergency Manoeuvre (timestamp)
6. Detected collision by system (timestamp)
7. ALKS failure (timestamp)
8. Other system or vehicle failure (timestamp)
9. EDR trigger input (timestamp)
10. Minimal Risk Maneuver engagement by the ALKS (timestamp)
11. [Other data elements?]

Single time stamp may be allowed for multiple elements recorded simultaneously within the timing resolution of the specific data elements. If move than one~~several~~ ~~elements~~ element is~~are~~ recorded with the same timestamp, the information from the individual elements should be presented in chronological order.

Additional elements may be required at the national or regional level.

2.3. Data format

Each timestamp (date and time) attached to this data shall enable the determination of when ~~to determine when~~ the interaction occurred.

2.4. Data storage

DSSAD data shall be available for at least the last [6 months or 2500 timestamps].

Once these storage limits of DSSAD are achieved, additional data storage may erase the previous data following a first in first out procedure.

The DSSAD [may] be fitted with an embedded hardware, allowing authentication and access to the data.

2.5. Data retrievability

The data shall be retrievable after an impact according to [R94/95/137, FMVSS, or other relevant national crash test procedures] by [commercially available tool or electronic communication interface]. If the main on-board vehicle power supply is not available, it shall be possible to retrieve all data as listed in 2.2 from the DSSAD using procedures chosen by the manufacturer].

The manufacturer shall provide an information package to any interested manufacturers or repair of components, diagnostic tools or test equipment in machine readable way (e.g. ISO 22901) which includes the information about how the timestamped data can be retrievable and interpretable via the use of the electronic communication interface.

[2.6 System self-diagnosis – (Germany to double check what is important on this aspect)

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

- 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

[2.7. Protection against manipulation

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

2.8. Information to the driver or vehicle owner

Information provided to the driver or vehicle owner, if any, shall be issued based on national or regional law.

2.x Definitions:

[Interaction is defined as xxxx]

Odds and ends

Furthermore, the manufacturer shall provide authorities or parties entrusted by national or regional legislation the information which allows access to the timestamped data.

2.5.3 If the access to timestamped data is protected by a security algorithm, the manufacturer shall ensure authorities and parties authorized by national or regional legislation the authorization to access the timestamped data in an easy manner.