Proposals Consolidated on Document EDR-DSSAD-03-06 (Japan)

The modifications to the existing text of the proposed document EDR-DSSAD-03-06 (Japan) are marked in bold for new text and strikethrough for deleted text.

Proposal for DSSAD Section in ALKS requirements

Section XX: DSSAD

1. Purpose (to be discussed)

x. Definitions (to be combined with Definition Part)

x.1. "*Data Storage System for Automated Driving (DSSAD)*" means a system which aims at giving a clear picture of the significant interactions between the driver and the ADS by storing a set of data.

x.2. "*Data*" means a series of timestamped information entries related to a logic signal indicating that the ADS was switched ON or OFF, or a specific significant interaction between the driver and the system occurred at a precise time.

x.3. "*Storing data*" : means collecting and keeping the collected data for future retrieval or "read only" access.

(CITA-EVU)

x.4. "*Backend*" is an external storage location regulated by national or regional law where data elements of the DSSAD are stored and maintained in accordance with national or regional legislation and makes the data available to authorized parties.

(CITA-EVU)

x.5. "*Data transmission*" is the process of sending data over a communication medium directly from the vehicle to a backend.

(CITA-EVU)

x.6. "*Data set*" is a data matrix containing all contiguous data elements listed in paragraph 6.2. that were triggered from the time the ALKS was activated until it was manually or automatically deactivated.

(CITA-EVU)

x.7. "*Over the air (OTA) interface*" means an interface that can establish a wireless connection with a backend and allow data transfer thereto wirelessly instead of using a cable or other local connection.

(ICA)

x8. "Event" means a crash or physical occurrence that causes the trigger threshold to be met or exceeded.

Commented [GL1]: There should be a common trigger mechanism / threshold for EDR and DSSAD. The current threshold for EDR (based on SRS/airbag deployment) does not capture a range of accidents, e.g. low-velocity pedestrian impact. and would be insufficient for DSSAD.

Work is currently underway to develop a trigger threshold specification. This will likely need to evolve as technology advances to ensure that an accurate mechanism is in place.

2. Specifications

2.1. Each vehicle equipped with a DSSAD complying with the definition of Paragraph x.1. shall meet the requirements specified in paragraph 2.2 for data elements, paragraph 2.3 for data format, paragraph 2.4 for data storage, paragraph 2.5 for retrivability, and paragraph 2.6 for information to the driver.

2.1.1. Data shall be available by using a dedicated retrieval tool or any other solution.

(CITA-EVU)

~~2.1.1. Data shall be available by using a dedicated retrieval tool or any other solution.~~

Commented [GL2]: « any other solution » is too vague – we would refer to the suggested data retrievability secion on p. 6

Commented [SK3]: See no. 2.5.1.

2.1.2 The data shall be stored on-board unless it ensures that there is adequate protection against manipulation.

(CITA-EVU)

2.1.2 The data shall be stored on-board **and on a backend**. ~~unless it ensures that there is adequate protection against manipulation.~~

Commented [GL4]: We would agree with this.

2.2. Data elements

2.2.1 Each vehicle equipped with a DSSAD shall store information which be able to determine elements listed below;（If duplicate, record in combined is allowed.）

- ✧ Time stamped switches of the ADS from a status to another status
- ✧ Time stamped Transition Demand by the ADS
- ✧ Time stamped Minimal Risk Maneuver engagement by the ADS
- ✧ Time stamped Override through steering, brake, and accelerator control by the driver
- ✧ Time stamped Driver not available
- ✧ Time stamped System failure
- ✧ ODD status information (road condition, vehicle condition, environmental condition) when the system defines that vehicle will exit or exits the ODD limits)

(Germany)

- ✧ Vehicle identification number
- ✧ ADS function equipment
- ✧ Operation mode of ADS (when is stored continuously and when discretly?)
- ✧ Transition Demand by the ADS (when is stored continuously and when discretly?)
- ✧ Minimal Risk Maneuver engagement by the ADS (when is stored continuously and when discretly?)
- ✧ Emergency Maneuver engagement by the ADS (when is stored continuously and when discretly?)
- ✧ Override by the driver (when is stored continuously and when discretly?)
- ✧ Reasons for automatic mode changes
- ✧ (Confirmed) Interactions with driver
- ✧ Vehicle Dynamics : Vehicle speed
- ✧ Vehicle Dynamics : Braking status

- ✧ Vehicle Dynamics : Steering input
- ✧ Environment : Ambient temperature
- ✧ Environment : Front wiper status
- ✧ Environment : Brightness / illumination
- ✧ EDR activation (Event ? or to see EDR system is ready? By Chair)
- ✧ Vehicle Location

(CITA-EVU)

2.2.1 Each vehicle equipped with a DSSAD shall store information which be able to determine elements listed below;（If duplicate, record in combined is allowed.）

- ✧ **Position and** Time stamped switches of the ADS from a status to another status
- ✧ **Position and** Time stamped Transition Demand by the ADS
- ✧ **Position and** Time stamped Minimal Risk Maneuver engagement by the ADS
- ✧ **Position and** Time stamped Override through steering, brake, and accelerator control by the driver
- ✧ **Position and** Time stamped Driver not available
- ✧ **Position and** Time stamped System failure
- ✧ ODD status information (road condition, vehicle condition, environmental condition) when the system defines that vehicle will exit or exits the ODD limits)
- ✧ **(*Position and Time stamped C-ITS signals*)**

(ICA)

2.21 Each vehicle equipped with a DSSAD shall store information which be able to determine elements listed below;（If duplicate, record in combined is allowed.）

- ✧ Vehicle Identification Number
- ✧ GPS event time stamp of the event
- ✧ Activation status of each automated driving feature at the time of the event
- ✧ Time stamped switches of the ADS from one status to another
- ✧ Time stamped driver acceptance between automated / manual mode
- ✧ Time stamped record of driver intervention through steering, braking, accelerator or gear shift
- ✧ Driver seat occupancy status
- ✧ Time stamped user engagement commencement
- ✧ Time stamped Minimal Risk Manoeuvre engagement
- ✧ Time stamped System failure with fault code

Commented [GL5]: Other unique identifiers may be possible but VIN seems the most sensible mechanism

Commented [GL6]: Description and examples as per email.

This is the absolute minimum set of data elements that is requried to determine whether the ADS or human was in control. Other data elements (e.g. speed) may be helpful for road safety and other purposes.

2.3. Data format

Each data element listed in Paragraph 2.2 shall be recognized without any possible confusion by the codification that will be chosen by the manufacturer.

Each time stamp attached to this data shall enable to determine when the significant interaction (change of ADS status, Transition Demand release, Minimum Risk Maneuver or Emergency Manoeuver or Override by the driver) occurred with a resolution of [1 second] in GMT time.

(CITA-EVU)

2.3. Data format

Each data element listed in Paragraph 2.2 shall be recognized ~~without any possible confusion~~ by **standardised format.** ~~codification that will be chosen by the manufacturer.~~

Each time stamp attached to this data shall enable to determine when the significant interaction (change of ADS status, Transition Demand release, Minimum Risk Maneuver or Emergency Manoeuver or Override by the driver) occurred with a resolution of [1 second] in GMT time.

(CITA-EVU) to insert

(2.3.2. Position determination

2.3.2.1. Horizontal position error shall not exceed:

(a) Under open sky conditions: 15 m at a confidence level of 0.95 probability with Position Dilution of Precision (PDOP) in the range from 2.0 to 2.5;

(b) In urban canyon conditions: 40 m at a confidence level of 0.95 probability with PDOP in the range from 3.5 to 4.

Commented [GL7]: We do not think that this level of accuracy is sufficient ; however, it is unclear whether this needs to be specified in the regulations at all.

2.3.2.2. Sensitivity at receiver input shall be:

(a) GNSS signals detection (cold start) do not exceed 3,600 s at the signal level on the antenna input of the AECC of minus 144 dBm;

(b) GNSS signals tracking and navigation solution calculation is available for at least 600 s at the signal level on the antenna input of the AECC of minus 155 dBm;

(c) Re-acquisition of GNSS signals and calculation of the navigation solution is possible and does not exceed 60 s at the signal level on the antenna input of the AECC of minus 150 dBm.

2.3.2.3. Cold start time to first fix shall not exceed

(a) 60 s for a signal level down to minus 130 dBm;

(b) 300 s for a signal level down to minus 140 dBm.

2.3.2.4. GNSS signal re-acquisition time after a block out of 60 s at a signal level down to minus 130 dBm shall not exceed 20 s at the recovery time of the navigation satellite visibility.

2.3.2.5. The GNSS receiver shall be able to obtain a position fix at least for every second.

2.3.2.6. Accuracy shall be provided for the complete speed range of the automated driving function.)

2.4. Data storage

DSSAD shall be able to store a minimum of [X.000] timestamped significant interactions or cover a minimum period of [6] months of use, whichever is achieved first.

Once these storage limits of the DSSAD are achieved, additional data storage may erase the previous data, following the "First In / First Out" rule, and data over these limits may be impossible to retrieve.

(CITA-EVU)

2.4. Data storage

DSSAD shall be able to store a minimum of [X.000] timestamped significant interactions or cover a minimum period of [6] months of use, whichever is achieved first.

Once these storage limits of the DSSAD are achieved, additional data storage may erase the previous data, following the "First In / First Out" rule~~, and data over these limits may be impossible to retrieve.~~

(CITA-EVU) to insert

2.4.2. Notwithstanding paragraph 2.4.1. data shall be retrievable by the methodology described in paragraph 2.5.1. within the national or regional legislative storage periods. After these storage periods, data shall be impossible to retrieve.

2.4.3. The DSSAD shall be fitted with an embedded hardware, allowing authentication on, and access to the over the air (OTA) interface.

2.4.4. The DSSAD shall be able to recognize, when a data transmission (to a backend) is successfully completed.

2.4.5. After the end of a position and timestamped event, the DSSAD shall send the data set to a backend over an end-to-end protected wireless connection.

2.4.6. If the sending of data failed or is not possible, then the DSSAD shall retry sending the data, if a secure and active wireless connection is available.

2.4.6. Notwithstanding paragraph 2.4.1. stored data in the DSSAD shall be deleted after the DSSAD has registered a successful data transmission to the backend.

2.5. Data retrievability

If the main onboard vehicle power supply is not available, it shall be possible to retrieve stored timestamped data from the DSSAD with the appropriate tool or method provided by the manufacturer.

After a UN Regulation No. 94 (Frontal collision) impact test, it shall be possible to retrieve timestamped data stored prior to the impact, from the DSSAD, with the appropriate tool or method provided by the manufacturer.

(CITA-EVU) to insert

2.5. Data retrievability

2.5.1. **The data set shall be retrievable via the electronic vehicle interface (OBD and OTA).**

If the main onboard vehicle power supply is not available, it shall be possible to retrieve stored **position and** timestamped data from the DSSAD with the appropriate tool or method provided by the manufacturer.

After a UN Regulation No. 94 (Frontal collision) impact test, it shall be possible to retrieve **position and** timestamped data stored prior to the impact, from the DSSAD **via the electronic vehicle interface** (**OBD and OTA**) ~~with the appropriate tool or method provided by the manufacturer.~~

2.5.3. **For the purpose of type approval it shall be possible for Type Approval Authorities and Technical Services to access and read data via the electronic vehicle interface (OBD and OTA).**

2.5.4. **At Roadworthiness testing, including the periodic technical inspection, it shall be possible for responsible authorities to access and read at least the most recent data set via the electronic vehicle interface (OBD and OTA) to test the storage functionality and the plausibility of the data set.**

2.5.5. **The manufacturer shall provide an information package to Type Approval Authorities, Technical Services and authorities responsible for Roadworthiness testing which includes the information how to grand access and retrieve the data stored in the DSSAD required by this regulation.**

(ICA)

Data retrievability

Each manufacturer of a motor vehicle equipped with an ADS must ensure by licencing agreement or other means that a tool(s) and OTA access is available that is capable of accessing and retrieving the data stored in the DSSAD required by this regulation. The tool(s) and OTA access shall be available no later than when the Type Approval is granted.

(ICA)

System deactivation

It shall not be possible to deactivate the DSSAD.

2.6. Protection against manipulation

DSSAD should be ensured that there is adequate protection against manipulation of stored data such as anti-tampering design.

(Germany)

(Question: “Check” means “Self-Check of DSSAD?”)

- ✧ Malfunctions
- ✧ Complete file recorded / sent

- ~~Last data retrieval~~
- Communication with EDR

2.7. Information to the driver

The manufacturer shall provide in the vehicle owner's handbook, or by any other communication means in the vehicle, the necessary information about DSSAD.

The manufacturer shall provide the following information in the vehicle owner's handbook, or by any other communication means in the vehicle.

- The vehicle is equipped with DSSAD
- The purpose of DSSAD
- No personal information is included
- The way to retrieve data