Submitted by the experts from OICA

Informal document **GRVA-02-21**
2nd GRVA session, 28 January – 1 February 2019
Agenda item 5(a)

Data Storage System for Automated Driving

Preliminary considerations

OICA supports the development of Data Storage for Automated Driving within the scope of GRVA, while EDR could be developed within the scope of GRSG, as decided during March 2018 ITS/AD 14th session.

This position is based on the principle that EDR and DSSAD should definitely not be mixed or overlapping, in terms of functions, and in terms of concept as well:

- *the EDR function should continue to be developed, within an unchanged spirit, as "focused on accident reconstruction", and as so, should remain a mean to record a batch of retrievable and relevant sampled continuous data, during the very short period of time preceding a crash, triggered by a specific event, and dedicated to a wide variety of vehicles, independently of their fitment with any Automated Driving function, while*

- *the DSSAD function should newly address a very complementary but different function, "focused on the determination of interactions between an Automated Driving function and the human driver who may engage and disengage it", and as so, should be a mean to continuously record a batch of retrievable and relevant timestamped data entries, on a continuous basis, not triggered by any specific event, and to keep them retrievable for an extended period of time.*

As a consequence of this, DSSAD fitment would only make sense as a mandatory function when "driving delegation" becomes possible, that is to say "only for vehicles fitted with an Automated Driving system", as opposed to EDR function.

And the nature of the data available through DSSAD would be extremely linked to those Automated Driving systems and to the technical regulations that will apply to them.

A continuous coordination between the experts in charge of the development of technical regulations addressing Automated Driving systems and those in charge of the development of technical regulations addressing DSSAD would then be extremely beneficial.

In a first approach, the technical requirements applying to DSSAD could even be developed and integrated inside the technical regulation that will address the very first Automated Driving systems that will introduce "driving delegation".

Background

This text represents a first draft of technical requirements for a "Data Storage System for Automated Driving", as presented by OICA in March 2018 ITS/AD session n°14.

As "certification scheme neutral" (Self-Certification or Type Approval), it includes technical requirements only (chapters such as "Definition of type", "Application for Approval" or "Approval" are not included). It could become a "stand-alone regulation" as well as a "part of a regulation covering a wider spectrum". Any option in this regard remains neutral regarding the requirements themselves.

These requirements were established in respect of the initial concept of a function or device dedicated to the particular aspect of "driving delegation" that is introduced with Highly Automated Driving.

It is important to keep in mind that this DSSAD concept is dedicated to AD, and hence is complementary to the concept of Event Data Recorder, which is not particularly dedicated to AD. As a reminder, the 14th ITS/AD meeting decided that EDR should fall into the perimeter of GRSG.

Content:

§ 1 Purpose.....
§ 2 Application scope.....
§ 3 Definitions .....
§ 4 Requirements for vehicles .....
§ 5 Data retrieval tools .....

1. Purpose

This regulation specifies requirements for vehicles equipped with Data Storage Systems for Automated Driving (DSSADs) concerning the collection, storage, and retrievability of motor vehicles fitted with a [Highly Automated Driving system (SAE Levels 3, 4 & 5 classification)] and a driver who is able to engage this system. It also specifies requirements for vehicle manufacturers to provide tools (if needed) and/or methods so that authorized investigators are able to retrieve data from DSSADs.

The purpose is to ensure that DSSADs collect and store, in a readily usable manner, valuable data for effective investigations and analysis, when a significant safety related event occurs, and will make possible :

- providing a clear picture of the interactions (i.e. activation/deactivation of the system and transition scenario / driver-take-over) between the human driver and Highly Automated Driving (HAD) system, and

- determining in an objective manner who, from the human driver or the HAD system, "was requested to be in control of the driving task", and "who either the human driver or the HAD system was actually in control of the driving task", and

2. Application scope

This regulation applies to vehicles of [M & N categories] that have the possibility to have a driver and are equipped with a Highly Automated Driving (HAD) system that once engaged by the driver, takes the full control of the driving task.

3. Definitions

For the purpose of this Regulation,

3.1 **"Data Storage System for Automated Driving (DSSAD)"** means a system which aims at making clear « who was requested to drive » and « who was actually driving » (it can be different, especially during [transition procedure]) by storing a set of data that will give a clear picture of the interactions between the driver and the Highly Automated Driving system.

3.2 **"Highly-Automated-Driving" (HAD) system** means a [system that takes the full control of the driving task when engaged by the human driver (classified as SAE Level 3, 4 or 5).]

3.3 **"Data"** : the nature of the data that will be stored by the DSSAD is a series of timestamped data entries indicating that a specific basic signal or event (in general, an interaction between the driver and the system) occurred at a precise time.
The system will enable the collection and storage of these timestamped data entries.

3.4 **"Storing data"** : collecting and keeping the collected data for future retrieval or « read only » access.

3.5 "**Minimal Risk Maneuver"** :
(Note: *copy definition from UN-ECE Regulation for ACSF-B2 when available)*

3.6 "**Status of the HAD system"** :

(Note: this section ***to be completed after ACSF-B2 regulation is finalized*** *and to be harmonized with ACSF-B2 definitions)*

> ***[Off:*** *(or "switched off") the system cannot control the vehicle because it is completely disengaged.]*
>
> ***[Activated:*** *the system is switched ON and the conditions for being active are met. In this mode, the system takes full control of the driving task.]*
>
> ***[Transition Demand:*** *instruction from the system that the driver has to take over control of the full driving task.]*
>
> ***[Override****: consists in one significant action of the driver on one of the lateral or longitudinal commands, keeping in mind the driver's significant action is always prioritized by the vehicle. After an override, the system shall switch to "transition" mode.]*

4. Requirements for vehicles

Each vehicle equipped with a DSSAD must meet the requirements specified in § 4.1 for data elements, § 4.2 for data format, § 4.3 for data storage, § 4.4 for retrivability, and § 4.5 for auto-diagnostic and § 4.6 for information in owner's manual.

Data must be available, by using a dedicated retrieval tool or any other solution of its choice (the data can be physically located on-board or off-board of the vehicle)

4.1 Data elements

Each vehicle equipped with a DSSAD must collect and store all of the data elements listed below :

- **Time stamped switches of the HAD system from a status to another status ("OFF", "activated")**

  (Note: list of the possible status will be given by ACSF-B2 regulation)

- **Time stamped Transition Demand by the HAD system and their nature (visual, audible, haptic)**

  (Note: list of the possible TD will be given by ACSF-B2 regulation)

- **Time stamped Minimal Risk Maneuver by the HAD system and its type (if several types) and time stamped end of this Minimal Risk Maneuver**

  (Note: list of the possible MRM will be given by ACSF-B2 regulation)

- **Time stamped Take-Over by the human driver and its type (if several types)**

  (Note: list of the possible TO will be given by ACSF-B2 regulation)

4.3 Data format

Each data element listed in § 4.1 must be recognized without any possible confusion by the codification that will be chosen by the manufacturer.
Each time stamp attached to this data must enable to determine when the event (change of HAD system status, TD emission, MRM engagement/end, OR, TO) occurred with the resolution of 1 second in GMT time (provided by [GPS]).

4.4 Data storage

DSSAD will be able to store a minimum of [25.000] timestamped events or a minimum period of [3] months timestamped flags history, whichever is achieved first.
Additional data storage may erase the previous data, following the "First In / First Out" rule.
After this period, data may be impossible to retrieve.

4.5 Data retrievability

It will be able to retrieve stored timestamped data with the appropriate tool or method provided by the manufacturer from the DSSAD even if the onboard vehicle power-supply is not available.

4.6 DSSAD malfunction

The AD system shall not be possible to engage when DSSAD is out of order.

4.6 Information in owner's manual

The owner's manual in each vehicle covered under this regulation must provide the following statement :

"This vehicle is equipped with a Data Storage System for Automated Driving (DSSAD). The main purpose of this DSSAD is to collect and store timestamped basic interactions between the human driver and the Highly-Automated-Driving system, such as switches of the HAD system from one status to another, Transition Demands from the HAD system, and Overrides/Take-Over from the human driver. The DSSAD is designed to store these data for a [3 months] period of time.
These data can help providing a better understanding of the interactions between the driver and the HAD system.
NOTE: no personal data (e.g., name, gender, age, and location) are recorded. However, other parties, such as law enforcement, could combine the DSSAD data with the type of personally identifying data routinely acquired during an investigation.
To read data recorded by a DSSAD, special equipment may be required, and access to the vehicle or the DSSAD may be needed. In addition to the vehicle manufacturer, other parties, such as law enforcement, that have the special equipment and/or authorization, can read the information if they have access to the vehicle or the DSSAD."

5. Data retrieval tools

Whenever a dedicated tool is necessary to retrieve the data, each manufacturer of a motor vehicle equipped with a DSSAD shall ensure by licensing agreement or other means that a tool(s) is available that is capable of accessing and retrieving the data stored in the DSSAD, that are required by this regulation.
The tool(s) shall be available [when the approval according to this regulation is granted / not later than 90 days after the first sale of the motor vehicle for purposes other than resale].