Document No. ITS/AD-14-09
(14th ITS/AD, 15 March 2018, agenda item 5-1)

DATA STORAGE SYSTEM FOR AUTOMATED DRIVING (DSSAD)

Submitted by experts of OICA

14. IWG ITS/AD, Geneva
15th of March 2018

DSSAD : Purpose of the Data Storage System for Automated Driving

Definition :

The **D**ata **S**torage **S**ystem for **A**utomated **D**riving is a device or a function that :

records and stores a set of data (“timestamped flags”) during the automated driving sequences

of any vehicle equipped with Level 3 / Level 4 / Level 5 Automated Driving Systems (ADS),

in order that **whenever a significant safety related event occurs,** it can provide

a clear picture of the **interactions between the driver and the system**,
before and after (*whenever possible*) the event, in order to **establish :**

- **if the driver or the system was requested to be in control of the driving task,** and

- **who was actually performing the driving task.**

DSSAD : Set of data to be stored

- **STATUS/MODE OF THE SYSTEM**

  Several status and/or **modes** will potentially exist :

  => **OFF** (“disengaged”), **STAND-BY**, **ACTIVE**, **FAILURE**, **LIMITED**, **TRANSITION**,…

- **TRANSITION DEMAND (TD) :**

  Several Transition Demand types will potentially exist, depending from the context :
  A-Type for “comfortable/planned” situations, like end of the Use-Case, and **B-Type** for other “unplanned” situations, **C-Type** ?...

  The “warning cascade” could vary from $\mathbf{TD_A}$ and $\mathbf{TD_B}$ depending on the needs and requirements and each component of the TD cascade, may be stored independently, because released through different channels, like “**visual**”, “**audible**”, “**haptic**” for example.

  => **Each Transition Demand** may be stored as a **cascade of several signals :**
  $TD_A = \mathbf{TD_{A1} + TD_{A2} + TD_{A3}}$ $TD_B = \mathbf{TD_{B1} + TD_{B2}}$ …etc…

- **MINIMAL RISK MANOEUVER (MRM)** :

  Several MRM types (A-Type, B-Type,…) will potentially exist, depending from the context :

  => **Each $\mathbf{MRM_A}$, $\mathbf{MRM_B}$**… may be differentiated.

- **OVERRIDE & TAKE-OVER (OR & TO)** :

  Several OR and/or TO types (A-Type, B-Type, etc…) will potentially exist.:

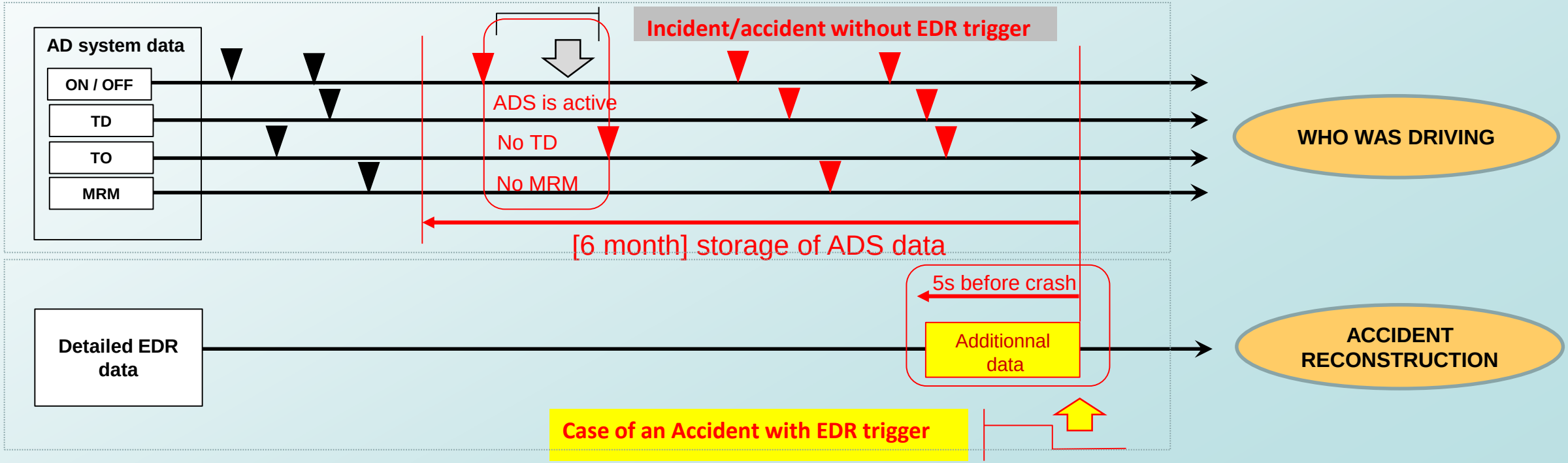
  => **Each $\mathbf{OR_A}$ / $\mathbf{OR_B}$ / $\mathbf{TO_A}$ / $\mathbf{TO_B}$ / $\mathbf{TO_C}$**… may be differentiated.

DSSAD : complementary & independent to EDR

« Different data storage systems for different purposes »

In the case of an accident with inflation of at least one airbag, the **complementary Event Data Recorder (EDR)** system will provide many **additional** information with its usual possibilities and limitations :

- With trigger : **ADS data** and **Detailed EDR data** (record @ trigger event)
  - Trigger: Airbag deployment & strong deceleration (Δv > 8 km/h within 150 ms as in US part 563 EDR)
- Without trigger : **ADS data** only (including timestamp / continuous [6] month storage)



Data Storage context :
Only DSSAD applies to AD only

REGULATED

Light Vehicles M1/N1

ACCIDENT RECONSTRUCTION

Accident Emergency Call System

(GPS/Galileo/Glonass position, GMT time stamped, retention system status, VIN…

« US » EDR

speed, accelerations, restraint systems deployment,… trigger time stamped

All Vehicles equipped with Lev 3, 4 or 5 AUTOMATED DRIVING SYSTEMS

WHO WAS DRIVING

DSSAD

System status/mode, Transition Demands from system HMI, Driver's Override & Take Over, MRM activations

OPTIONAL
(NO TECHNICAL REGULATION)

« other data »

Video scene recording, insurrance system data, fleet management tool data, other **personnal data** (depending on regional privacy laws)…

*"It might be important to collect data in retrieval format about **who was in control and of what** throughout the operation in case of an unexpected event that could impact road traffic safety."*

(WP1 – IGEAD – 07-04 – Guidance for Automated Vehicles – discussion paper)

CONCLUSION : a strategy for DSSAD

	EDR (M1/N1)	DSSAD (All vehicles with ADS)
Purpose	Supporting crash analysis and reconstruction	Support legal information needs on vehicle control (Driver/System)
How	Record data when triggered (momentaneous)	Store data over a longer period
What data	Data relevant to crash analysis - Vehicle speed - Vehicle Speed reduction - Engine throttle - Service brake - Ignition - Airbag deployment - ..	Data relevant to vehicle control: - AD system ON/OFF - Transition Demand - Take Over - Minimum Risk Manoeuver - Repective data timestamps
Reference	FMVSS **49 CFR Part 563**	To be discussed (OICA proposal available)
Application		
"conventional vehicle"	Applicable	No need
"vehicle with Automated Driving function" (LEV3, 4 & 5)	Applicable	Applicable

Proposed strategy for Automated Driving functionalities:

- **Implement the concept of DSSAD in ACSF B2 Level 3 – highway application** (*short term*) **& in "horizontal regulation on Automated Driving"** (*mid term*)

DATA STORAGE FOR AUTOMATED DRIVING

ANNEXES

DSSAD : Glossary of terms

Data : data to be displayed or utilized by some CPUs of the vehicle (e.g. « speed of vehicle » is the information that is displayed to the driver through the speedometer, with tolerance as given by UNECE R39. It is not the absolute speed of the car)

recording data : keeping the instant value of several continuous information or an instant message (both available in the vehicle's CAN or ECUs) in a volatil memory. These data may be recorded and overwitten continuously : they are not available after a while, if not stored.

Storing data : keeping the recorded data in a non-volatil memory for future retrieval or « read only » access.

Trigger : parameter or signal, which threshold is achieved or exceeded when a significant safety related event occurs.

DSSAD : Data Storage System for Automated Driving, which aims at making clear « who was driving before (and possibly after) a significant safety related event » and « who was requested to drive » (it can be different, especially during transition driving sequences.

EDR : Event Data Recorder, which aims at a better understanding of the retention system action and vehicle conditions durong a severe crash. EDR is described in North American CFR Part 563.

AECS : Accident Emergency Call System, which aims at providing a Public Safety Answering Point with a set of data concerning a severe crash that just occured. AECS are described in European e-Call regulation, Russian ERA-Glonass regulation, and will be in UNECE Reg.

Significant safety related event : Event that can put human beings in danger. Some of these may be subject to retention system deployment, some others not. Some of these may be subject to emergency manoeuver before impact and some others may not. Minimal Risk Manoeuver should be performed without emergency manoeuver, and without impact, but it is however considered as a significant safety related event.

Minimal risk manoeuvre : procedure aimed at minimizing risks in traffic, which is automatically performed by the system (e.g. when the driver does not respond to a "transition demand").

Emergency Manoeuvre : manoeuvre performed by the system in case of a sudden unexpected event in which the vehicle is in imminent danger to collide with another object, with the purpose to avoid or mitigate a collision.

ANNEX 2 : Detailed principle of the DSSAD

As it is proposed to be stored and available **for [**6 months**] or [**45.000**] flags** (the first achieved of both)**, the DSSAD can always bring the answer to the question** “who was driving ?” **to the authorized person or administration.**

Determination of “**who is allowed to access the data**” may vary from a country to another.

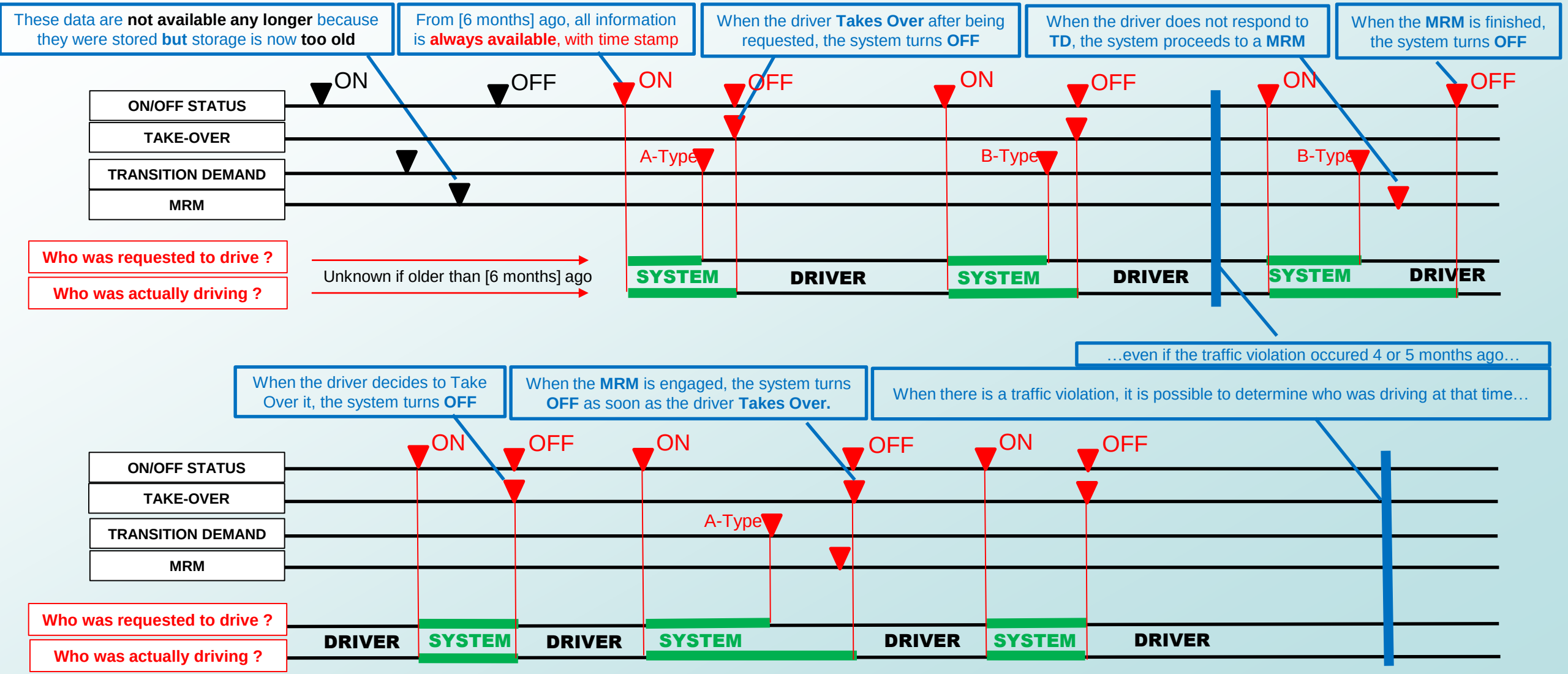
It should remain under the responsibility of the OEM to decide the right technical solution in order to **restrict access** to the authorized person/administration only, and to guaranty that the **Read Only Data cannot be corrupted**.

Maximum number of elementary events to be stored by the system remains to be decided. (45.000 ?)

(considering an average number of 5 elementary events per sequence of use : 45.000 = 50 sequences (of an average 5 events) / day , during 6 months)

ANNEX 2 : Detailed principle of the DSSAD

Use the Powerpoint version
With animations for better
understanding of the concept.



DSSAD : Important considerations regarding previous slide

The previous slide illustrates the concept of DSSAD, as proposed by the cluster n°2.

For simplification of the drawing, some hypothesis were considered, which do not necessarily reflect the future conclusions and detailed requirements that will be established regarding SAE Lv3 & above systems.

Simplifications considered in this slide are :

1- the system only has 2 possible status : **ON** (active) and **OFF** (disengaged),
2- the **Transition Demand (TD)** is only “one shot” and A-type or B-type only,
3- the driver directly **Takes Over (TO)** the system, without any preliminary **Over-Ride** and/or **Transition Sequence**
4- the system automatically switches to **OFF** as soon as the driver takes over or the **MRM** is finished,
5- there is only one **MRM** type that is engaged [X] seconds after the **TD** in the case there was no **TO** by the driver

Reality will be a little bit more complicated, but it does not change the concept itself.

The detail of the set of data to be stored will be possible to establish only after the requirements regarding the principles to be followed by these systems are given by the future dedicated regulation.

NB : All the potential STATUS/MODES OF THE SYSTEM, and definitions of OVERRIDE & TAKE-OVER, that are given in the glossary of terms, were inspired by the ACSF draft for E-systems, as it exists today. As so, they are only indicative, and modifications could be introduced by future regulation on these systems.